INTERNET SECURITY ALLIANCE

ANSI
American National Standards Institute

THE FINANCIAL MANAGEMENT OF CYBER RISK

An Implementation Framework for CFOs

"An excellent guide for organizations to manage the risk and exposure derived from digital dependence"

– Melissa Hathaway
President of Hathaway Global Strategies and
former Acting Senior Director for Cyberspace
for the National Security Council

"An invaluable resource for every C-level executive"

– David Thompson
CIO and Group President
Symantec Services Group

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The following professionals participated in one or more of the ISA-ANSI sponsored workshop meetings. The views expressed in this document are those of the individual workshop participants and do not necessarily reflect the views of the companies and organizations listed.

American International Group	Robert Roche
Allen Associates	Mary Beth Allen*
Allied World Insurance Company	Michael Murphy
American National Standards Institute	Jessica Carl, Karen Hughes, Peggy Jensen, Brian Meincke, Liz Neiman, Fran Schrotter
Carnegie Mellon University	Julia Allen
Catalyst Partners LLC	Rich Cooper
Chartis	Nancy Callahan
CNA Insurance	John Wurzler
Crimson Security	Narender Mangalam
Cyber Security Assurance, LLC	E. Regan Adams
Direct Computer Resources, Inc.	Joe Buonomo, Ed Stull, Bill Vitiello
Ferris & Associates, Inc.	John Ferris
Financial Services Technology Consortium	Roger Lang, Dan Schutzer
Guy Carpenter & Company LLC	Harry Oellrich*
HealthCIO Inc.	Jonathan Bogen
Herbert L. Jamison & Co., LLC	John Ercolani
Hunton & Williams	Lon Berk*
ID Experts	Christine Arevalo, Bob Gregg, Rick Kam*
Independent consultant	James Wendorf
Internet Security Alliance	Larry Clinton, Brent Pressentin
Jones Day	Gwendolynne Chen
Meritology	Russell Thomas
The MITRE Corporation	Michael Aisenberg
National Institute of Standards and Technology	Dan Benigni
New World Technology Partners	Robert Gardner
Northrop Grumman	Mark Leary, Rebecca Webster*
Packaging Machinery Manufacturers Institute	Fred Hayes
Perot Systems Corporation	Bruno Mahlmann, Katie Ortego Pritchett
Phillips Nizer LLP	Thomas Jackson*
Prolexic Technologies	Paul Sop
QUALCOMM Inc.	Mark Epstein
Reed Elsevier	Arnold Felberbaum*

Robinson Lerer & Montgomery	Anne Granfield, Michael Gross
Salare Security LLC	Paul Sand
Society for Human Resource Management	Lee Webster
U.S. Chamber of Commerce	Matthew Eggers
U.S. Cyber Consequences Unit	Warren Axelrod, Scott Borg
U.S. Department of Commerce	Michael Castagna*
U.S. Department of Homeland Security	Thomas Lockwood
U.S. Department of Justice	Martin Burkhouse
U.S. Securities and Exchange Commission	Ralph Mosios
University of California, Berkeley	Aaron Burstein
University of Maryland	Momodu Fofana
Zurich North America	Richard Billson, Brad Gow, Ty Sagalow

** Task Group Leader*

Thanks and acknowledgement are given for the support and participation of all the organizations that supplied experts to this initiative. Without the contributions of these individuals and their collective expertise, particularly those that participated on the workshop task groups, this final deliverable would not have been possible.

- Special acknowledgement and appreciation is given to Ty R. Sagalow of Zurich North America and Joe Buonomo of Direct Computer Resources, Inc., for being the workshop leaders of this initiative. Their leadership and dedication in helping to shape the initiative, lead its proceedings, and build consensus for the final deliverable were instrumental in reaching a successful outcome.

- Appreciation is given to the American National Standards Institute (ANSI) and the Internet Security Alliance (ISA) for the effective project management that kept this initiative on track and allowed for a successful delivery of the final publication in a timely manner, particularly Fran Schrotter, Karen Hughes, and Jessica Carl of ANSI, and Larry Clinton, Marjorie Morgan, and Brent Pressentin of ISA.

- Special acknowledgement is given to Zurich North America, Robinson Lerer & Montgomery, Direct Computer Resources, Inc., and Phillips Nizer for generously hosting and sponsoring the workshop sessions and meetings.

- Thank you to the following special advisors for their review and insightful comments on the advance proof copy which contributed to the final version presented here:
  – Dr. Donald R. Deutsch, Vice President, Standards Strategy & Architecture, Oracle
  – Ron Dick, Former Director, National Infrastructure Protection Center (NIPC)
  – Dr. John Fox, President & CEO, FFC Computer Services, Inc.
  – Bob Gregg, CEO, ID Experts Corp
  – Roberto J. Lagdameo, Director of Finance, Collington Episcopal Life Care Community, Inc.
  – Alan C. Levine, CIO, John F. Kennedy Center for the Performing Arts
  – Richard F. Mangogna, President & CEO, Mason Harriman Group (formerly DHS/CIO)
  – Mike Mancuso, CFO of CSC
  – Christopher J. Steinbach, President & CEO, The Newberry Group, Inc.
  – Sandy B. Sewitch, CFO, General Kinetics, Inc.

- Thank you to Ed Stull, Direct Computer Resources, Inc., and Robert Gardner, New World Technology Partners, for leading this special advisor review effort and for providing the consolidated and insightful feedback to the workshop leaders.

EXECUTIVE SUMMARY

Business is currently on the front lines of a raging cyber war that is costing trillions of dollars and endangering our national security.

Effective, low-cost mechanisms are already in place to shield against many elements of the cyber threat. But too often executive leaders wait until they are compromised to put a reactive plan into action, damaging their company's reputation and incurring additional cost.

Greater understanding and guidance are needed to help businesses bolster information security and reduce vulnerability to cyber attacks.

That is why the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI) have developed this free, easy-to-use action guide, which brings together the independent research and the collective wisdom of more than sixty experts from industry, academia, and government.

All of these experts agree: the single biggest threat to cybersecurity is misunderstanding.

Most enterprises today categorize information security as a technical or operational issue to be handled by the information technology (IT) department. This misunderstanding is fed by outdated corporate structures wherein the various silos within organizations do not feel responsible to secure their own data. Instead, this critical responsibility is handed over to IT, a department that, in most organizations, is strapped for resources and budget authority. Furthermore, the deferring of cyber responsibility inhibits critical analysis and communication about security issues, which in turn hampers the implementation of effective security strategies.

In reality, cybersecurity is an enterprise-wide risk management issue that needs to be addressed from a strategic, cross-departmental, and economic perspective. The chief financial officer (CFO), as opposed to the chief information officer (CIO) or the chief security officer (CSO), is the most logical person to lead this effort.

This publication was created to provide a practical and easy-to-understand framework for executives to assess and manage the financial risks generated by modern information systems:

- Chapter One explains the true economic impact of cyber events and describes a six-step process for addressing the issue on an interdepartmental basis.
- Chapter Two focuses on the single biggest organizational vulnerability of cyber systems – people. The largest category of attacks on cyber systems is not from hackers to the system, but from insiders who already have access. This chapter describes numerous mechanisms to aid the HR department in mitigating this threat.
- Chapter Three provides a framework for analyzing the ever-changing legal and compliance regimes that organizations will have to manage as governmental attention naturally increases.

- Chapter Four describes how operational and technical issues can be better understood and integrated into an enterprise-wide risk management regime.

- Chapter Five lays out the comprehensive communication program that organizations need to prepare before, during, and after a cyber incident. Multiple different audiences need to be addressed, and this chapter provides a framework for developing and implementing these critical programs.

- Chapter Six addresses the issue of risk management and transfer. Even the most prepared organizations can still be compromised. Prudent organizations will have prepared for this eventuality, and this chapter provides the framework for conducting this analysis.

By now virtually every company has factored the positive aspects of digitalization into their pro-growth business plans, perhaps through web marketing, online inventory management, or international partnerships. But the potential risk these new cyber systems create has not received the necessary attention from decision makers, leaving the door open to potential cyber attacks and data breaches. Those companies that bury these concerns in overburdened IT departments and fail to address these issues head-on through an enterprise-wide, financially based analysis are not just endangering their own intellectual property, market share, and consumer faith, they are also putting our national security at risk.

Cybersecurity is vital to our economic well-being – both on an enterprise level and a national level. ISA and ANSI are pleased to offer this volume as a pragmatic first step in the effort to create a sustainable system of 21st century information security. If you have questions about this initiative or would like to get involved, please contact us at www.isalliance.org or www.ansi.org.

CHAPTER ONE

A Framework for Understanding and Managing the Economic Aspects of Financial Cyber Risk

The growing cost of ignoring cybersecurity – is your organization properly structured to assess and manage financial cyber risks?

Most American businesses are not prepared to identify and quantify the financial losses incurred during cyber events – nor are they properly structured to manage cybersecurity risk in general.

Deloitte's 2008 study *Information Security & Enterprise Risk* concluded that, in 95% of U.S. companies, the chief financial officer (CFO) is not directly involved in the management of information security risks. The study also found that 75% of U.S. companies do not have a chief risk officer.

The Deloitte study went on to document that 65% of U.S. companies have neither a documented process through which to assess cyber risk nor a person in charge of the assessment process currently in place (which, functionally, translates into having no plan for cyber risk at all).[1]

Notwithstanding the progressive steps that have been taken in some organizations, the Carnegie Mellon University (CMU) CyLab 2008 *Governance of Enterprise Security Study* concluded: "There is still a gap between information technology (IT) and enterprise risk management. Survey results confirm that Boards and senior executives are not adequately involved in key areas related to the governance of enterprise security."[2]

95% of U.S. CFOs are not involved in the management of their company's information security risks.

The CMU study also provided alarming details about the state and structure of enterprise risk management of cybersecurity. The study pointed out that:

- Only 17% of corporations had a cross-organizational privacy/security team.
- Less than half of the respondents (47%) had a formal enterprise risk management plan.
- Of the 47% that did have a risk management plan, one-third did not include IT-related risks in the plan.

These structural and management problems have raised concerns at the highest levels of government. President Obama himself articulated the problem when he spoke at the White House on May 29, 2009:

> "It is not enough for the information technology workforce to understand the importance of cybersecurity; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts."[3]

1 Deloitte, *Information Security & Enterprise Risk 2008*, Presentation to CyLab Partners Conference, Carnegie Mellon University, Pittsburg, PA, October 15, 2009.

2 CyLab, *Governance of Enterprise Security Study*, December 2008.

3 White House, Remarks by President Obama on Securing our Nation's Infrastructure, May 29, 2009.

The President's Cyber Space Policy Review – which was drafted after senior National Security Agency staff conducted an intensive analysis of current public and private sector efforts to combat cyber attacks – identified what would have to be done to address the growing problem with enterprise cybersecurity:

> "If the risks and consequences can be assigned monetary value, organizations will have greater ability and incentive to address cybersecurity. In particular, the private sector often seeks a business case to justify the resource expenditures needed for integrating information and communications system security into corporate risk management and for engaging partnerships to mitigate collective risk."[4]

Why should you care? The potentially significant hit to the bottom line

In 2004, the Congressional Research Service estimated that American businesses lost a stunning $46 billion due to cyber theft.[5] Since then, things have gotten much worse.

On May 29, 2009, the Federal government issued a report that stated that, between 2008 and 2009 **American business losses due to cyber attacks had grown to more than $1 trillion worth of intellectual property**.[6] This staggering number does not even count the additional losses due to:

- Theft of personally identifiable information (PII)
- System inefficiency and downtime
- Loss of customers
- Negative impacts on corporate share values (which, research has shown, follow publicity of cyber incidents)

Unfortunately, the problem is continuing to grow.

Symantec, the nation's leading provider of security software, reports that the number of new cyber threats to the Internet jumped nearly 500% between 2006 and 2007, and then more than doubled again between 2007 and 2008. This represents a 1,000% increase in new threats to corporate Internet users in just two years.[7]

Not only is the growing cyber threat endangering the profitability of American business, but it is also endangering our national security. In Congressional testimony on February 2, 2010, the Director of National Intelligence for the United States, Dennis Blair, quoted from the U.S. Intelligence Community's Annual Threat Assessment:

> "The national security of the United States, our economic prosperity, and the daily functioning of our government are dependent on a dynamic public and private information infrastructure, which includes telecommunications, computer networks and systems, and the information residing within. This critical infrastructure is severely threatened….I am here today to stress that, acting independently, neither the U.S. government nor the private sector can fully control or protect the country's information infrastructure. Yet, with increased national attention and investment in cybersecurity initiatives, I am confident the United States can implement measures to mitigate this negative situation."[8]

4 Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009.

5 Congressional Research Service, Report to House Committee on Homeland Security, 2004.

6 Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009.

7 Presentation to the U.S. Department of Commerce Economic Security Working Group, Internet Security Threat Report, January 7, 2010.

8 U.S. Senate hearing before Senate Select Committee on Intelligence. Testimony of Dennis Blair, Director of National Intelligence, February 2, 2010.

Despite the avalanche of statistics and expert testimony that point to the need for greater attention to be paid to corporate information security, the facts are that many companies are not properly analyzing their risk, nor are they making the modest investments in security that are needed.

The *Global Information Security Survey* conducted by PricewaterhouseCoopers is the largest corporate information security survey in the world. Their 2009 report reveals that **nearly half (47%) of all the enterprises studied reported that they are actually reducing or deferring their budgets for information security initiatives**, even though a majority of respondents acknowledged that these cost reductions would make adequate security more difficult to achieve.[9]

Between 2008 and 2009, U.S. businesses lost more than **$1 trillion** worth of intellectual property to cyber attacks.

The 2010 Center for Strategic and International Studies (CSIS) study *In the Crossfire: Critical Infrastructure in the Age of Cyber War* confirmed this finding and suggested the situation was even more dire. It reported that more than 40% of respondents acknowledged that they were either not very prepared or not at all prepared to defend against cyber attacks.

Nonetheless the survey showed that enterprises worldwide are cutting back on information security. According to the study, **66% of the American firms that CSIS interviewed had reduced information security spending in the previous year, and in 27% of firms the reductions were in excess of 15%.**[10]

These independent survey findings confirm what the ISA-ANSI Financial Cyber Risk Management Project determined in 2008 with our first publication, *The Financial Management of Cyber Risk: 50 Questions Every CFO Should Ask*. In an effort to further help organizations understand the true costs of cybersecurity, ISA and ANSI have continued our efforts and have authored this new publication, which sets out to:

- Articulate the need for businesses to systemically assess and manage the financial dimensions of their cyber risk.
- Outline a procedure for getting started.
- Provide a detailed program for the functional departments of an organization to use in their development of the needed cross-departmental analysis.

Each chapter is organized around a series of questions that operational departments should consider in addressing their financial cyber risk and provides the basic information and guidance for use in analyzing these issues. After these issues have been analyzed, each organizational department needs to be brought together to develop an enterprise-wide cybersecurity architecture which is funded, reviewed, and updated to keep pace with evolving cyber attacks.

Not every organization will have the capacity to enact all of the measures referred to in the frameworks that follow. Each organization, however, should at least consider the full range of cybersecurity actions described here. That way, if courses of action are not pursued, it will be the result of a deliberate policy choice, rather than an administrative lapse.

The issues raised in the questions also need to be considered on an enterprise-wide basis. The reader may note that similar issues are raised in more than one chapter. This is a result of the fact that, when addressing a cross-organizational issue such as cybersecurity, various departments may view the same issue from different perspectives. Management needs to resolve these differences to formulate a sustainable program of cost-effective cybersecurity that is consistent with the individualized business plans of each organization.

9 PricewaterhouseCoopers, *Trial by Fire*, 2009.

10 Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2009.

If corporations are losing so much money, why don't they adequately invest in improved cybersecurity?

According to the CSIS report, "Making the business case for cybersecurity remains a major challenge because management often does not understand either the scale of the threat or the requirements for the solution."[11]

The fact is that the current private-sector workforce, most of whom will remain working for decades to come, is largely uneducated about cybersecurity. For the most part, the people in this group (especially senior executives) are what demographers are now calling "digital immigrants" – they were not born into today's digital world and may face "language barriers" when it comes to the rhetoric of information security.

It is this enormous workforce that serves on the front lines of today's cyber wars. Yet these workers are largely unfamiliar with, and sometimes inhibited by, the technology and the mechanisms that are necessary for our collective defense. Also, and perhaps more importantly, corporate leadership is structured in such a way that the real financial issues it faces with respect to cybersecurity are masked. As a result, cyber threats are under-realized, funding is not properly allocated, and proper defense is compromised.

Due to this structure, cybersecurity is too often thought of as an IT issue rather than the enterprise-wide risk management issue it really is. Although cybersecurity obviously has a critical IT component, it is not a simple problem that can be solved with a technological fix. In fact, the single largest category of attacks is carried out by insiders, many of whom have access to the technological controls and thus cannot be stopped by technological solutions alone.

According to Verizon, **87% of breaches** could have been **avoided** through reasonable security controls.

The January 2010 Mandiant M-Trends report notes that "most organizations struggle to detect real incidents. Relying solely on automated security does not increase the likelihood an organization will be targeted, but it does increase the likelihood it will be in the state of continual compromise."[12]

The mistaken assumption that "the IT guys can handle the problem" leads to the dangerous situation wherein most employees don't feel that they need to be responsible for the security of their own data. So although a corporation's finance, human resources, marketing, legal, and other departments all own data, the tendency is to believe that the responsibility for securing that data rests down the hall with the IT department. This attitude substantially weakens overall corporate security.

A "technology-only" approach to managing cybersecurity cannot operate successfully. Organizations that take a solely IT-centric approach will be blind to the financial dimensions of cyber risk management and, accordingly, will neither be empowered to properly analyze cyber risk and its management nor properly appreciate the true costs of funding the required solutions.

The PricewaterhouseCoopers 2008 Global Information Security Survey confirmed that this is largely the structure under which most enterprises operate. The study also noted that we will not get a handle on the problem until we appreciate cybersecurity as a strategic and economic issue as much as an operational/technical one:

> "The security discipline has so far been skewed toward technology – firewalls, ID management, intrusion detection – instead of risk analysis and proactive intelligence gathering. Security investment must shift from the technology-heavy, tactical operation it has been to date to an intelligence-centric, risk analysis and mitigation philosophy…. We have to start addressing the human element of information security, not just the technological one; it's only then that companies will stop being punching bags."[13]

11 Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2009.

12 Mandiant, *M-Trends: The Advanced Persistent Threat,* 2010.

13 PricewaterhouseCoopers, *The Global State of Information Security*, 2008.

Even companies that do try to properly assess their cyber risk may be hindered by outdated techniques for measuring the success of security programs, which often fail to assess new threats. As attacks become more stealth and sophisticated, many organizations do not realize that they are under attack simply because they are looking at the wrong metrics.

In addition, many organizations mistake compliance with security. The January 2010 Mandiant report states that "organizations that take information security seriously and move beyond just meeting compliance guidelines have the best chance of detecting and remediating advanced persistent threats."[14]

Documenting adherence to sometimes overly simplistic regulatory or contractual requirements may not necessarily result in actual security improvements. In fact, there is growing evidence that the resources applied to compliance may actually detract from true security efforts. While it is clear that regulatory and/or contractual requirements must be abided – indeed we devote an entire chapter to that issue – it is a mistake to assume good compliance necessarily equates to a safer organization.

The bottom line is summed up succinctly by Gordon and Loeb in their groundbreaking work, *Managing Cybersecurity Resources: A Cost Benefit Analysis*: "It is a myth to assume that the role of risk management in cybersecurity is well understood. The reality is that many cybersecurity managers inadequately understand the full scope of risk management related to cybersecurity."[15]

The good news: we know what to do.

Expert testimony, including that from government representatives, has confirmed that we know how to address the vast majority of cybersecurity issues; we are simply not addressing them. The key, ultimately, is implementation.

Referring again to PricewaterhouseCoopers' *The Global Information Security Survey*, the study found that organizations that followed best practices had zero downtime and zero financial impact from cyber attacks, despite being targeted more often by malicious actors.[16]

An almost identical finding was reported in Verizon's *2008 Data Breach Investigations Report*.[17] The Verizon study drew on more than 500 forensic engagements over a four-year period, including literally tens of thousands of data points. The study reported that, in 87% of cases, investigators were able to conclude that a breach could have been avoided if reasonable security controls had been in place at the time of the incident.

In October 2008, Robert Bigman, chief of information assurance for the Central Intelligence Agency (CIA), told attendees at the annual Aerospace Industries Alliance conference that, contrary to popular belief, most cyber attacks were not all that sophisticated. Mr. Bigman estimated that "you could reject between eighty and ninety percent of attacks with the use of due diligence." He also added that "the real problem is implementation."[18]

On November 17, 2009, Richard Schaffer of the National Security Agency made a very similar assessment in sworn testimony before the Senate Judiciary Committee. In his testimony Mr. Schaffer noted that 80% of cyber attacks were preventable using existing standards/practices and technologies.[19]

14 Mandiant, *M-Trends: The Advanced Persistent Threat,* 2010.

15 Gordon, Lawrence and Loeb, Martin, *Managing Cybersecurity Resources: A Cost Benefit Analysis*, McGraw Hill, 2006.

16 PricewaterhouseCoopers, *The Global State of Information Security*, 2008.

17 Verizon Business Risk Team, *2008 Data Breach Investigations Report.*

18 Aerospace Industries Association Annual Conference, Robert Bigman comments on Cybersecurity, Washington, DC, in October 2008.

19 U.S. Senate, hearing before the Committee on Judiciary, Subcommittee on Terrorism and Homeland Security, Testimony of Richard Schaffer, November 17, 2009.

If we know that there is a massive problem and we know how to solve it, why are we not doing it? The CSIS 2010 report provides a succinct answer:

> "Cost is the biggest obstacle to ensuring the security of critical networks…. The number-one barrier is the security folks haven't been able to communicate the urgency well enough and haven't been able to persuade the decision makers of the reality of the threat."[20]

How to get started

Technology integrates modern corporations, whether workers are located across the hall from one another or halfway around the world. But corporate structures and decision-making processes remain in a siloed and unintegrated past, where each department makes decisions independently and without appreciation for the digital interdependency that is today a corporate fact of life.

The financial risk management discipline that chief financial officers and chief risk managers have classically used to deal with brick-and-mortar risks has not yet been systematically applied to digital risks. Gordon and Loeb's *Managing Cybersecurity Resources: A Cost Benefit Analysis*[21] is the first book to provide such a framework, but it generally assumes that management is successfully appreciating the risks associated with cyber events. Our publication calls that assumption into question. However, once financial risks are properly understood, a sophisticated cost-benefit analysis of risk such as that outlined by Gordon and Loeb can be put into effect.

Corporations need to truly understand the financial impacts of insufficient cybersecurity. In addition, they need to enact management systems, as guided by their CFOs or an equivalent executive, that bring all of the necessary executives to the table to address cybersecurity issues on an enterprise-wide basis. This process would certainly involve security and technology personnel, but these groups would not be in charge of cyber risk management. An enterprise-wide structure must include, at minimum: financial, legal, operational, human resources, communications, public policy, investor relations, compliance, risk management, and senior corporate officials.

Beginning in 2008, ISA and ANSI set out to develop a practical methodology that corporations can easily use to address both the risks and the potential financial losses created by the lack of appreciation of the cyber risk interdependencies. Representatives from more than sixty private sector organizations and government agencies met at seven regional conferences and participated in multiple smaller conferences to discuss and determine the procedures that are detailed in the succeeding chapters of this publication.

In order to get this process started, we recommend, at minimum, a simple six-step program:

Step 1: Own the Problem

By now virtually every organization has integrated the wonders of the digital revolution into their business plan with respect to record keeping, supply chain management, online sales, and more. The unfortunate downside of digitalization – data security – has largely been relegated to an isolated, and often under-funded, operational department.

Senior executives with cross-departmental authority such as CEOs or CFOs (or CROs) must take strategic control, not operational control, of the cyber system that is the nerve center of their corporate operation. These executives must appreciate, or learn, if need be, the true role that technology plays in the modern organization, including the financial risks that technology places on the organization and the steps that must be taken to manage risk appropriately.

20 Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2009.

21 Gordon, Lawrence and Loeb, Martin, *Managing Cybersecurity Resources: A Cost Benefit Analysis*, McGraw Hill, 2006.

Step 2: Appoint a Cyber Risk Team

It is unrealistic to expect that senior executives would be able to determine all of the questions, let alone all of the answers, to the multiplicity of cyber issues that are generated within their organizations' various departments. Yet the financial importance of cybersecurity and its many ramifications means that senior executives cannot afford to delegate the subject entirely to specialists or to junior managers.

This means that executives should take the step of forming and leading a Cyber Risk Team that can address cybersecurity from a strategic perspective. This team will need to obtain input from the affected stakeholders and relevant professionals, assess this input and feedback, and make key strategic decisions from an enterprise-wide perspective.

This publication provides senior management with the questions to ask and makes suggestions on how to approach the issues raised by these questions (the "answers" of course will vary from organization to organization). It provides, in short, a guide to assembling and managing the Cyber Risk Team.

The affected stakeholders should be drawn from the departments or functions identified in the subsequent chapters, and each department leader should be charged with conducting a rigorous analysis based on the questions and frameworks outlined in the chapters.

It is understood that each organization will have its own unique perspectives on and modifications to the outlined issues; however, we believe these outlines provide a useful starting point for the more specific discussions they will generate.

Regular meetings of the Cyber Risk Team assure that everyone is speaking the same language when it comes to enterprise-wide security.

Step 3: Meet Regularly

A face-to-face setting is ideal for the initial meeting of the Cyber Risk Team. Where an in-person meeting may be difficult in some geographically disparate organizations, at minimum an initial teleconference or videoconference should be held. Subsequent regularly scheduled follow-ups should occur, ideally in the form of quarterly check-ups. The regularity of these meetings is important since cyber threats and attacks, as well as mitigation strategies, shift frequently.

Face-to-face discussions can be particularly useful to counter the challenges of separate business units that don't "speak the same language." Meeting in person is important because approaching what will be a novel issue in a potentially novel fashion may well lead to misunderstandings, both with respect to organizational strategy and the unique perspectives of various departments.

Step 4: Develop and Adopt a Cyber Risk Management Plan across All Departments

The January 2010 Mandaint M-Trend report found that "unplanned remediation efforts almost always fail to resolve an incident. The majority of large corporations targeted…remain compromised after numerous remediation efforts unless those remediation efforts are planned, coordinated across business lines, incisive, and executed at the appropriate time."[22]

The chapters that follow suggest actions to be taken within certain functional areas and describe how these areas should interact with other related areas. The Cyber Risk Team should determine which actions and roles, either existing or new, are to be allocated to each functional area and establish the means through which to communicate and coordinate among the functional areas. The result should be a well defined, holistic information security architecture.

22 Mandiant, *M-Trends: The Advanced Persistent Threat,* 2010.

The plan needs to include provisions for increasing employee awareness as to the criticality of cyber systems and data. Employees must be clear about company policies on data categorization, data retention, and incident response. The enterprise's plan also needs to include provisions for securing connections with business partners, out-sourced suppliers, and other remote connections.

The plan should also include a formally documented incident response and crisis communications plan to notify stakeholders (and the media, when appropriate), since even the best-protected companies cannot eliminate the real risk of a cyber incident that results in a "crisis" to be managed. In the wake of a cybersecurity event, an effective communications strategy can materially minimize the potential financial harm – including the "indirect" costs of potential damage to a company's reputation, its brand, its customer loyalty, and its employee's morale. All of these factors can have substantial impact on shareholder value.

Step 5: Develop and Adopt a Total Cyber Risk Budget

Based on the Cyber Risk Plan, the cross-organizational team should calculate the gross financial risk for the organization. First, it is important for senior management to understand the potential financial impact of a cybersecurity event, which can be substantial. Obviously, this impact will depend on the type of organization and the type of incident, as the total costs of some types of cybersecurity events are easier to estimate than others.

For example the CSIS survey of critical infrastructures published in January 2010 revealed that the cost of twenty-four hours of downtime from a major incident among critical infrastructure enterprises would be, on average, $6.3 million. A company in the oil and gas industry can expect a cost of up to $8.4 million per twenty-four hours of downtime.[23]

More generally, a study from the Ponemon Institute estimated that in 2009 the average cost of data breaches per compromised record was $204. The range of total cost among the forty-five data breach incidents contained in the 2009 study was a minimum of $750,000 to nearly $31 million.[24] Of those figures, 60% are "direct" costs such as investigations and forensics, audit and consulting services, notification of affected individuals, public relations and communications, legal defense and compliance, and credit and identity monitoring. The remaining 40% of the total breach cost is accounted for by the "indirect" cost of lost business.

Using the Ponemon cost estimates, an example of the cost of a data breach of 10,000 records that include PII data, assuming the company carried breach insurance with an 80% coverage of direct costs, would be*:

Cost per record:

- $204 total cost
- $60 "direct" costs
- $144 "indirect" costs

Total estimated cost:

- "Direct" costs: 10,000 x $60 = $600,000
- Insurance coverage: $600,000 x 80%* = $480,000
- Net financial cost: $600,000 x 20% = $120,000
- "Indirect" cost: 10,000 x $144 = $1,440,000

Total net cost of PII breach = $1,560,000

* The costs covered by an insurance policy vary and may have specific sub-limits or deductibles for expense categories (i.e., call center, communications, etc.)

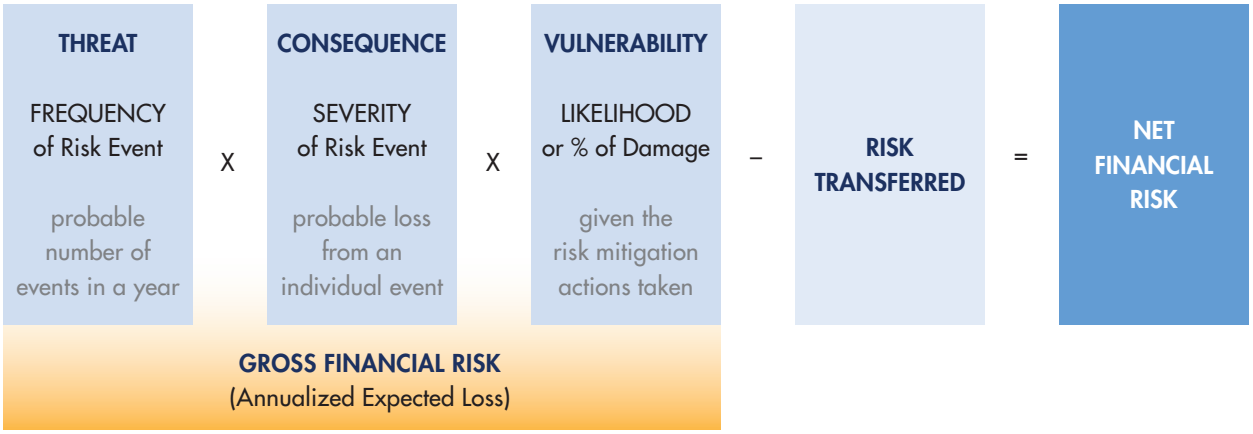
23 Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2009.

24 Ponemon Institute, *2009 U.S. Cost of a Data Breach Study*.

Regarding intellectual property and sensitive customer data loss, a recent study from the Purdue University Center for Education and Research in Information Assurance and Security found that more and more vital digital information is being transferred between companies and continents – and more is being lost. The study found that in 2008 companies lost on average $4.6 million in intellectual property.[25]

The most common risk measure technique among information security professionals is to combine the probability of loss with the expectation of loss summing the product of both to get the annual loss expectancy (ALE). However, as the field has matured, the notion of expected loss and techniques to measure it have also improved.

In the first publication to emerge from the ISA-ANSI Financial Cyber Risk project, *The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask*, we presented a graphic formula for the assessing of net financial risk. This chart is reproduced below:



As companies go through the questions posed in this work, they will find that the answers can be plugged into the above formula, enabling them to better quantify their own net and gross cyber risk. However, it is important to understand that the quantitative evaluation of these factors (threat, consequences, and vulnerability) must be qualified by the degree of confidence the organization has in the accuracy of each factor. In other words, in addition to the probability of loss, there is the probability of the estimate of the probability of loss being accurate. Once the risk equation has been qualified by the degree of confidence, it provides a sound basis for guiding all risk management decisions.

More sophisticated analytical tools are available in the academic and professional literature (see Gordon and Loeb 2006[26]), which can assist managers in the process of assessing costs and benefits. However, these systems are dependent upon the date put into the models so that they fully appreciate the real risks associated with cyber systems and avoid the "garbage in – garbage out" problem. It is this foundational step that is the main focus of the ISA-ANSI financial risk management project.

There are several industry guidelines that yield rough approximations for such calculations, such as the 5-6% of the IT infrastructure budget, or 1.5% of an enterprise's revenue (as suggested by authorities such as Forester or Gartner). The PricewaterhouseCoopers study cited earlier found that the "best practices group of companies, which almost entirely escape the effects of attacks on their cyber systems, were spending 30% more on information security than average

25 Purdue University Center for Education and Research in Information Assurance and Security, *Unsecured Economies: Protecting Vital Information*, 2009.

26 Gordon, Lawrence and Loeb, Martin, *Managing Cybersecurity Resources: A Cost Benefit Analysis*, McGraw Hill, 2006.

corporations."[27] However, as will likely become clear, many of the steps to be taken do not cost a great deal of money, and, thus, can be implemented in most organizations in a cost-effective fashion.

Naturally, appropriate budgets for individual companies may vary. Whichever formula an organization chooses, it is important to run this calculation through a cross-departmental risk management team to get a true enterprise-wide perspective on financial cyber risks and to develop a consensus on the budget.

Step 6: Implement, Analyze, Test, and Feedback

The Verizon forensic analysis of 500 actual enterprise security breaches (cited earlier) found that in nearly 60% of the incidents, the organization had policies in place that may well have prevented the breach, but failed to follow them.[28]

As detailed in the later chapters of this publication, it is important that the cyber risk management plan developed use clear metrics and that these metrics, including audits and penetration testing, be reviewed regularly both in terms of cyber risk management and budget.

The results of these examinations and tests should be used as feedback to update and upgrade each segment of the cyber risk management plan. According to the Verizon study, in 82% of the cases examined, information about an upcoming attack was already available and either went unnoticed or was not acted upon.

It is also important to focus on security basics rather than becoming focused solely upon sophisticated attacks. Verizon found that in 83% of the attacks studied, breaches came from attacks not considered to be very difficult to handle. In these cases many organizations were apparently so focused on stopping sophisticated attacks they failed to take care of the basics.

Cybersecurity is an ever-evolving field. Even with broad application of the program and suggestions herein, strong financial incentives still favor the attackers. Thus, organizations can expect new threats to emerge in an attempt to circumvent the defensive measures that they have put in place. Organizations will need to continuously monitor and improve upon their cybersecurity policies over time to maximize their security and, ultimately, their profitability.

Consider the following conversation that occurred between the CFO and the senior cybersecurity officer (CO) in a major U.S. corporation at the end of a meeting that lasted close to an hour.

"So my office gets the $7 million investment to upgrade the firm's network security?" asks the CO.

"You haven't made the business case for such an expenditure," replies the CFO.

In a moment of uncontrolled frustration the CO says to the CFO, "You don't seem to understand the importance of cybersecurity to our firm!"

At that point, the CFO replies with apparent sarcasm, "You don't seem to understand the basic economics and finance."

The two individuals agree that another meeting after a two-day cooling-off period would be appropriate.

From *Managing Cyber Security Resources: A Cost Benefit Analysis*, by Lawrence A. Gordon and Martin Loeb, McGraw Hill, 2006.

27 PricewaterhouseCoopers, *The Global State of Information Security*, 2008.

28 Verizon Business Risk Team, *2008 Data Breach Investigations Report.*

CHAPTER TWO

A Framework for Managing the Human Element

Key Results

- Ensure all stakeholders are well informed of cybersecurity and its financial impact to the organization
- Commit to clear and consistent cybersecurity procedures and expectations
- Establish reinforcing infrastructure and talent support systems

Introduction

The human capital element is fundamental to any business issue. And in today's marketplace, the importance of investing in human capital is more important than ever before. Nobel Prize-winning economist Gary S. Becker, who coined the term "human capital," says that "the basic resource in any company is the people. The most successful companies and the most successful countries will be those that manage human capital in the most effective and efficient manner."[1]

There is no more important investment in the IT security space than an investment in personnel. Despite all of the technological advancements, security assurance often comes down to the highly trained, perceptive administrator, who, while burning the midnight oil, traces an anomaly to its logical conclusion and adroitly reacts to defend the organization. Without knowledgeable people to protect information and systems, cyber risk will have greater impact. But how do you make certain that your organization is prepared for cyber risk from a people perspective? Organizations clearly need to establish a talent management plan that addresses this issue. Any leadership team will want to develop specific guidance on how to attract, acclimate, invest, and engage cyber-savvy employees to ensure the best possible chance of mitigating financial risk.

Equally important to the human capital discussion is the awareness that more people than just employees have access to company information via integrated networks and data interdependencies. Data access decisions must be made consciously for all stakeholder levels to include company representatives, teammates, contractors, guests, and administrators.

Indeed, anyone who touches a company's information and systems should have full awareness and appreciation for the financial impact associated with cyber risk. Requirements for vetting talent for network access should be well established – to include criminal history, professional integrity, and citizenship requirements (if appropriate) – in advance of receiving access credentials. In the best possible scenario, organizational leadership will commit to a fundamental value of cybersecurity, thereby creating a culture of awareness that guides policy, process, and decision making.

Because it is not yet well understood, many organizations consider cybersecurity the sole responsibility of the information security function, and, possibly, a concept that is limited to only those technical few with administrator roles or specific management responsibilities for the network. Unfortunately, this perspective fails to acknowledge the modern, integrated workplace, which relies heavily on information systems to engage in business with other employees, clients, vendors, consultants, and teammates.

1 Manville, Brook, "Talking Human Capital with Professor Gary S. Becker, Nobel Laureate," LiNE Zine <http://www.linezine.com/7.1/interviews/gbbmthc.htm>.

On top of the cost associated with actual cybersecurity attacks or breaches, the human element also incurs replacement and lost-revenue costs. The replacement cost of talent that the company will expend has been estimated to range between one to five times an employee's salary, which for technical talent can average over $100,000 per year. The amount of time that it takes to replace an employee is also a significant consideration, and that cost can be calculated by the sum of the following factors:

- Advertisement (# ads x cost per ad)
- Agency (if used; generally 20-30% annual salary of final candidate + fees)
- HR staff (# hours spent x hourly rate)
- Interviews (# candidates x # interviewers x interviewer hourly rate x # hours spent)
- Background screening
- Productivity lost (difficult to calculate – should also include team morale)
- Relocation/sign-on (assuming unrecoverable)
- Orientation and training (assuming unrecoverable; # hrs spent x hourly rate)

Organizational leadership will play an essential role in establishing the value of the organization's cybersecurity culture and talent. Just as the responsibility for cybersecurity crosses all lines of the organization, these questions should be asked across the senior leadership team and across multiple functional areas.

Question

How do we attract, acclimate, invest in, and engage critical cybersecurity technical and leadership talent, including those in functional areas requiring cybersecurity savvy?

A framework for attracting and retaining the right workforce

As corporate reliance on information systems expands, the need for cyber-savvy talent grows exponentially. According to a new study by the Partnership for Public Service, the need for information technology-specific, mission-critical personnel in the U.S. government alone exceeds 270,000 new employees by fall 2012.[2]

At the same time, however, high school and college students' interest in science, technology, engineering, and math (STEM) has significantly declined over the last several years, creating a severely limited talent pool. Organizations will be challenged to identify company-specific discriminators by which to provide candidates and employees with a strong enough value proposition to attract and engage their interest over the entire employment lifecycle. This value proposition must be substantial enough to address talent needs at all levels, from executives to administrators, and across multiple disciplines – engineering, technical, managerial, legal, and administrative.

A dynamic talent management strategy is essential to answering this question. Talent planning ties the organization's workforce activities directly to its business strategy and objectives. Through talent planning, the organization identifies the workforce it needs for its current and future business activities and plans the actions to be taken to ensure that the required workforce is available when needed. Workforce planning could include partnerships, alliances, acquisitions, independent contracting, and other means for ensuring that the required components of workforce competencies are provided in support of business plans and objectives. Strategic workforce plans provide those responsible for workforce activities in units with a reference for ensuring that those people perform their responsibilities with an understanding of how the unit's workforce activities contribute to the business.

2 Partnership for Public Service, *Where the Jobs Are 2009: Mission-Critical Opportunities for America*, 2009.

Of course, a first step in establishing these plans is to determine appropriate staffing levels. Although this figure is highly dependent upon an individual company's characteristics and environment, general industry consensus suggests that IT security budgets should be 5–10% of the overall IT budget. From this, one can extrapolate that staffing levels for IT security personnel typically should fall within the same range – 5–10% of overall staffing for IT.

But addressing the number of IT professionals to hire does not always fit perfectly into a formula or specific model. Given the importance of IT security, your firm may need to consider additional staffing levels for daily operations, key migrations, initiatives, and security itself. Make certain to ensure that current staffing levels cover all important functions of an IT security program. These functions include IT risk management, data security, forensics, operational resiliency, incident detection and response, training, network/system/application security and operations, personnel security, physical security, compliance, and internal audit. For the most critical assets and processes, it is imperative to maintain a clear separation of duties between IT operations and IT security. Healthy tension exists between the two, but all too often decisions are made in favor of the former at the expense of the latter. If the asset or process is critical, make certain to ensure separation of duties. Lastly, security applications improve efficiency but do not necessarily substitute for personnel. These applications are ultimately as good as the people who operate them. Adding new applications not only requires new skill sets, but may also require additional personnel. Truly effective organizations both source and hire employees with demonstrated depth in cybersecurity, while also screening all potential employees for the right attributes for maintaining a cyber-secure working environment. Once hired, these competencies must be nurtured in the organization by aligning them with the firm's performance management, rewards, training, and retention management systems.

Highly qualified staff in the area of IT security is a scare resource. Identifying the right personnel with the right skill sets further complicates matters. There are various competency studies, produced by industry and government, which identify the core skills required for personnel in IT security program functions. These skills can be used as a benchmark when evaluating prospective employees. Similarly, industry-sponsored certifications can be used to gain insight into potential candidates.

Critical skills for this domain are those that, if not performed effectively, could jeopardize the successful performance of these assigned tasks. Training needs related to these critical skills should be identified for each individual. Then, each unit is responsible for developing a training plan based on the needs identified for each individual. Training in critical skills is delivered in a timely manner and is tracked against the unit's training plan. In addition to the training investment, investments in state-of-the-art technology, facilities, and continuing external educational and networking opportunities play a significant role in keeping talent tied to the organization and, ultimately, engaged in higher performance over the longer term. To best track this, performance management strategies based on business objectives should be established to measure both unit and individual performance.

Both external candidates for positions and key internal resources will quickly realize their value and will demand higher levels of compensation for their skills, including robust health and welfare benefits, leave accruals, and base and variable compensation packages. The competition will be fierce for those candidates who possess strong technical and leadership skills, and especially so for those candidates with multi-disciplinary experiences. Candidates with both financial and computer science backgrounds, for example, will have far more insight into the financial implications of the information networks by which the company does business than a candidate who was strictly educated in the computer sciences. Similarly, candidates with experience across multiple markets or industries (like a combination of defense and commercial network architecture experience) may bring far more creative insight into how cybersecurity might be accomplished than someone who has experience in only one market or industry. A thoughtfully prepared talent management strategy will be essential for ensuring that the best talent joins and stays with the company.

By fall 2012, the U.S. government is expected to hire more than 270,000 new cyber-savvy employees.

Methods for attracting, acclimating, investing in, and engaging critical cybersecurity technical and leadership talent, including those in functional areas requiring cybersecurity savvy:

- Develop a talent management strategy that emphasizes the need for cybersecurity savvy.
- Define the knowledge, skills, and attributes of the talent necessary to maintain cybersecurity (to include ethics and integrity).
- Commit to the skills development and resource investments necessary to maintain competitiveness and employee engagement.
- Incorporate these criteria into the sourcing and screening processes.
- Imbed these criteria in the performance management system.

Question

Do we adequately address international stakeholders?

A framework for managing international partners

In addition to all of the aspects covered in the previous framework, international staff requirements call for even more stringent applications. Operating in the global marketplace has brought considerable challenges to organizations that must abide by international employment and labor laws in the various federal, country, state, and local environments. Identifying, analyzing, and mitigating the attendant legal risks are essential to avoid violating laws that can lead to fines and criminal penalties.

Multiple layers of legal considerations include international treaties between countries represented by organizations such as the ILO (International Labor Organization), the WTO (World Trade Organization), the OECD (Organization for Economic Cooperation and Development), and the EU (European Union). Legal topics in individual countries, states, and local municipalities that should be analyzed and considered are:

- Basic composition of the country's laws in domestic and international environments
- Departments responsible for labor and employment law between federal, state, regional, or local governments
- Administrative policies and procedures for those employment and labor laws
- Structure of judicial and dispute resolution system for labor law, including appeals system
- Background investigation, selection, interviewing, hiring, contracts of employment with individuals, and on-boarding processes
- Privacy
- Code-of-conduct and confidentiality
- Collective bargaining or work councils
- Wages, hours of work, taxes, and leave (vacation, sick, approved absences, etc.)
- Discrimination
- Compensation, pensions, working environment, and benefits
- Immigration, visas, taxation, travel restrictions, and relocation

In some countries these considerations extend to greater involvement in employees' personal lives (e.g., housing arrangements, health care, children's education, safety, security, and higher living costs).

Method for adequately addressing international stakeholders:

- Research and ensure compliance with international practices and regulations.

Question

Do we have an effective, deployable strategy to address awareness of the financial impact of cyber risk?

A framework for increasing employees' cybersecurity awareness

Effective preventative and remedial responses to cyber threats depend upon the creation of a fully competent strategy to address the financial impact of cyber risk. Reducing the risk of harm to organizations compels leadership to assess all stakeholders' understanding of how cyber risk impacts business operations, and how leadership actions can prevent or facilitate financial loss to the organization depending on how seriously they take cybersecurity. This begins from the inside out.

Focusing employee attention on the financial seriousness of cyber risk is critical to the development and execution of a cyber risk mitigation plan. Without a clear understanding of the potential impact each incident might have on the organization, employees and other cyber stakeholders may make decisions that are contrary to the organization's well-being. Policies and procedures may be interpreted loosely and applied inconsistently. Access may be granted without consideration to information sensitivity or regulatory compliance. Cyber-related policies and procedures should provide the organization with a basis for creating a cyber-secure culture, where everyone in the organization understands their role in keeping information and systems safe from individual vulnerabilities and potential threats. Each point of departure from these procedures provides an opportunity for additional loss of control, and the potential for greater financial risk.

Upon first introduction to the company, stakeholders (to include employees, vendors, clients, and others responsible for data and systems) should receive messaging that demonstrates the organization's commitment to risk mitigation with an explanation of how functional systems are interrelated, interdependent, and vulnerable without great awareness and caution. Follow-up to this introduction (in the form of newsletters, formal training, and knowledge recertification) should occur on a regular basis to remind stakeholders of their cybersecurity responsibility. As reinforcement, the performance management strategy should tie directly to expected behaviors, appreciating and providing critical corrective feedback as appropriate.

From the headlines

Lincoln National Discloses Potential Data Breach – Reported January 15, 2010

Lincoln National Corp. (LNC), a financial services company based in Radnor, PA, recently disclosed a security vulnerability that may have leaked personal data of 1.2 million customers. The breach of the Lincoln portfolio information systems had been reported to the Financial Industry Regulatory Authority (FINRA) by an unidentified source last August.

According to the disclosure letter that LNR sent to the attorney general of New Hampshire, the unidentified source sent FINRA a username and password that could access the portfolio system. This username and password had apparently been shared among employees of the company and vendors, which is not permitted under LNC security policy.

A forensics investigation revealed that LNR and another one of its subsidiaries, Lincoln Financial Advisers, were using shared usernames and passwords to access the portfolio information management system. The forensics team found a total of six shared usernames and passwords, which were created as early as 2002.

Internal communications planning will go a long way to help focus network stakeholders' attention on their responsibility for cybersecurity, but external communications planning is also essential to ensuring the least amount of risk to the organization. Regularly scheduled and consistent external messaging will help to ensure the best possible chance of success for risk mitigation activities. The strategy should align with the company's objectives and should tie closely to communication vehicles that are already employed and effective. Cybersecurity awareness should be an intimate part of the company's culture rather than a stand-alone program. The strategy may take time to assimilate into the culture; stakeholders may initially reject the concept because it is too far-fetched, unrealistic, or burdensome. Whatever the reason for the initial rejection, stakeholder compliance and, ultimately, full cultural embrace should come as a result of genuine commitment, integration with business objectives, clear messaging, and regular reinforcement.

Methods for ensuring an effective, deployable strategy to address awareness of the financial impact of cyber risk:

- Create and deploy a messaging plan on the financial impact of cyber risk.
- Facilitate learning discussions on cyber risk prevention and mitigation.
- Tie employee reward programs (merit and bonus) to the effective implementation of cyber risk mitigation programs.
- Institute a periodic training and certification process for the financial impact of cyber risk, assessing employee understanding of why cybersecurity is their personal responsibility.
- Include external communications in the overall strategy.
- Based on the cyber-awareness strategy, draft a communications plan that reinforces key messages on a regular, continuous basis.
- Equip direct supervisors with talking points and other communications tools, and require supervisors to discuss cyber issues with their direct reports at least monthly.
- Conduct a training-needs assessment within the organization to determine what development is required to reinforce key cyber-awareness messages.
- Evaluate the training and communications for effectiveness and repeat as necessary.

Question

Do we provide off-site and remote stakeholders with sufficient training and communication to mitigate cyber risk?

A framework for broadening the impact of your cybersecurity program

Parties outside of the primary company facility – telecommuters, customer co-located staff, vendors, teammates, and investors – demand unique consideration in training and communications plans. While standard operating procedures provide basic rules on remote access, alternative communications and training vehicles should address specific circumstances relative to home office work environments, as well as other facilities that are under separate control.

Consumer education is a key component of enhanced security for those organizations that allow their customers remote access to their systems – online banking and account management are two good examples.

Distance from the primary facility, if there is a primary facility, will make on-going compliance more difficult to ensure, will weaken management's leadership role, and will hamper the cultivation of strong reporting relationships. An aggressive and targeted communications and training campaign builds confidence with these stakeholders and provides an essential early warning system for potential cybersecurity threats. Continued leadership vigilance to managing the issue is essential.

For those companies that allow their customers remote access to their systems, such as in online banking or account management, customer education is a critical component. Through consistent and targeted messaging, these companies must educate their customers and instill them with a sense of security awareness and good security practices.

Company leadership will need to make certain that alternative facilities provide sufficient access for communications and training distribution in support of the primary company's cybersecurity culture. Conflicts in ethical practices may result in damaging activities and in stakeholder confusion on the roles and responsibilities required to maintain cybersecurity. Inadequate training deployment to remote stakeholders may cause inconsistent technical skills and improper network access, or result in information management procedures that increase financial risk.

Methods to provide off-site and remote stakeholders with sufficient training and communication to mitigate cyber risk:

- Based on the cyber awareness strategy, draft a communications plan that reinforces key stakeholder messages on a regular, continuous basis.
- Equip investor support, employees, and other communicators with talking points and other communications tools and encourage these people to discuss cyber issues with their stakeholders on a regular, periodic basis as appropriate for the business.
- Co-develop, expand, and evaluate the training and communications programs for effectiveness and repeat as necessary.

Question

Do we routinely audit network access throughout the network stakeholder life cycle, especially at termination or out-processing?

A framework for assuring network security throughout the network stakeholder life cycle

While it may be easy to agree on how important it is to be diligent in monitoring stakeholder access, the size and complexity of the organization may make this a challenging activity. Smaller organizations may be able to keep track of who has system access on a simple spreadsheet, but these organizations may miss key life cycle triggers (like changes in job function or transfers between business units) that would require updates to information access if the spreadsheet is not systematically linked to the database that manages employment events. For example, a customer service representative who moves from the call center to the showroom probably no longer needs the same level of system access to client accounts.

Larger, more complex companies absolutely need integrated systems to provide automated notification of employment changes to ensure that employees on the move have access to only that which they need to successfully perform their roles. Organizations responsible for multiple thousands of employees across the U.S. and abroad must leverage integrated infrastructure to manage their employee base, to coordinate basic network log-in access upon new hire, to manage access to specific systems throughout employment, and to ensure account termination when an employee leaves the company.

The worst case scenario would be for retired or resigned employees, or – even worse, unconnected non-employees – to continue to possess active network log-ins or system access. This would result in excessive and completely unnecessary risk with great potential for human vulnerability issues.

For these reasons, companies should, at the bare minimum, ensure that network accounts terminate immediately at the end of the stakeholder's relationship with the company. Information access at this point in the life cycle should neither be ignored nor considered a minor concern. It is during these transitions that the loss of data control and the invasion of organizational systems are the most likely, given cut ties and new relationships developing with competing employers. Whether resolving the termination of a disgruntled employee or closing a transaction with a departing vendor, organizational leaders must ensure that any end to the relationship with a stakeholder also closes the door to cyber risk.

Methods to routinely audit network access throughout the network stakeholder life cycle, especially at termination:

- Establish an out-processing approach that ensures all risk is managed effectively and deliberately during the final transaction.
- Establish a review process to determine which steps at the end of an assignment, position, or transaction require an incremental or absolute termination of access to organizational electronic assets.
- Monitor and improve these processes as needed.

Question

Do our performance management and compensation strategies provide adequate support for our cybersecurity mission?

A framework for providing effective incentives to create a culture of security

Positive employee reinforcement is a critical leadership piece to ensuring that the cybersecurity mission is met. Unless employment infrastructure relative to performance management and compensation clearly supports the commitment to the cybersecurity culture, limited progress may be made in shifting the attitudes about the importance of risk mitigation.

People respond to clearly established, managed goals and objectives that are reinforced with monetary incentives.

Performance management involves creating and monitoring measurable objectives for a specific period of time which result in eligibility for merit increases on an annualized basis, adjusted for performance level. Whether an organization uses a multiple point scale, pass/fail, or open discussion formats is not as important as the regularly scheduled performance discussion itself. It is during these discussions that the relationship between employee and supervisor is strengthened and the critical exchange on cybersecurity awareness, expectations, and evaluation is accomplished.

Make implementation of cyber risk mitigation programs part of the employee assessment process.

These discussions should not be limited to an annualized basis but should be ongoing throughout the performance period to ensure alignment and engagement. It also actively demonstrates leadership commitment to discuss problems and solutions through the creation of an atmosphere of continuous employee improvement.

Placing monetary value on the cybersecurity priority will further demonstrate an organization's serious commitment. Strong general compensation packages that include variable special benefits like pension, 401K matching plans, negotiable leave plans, signing bonuses, and long-term incentives will likely be necessary to attract key cyber talent in a highly competitive market.

Equitable base-compensation increases and continuing long-term incentives are essential to keep talent inside the company. Targeted variable-compensation programs to reward specific, objective activities serve to enhance performance on shorter-term goals and increase employee focus on the cybersecurity mission.

Methods to determine whether performance management and compensation strategies provide adequate support for our cybersecurity mission:

- Link the cyber awareness program deliverables to key measures in employee performance evaluations.
- Tie employee reward programs (merit and bonus) to the effective implementation of cyber risk mitigation programs.
- Establish spot award programs that provide quick and vivid incentives toward operating in a secure manner.

Question

Does our progressive discipline policy adequately address our need for threat investigations involving poor performers and network stakeholders demonstrating suspicious or disruptive behavior?

A framework for detecting security threats within the system

Because the risk for poor information management is so high, disciplinary policies have to be established and equitably enforced to address potential issues. Leaders will need to assess the need for processes from one-time, individual course corrections to anonymous threat reporting systems depending upon the company's network architecture complexity and experience. The level of cultural support for cybersecurity and the general investment in business ethics education may reduce the need for disciplinary activities, but the level of employee performance and successful remediation can vary greatly.

The most important aspect of progressive discipline is the consistent interpretation of threat issues and the application of the policy itself. Employees will observe inconsistencies and assess them as leadership weakness and as a lack of commitment to the mission. Non-employee stakeholders won't take internal policies seriously unless these stakeholders are also held accountable for the information and systems that they support. Because this level of exposure is also potentially immediately visible to the public, the company has heightened liability for urgent action to avoid damage to its public reputation.

Methods to determine whether the progressive discipline policy adequately addresses our need for threat investigations involving poor performers and network stakeholders demonstrating suspicious or disruptive behavior:

- Determine where risks exist for disruptive or abusive use of cyber assets in the workplace.
- Communicate during goal-setting sessions the risk of failing to manage cyber assets prudently.
- Audit the use of cyber assets, and if poor performance emerges, respond quickly and consistently.
- Use all appropriate internal and external remedies to reduce the risk of exposure.
- Engage the crisis management team immediately for needs assessment.

Question

Do we have plans in place to mitigate the human vulnerability variable?

A framework for addressing the "insider threat"

People are human and, therefore, are vulnerable to social trickery, persuasion, coercion, personal weakness, and lapses in integrity. These vulnerabilities, known as "social engineering tactics," may lead to non-technical intrusions, and are likely the most effective and inexpensive way for hackers or bad elements to obtain access to vital company information or systems.

While unfortunate, this variable represents the greatest wild card in cyber risk, given that it is generally triggered by personal human threat including financial hardship, relationship turmoil, or, in some cases, peer pressure or pure challenge. This variable is the most difficult to plan for, given its elusive and random nature, which makes it even more important for CFOs to include in their talent considerations.

Social engineering is the act of manipulating people into performing actions or divulging confidential information.

The term is typically used when trickery or deception is employed to gather information, commit fraudulent activity, or gain access to computer systems.

Checks and balances should be established to mitigate the risk of this particular variable, including data integrity assessments and mission assurance guidelines. A company must also ensure that its business ethics position is clearly and regularly communicated to include its commitment to cybersecurity. Continual reminders of how important ethical behavior is to the company's reputation will help to reinforce the culture.

Leadership modeling of the positive behaviors followed up with consistent execution of discipline when the need arises will demonstrate that the company takes the issue seriously. This leadership should be reinforced by consistent policy and procedure, as well as by physical protection of hardware assets. Bottom line, the company's leadership will need to provide employees with adequate motivation to stay on the straight and narrow, while, at the same time, acknowledging the likelihood of vulnerability by establishing multi-layered defense or human engineering tactics for accessing information (e.g., redundant systems, or multi-person approval systems), reporting mechanisms, and equitably applied, progressive discipline policies.

Methods for mitigating the human vulnerability variable:

- Require a screening investigation for prior criminal record upon request for employment and data systems access.
- Champion business ethics as fundamental to the business culture.
- Provide access to a hotline mechanism for anonymous reporting of suspicious behavior.
- Establish and deploy a progressive discipline process that clearly outlines consequences for breach or risk behaviors.

Question

Does our organizational structure support key functional integration to ensure threat mitigation and rapid crisis response?

A framework for cross-departmental coordination for improved security

Organizational structure can dramatically affect how quickly an organization can respond to cyber risks. Lack of technical or functional integration may cause duplication of effort or business-damaging assumptions to be made when working on time-critical crisis response. Lack of basic communications or business relations across critical organizational functions may cause missteps in interpreting cyber policy and procedure. Organizations should be diligently evaluating the organizational structure for performance alignment to mitigate the possibility for these mission conflicts.

Increasing coordination across business units and departments makes for more effective threat mitigation.

Performance alignment evaluation efforts focus on how the various components of performance fit together across workgroups, functional areas, units, and the entire organization. Understanding these presents a complete picture of performance within the organization and how the integration of its various business activities are affected by workforce practices and activities. These analyses allow management to integrate the entire enterprise and use workforce activities strategically to achieve organizational business objectives and goals.

These evaluations can also provide the basis for effective cyber prevention and mitigation planning. By acknowledging the functional design of the existing organization, the Cyber Risk Team can maximize existing relationships and organizational efficiencies to construct the most facile and integrated approach to decision making and communications.

The goal in developing a Cyber Risk Plan is not to subvert or overturn the existing functional management structure but, instead, to use it more effectively. An effective Cyber Risk Plan adapts to the organization's existing leadership and functional structure while identifying and repairing gaps in security among departments, workers, and supervisors.

Regardless of the function or department, **employees must see cybersecurity as relevant to what they do locally as well as influential to the organization's success as a whole**.

Methods for using the organizational structure to support key functional integration to ensure threat mitigation and rapid crisis response:

- Audit the existing organizational structure so that there is a full understanding of the role of key functions and how they interact with other functions.
- Establish functional teams to determine how to imbed cyber-secure practices in each of these functions, consistent with their roles and responsibilities.
- Implement these cybersecurity regimens and test their efficacy through surveys and drills.

Question

Do we adequately address stakeholder responsibility for protecting our social networking, share center, and prohibited public sites?

A framework for developing a security program to govern personal use of new media

Although social networking is an exciting way to expand relationships that could lead to enhanced business opportunities, innovation, and performance, social networking's pure novelty carries significant risk to control of informational assets and the spread of electronic malcontent like viruses, worms, and spies.

Lack of adequate planning for these increasingly open, collaborative spaces may tempt the less experienced, less savvy talent to share much more than appropriate. In cleared space, this poses an even greater risk for accidental exposure of classified information.

Organizational leaders must clearly communicate stakeholder responsibilities and liabilities when exchanging information in social networks. Whether participating in live online exchanges or surfing the Internet, stakeholders must be held accountable for the information they share, post, and download.

That said, too much censorship on the networks and Internet may pose a risk to the collaboration, creativity, and research that these tools were designed to enhance. Leadership should consider cost-benefit analysis of the severity of limitations for stakeholder access and should make decisions based on what is best for the organization's particular business model.

Depending upon the market in which the organization plays, open networking and access may make good business sense. It is most important to ensure that leadership considers the potential risks and incorporates the appropriate safeguards (via standard operating procedures, regular communications, and training).

Social networking can carry significant risk to control of informational assets, but in some instances open networking and stakeholder access may make good business sense.

Methods to address stakeholder responsibility for protecting our social networking, share center, and prohibited public sites:

- Have the legal department draft guidelines of behavior for social networking and communicate these guidelines directly to stakeholders.
- Through the IT department, establish barriers to the exchange of specific types of information while involved in a social network.
- Aggressively respond to violations of organizational policy using internal management systems or third-party remedies.

CHAPTER THREE

A Framework for Managing Legal and Compliance Issues

Key Results

- Expertise in key legal and regulatory requirements that relate to an organization's business, technology, and vendor activity in an effort to best shape policies and practices to effectively manage reputational, legal, and financial risk
- Oversight of retention, privacy, and data security practices and strategic solutions that support reasonable and defensible data risk mitigation strategies
- Insight into legal and compliance's role in integrating an overall process to manage vendor risk, contract liability, and cybersecurity risk transfer

Introduction

An analysis of legal and regulatory aspects of cyber risk requires a multi-jurisdictional review of the company's obligations that evaluates the impact of different jurisdictions in which the company does business and engages in cyber transactions. A comprehensive compliance program is the foundation for ensuring that an organization addresses their obligations to maintain compliance at a level commensurate with the organization's risk and management expectations. Oftentimes, the review of regulatory and legal obligations involves consideration of guidelines and requirements that were enacted well before businesses and consumers became so dependent upon the integrity and security of the data exchanged and stored over the Internet.

Where laws are typically tied to a state of region, cyber transactions occur in a realm without fixed borders, where information travels at the click of a mouse. No company is immune to the application of territorial laws to business conducted through the Internet. The analysis of competing laws and regulations of different jurisdictions should be evaluated, as well as the standards of practice developed for industries with similar operations. As regulations and practices change with regard to valid uses of regulated data, it is important to implement a sustainable process that reviews the data storage and the classification of the data use on an annual basis.

Questions

Have we analyzed our cyber liabilities? What legal rules apply to the information that we maintain or that is kept by vendors, partners, and other third parties? What laws apply in different states and countries in which we conduct business?

A framework for addressing third-party liability and multi-jurisdictional issues

Although every company has cyber exposures, the evaluation of cyber risk is not a "one-size-fits-all" exercise. In order to conduct an evaluation of legal and regulatory risk, a company must first weigh the costs and benefits associated with such an evaluation. A company must also examine its jurisdictions of operation, the data types it maintains and exchanges, and the importance of such maintenance and exchange to its operations.

All of this analysis should be conducted before a company can determine the extent of any legal and regulatory evaluation with respect to cybersecurity.

From the headlines

UK: Data breaches to incur up to £500,000 penalty – Reported January 12, 2010

The United Kingdom's Information Commissioner's Office (ICO) will be able to order organizations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act. The ICO has produced statutory guidance about how it proposes to use this new power, which has been approved by the Secretary of State for Justice, and has been laid before Parliament today. These new powers, designed to deter personal data security breaches, are expected to come into force on April 6, 2010.

When serving monetary penalties, the Information Commissioner will carefully consider the circumstances, including the seriousness of the data breach; the likelihood of substantial damage and distress to individuals; whether the breach was deliberate or negligent; and what reasonable steps the organization has taken to prevent breaches.

The power to impose a monetary penalty notice is designed to deal with serious breaches of the Data Protection Act and is part of the ICO's overall regulatory tool kit which includes the power to serve an enforcement notice and the power to prosecute those involved in the unlawful trade in confidential personal data.

Cybersecurity and compliance implicate many areas of corporate governance within an organization. Cyber exposure arises out of corruption and/or theft of data, loss of trade secrets or competitive advantage, as well as the failure of systems to remain operational, and subjects the company to class actions and other forms of mass tort litigation, shareholder derivative suits, and governmental investigations.

The analysis can also be complicated by the numerous jurisdictions and agencies that may be involved, as well as the manner in which laws relating to cybersecurity have historically developed. For example, within the United States, certain laws relating to security breaches and loss of personally identifiable information (PII) have developed piecemeal in individual states. For example, almost all states have now implemented laws requiring notification of a data breach to affected individuals.[1] State laws in this area are not uniform, and careful consideration should therefore be given to the class of individuals to whom notification must be made, as well as the form of the notification, given that affected individuals will likely reside in multiple states.

International laws and jurisdiction differ significantly. With regard to data protection, the European Union (EU) has among the strictest regulatory requirements in the world. PII may not be transferred to a jurisdiction outside the EU unless the European Commission has determined that the other jurisdiction offers "adequate" protection for PII.

In order to assist U.S. companies in complying with EU Directive 95/46/EC, the U.S. Department of Commerce developed a program in consultation with the EU which is known as the U.S. European Union Safe Harbor Framework.

U.S. companies can qualify for participation in Safe Harbor provided they comply with the seven principles outlined in the Directive:

- **Notice**: companies must inform individuals that their PII is being collected and how it will be used.
- **Choice**: companies must give individuals the ability to choose whether their personal information will be disclosed to a third party (opt out). For sensitive information, affirmative or explicit choice must be given (opt in).
- **Onward Transfer (Transfers to Third Parties)**: companies may only transfer PII to third parties that follow adequate data protection principles.
- **Access**: individuals must be able to access their PII held by an organization, and correct or delete it if it is inaccurate.
- **Security**: companies must make reasonable efforts to protect PII from loss, unauthorized disclosure, etc.
- **Data Integrity**: PII must be relevant for the purposes for which it is to be used.
- **Enforcement**: there must be effective means of enforcing the rules and rigorous sanctions to ensure compliance by the organization.

1 See Appendix, "State Security Breach Notification Laws."

Question

Have we assessed our exposure to theft of our trade secrets?

A framework for protecting trade secrets

Protecting trade secrets is vital to the competitiveness of companies large and small. Trade secrets are also notoriously difficult to protect. Under most state laws, a company must make "reasonable" efforts to keep such information secret in order to have a legally enforceable trade secret right. Though this practice gives companies considerable latitude in deciding how to protect their trade secrets, companies should carefully consider how to prevent trade secret theft, rather than focusing on what is sufficient to enforce a right after a suspected theft.

Basic principles of information security can provide a helpful guide to determining what measures are justified by their costs. Understanding what information is economically valuable to the company, and why, is a place to begin. From there, the company might consider how it governs internal access to trade secrets.

In some cases, restricting access to employees with a need to know may be appropriate. As employees change roles or leave the company, their access to trade secrets should change accordingly. Finally, implementing a system to audit access to trade secrets can help deter, as well as remedy, violations of company policy.

Of course, companies must also consider the risks that competitors, business partners, and customers pose to their trade secrets. Physical security, computer and network security, and contractual measures all have roles to play.

Depending on the type of business involved, a company may be at risk of trade secret theft by highly sophisticated attacks carried out in person, by software, or over the company's networks. Attacks in these circumstances may warrant reporting to state or federal law enforcement authorities.

Finally, in some cases, trade secret protection might be incidental if a company has other obligations to protect information. Serving as a third-party processor of PII, for example, might bring with it a contractual obligation to protect the information.

Similarly, performing classified work for the government generally requires a company to comply with regulations specifically designed to govern those circumstances.

From the headlines

Reported October 15, 2009

A former product engineer at Ford Motor Co. has been charged with stealing sensitive design documents from the automaker worth millions of dollars.

Xiang Dong Yu, of Beijing – also known as Mike Yu – was arrested at Chicago's O'Hare International Airport upon his entry into the U.S. from China, where he is working with a Ford rival.

Yu, 47, was charged with theft of trade secrets, attempted theft of trade secrets, and unauthorized access to protected computers. Yu had access to trade secrets contained in Ford system design specification documents. The documents contained detailed information on performance requirements and associated testing processes for numerous major components in Ford vehicles.

The documents, created and maintained by subject matter experts at Ford, are used by design engineers when building new vehicles and by suppliers providing parts to the company. According to the indictment papers, Ford has spent "millions of dollars and decades on research, developing, and testing" to create the requirements in the system design documents.

Yu allegedly attempted to sell the stolen documents to a Ford competitor in China.

Question

Have we assessed the potential that we might be named in class action lawsuits?

A framework for addressing class actions

Despite the continued unwillingness of courts to entertain class action lawsuits for negligent failures to safeguard data based on claims associated with the cost of preventing malicious use of personal information as opposed to actual losses associated with fraudulent use, the defense of class action lawsuits is increasingly costly and the potential liability to individuals whose personal or financial data is stolen or compromised continues to be of significant concern.[2] Increased emphasis should be given to the prevention of data loss, including the following steps:

- Inventorying records systems and storage media to identify those containing sensitive information.
- Classifying information in records systems according to its sensitivity.
- Refraining from the use of protected information in testing software, database applications, and systems.
- Implementing comprehensive security and privacy procedures, and monitoring employee compliance.
- Identifying, monitoring, and documenting, on an ongoing basis, compliance with regulatory requirements and contractual obligations with regard to data privacy and security.
- Implementing procedures to control and prevent unauthorized access to and disclosure of sensitive information.
- Contractually obligating service providers and others that handle sensitive information to follow internal security and privacy policies and procedures, comply with regulatory requirements, and monitor their compliance.
- Using intrusion detection and access control measures, in conjunction with encryption and other obfuscation technologies, to prevent, detect, and respond to security breaches and the loss of sensitive data.

Preparedness for notification is also of increased importance, including such activities as:

- Developing a comprehensive incident response plan and identifying individuals responsible for its implementation.
- Obtaining guidance from law enforcement agencies with expertise in investigating technology-based crimes.
- Identifying law enforcement authorities and any government agencies to be notified in the event of a breach.
- Documenting incident response actions and making changes in technology and response plans as needed.

Organizational compliance programs should also include steps for reviewing and updating internal privacy policies for employees and customers as well as the appropriate disclaimers.

2 One example is the case of Heartland Payment Systems, which provides payment processing services for merchants in connection with bank card transactions, a breach was discovered involving the use of malicious software to collect unencrypted payment card data being processed during the authorization of bank card transactions. Over a period of approximately seven months following its disclosure of the breach, seventeen class action lawsuits were filed against Heartland asserting claims on behalf of cardholders whose transaction information is alleged to have been placed at risk in the course of the breach, and ten class action lawsuits were commenced on behalf of banks that issued payment cards to those cardholders to recover the cost of issuing replacement cards and losses resulting from unauthorized transactions. The cardholder and financial institution lawsuits variously assert claims for negligence, breach of contract, violations of the Fair Credit Reporting Act and state data breach notification statutes, and unfair and deceptive practices. During the same period, four securities class actions were brought alleging that Heartland and two of its officers made material misrepresentations and/or omissions to its shareholders concerning the breach and that certain Heartland officers and directors engaged in insider trading of its securities. In addition, a merchant class action lawsuit was commenced on behalf of merchants against whom Heartland has asserted claims or fines in connection with compromised credit card data. Heartland Payment Systems, Inc., Form 10-Q for the quarterly period ended June 30, 2009, filed Aug. 7, 2009, at 6-7, 52-55, 59-61 (available at: http://www2.snl.com/Irweblinkx/file.aspx?IID=4094417&FID=8179567&O=3&OSID=9).

Question

Have we assessed the potential for shareholder suits?

A framework for addressing shareholder suits

Shareholder suits alleging mismanagement, or based on claims of intentional non-disclosure or selective disclosure of material information, may result from losses attributable to failures to assess adequately the vulnerability of networks and computer systems to outside intrusions. Suits may also result from ineffective safeguards against and lack of preparedness for data breaches; failures to execute incidence response plans on a complete, competent, and timely basis; delays in giving required notifications; and making inaccurate and misleading privacy and data security claims.[3]

In addition to the points outlined above, consideration should be given to:

- Instituting heightened board of directors oversight of data security and information technology matters and of senior management personnel charged with safeguarding sensitive information.
- Increasing involvement on the part of audit and risk management committees.
- Ensuring that adequate insurance is in place for data security risks.
- Evaluating and improving upon the training of employees to recognize the limits placed on the collection, use, and dissemination of sensitive data, and to identify and respond to security threats.
- Ongoing monitoring and assessment of the company's compliance with regulatory and contractual obligations, and performance by third parties of their contractual obligations to the company for data privacy and security.

Question

Have we assessed our legal exposure to governmental investigations?

A framework for managing governmental investigations

No matter what the ultimate result of a governmental investigation may be, responding to investigative demands will cost money, disrupt operations, and may harm customer and other business relationships. At the state level, given the burdens and inconsistent requirements of breach notification laws, there is a significant risk of governmental investigation in the event of data breach. Typically, state attorneys general have broad authority to investigate incidents or practices that harm consumers. Federal laws also impose a variety of data protection obligations and authorize a broad array of federal agencies to investigate data breaches as both civil and criminal matters.[4] Moreover, given the data privacy laws in the European Union and elsewhere, there is a significant risk to U.S.-based companies with international operations.

In the United States at the federal level, a number of agencies may become involved following a data breach:

- Health care providers and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) may be subject to investigation and penalties for unauthorized disclosures of personal health information.

3 In the case of Heartland, a shareholder derivative action was commenced against members of its board and certain of its officers asserting claims for breach of fiduciary duty, unjust enrichment, abuse of control, gross mismanagement, and waste of corporate assets, alleging that the defendants caused Heartland to disseminate materially misleading and inaccurate information to its shareholders, ignored inadequacies in its internal controls, and failed to make a good faith effort to correct the problems or prevent their recurrence.

4 See Appendix, "Federal Security Breach Notification and Data Protection Laws."

- Financial institutions that make unauthorized disclosure of personally identifiable financial information are subject to investigation by the financial regulator that oversees their business.
- Companies that own or operate chemical facilities must make cyber risk part of their overall risk assessments. Failing to do so could result in an investigation by the Department of Homeland Security.
- The Federal Trade Commission (FTC) may use its authority to address "unfair or deceptive acts of practices" (FTC Act § 5, 15 U.S.C. § 45) to investigate unauthorized disclosures of PII as a result of security breaches.

At the state level, in all 50 states as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands, "mini-FTC Acts" authorize their attorneys general or consumer protection agencies to investigate unauthorized disclosures of PII under broad grants of authority similar to those of the FTC. Internationally, perhaps the greatest risk arises from the European Commission's Directive on Data Protection. The Directive, which went into effect in 1998 and is enforced through conforming laws adopted by individual member states, sets requirements on the protection of "personal data" and limits how firms may use and disclose such data. As discussed on page 32, Safe Harbor negotiated between the United States and the European Commission exempts U.S. companies from the requirements of the varying national laws that implement the Directive, but to take advantage of the Safe Harbor companies must comply with the Directive's principles and file an annual certification of compliance with the U.S. Department of Commerce.

In an effort to limit these risks, companies should:

- Assess frequently the breach notification process and its compliance with federal and state regulatory requirements, as well as the standards imposed by other countries.
- Review any newly imposed requirements with legal counsel and compliance officers to determine their impact and make any necessary changes in policies and procedures.

Questions

Have we assessed our exposure to suits by our customers and suppliers? Have we protected our company in contracts with vendors?

A framework for customers, suppliers, and vendors

Companies may do business with hundreds of third parties. Despite internal compliance programs and controls, companies may expose themselves to considerable risk by actions of their suppliers, subcontractors, service providers, and partners. For example, banks outsource many services, but they cannot outsource the responsibility to meet their regulatory and legal requirements. Companies should clearly formulate and articulate security responsibilities through vendor contractual requirements to avoid regulatory fines and injunctions. Likewise, companies should establish a program to maintain an integrated picture of vendor relationships, spot gaps or overlaps, and seize opportunities to consolidate contracts and reduce costs.

Organizations that have regulatory obligations to retain information relative to their industry should have a defined data classification, retention, and destruction policy. Procedures should be established to securely store or destroy these records according to the policy. When outsourcing storage or destruction activities to third parties, a clear articulation of the storage or destruction requirements should be outlined in the contractual agreement. The vendor should be carefully vetted for their capability to transmit or transport, store, and/or destroy the data entrusted to them.

Assessing the financial risk of exposure to suits arising out of such liabilities requires an analysis of:

- The nature of the company's cyber transactions, including how customers and suppliers depend upon the operation of systems for their business operations.

- The nature of the data stored, received, and transmitted, including data from customers and suppliers.
- The laws and regulations of the jurisdictions in which the company, its customers, and suppliers operate.
- Steps the company takes to protect its customers' and suppliers' data, such as encryption and perimeter security.
- Steps the company takes to ensure its ability to detect and react appropriately to cyber breaches.
- Programs to review and update its data security and breach notification policies and procedures on a regular basis.

The key to assessing cyber exposures is identical to the key to reducing those exposures – a careful and proactive review of the nature of the company's transactions, obligations, and security and mitigation programs.

Cyber liabilities can arise in tort, in contract, or under statutory law. Tort liability generally arises where a business fails to exercise reasonable care in the discharge of its duties to another. Despite the widespread use of cyber transactions and the consequent storage and transmission of sensitive and confidential data concerning customers and business partners, the law has yet to define generally applicable, appropriate standards of care in this area. Perhaps such generally applicable guidance cannot be fashioned, as what is considered secure depends upon the different technologies available.

Additionally, the scope of a company's duties with respect to the storage, transmission, and preservation of data varies both with the type of data and the nature of the company's business. Every company needs to know that the protection afforded data should be a function of the nature of the data transmitted and stored and, perhaps most significantly, that there is no such thing as guaranteed security in cyberspace. There is always a chance, no matter how unlikely, that what appears to be a secure encryption is broken, and that the most protected system can be hacked or overcome by denial of service attacks.

The key is to take steps to ensure that what has been done to protect against attacks is as reasonable as it can be. This means looking at security as a process that can be updated and amended as reasonably necessary. In addition to contract and tort principles, statutory and regulatory rules impose obligations upon companies' treatment of electronic information.

Outsourcing IT functions to a vendor may be done for a number of reasons – cost savings, the ability to provide better customer service, the availability of specialized expertise outside the company, and other practical considerations. Application Service Providers (ASPs) offer web-hosted business application software that may be preferable to a company purchasing the software on its own. The company can pay a monthly rental fee rather than paying for a software license upfront, and the internal IT overhead can be reduced. Data warehouses may have benefits beyond cost savings. For example, data warehouses can mesh with, and increase the value of, operational business applications such as customer relationship management (CRM) systems.

From the headlines

Transportation Security Administration (TSA) Contract Worker at Boston Airport Accused of Selling TSA Employee Identities – Reported January 2, 2009

A recent data breach at Boston's Logan International Airport involving a TSA contract clerical worker, coming amid other high-profile Transportation Security Administration lapses, casts another cloud over a federal agency engulfed in turmoil.

This latest breach involved a female TSA contract worker who has been accused of selling the identities of at least 16 TSA workers at Logan. The fraud started in November 2008 and continued through 2009. According to a TSA statement, the agency and state police are investigating and added that there was little risk an infiltrator could obtain a security clearance with the data.

A company must, however, balance the cost savings with the risks involved with dealing with any vendor, including concerns about cybersecurity. Application software and sensitive data are often installed and stored, respectively, in a remote facility that is not owned or managed by the company's employees. Access to the applications and data occur over the Internet, thereby potentially increasing the risk of loss or theft of critical corporate data and PII.

Warranties and indemnities are critical provisions in vendor contracts and should be tailored to minimize the risk of cyber liabilities. Warranties that are generally applicable to all contracts include compliance with legislation and regulatory requirements (e.g., data privacy laws) and a commitment to appropriately protect confidential company and client data.

A more detailed provision of the vendor's obligations is often set out in a Service Level Agreement (SLA). The SLA should include detailed documentation on security measures, response time to security issues (which should be described in number of hours), and backup recovery procedures. Financial remedies for security breaches and unscheduled downtime should be clearly stated. Downtime penalties are usually minor and typically take the form of proportional fee refunds, whereas greater penalties, such as a payment by the vendor to the company of a multiple amount of the value of the contract, should apply to security breaches.

Warranties and indemnities are only as good as the financial worth of the vendor. Due diligence of the vendor's financial health should often be combined with a requirement that the vendor have in place appropriate insurance policies, including professional liability and network security insurance. These types of insurance give the company comfort that a third party has thoroughly evaluated the vendor's IT infrastructure and financial status.

Question

What can we do to mitigate our legal exposure and how often do we conduct an analysis of it?

A framework to analyze legal mitigation strategies

Once a company determines the types of cyber liabilities to which it may be subjected, the company's overall legal exposure may be calculated. The first step is to determine the likelihood of a lawsuit arising from each identified cyber liability. Legal exposure then becomes the sum over all such liabilities of the probability of a lawsuit arising out of that liability times the probability of an adverse judgment times the average severity of such an adverse judgment plus the legal fees to be incurred in connection with a lawsuit on this theory. Theories of cyber liability and the nature of cyber attacks are fluid and, for the most part, beyond the company's control. A company can, however, take steps to minimize the likelihood of an adverse judgment as well as the amount of legal expenses.

The most important thing a company can do to minimize its legal expenses and the likelihood of an adverse judgment is to put in place and document a proactive approach to cybersecurity. But even the soundest approach to cybersecurity, as noted, cannot prevent cyber incidents and cannot defend against lawsuits. Security by obscurity is often the weakest form. And, in the legal context, obscurity makes it more difficult both to defend a case and to manage legal expense. Forcing counsel to recreate the steps taken only increases legal fees. As such, it is important that clear records be kept of what was done and when to address security concerns. True, such records may make it easier for plaintiffs' counsel. But on balance, where a company has adopted an appropriate cybersecurity process, such considerations are outweighed by the value these records will have concerning the company's defense. Additionally, sophisticated plaintiffs will use the new rules of electronic discovery to fill in any gaps that may exist in the company's security records, and such discovery can only severely increase the cost of litigation.

CHAPTER FOUR

A Framework for Operations and Technology

Key Results

- Cyber security policies need to be founded on a holistic assessment of cyber attack risks that account for:
  - The kinds of cyber attacks that are threatened and their likely frequency.
  - The consequences of those cyber attacks.
  - The degree of vulnerability to those consequences, given the security measures.
- The company needs to classify information systems and data according to their sensitivity and then acquire technology and establish processes to appropriately safeguard them.
- The company's cybersecurity practices need to be guided by a set of cybersecurity standards or frameworks, chosen to suit the company's particular needs.
- Physical security and cybersecurity are both dependent on each other and are increasing converging into one discipline.
- Responding effectively to security incidents requires well-planned actions and regular practice.
- The key to coping successfully with severe cyber attacks is a well-thought-out business continuity plan, founded on business impact assessments.

Introduction

If information is the basis of our modern economy, then, at the organizational level, information forms the basis of competitive advantage. Due to the paramount importance of information, information technology (IT) decisions are no longer solely the domain of the chief information officer (CIO), chief technology officer (CTO), and chief information security officer (CISO), but, instead, are the central issues for the entire C-suite.

IT and the data it processes must be safeguarded from a myriad of pernicious threats, whether these threats originate internally or externally. To accomplish this in a cost-effective way, it is essential to understand the contributions that information systems make to the business and their impact on the bottom line. This means recognizing the relative criticality of the various information systems, as well as requirements for confidentiality, integrity, and availability. More broadly, companies have to understand these critical elements for their entire ecosystem – their suppliers, partners, service providers, and customers – and deal with the challenges of a mobile workforce.

With the realization of cybersecurity's importance, focus has shifted to economic decisions. Even as cyber threats loom, the economic recession, stagnant IT budgets, and strained economic forecasts demand answers to questions such as:

- What level of operational losses can we expect from cyber attacks, given our current security measures?
- What kinds of external liabilities might we face as a result of cyber attacks?
- What is the most cost-effective way to reduce our likely losses and liabilities, given the losses of efficiency that security measures can cause?
- How does the marginal cost of each additional security measure compare to its marginal benefit?

There is no single formula or actuarial table that can provide answers to such questions. However, in accordance with the theme of this study, a multi-stakeholder analysis can shed enough light on these questions to help steer decision making.

This analysis shows that building a resilient organization is the way to face these challenges. Resilience is built on the understanding that business comes first, but that business must be conducted through a risk management-based cybersecurity program that weighs operational needs against security necessities. This program assesses risk by combining business and IT to develop recommendations that are targeted to the bottom line, while understanding that the assumption of risk is inherently a business decision.

The guidance that follows can aid decision making around various technology and process considerations, especially with regard to assessing various "technologies du jour," such as application security, cloud computing, and network access control.

Questions

What is our biggest single vulnerability from a technology or security point of view? How vulnerable are we to attack on the confidentiality, integrity, and availability of our data and systems? How often are we re-evaluating our technical exposures?

A framework for determining vulnerability

Assessing information security risks is an important component of an organization's risk management practices. The identification and assessment of risk is the prime input into the economic calculus necessary to allocate limited budgets wisely. Through this assessment, a company will identify high-priority systems and processes for its ecosystem, prioritize vulnerability mitigation at the systems level, and provide an approximate understanding of risk at the organizational level.

Far too often in the IT security discipline, this process is solely focused on vulnerability. What is the vulnerability that needs to be mitigated or eliminated? The reality is that there are many, and they constantly morph. So, then, how should the confidentiality, integrity, and availability of information and systems be ensured? The simple answer is a holistic risk management process that constantly improves the layered defenses of an organization.

This holistic approach must express information security risk as business risk. Given the multi-dimensional aspect of risk for any business, IT security must be understood in conjunction with an organization's corporate culture, its global objectives, and its risk tolerance. Practitioners within the IT field often have a myopic perspective on risk that is not embraced by their business counterparts. This narrow interpretation of risk discounts the benefits inherent in the trade-off between risk and return, and focuses instead on the attainment of regulatory compliance or vulnerability management.

There is no such thing as guaranteed security in cyberspace.

The key is to take protective steps that are as reasonable as possible.

The union of business and IT security risks should be developed through a risk model. This model should be constructed jointly by business and security professionals, so as to enable prioritization and a probabilistic perspective on threat, consequence, and vulnerability. This quantitative analysis should be augmented by qualitative factors as necessary. This assessment can be broadly based, but it should be focused on those data, components, systems, and aggregate-organizational risks that impact critical business processes.

Ultimately, the output of such a model should be the explicit identification of residual risk, or risk that persists after the application of technical and organizational controls. The model should elucidate the appropriate risk management options (i.e., eliminate, mitigate, accept, and transfer). One must remember that models are inherently imperfect and that trying to make them too detailed or too precise will itself become an exercise in diminishing returns. The aim is simply to pursue the analysis far enough so that effective decision making about risk mitigation becomes possible. The final analysis should make use of visualization to further support decision making and to clarify investment options.

This analysis should commence at the information system level. The first step for any organization is to determine the state of their current level of security exposure using a risk assessment methodology. Many such methodologies are in place, but commonalities include identification of the following:

- Threats and threat frequency
- Criticality of the systems that might be targeted
- Consequences of a successful attack
- Vulnerabilities remaining after implementation of IT security controls
- Residual risk

The key factors here are threat, consequence, and vulnerability. The criticality of the systems is really a function of the consequences that would follow if these systems were successfully attacked. The residual risk is really a way of stating the product of the three main factors, when they have been multiplied together. To augment this assessment, a vulnerability management program becomes essential. The frequency of this activity should be a function of the data and system's sensitivity, revenue generation, regulatory/reporting requirements, and whether the system is Internet-facing.

Once risk is managed at the system level, risk must be aggregated to form an organizational risk posture. This posture must conform to the objectives and risk tolerance of the organization. Although IT architectures should allow for compartmentalization of information systems, it is important to understand that the interdependent nature of these systems means that the risk assumed by one is realized by all. The assumption of risk should fall within the domain of business units – not IT departments.

The IT security area has been challenged by an absence of reliable metrics. However, just as imprecision in modeling should not forestall the use of risk models, imprecise metrics are still useful. Metrics can assist in making sure the mitigations and controls are headed in the right direction. Metrics can measure the degree to which various security measures have been implemented, such as personnel training, vulnerability mitigations, and secure configurations. Metrics can cover operational achievements, such as vulnerability detection and incident management. And finally, metrics can provide estimates of the actual financial losses due to past cyber attacks. Although comprehensive estimates of future cybersecurity risks are difficult to achieve, many of the component measurements are already a practical possibility.

Given that the risk management processes are hampered by imprecision, and that IT security is by nature constantly evolving, organizations must create layered defenses to ensure critical data, systems, and processes are protected by a defense-in-depth approach. Iterative risk assessments will reveal other defensive countermeasures that can serve to reduce further the probability of IT security incidents.

Question

What is the maturity of our information classification and management program?

A framework for implementing an information classification and management program

A mature information classification and management program keeps the company competitive and helps to avoid unnecessary losses. In practice, this means that the company needs to establish clear policies, rules, and processes governing the creation, use, retention, and destruction of information. The policy should include the following data processes:

- Classification
- Retention
- Protection
- Destruction of information
- Access controls
- Audit and assessment
- Discovery

The policy should be based on cost-benefit analysis, with a clear prioritization of systems and data. Policies, procedures, and rules should be established to govern the categorization of information in terms of its sensitivity and its required level of protection. For every system and body of data, the expenditure on protection should be commensurate with its business impact. The relative priority of information systems can be determined by estimating loss in each case from:

- Unintended disclosure
- Unavailability
- Unauthorized modification
- A lapse in accountability (e.g., compliance)

The classification categories should correspond to the severity of the financial, legal, and reputational loss if unauthorized disclosure, theft, or modification of data results occurs. For instance, the Federal Information Processing Standard 199, *Standard for Security Categorization of Federal Information and Information Systems*, requires that information be categorized as high, moderate, or low. Once information owners make this determination, the categorized information can be aggregated, and the "high water mark" can be determined for the data that resides in the system. This process results in the system being categorized at the same level as the most sensitive information found on the system. Once the data and system categorization is understood, the proper controls can be mapped to safeguard both the system and the data.

Enforcement of these policies, procedures, and rules requires the information manager to know where all the sensitive information resides, on what devices, and when it leaves the enterprise. This includes not only the original record but also any copies that have been made. This also includes knowing who has attempted to access or modify the data, whether that person had the right entitlements and credentials, and, if allowed, what was done with the data (if it was read, copied, modified, or transmitted). Logs of access attempts should be kept and should be monitored for any unusual or suspicious behavior.

Question

Where do we stand with respect to any information security/technology frameworks or standards that apply to us?

A framework for determining applicability of standards and technologies

A cybersecurity framework is an essential set of roles, activities, technical standards, and best practices required to ensure an acceptable level of cybersecurity for organizations. There are various cybersecurity frameworks that can be modified to meet the unique requirements of any organization. These frameworks can provide valuable information about a company's risk posture relative to the industry as a whole. Once a company determines its risk posture within its industry, the company can ensure this posture complements its risk tolerance and business objectives.

Understanding a company's position within an industry is no easy task, but the implementation of a framework is an essential first step. Once the framework is implemented, it forms a benchmark that can be used to assess a cybersecurity program. Deviations that weaken or strengthen the security posture should be noted. Additionally, third-party audits and benchmarking with peers within an industry can be quite helpful in understanding one's relative security posture.

The choice of a framework is highly dependent upon the unique characteristics of the firm and its industry, as well as the firm's strategic positioning. Equally important to the decision is the compliance and regulatory regime through which the firm must navigate. To deal with the totality of compliance and regulatory requirements, as indicated earlier, frameworks must be tailored and a risk management approach must be used to map and harmonize overlapping or conflicting requirements.

These frameworks can also provide guidance on:

- Compliance and risk management activities
- Secure system development and/or system acquisition
- Control selection and implementation
- Security program management
- Data management and classification

In addition to providing practical guidance on security practices, frameworks can introduce "cultural" changes to an organization, which will often require a change management process. Effective frameworks will accommodate the different cybersecurity perspectives from various stakeholders. Perhaps most important, well-chosen frameworks will assist in providing a comprehensive understanding of an organization's ability to manage risk.

Some of the more widely used frameworks include:

- Cybersecurity standards and check lists, such as the ISO/IEC 27000 family of Information Security Management Systems standards; the PCI Data Security Standard; and the US-CCU Cybersecurity Check List
- Cybersecurity system of controls, such as ISACA Control Objectives for Information and related Technology (COBIT)
- Cybersecurity process management, such as US-CERT's Resiliency Management Model
- Cybersecurity system and software development, such as the SEI Capability Maturity Model Integration (CMMI); ISO/IEC 21827 Systems Security Engineering Capability Maturity Model; and the OWASP Software Assurance Maturity Model
- Cybersecurity system partnerships, such as ANSI Accredited Standards Committee X9 and the Federal Financial Institutions Examination Council (FFIEC) Handbooks
- Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*

Question

What is the assessment of physical security controls at each of our sites (data center, home office, field offices, and other sites)?

A framework for determining the physical-cyber interface

Physical security controls form the foundational element of any IT environment. Without the proper physical security controls in place and effectively operating, no other security assurances are possible. Equally important is the overlap between physical security and safety. Whatever the threat, physical security not only enables a sound IT security program, but also protects an organization's most important assets – its human capital. Even with the adoption of sophisticated countermeasures in the IT security area, organizations must not lose sight of physical security's central role.

Any comprehensive assessment of physical security must employ a process that implements controls commensurate with the risk identified. Similar to cybersecurity controls, the application of security controls should be based on a cost-benefit analysis that compares annualized loss of the asset against the annualized loss of the control.

Physical security encompasses the processes and countermeasures necessary to safeguard information systems and data as well as personnel and facilities. In addition to the more traditional controls commonly associated with physical security, such as fencing, lighting, and guards, this discipline has become highly sophisticated in its own right, and it has begun to converge with IT security. For instance, this convergence can be seen in access controls, biometric devices, environmental controls, and Radio-Frequency Identification (RFID). This convergence offers greater opportunities to align IT and physical security, but it also introduces new risks to that controls that had not previously been automated.

The ISC2 Common Body of Knowledge lists the goals of a physical security program as:

- Deter
- Delay
- Detect
- Assess
- Respond

Careful evaluation of the threats relevant to physical security is vital to the development and operation of an effective program. Threats may be characterized, in general terms, as either man-made or natural/environmental. Man-made threats include deliberate, malicious attempts to enter protected premises and gain access to, or simply remove, IT assets, whether physical or data-related. More serious man-made threats may also involve actions taken to destroy, or render unusable, a room, area, building, or complex of buildings. Environmental threats include failure of air conditioning, power, or telecommunications equipment, or damage caused to facilities or equipment by storms, floods, lightning, chemical spills, or any other activity that damages or prevents access to IT resources.

As in an IT environment, assessments must be done frequently to audit and test physical countermeasures to ensure they are effectively performing their intended functions and are meeting regulatory requirements.

Question

How prepared are our incident response plans?

A framework for incident response

Today's threat environment makes IT security-related incidents inevitable. The sophistication of attacks challenges even the most IT-savvy organizations. The key to success in this environment is to construct a layered defense, including incident detection and response capabilities, and to quickly sense and respond to these incidents. An investment in this capability will lead to cost savings because it will limit the spread of an incident and the infrastructure affected.

There are essential proactive and reactive steps that are necessary. On the proactive side, a defense-in-depth architecture must be deployed that will give early warning to anomalous activity that occurs at the application, system, or network level. Perimeter defenses are not adequate. System and application-based defensive mechanisms such as anti-virus, anti-malware, and intrusion prevention systems need to be fully integrated throughout the infrastructure. Vulnerability management must be frequently practiced to ensure patch levels are maintained and configurations are securely implemented.

When proactive measures fail, an incident response capability is required. Here, organizations must be guided by the famous quote "make haste slowly." In other words, responding to incidents is not only time-sensitive, but also process-intensive. A misstep can result in the destruction of evidence or can seriously hinder the discovery of the exploit or its origins. This reality needs to be balanced with the need to quickly contain an incident to defend the organization and return critical systems to operation.

A critical step in incident response is the creation of an incident detection and response team. Organizations need 24/7 coverage by personnel who are both business savvy and extremely technical. The technical skill sets are broad and include incident detection, monitoring, packet inspection, traffic analysis, and forensics. This team must also be adept at translating their technical know-how and findings so as to communicate effectively with business stakeholders.

The incident response plan should provide clear procedures to respond quickly and accurately to those situations identified during the risk assessments. It should include the critical internal and external stakeholders that may need to be consulted or alerted to incidents. The plan should include the necessary checklists and the procedures needed to lay out possible containment strategies, to identify evidence that might need to be gathered and specify how it is to be collected and

handled, to define possible methods to identify the attacker or the source of the attack, and to define processes that eradicate the incident and, ultimately, fully recover normal business operations. Once normal operations have been restored, the organization should study the incident and its response to the incident in order to adjust appropriately its proactive and reactive measures for future incidents. The plan should address each phase of the incident lifecycle as identified by the National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*[1]:

- Preparation
- Containment, eradication, and recovery
- Detection and analysis
- Post-incident activity

An organization's preparation is dependent upon the frequency with which its response plans are exercised. All plans need to be regularly exercised, tested, and updated to ensure that the plans allow appropriate, timely, and effective actions.

Questions

If our system goes down, how long until we are back up and running, and are there circumstances where we do **not** want to be back up quickly? How prepared are our business continuity plans? What is our risk exposure of technology or business operations failures at our vendors and service providers?

A framework for what to do when the system goes down

The primary mission for a business, company, or organization is its survival. To this end, firms must continuously navigate risk and uncertainty to continue to serve their stakeholders. One necessary element of survival, especially in turbulent markets, is a laser-like focus on meeting profit and loss (P&L) targets. This focus must be balanced with an equally important prerequisite for survival – a sound business continuity plan (BCP).

The purpose of a BCP is to minimize the effects of downtime, to recover to an acceptable level as quickly and safely as possible, and to restore operations to normal levels. A sound BCP encompasses disaster recovery planning. It addresses issues ranging from minor glitches (e.g., temporary loss of corporate email) to major disruptive events (e.g., loss of a facility due to an earthquake). A BCP mitigates the disruption of business services, processes, and assets (technology, information, facilities, and people). Put simply, a good BCP ensures an adequate level of preparedness in the face of a disruption.

Prioritization is essential to ensure that limited capital is optimally allocated. It is not feasible to protect all services, processes, and assets at the same level, especially once firms assess their dependence on service providers. Furthermore, the less downtime organizations are willing to accept, the more costs increase. Risk tolerances and thresholds as well as expected service levels (such as availability, capacity, response times, and performance targets) must be considered in prioritizing assets and in determining how much to invest in asset protection.

The heart of the BCP is the business impact assessment (BIA). The BIA is a business-driven process that that identifies, assesses, and prioritizes an organization's critical services, processes, and assets. In identifying the effects of disruptions on these high-value resources, the BIA estimates the maximum tolerable downtime, recovery time objectives, and recovery point objectives. These measures will inform business and technology personnel on the up-time requirements for IT systems; in other words, how long until systems must be back up and running.

1 NIST, *Computer Security Incident Handling Guide*, 2008

A comprehensive BIA will cover an organization's essential business partners as well as the organization itself. All business continuity planning and management should be guided by the BIA results and supported by risk assessments, ensuring that the organization is as prepared as possible if and when key business services are interrupted.

Based on BIA results, organizations need to develop a business continuity plan that lays out a strategy for response, recovery, restoration, and return to normal operations. As recommended by the Carnegie Mellon University Software Engineering Institute's Resiliency Management Model[2], this is a continuous and iterative process, and it includes:

- Determining roles, responsibilities, authority, and ownership for essential resources, defining the continuity strategy, and setting policy.
- Developing enterprise-wide and service-specific plans, where needed, which reflect strategy and policy, including operation of services under degraded conditions, recovery and restoration actions that limit and contain damage, key stakeholders, and adequately trained key personnel and communications channels and procedures.
- Defining emergency procedures, fallback procedures, temporary operational procedures, and resumption procedures.
- Selecting preventive, detective, and corrective controls that reflect asset protection strategies. This includes the use of insurance as one option for sharing risk.
- Ensuring that processes are in place for regular asset maintenance and capacity management.

It is important to stress that an effective BCP should address the organization's entire ecosystem, which inevitably includes external service providers. An organization's risk exposure must be assessed in terms of its dependence on external service providers for critical business functions. Given the growing use of third parties to provide essential services and operate key assets, business continuity and operational resiliency are greatly affected by these relationships. Business leaders need to ensure that appropriate terms and conditions, such as those described above, are included in procurement and acquisition contracts. In most cases, this means that external providers should be held to the same requirements as internal providers.

As with response plans, how prepared an organization is for a business continuity challenge will depend on the extent and the frequency with which the business continuity plans are exercised. All continuity plans need to be regularly practiced, tested, and updated to ensure that everything will go according to plan in the event of a disruptive event, including service interruptions and security incidents. Testing and test planning include defining objectives along with scenarios that will exercise these, such as:

- Table-top exercises
- Demonstrations
- Testing with vendors and services providers
- Simulations
- Recovery testing at primary and backup sites
- Comprehensive, real-world rehearsals

When an organization's personnel are able to rise to the challenges of a series of demanding cybersecurity exercises, they can feel confident that they are reasonably well prepared for the comparable real world events.

2 CERT Resiliency Management Model (http://www.sei.cmu.edu/solutions/risk/resilientops.cfm), see also Section IV of the Chapter 5 Appendix at the end of this document.

CHAPTER FIVE

A Framework for Managing External Communications and Crisis Management

Key Results

- Awareness of the importance of creating a formally documented incident response and crisis communications plan in advance of a cybersecurity issue
- Recognition of the substantial reputational and financial damage that can result from poorly handled communications about a cybersecurity incident
- Appreciation of the multiple audiences and issues that must be considered in communicating about cyber incidents
- An understanding of how to choose appropriate strategies and tools for managing communications about cyber incidents, including pre-incident, during an incident, and post-incident

Introduction

Cybersecurity events can significantly impact a company's relationship with a variety of stakeholders, including customers, employees, business partners, and investors, as well as regulators and law enforcement officials. With today's 24-hour news cycle where coverage of an event adverse to a company's reputation can appear on Twitter or on a cable news channel's footer in moments, careful planning and expert execution are no longer luxuries. In the wake of a cybersecurity event, an effective communications strategy can materially minimize the potential financial harm – including the "indirect' costs of potential damage to a company's reputation, its brand, its customer loyalty, and its employee's morale. All of these factors can have substantial impact on shareholder value.

Unfortunately, even the best-protected companies cannot completely eliminate the real risk of a successful cyber incident that results in a crisis to be managed. A prudent business should be prepared with a formally documented incident response and crisis communications plan in place to notify stakeholders and the media (when appropriate). Such a plan should address:

- Meeting the heightened reporting requirements by national and state regulators for losses of personally identifiable information (PII) or personal health information (PHI)
- The possibility of the loss or theft of valuable intellectual property or confidential company data (such as trade secrets, industrial designs, and client lists)
- Extended service outages and harm to people or property

Company executives should periodically review their company's incident response and crisis communications plan to ensure it remains up to date and actionable. Again, the failure to communicate effectively during a cybersecurity event may result in significant unplanned expenses, devaluation of the company, regulatory fines or penalties, and civil litigation.

In addition to a reactive communications plan, an increasing number of companies are developing a proactive communications strategy regarding computer security and privacy. At a minimum, all companies collecting data over the Internet require an Internet privacy policy that should be publicly disclosed. Many public companies include technology, security, and privacy issues as business risks in their filings to the U.S. Securities and Exchange Commission (SEC). Some companies characterize their security and privacy practices in marketing material as part of their value proposition. In all cases, content should be reviewed for accuracy and regulatory compliance.

For this chapter, our approach to developing a methodology for responses to the questions an executive should ask with respect to external communications and crisis management is to organize the material into pre-incident planning, incident response, post-incident review, and ongoing communications sections.

Questions

Do we fully understand the overall financial impact of mishandling communications with our key stakeholders following a cybersecurity event? Have we budgeted for a cybersecurity event?

A framework for pre-incident planning

Companies should evaluate their risk and costs associated with a cybersecurity event and should budget appropriately. One aspect of this consideration is the decision to purchase insurance, which transfers some of the potential costs to an insurance carrier. In addition to estimating the financial impact of a cyber breach, companies should perform a cyber risk assessment and identify specific actions that would mitigate the risk of a breach.

Businesses can draw on resources that are publically available (and in many cases free), or they can engage security consulting firms to perform independent audits that assess risk and provide mitigation strategies. This process may also be part of business continuity planning discussed earlier in the document or a part of the underwriting process for obtaining cyber liability or data breach insurance that is referenced later in this document.

Questions

Do we have a documented, proactive crisis communications plan? Have we identified and trained all the internal resources required to execute the communications plan? Do we have contacts at specialist crisis communications firms if we need their services? In the case of a cybersecurity event involving personally identifiable information (PII), do we have a system in place to quickly determine who should be notified, and how?

A framework for developing an incident response and crisis communications plan

Practical experience demonstrates that many of the communications risks and pressures imposed by a cybersecurity event can be anticipated, and reduced to some degree, with appropriate planning and practice. The first step is to develop a robust, written incident response plan that includes crisis communications activities as well as other operational guides for other internal departments.

This type of plan is cross-functional and is developed in advance of a cybersecurity event by IT, the privacy office, corporate communications, and other members of senior management, with input from legal. The plan should identify the likely (or even unlikely) cybersecurity event scenarios; the disclosure, notification, and legal requirements for each scenario; and the appropriate steps to mitigate potential harm to the company's reputation. While each cybersecurity event has unique aspects, this plan must also provide guidelines and rules around event discovery, investigation, risk assessment, and resource allocation.

A critical element to the plan is to identify in advance members of the Crisis Working Group – the "rapid response"team that will swing into action upon learning of a cybersecurity event. Typically such a group might include senior representatives from communications, IT, privacy, compliance, legal, investor relations, major business units impacted, human resources, and government affairs.

Companies should establish a clear process for convening the group on very short notice, and this process should include notification procedures and up-to-date 24-hour contact information.

The plan should ensure that the appropriate resources are in place to respond effectively to all impacted stakeholders, proper government/regulatory authorities, and media (as necessary) within the first 48 hours of a cybersecurity crisis – this is the window of opportunity when reputations are made or broken. The plan should also lay out a streamlined decision-making process to manage emerging issues on a real-time basis.

Incident response and crisis communication plans should not be "off-the-shelf" documents, but should be carefully tailored to the specifics of each company. Such a plan requires thoughtful consideration of which key audiences should be notified and how. In some circumstances (e.g., certain data breaches), notification to key regulatory bodies as well as the public is mandated, unless it might impede a criminal investigation. In other scenarios, it is an important courtesy. In yet others, public notification is unnecessary and may even be counterproductive or dangerous.

Guidelines for External Communications

An important element to incident response preparedness is planning how to communicate consistently and effectively to all appropriate stakeholders following a cybersecurity event.

Along with a timeline or "rollout" of key communications activities, the communications plan should anticipate the creation of the full set of communications materials, segregated by audience. A sample list of key documents is included in the Appendix of this document, including media statements or press releases, employee letters, client talking points, FAQs, and more. Documents and messaging will need to be carefully tailored to each specific constituency.

The plan should identify an appropriate company spokesperson and/or outside communications counsel who can speak to the press, if necessary. In particularly sensitive circumstances, this could mean the CEO or board chairman. If the designated spokesperson is an internal staff member, the company should ensure that this person undergoes proper media training in advance of any crisis situation.

The plan should anticipate the potential for aggressive 24/7 media attention. The plan should prepare for responding to media inquiries in a manner that delivers a clear message to parties affected directly or indirectly, as well as to other key stakeholders. In addition, it should include a process for aggressive monitoring of the media and the blogosphere for coverage or leaks – a service that can be provided by an outside communications firm – as well as a process for the real-time distribution of the coverage to the Crisis Working Group.

Having these processes in place will help to ensure a rapid and consistent response to any rumors, while allowing executives to monitor and track that company statements are being widely and accurately reported.

From the headlines

Suffolk County National Bank Breach; 8,300 Online Banking Login Credentials Stolen – Reported January 12, 2010

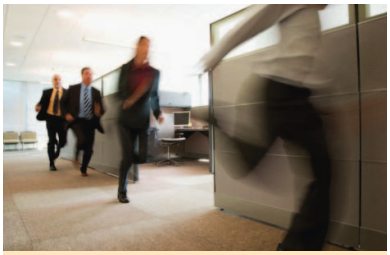
In December 2009, Suffolk County National Bank (SCNB) discovered the server that hosts log-in credentials for more than 8,300 of its online banking customers had been stolen by hackers who broke into the server that hosted its online banking system.

The intrusion at SCNB, located about an hour east of New York City, happened over a six-day period that started on November 18, 2009, and was discovered on December 24, 2009, during an internal security review. In all, credentials for 8,378 online accounts were stolen, which is less than ten percent of SCNB's total online accounts.

According to statements from the bank, it immediately isolated and rebuilt the compromised server and took other measures to ensure the security of data on the server. To date, the bank has found no evidence of any unauthorized access to online banking accounts, nor received any reports of unusual activity or reports of financial loss to its customers.

The bank began notifying affected customers on January 11 and ***claims that the two-week delay*** was necessary to ensure it could make an absolutely conclusive statement about what happened.

Depending on the severity of the crisis, a company may wish to consider establishing an "Operations/War Room" where potentially damaging charges and actions can be, in real-time, aggressively monitored and reported; vulnerabilities can be assessed; and, where appropriate, rapid, timely responses can be developed and executed.



A firm that specializes in crisis communications can help mobilize your company's notification effort.

The plan should include a process for regularly updating contact lists of key constituents that may need to be reached quickly, including trade and national media contacts, public officials, and other stakeholders.

A serious cybersecurity event can easily overwhelm the ability of a company's communications staff to respond in a timely manner. It can, therefore, be helpful to engage a crisis communications firm in advance to assist in the response plan development and to be "on call" to provide immediate service in the event that you require help.

Crisis firms can provide an embedded communications infrastructure – a SWAT team, if you will – of experienced professionals who can help to manage the strategic and tactical response to the crisis. In addition, firms specializing in data breach remediation can be particularly helpful with handling notifications to affected individuals.

Testing the plan

Finally, best practice also dictates that a company should conduct a crisis simulation exercise with their Crisis Working Group at least once a year in order to take the incident response rollout from a hypothetical situation to actual execution. These "table-top" simulation exercises can be run by incident response and crisis communications experts such as strategic communications firms, data breach prevention and remediation firms, and insurance risk managers.

Questions

Have we evaluated the appropriate communications responses to our key stakeholders? Do we have a template timeline for executing the communications plan? Have we considered that, depending on the situation, we may need to craft different messages for different types or levels of clients or employees?

A framework for initiating the incident response communications plan

The incident response plan is initiated when a cybersecurity event including, but not limited to, loss or unauthorized access to personally identifiable information (PII), personal health information (PHI), corporate secrets, or internal financial information is discovered. Best practice identifies four phases in implementing a successful incident response plan: assessment, response, protection, and recovery. These phases are outlined below, using an example of a data breach that included unsecured PII data:

Assessment

The first step is to assess what exactly has taken place and what data or information was lost or improperly accessed, if any. The Crisis Working Group should be gathered immediately, either in person or by conference call, to determine the steps needed to move forward.

In many instances, a detailed forensics review will be needed to determine what was fully accessed, when it was accessed, by whom it was accessed, and if the improper access could happen again. The Working Group may wish to outsource the forensics efforts through the company's external legal counsel to protect information about the event through client/attorney privilege while the investigation is ongoing.

An immediate effort to determine which regulations apply – federal, state, local law enforcement – should be undertaken. If PII or PHI was involved, consideration of data breach notification regulations will be necessary.

Incident Response

As the full assessment is under way, the Crisis Working Group should follow the incident response and crisis communications plan. Ideally, a company would communicate externally about a cybersecurity event only when a full assessment or forensics review has been completed.

Unfortunately, due to regulatory requirements, the twenty-four hour news cycle, and the length of time it often takes to complete an investigation, this may not be possible. The company may well have to begin communicating about the event before a full assessment or forensics review has been completed, which makes the careful crafting of the messaging and answers to potential questions – from stakeholders or the media – particularly important.

However, companies should not rush to communicate in order to pre-empt a leak to the media, but, instead, should take the time to effectively roll out the communications plan. Some companies have prematurely stated publicly that there is little risk of harm to the affected individuals in the case of a data breach, only to suffer the embarrassment and reputation damage of having to later revise that assessment.

Overall, the key is to ensure that the incident is accurately represented, and that all affected individuals, if any, are identified and notified within the appropriate timeframe as required by regulations. Again, consulting with external experts in crisis communications, data breach remediation, and insurance may save time in identifying how to best respond and reach out to all stakeholders.

In today's twenty-four hour news cycle, the media will be anxious to hear from your company in the event of a breach.

But don't rush to get a message out there without thoroughly reviewing your crisis communications plan. The most important thing is to assure that the incident is accurately represented.

Protection

The plan should also anticipate providing services to those who have been affected to minimize potential harm. In a data breach scenario where PII was lost or stolen, offering affected individuals some form of resolution services (e.g., identity theft recovery services, identity monitoring products) is considered best practice.

There are several forms of identity monitoring products on the market. Some only cover credit risks, while newer versions also cover public records and Internet chat room monitoring. More effective products are emerging and should be evaluated to mitigate the risk of new forms of ID theft (e.g., medical ID theft). Studies have shown that offering these services increases positive consumer perception and reduces potential loss of customers.[1]

Recovery

Identity theft recovery services can determine the probability that the breach of PII or PHI data was caused by the organization. These services can also determine the probability that any identity theft issues of affected individuals were caused by this particular data breach.

For the individuals who are confirmed victims of identity theft, this type of service should restore the victims to pre-theft status by eliminating damages to their identity. Eliminating damages can also reduce the likelihood of litigation (i.e., actual damages are a requirement for litigation).

1 Ponemon Institute, *2009 U.S. Cost of a Data Breach Study*.

Other Tips: Best Practices

- If the event was malicious, maintain a legal chain of evidence. Most incidents are accidental, but when the forensic investigation finds evidence of malicious intent, you should involve the legal, human resources, and fraud departments, and you should ensure that all of the proper steps are taken to preserve the chain of evidence to facilitate apprehension and prosecution of the perpetrators.

- Determine whether the costs related to the incident are covered by insurance. Today, many organizations have cyber liability or data breach insurance policies in place that cover the majority of costs associated with a cyber incident – forensics investigation, legal, call center, assistance services provided to individuals, and, perhaps, outside public relations firm expenses.

  It is prudent to check with your risk manager and/or insurance provider to understand what costs may be covered and if there are any requirements for vendors that would be eligible for reimbursement under the insurance policy. In many cases, insurance providers have identified expert resources that provide quality response services to clients.

- Consider outsourcing response efforts to specialists. Many organizations do not have the expertise or resources to effectively respond to a cyber incident. An effective alternative that helps mitigate overall risk is outsourcing all or some of the incident response and crisis communications to specialists.

  Outsourcing increases the probability of a positive outcome, namely, compliance with regulations, avoidance of negative press coverage, and reduced litigation exposure.

- When a cybersecurity event happens to a competitor firm, be prepared to respond to inquiries. If a competitor is hit with a major cybersecurity issue, the Crisis Working Group should immediately prepare standby responses for investor, press, customer, or employee questions. Resist the temptation to gloat or brag that this would never happen to your company, especially to the press.

Question

Have we implemented improvements as a result of an actual execution (real or mock) of the plan?

A framework for post-incident review

It is important to assess the effectiveness of the incident response and crisis communications plan at appropriate intervals during a cybersecurity event. The plan's effectiveness should be measured both quantitatively and qualitatively soon after the plan is executed. In the absence of an actual cybersecurity event, the plan should also be reviewed and updated periodically, at minimum on a yearly basis.

Evaluating – and revising, if necessary – the incident response and crisis communications plan will foster an environment of continuous improvement within your organization.

Quantitative measures

Quantitative measures for assessment should include the following:

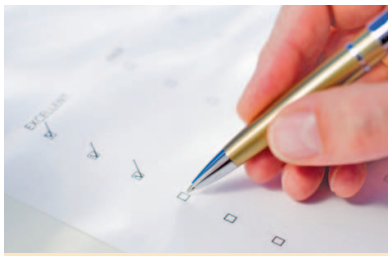
- Costs incurred compared to forecast
- Implementation time compared to plan
- Resources required compared to budget
- Timeliness of communication and consistency of message compared to expectations
- Impact on corporate reputation as perceived by key stakeholders

Qualitative measures

In addition, qualitative measures for assessment should include the following:

- Level of satisfaction of constituents
  - A critical component in an assessment of the effectiveness of a company's response to a cybersecurity event should be the level of satisfaction of the company's key constituents. At a minimum, internal constituents – including management, members of the Crisis Working Group, the company spokesperson, and employees – should be asked to rate how well the crisis communications plan met their needs and expectations. The results should be compiled and reviewed by the Working Group.

  - Ascertaining the response of external constituents – including affected individuals, business partners, investors, and government/regulatory authorities – could include proactive outreach, where appropriate, by appropriate business unit heads (e.g., the heads of investor relations or government relations). However, care should be taken not to inadvertently "re-publicize" the incident and, thereby, cause further damage to the company's reputation.



A survey of internal constituents will indicate their overall level of satisfaction with the company's response to a cybersecurity event.

- Nature of media coverage, compared to desired coverage
  - In the wake of a cybersecurity event it is important to assess the quality and breadth of the media coverage, if any. Were the company's messages reported accurately and consistently? Did coverage include clear messages about the actions the company took to remedy the situation? If not, was this due to a lack of discipline by company spokespeople? Was press coverage disseminated in real time to the Working Group and errors in reporting corrected immediately?

- Affect on litigation risk and risk of governmental action
  - After an event, legal and compliance representatives should evaluate how much the crisis communications plan moderated the risk of litigation or governmental action.

Updating the plan

The post-response evaluations should be used to update the plan, including cost estimates, resource allocation and training, document templates, and project schedules.

Ongoing communications

Given the growing public awareness of company vulnerabilities to cybersecurity events, some well-prepared firms have adopted a proactive strategy to communicate their efforts on cybersecurity and privacy. This approach can help a company to build brand value and differentiation, enhance customer loyalty, address investor concerns, foster positive relations with governmental bodies and law enforcement, and adhere to regulatory reporting requirements.

Any such strategy should be undertaken with care, however. Since no company is completely immune from cybersecurity events, such a proactive effort could backfire if a subsequent cybersecurity event does occur.

A proactive communications program may include advertising, marketing material, web content, regulatory filings, and participation in industry and community activities – all in support of a clear, consistent, and positive message.

CHAPTER SIX

A Framework for Analyzing Financial Risk Transfer and Insurance

Key Results

- Even if managed properly, a cybersecurity event will lead to residual financial loss
- Specifically designed cyber insurance can be a useful tool in transfers of unwanted residual risk
- Sometimes a company qualified for insurance can use this as a positive fact in regulatory negotiations and civil lawsuit settlements

Introduction

After determining that the costs of cyber events against companies involved in our critical infrastructures could run to several million dollars a day, the Center for Strategic Infrastructure Studies polled executives regarding who they believed would pay these costs. More than half of the respondents replied that they expected insurance to cover the costs.[1]

These executives may be in for an unwelcome surprise.

In a separate study, Ernst & Young found that fully one-third of corporate chief technology officers (CTOs) confessed to not knowing for sure if they had insurance to cover cyber events, and, more alarmingly, another third believed they had cyber insurance coverage – and were wrong.[2]

Cybersecurity events can, and often do, result in substantial short-term direct costs such as lost income, business interruption, and significant legal expenses and liabilities, among others, which can severely strain the financial resources of a company.

Even when managed properly, a company remains at substantial risk from unknown or worse-than-anticipated loss events. Each company has to decide how it wishes to handle that residual risk, how much risk to accept, and how much, if any, risk to transfer through insurance.

Since the late 1990s, insurance companies have developed, and specialized brokers have emerged with respect to, a range of products which allow an entity to transfer many of these financial risks. Commonly known as cyber risk insurance or network security and privacy insurance, these policies are specifically designed to cover a host of cyber risks including legal expenses, settlements, judgments, business loss, and "extra expenses."

The questions on the following pages are those which would typically be asked of the risk manager for corporate insurance or of the individual responsible for the purchase of insurance to transfer the cost of recovering from a cybersecurity event.

1 Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2009.

2 Ernst & Young, *2003 Global Information Security Survey*.

Question

Doesn't the company already have insurance coverage for this?

A framework for determining if coverage exists

Unfortunately, traditional insurance policies, written well before the arrival of the Internet, do not generally cover cyber-related risks. For example, general liability policies purchased by companies today typically cover bodily injury and tangible property damage claims. The policies do not normally cover damage or theft to digital property, or litigation arising from most cyber events. Similarly, property policies, as a general matter, only cover tangible property loss arising from physical perils such as flood or fire.

Question

What does cyber risk insurance cover?

A framework for determining the extent of coverage

Because cyber insurance policies have been around only since the late 1990s, there is no universally accepted insurance form in the marketplace. Nevertheless, regardless of the particular language (which can be very important), superior cyber risk policies should provide the following coverage:

- Third-party litigation and regulatory investigations (especially those arising from theft of personally identifiable information) including legal expenses, judgments, and settlements
- First-party losses an insured company may suffer from business interruption, and "extra expenses" incurred due to a covered cybersecurity event
- With respect to PII theft events, enhanced coverage for crisis management expenses, state notification expenses, and other remediation costs

Exclusions vary from carrier to carrier but generally include no coverage if the insured:

- Fails to meet the minimum security requirements
- Fails to provide notice of a material change to the information provided in their application
- Breaches representations and warranties made in the application

There is usually an overall policy aggregate limit and a per-loss deductible, or "self-insured retention."

Question

What types of cybersecurity events are covered by this insurance, and how are our insured losses measured?

A framework for determining covered losses

If there is a failure of security and a successful breach that compromises a company's system or allows unauthorized access to sensitive information occurs, civil lawsuits from customers, suppliers, and others could arise. These civil lawsuits could result in substantial legal defense costs and potentially expensive settlement costs or adverse judgments. In addition,

investigations by regulatory bodies, including the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), or state attorney generals, could arise and could result in company costs for investigation and defense. Business interruption and related expenses associated with reduced network availability can also affect the bottom line and can reduce profitability. Over the short or long term, such events can lead to reputation damage.

The quantifiable measurement of third-party litigation is, of course, the cost of mounting a legal defense, plus the payment of any settlement or cost of an adverse judgment. Business interruption can be quantified in terms of numbers of transactions, dollars, or contracts per time period measured on a typical business day. The cost of reconstructing intangible assets may include forensic investigation, recompiling data, or transcribing information.

Question

Does the policy specifically cover identity theft issues?

A framework for specifying identity theft coverage

Many cyber/information risk insurance policies explicitly respond to events that could lead to identity theft, including the release of PII. Coverage may include reimbursement for the cost of notifying affected individuals and providing identity theft risk management services such as credit monitoring. Furthermore, many identity theft risk management services include personal identity theft insurance as a component of the service.

Question

Is there a directors' and officers' (D&O) exposure if we do not purchase the cover?

A framework for protecting directors and officers

In theory, if a company suffers a large uninsured financial loss where reasonable insurance was available in the market, failure to obtain insurance may be ground for a management liability suit by aggrieved shareholders. Furthermore, most D&O policies have an exclusion for a "failure to obtain insurance" claim.

Question

Where do we find an insurance broker who can assist in evaluating whether we need this type of insurance?

A framework for finding an insurance broker

Any insurance broker with a "P&C" (Property and Casualty) license can help with the purchase of this coverage. Almost all large insurance brokers in the United States have developed information security and privacy expertise. Many middle-tier or regional broking houses have also developed, or are in the process of developing, internal resources dedicated to this type of coverage as brokerage revenues from information security and privacy insurance continue to grow. Finally, there are also specialist wholesalers who serve as dedicated resources to retail brokers who have no in-house expertise. The essential lesson here is that this type of coverage is fairly new and can be quite complex, requiring the use of a brokerage firm schooled in the area.

Question

How do we evaluate insurance carriers with respect to this specialized coverage?

A framework for evaluating carriers

A growing number of insurers either currently offer, or are gearing up to offer, some form of cyber risk coverage. Key considerations for selecting an insurance company include:

- The insurer's ratings from the insurance rating agency A.M. Best as well as financial rating agencies such as Standard & Poor's, Moody's, etc.
- The length of time the carrier has been providing this specific coverage
- The maximum limits the carrier can offer on any one policy (known as the carrier's "capacity")
- The scope of coverage being sought or offered
- The price of the policy being sought or offered
- The insurer's claims-handling practices and reputation in "specialty" lines

Question

What does a policy cost?

A framework for evaluating covered loss

The cost of this policy will be comparable to that of many other corporate insurance policies. The actual cost of insurance depends on coverage, limits, and retention. For a very small company, this insurance may cost less than $1,000 per year. For a very large company, the cost may be over $1 million per year.

Question

What are the other benefits of purchasing a specific cyber risk insurance policy?

A framework for determining comparative benefit

In addition to the obvious benefit of legal and first-party expense reimbursement, the purchase of a specific cyber risk policy has a number of other indirect benefits, including:

- The ability to obtain an objective, usually free, review of a company's network security by a third party (i.e., the insurer or its agent)
- A better ability to understand the company's risk level compared to its peers (by examining the differences in premiums)
- Better quantification of net financial risk

Finally, the demonstration of the successful ability to purchase insurance could be a favorable factor with the company's regulators, or even in litigation.

APPENDICES

The appendices that follow are linked to specific chapters in the book, and contain tools and/or references designed to enhance the content of that specific chapter. All URLs bring the reader directly, or as close as possible, to the document being referenced. While many of these links should remain stable and accessible in the long term, please keep in mind that some links may become invalid over time and may necessitate a fresh search.

Any tools mentioned in the appendices are meant to be representative of those available. The list of tools is not exhaustive, and neither ANSI, ISA, nor the contributors of this document or their respective organizations endorse the use or purchase of these tools.

Chapter 2 Appendix – A Framework for Managing the Human Element

Possible Employment Framework

Attract	*Acclimate*	*Invest*	*Engage*	*Access*
Brand company as world-class cyber employer Employ workforce planning to include a targeted talent management strategy Offer competitive total compensation and benefits package Offer best-in-class facilities and technology Create a working environment that doesn't discriminate based on location – ensure equivalent opportunity for remote employees	Implement cyber security culture orientation Execute ongoing communications plan Provide training on specific roles and responsibilities based on job description Provide training on interrelationships and interdependencies across multiple functional areas Respect and acknowledge fast pace of technology advancement Educate on new levels of cyber risk	Provide access to continuing education and certification Continually modernize facilities, technology, and risk education Review and renew total compensation and benefits package Execute regular performance management feedback mechanism on annual basis at minimum	Implement rotational programs Encourage external industry networking opportunities Afford cross-training opportunities for additional functional insight Sponsor employee feedback sessions, and develop new methods and techniques based on feedback Seek employee involvement wherever possible	Require criminal background screening prior to hire Limit access to relevant, necessary, and sufficient information and systems Continually re-evaluate access needs Monitor access behavior Automate access revocation at threat confirmation and separation Commit to progressive discipline strategy
Communications and Training				
Cyber Security Culture – Ethics and Awareness				

Employment Life Cycle Activities

Acquisition	*Year One*	*Interim Years*	*Senior*	*Separation*
Screen for criminal history, basic educational and professional background Implement cyber security culture orientation and certify Provide training on specific roles and responsibilities based on job description Ensure clear connection between business objectives and cyber security commitment Provide access based on role	Execute ongoing communications plan Ensure remote employees have access to all relevant materials and information Re-certify on cyber security awareness and commitment Update access based on current role and responsibilities Monitor error rates and watch for suspicious behavior Provide immediate feedback Implement and document discipline and/or rewards	Provide access to continuing education and certification Continually modernize facilities and technology Re-certify on cyber security awareness and commitment Update access based on current role and responsibilities Monitor error rates and watch for suspicious behavior	Leverage longevity for mentoring new acquisitions and infusing cyber security culture Monitor requests to ensure that senior employee is not leveraging status to bypass standard operating procedures Update access based on current role and responsibilities Monitor error rates and watch for suspicious behavior	Catalog systems access in one-on-one prior to separation Ensure immediate access revocation upon termination to include all electronic devices (blackberry, smart badge, remote token, laptop, desktop, etc.) Require intellectual property certification Update personal and emergency contact information
Communications and Training				
Cyber Security Culture – Ethics and Awareness				

Chapter 3 Appendix – A Framework for Managing Legal & Compliance Issues

State Security Breach Notification Laws

Alaska	Alaska Stat. §§ 45.48.010 to .090
Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code Ann. §§ 4-110-101 to -108
California	Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen. Stat. § 36a-701b
Delaware	Del. Code Ann. tit. 6, §§ 12B-101 to -104
District of Columbia	D.C. Code Ann. §§ 28-3851 to -3853
Florida	Fla. Stat. ch. 817.5681
Georgia	Ga. Code Ann. §§ 10-1-910 to -912
Hawaii	Haw. Rev. Stat. §§ 487N-1 to -4
Idaho	Idaho Code Ann. §§ 28-51-104 to -107
Illinois	815 Ill. Comp. Stat. 530/1, 530/5, 530/10, 530/12, 530/15, 530/20, 530/25
Indiana	Ind. Code §§ 4-1-11-1 to -10; 24-4.9-2
Iowa	Iowa Code § 715C.1 to -2
Kansas	Kan. Stat. Ann. §§ 50-7a01 to 02
Louisiana	La. Rev. Stat. Ann. §§ 51:3071 to 3077
Maine	Me. Rev. Stat. Ann. tit. 10, §§ 1346 to 1350-B
Maryland	Md. Code Ann., Com. Law §§ 14-3501 to -3508
Massachusetts	Mass. Gen. Laws ch. 93H, §§ 1–6
Michigan	Mich. Comp. Laws § 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code Ann. § 30-14-1704
Nebraska	Neb. Rev. Stat. §§ 87-801 to -807
Nevada	Nev. Rev. Stat. §§ 603A.010 et seq., 603A.220
New Hampshire	N.H. Rev. Stat. Ann. §§ 359-C:19 to -C:21
New Jersey	N.J. Stat. Ann. § 56:8-163
New York	N.Y. Gen. Bus. Law § 899-aa; N.Y. State Tech. Law § 208
North Carolina	N.C. Gen. Stat. § 75-65; 2009 N.C. Sess. Laws 355
North Dakota	N.D. Cent. Code §§ 51-30-01 to -07
Ohio	Ohio Rev. Code Ann. §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. tit. 74, §§ 3113.1
Oregon	Or. Rev. Stat. §§ 646a.600, 602, 604, 624, 626
Pennsylvania	Pa. Stat. Ann. §§ 73-2301 to -2308, -2329
Rhode Island	R.I. Gen. Laws. § 11- 49.2-1 to -7
South Carolina	S.C. Code Ann. §§ 1-11-490, 39-1-90
Tennessee	Tenn. Code Ann. § 47-18-2101 to -2107

Texas	Tex. Bus. & Com. Code Ann. §§ 48.001 to -103, 521.001 et seq., as amended by H.B. 2004, eff. Sept. 1, 2009; Tex. Gov't Code Ann. § 2054.1125; Texas Loc. Gov't Code Ann. § 205.010
Utah	Utah Code Ann. §§ 13-44-101 to -102, 13-44-201 to -202, 13-44-301
Vermont	Vt. Stat. Ann. tit. 9, § 2430-2435
Virginia	Va. Code Ann. § 18.2-186.6
Washington	Wash. Rev. Code § 19.255.010
West Virginia	W. Va. Code § 46A-2A-101 to -105
Wisconsin	Wis. Stat. §§ 134.98, 895.507
Wyoming	Wyo. Stat. Ann. §§ 40-12-501 to -509
Puerto Rico	P.R. Laws Ann. tit. 10, §§ 4051-4055
Virgin Islands	V.I. Code Ann. tit. 14, §§ 2208-2212

Note: Currently there are five states with no security breach notification law: Alabama, Kentucky, Mississippi, New Mexico, and South Dakota.

Resources

- National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/Default.aspx?TabId=13489
- Commercial Law League of America, State Data Security Breach Notification Laws, http://www.clla.org/documents/breach.xls
- Georgia State University Law Library, Information Security and Data Security Breach Notification Laws, http://law.gsu.edu/library/index/bibliographies/view?id=296
- IT Law Group, Security Breach Disclosure Laws, http://www.itlawgroup.com/Resources/SecurityBreach.html
- Crowell Moring, State Laws Governing Security Breach Notification, http://www.crowell.com/pdf/SecurityBreachTable.pdf
- Mintz Levin, State Data Breach Legislation Survey, http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf
- Perkins Coie, Security Breach Notification Chart, http://www.perkinscoie.com/statebreachchart/chart.pdf
- Proskauer Privacy Law Blog, Security Breach Notification Laws, http://privacylaw.proskauer.com/2009/07/articles/security-breach-notification-l/showme-state-finally-shows-its-residents-a-data-breach-notification-law-other-states-tx-nc-me-make-changes/

Federal Security Breach Notification and Data Protection Laws

- Children's Online Privacy Protection Act of 1998 (15 U.S.C. §§ 6501-6506)
- Fair Credit Reporting Act of 1970 (15 U.S.C. §§ 1681-1681x)
- Federal Information Security Management Act of 2002 (44 U.S.C. § 3541-3549)
- Federal Trade Commission Act of 1914 (15 U.S.C. § 45)
- Gramm-Leach-Bliley Act of 1999 (15 U.S.C. § 6801(b); see also Standards for Safeguarding Customer Information Rule, 16 C.F.R. §§ 314.1 to .5, available at http://www.ftc.gov/os/2002/05/67fr36585.pdf; Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Part III of Supplement A to Appendix, at 12 C.F.R. Part 30 (Office of the Controller of the Currency); 12 C.F.R. Part 208 (Federal Reserve System); 12 C.F.R. Part 364 (Federal Deposit Insurance Corporation); and 12 C.F.R. Part 568 (Office of Thrift Supervision), 70 Fed. Reg. 15736-15754 (Mar. 29, 2005), available at http://edocket.access.gpo.gov/2005/05-5980.htm
- Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act") §§ 13402-13407; see also Breach Notification for Unsecured Health Information Interim Final Rule, 45 C.F.R. Parts 160 and 164, 74 Fed. Reg. 42740-42770 (Aug. 24, 2009), available at http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf; Health Breach Notification Rule, 16 C.F.R. §§ 318.1 to 318.9, 74 Fed. Reg. 42962-42985 (Aug. 25, 2009), available at http://www2.ftc.gov/os/2009/08/R911002hbn.pdf
- Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d-1320d-8)
- Veterans Affairs Information Security Enhancement Act of 2006 (38 U.S.C. §§ 5721-5728)

Chapter 4 Appendix – A Framework for Operations and Technology

Questions 1, 2, and 10

Document	*Date*
NIST SP 800-100 *Information Security Handbook: A Guide for Managers* http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf	October 2006
NIST SP 800-53 Rev. 3 *Recommended Security Controls for Federal Information Systems and Organizations* http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf	August 2009
NIST SP 800-53 A *Guide for Assessing the Security Controls in Federal Information Systems* http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf	July 2008
NIST SP 800-51 *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme* http://csrc.nist.gov/publications/nistpubs/800-51/sp800-51.pdf	September 2002
NIST SP 800-47 *Security Guide for Interconnecting Information Technology Systems* http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf	August 2002
NIST SP 800-39 *DRAFT Managing Risk from Information Systems: An Organizational Perspective* http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf	April 2008
NIST SP 800-30 *Risk Management Guide for Information Technology Systems* http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf	July 2002
NIST SP 800-37 Rev. 1 *DRAFT Guide for Security Authorization of Federal Information Systems:* *A Security Lifecycle Approach* http://csrc.nist.gov/publications/drafts/800-37-Rev1/SP800-37-rev1-FPD.pdf	August 2008
NIST SP 800-18 Rev.1 *Guide for Developing Security Plans for Federal Information Systems* http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf	February 2006

Questions 3, 7, and 8

Document	*Date*
The British Standards Institution *Business Continuity Management, Part 1: Code of Practice* ISBN 0 580 49601 5	November 2006
The British Standards Institution *Business Continuity Management, Part 2: Specification* ISBN 978 0 580 59913 2	November 2007
CERT Resiliency Management Model v1.0 Carnegie Mellon University Software Engineering Institute CERT Program http://www.sei.cmu.edu/downloads/resiliency-engineering.cfm	2009
Committee of Sponsoring Organizations of the Treadway Commission *Enterprise Risk Management — Integrated Framework* http://www.coso.org/-ERM.htm	2004
DRJ Editorial Advisory Board Generally Accepted Business Continuity Practices Committee and DRI International *Generally Accepted Practices For Business Continuity Practitioners* http://www.drj.com/GAP/gap.pdf	August 2007
Federal Financial Institutions Examination Council *"Business Continuity Planning" IT Examination Handbook* http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf	March 2008
ISO/IEC 20000-2:2005 *Information technology – Service management – Part 2: Code of practice* http://www.iso.org/iso/catalogue_detail?csnumber=41333	2005
ISO/IEC 27002:2005 *Information technology – Security techniques – Code of practice for information security management* http://www.iso.org/iso/catalogue_detail?csnumber=50297	2005
ISO/IEC 24762:2008 *Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services* http://www.iso.org/iso/catalogue_detail?csnumber=41532	2008
NFPA 1600: *Standard on Disaster/Emergency Management and Business Continuity Programs* http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf	2007
NIST SP 800-34 *Contingency Planning Guide for Information Technology Systems* http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf	June 2002

Question 4

- ISO/IEC 27000
  A growing family of ISO/IEC Information Security Management Systems (ISMS) standards
  http://www.27000.org/

- The Control Objectives for Information and related Technology (COBIT)
  A set of best practices (framework) for information technology (IT) management created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1996
  http://www.isaca.org/cobit

- ISO/IEC 21827 (SSE-CMM – ISO/IEC 21827)
  An International Standard based on the Systems Security Engineering Capability Maturity Model (SSE-CMM) developed by the International Systems Security Engineering Association (ISSEA)
  http://www.iso.org/iso/catalogue_detail.htm?csnumber=44716

- The Accredited Standards Committee X9 (ASC X9, Inc.) – Financial Industry Global Standards mission is to develop, establish, maintain, and promote standards for the financial services industry in order to facilitate delivery of financial services and products. ASC X9, Inc., is an ANSI (American National Standards Institute) accredited standards developing organization, accredited by ANSI since 1984 (see www.ansi.org for a list of accredited organizations)
  http://www.x9.org

Question 5

Document	*Date*
NIST SP 800-50 *Building an Information Technology Security Awareness and Training Program* http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf	October 2003
NIST SP 800-16 *Information Technology Security Training Requirements: A Role- and Performance-Based Model* http://csrc.nist.gov/publications/drafts/800-16-rev1/Draft-SP800-16-Rev1.pdf	April 1998
U.S. Department of Homeland Security *Information Technology (IT) Security Essential Body of Knowledge (EBK):* *A Competency and Functional Framework for IT Security Workforce Development* http://www.us-cert.gov/ITSecurityEBK/EBK2007.pdf	October 2007

Question 7

Document	*Date*
NIST SP 800-61 Rev. 1 *Computer Security Incident Handling Guide* http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf	March 2008
SANS *Computer Security Incident Handling: Step-by-Step* (Version 2.3.1) ISBN 978-0972427371	2003

Chapter 5 Appendix – A Framework for Managing External Communications and Crisis Management

This appendix consists of the following four sections:

I. Outline for an Incident Response Plan and Data Breach Response Policy
II. Sample documents in a typical large data breach scenario
III. Estimating the costs of a cyber incident that includes PII or PHI data
IV. Cyber risk assessment tools

I. Outline for an Incident Response Plan and Data Breach Response Policy

Purpose

The Incident Response Plan (IRP) is a comprehensive working document to assist organizations in dealing with a cyber security incident, data breach, or other critical incident. The IRP should be customized to an organization's specific policies, requirements, risk assessment, and industry.

Objectives

The Incident Response Plan will enable an entity to respond to any and all privacy-related incidents in an efficient and cost-effective manner that:

- Avoids or minimizes short- and long-term business losses resulting from a privacy-related data breach
- Avoids or minimizes damage to individuals whose personal information may have been compromised
- Meets industry and regulatory requirements and avoids breach-related penalties
- Avoids or minimizes the costs of litigation resulting from a breach
- Avoids or minimizes potential damage from similar breaches in future

Incident Response Plan

The exact details and actions taken in each phase will depend on the organization's policies, procedures, and the nature of the privacy-related incidents. The IRP should contain details on the following areas:

- Objectives
- Definitions
- Regulatory guidelines
- Data Breach Response Policy (see below)
- Scenarios
- Forensics/prevention
- Crisis communications
- Legal
- Remediation
- Notification strategy (when to notify and whether to outsource services)
- Additional materials, references, and worksheets

Outline of a Data Breach Response Policy

A Data Breach Response Policy provides an organization with a plan of action in the event of a privacy-related data breach. (Note that there will likely be some overlap between this plan and the crisis communications plan.) A data breach prevention and remediation firm such as ID Experts can assist client organizations in executing the plan, which includes the following actions:

- Containment
- Classification
- Internal reporting of an incident or breach
- Documentation
- Notification of executive staff
- Notification to victims
- Time for providing notification
- Responsibility for providing notification
- Contents of the notification
- Method of notification
- Substitute notification
- Additional notification requirements

II. Sample communications documents that might be utilized in a typical large data breach scenario include the following:

Core documents

1. Rollout/timeline
2. List of key audiences
3. Leak strategy
4. Key messages
5. Press release/media statement
6. Master QA
7. Breach notification letter

Potential ancillary documents

These are drawn from the aforementioned key messages, but are carefully tailored for the relevant specific audience:

1. Letter to affected clients/employees
2. Affected clients/employee talking points and FAQ
3. Letter to non-affected clients/employees
4. Non-affected clients/employees talking points and FAQ
5. Talking points for managers to use with corporate employees (after press release is out)
6. Email/letter to corporate employees
7. Reminder to employees about security procedures (separate email/letter)
8. Talking points for meeting with corporate employees and FAQ
9. Recorded message for client/employee calls to call center
10. Talking points for call center managers to brief call center employees
11. Script/QA for customer service reps to use with clients/employees
12. Email to call center employees with short script to redirect calls to specially trained teams
13. Talking points for investors and FAQ
14. Notice to government agency/officials
15. Notice to credit reporting bureaus
16. Website copy/process for quick establishment of a dedicated website or set up a "dark" website

III. Estimating the costs of a data breach that includes PII or PHI data

In January 2010, Ponemon Institute produced its fourth annual report on the cost of data breach. The report from Ponemon – a leading research center that conducts independent research on consumer trust, privacy, data protection, and emerging data security technologies (www.ponemon.org) – indicates that data breaches can have serious financial consequences on an organization.

According to this year's study, the average cost of a data breach has risen to $204 per customer record in 2009 versus $202 in 2008.

Ponemon established objective methods for quantifying specific activities that result in direct, indirect, and opportunity costs from the loss or theft of personal information, thus requiring notification to breach victims as required by law or policy.

Ponemon's current analysis of the actual data breach experiences of 43 U.S. companies from different industry sectors takes into account a wide range of business costs, including expense outlays for detection, escalation, notification, and after-the-fact (ex-post) response. They also analyze the economic impact of lost or diminished customer trust and confidence, measured by customer churn or turnover rates.

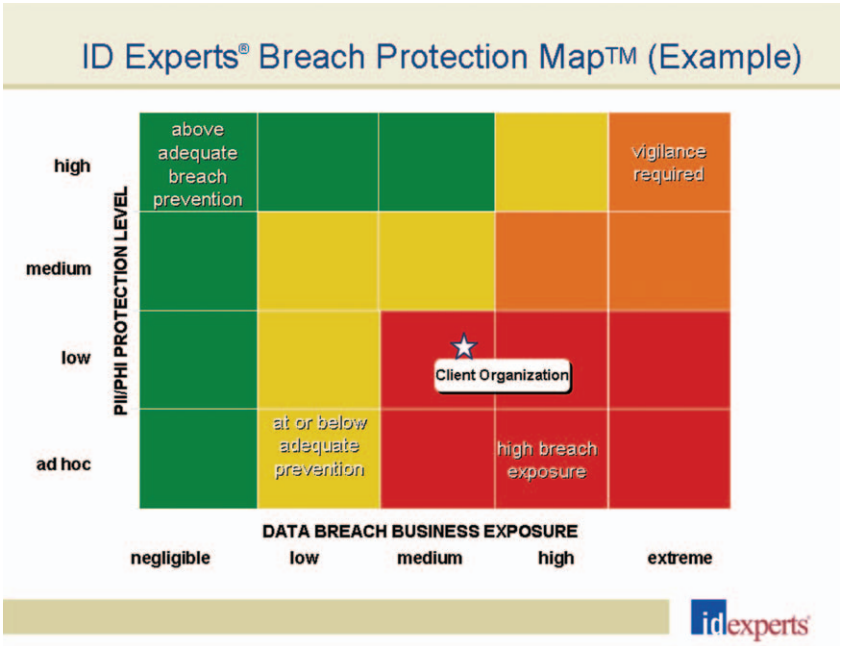
IV. Cyber risk assessment tools

There are several data security risk assessment approaches and tools in the market that help an organization assess and manage cyber risk. This is not meant to be an exhaustive list, but examples of resources that exist and are available as of the publication of this document.

Data Breach Risk Assessment Tool

ID Experts, the leader in comprehensive data breach solutions that provide the most positive outcomes, has developed a data breach risk assessment tool called Breach HealthCheckSM. This free tool helps organizations measure their breach exposure and protection level quickly, and then track their progress through changes in business processes and environment. Breach HealthCheck uses a scorecard and a mathematical model to produce a Breach Protection Index and a Breach Protection Map.

The ID Experts Breach Protection IndexTM (BPI) is produced by a mathematical model, which uses a pre-defined set of expert-weighted questions and a proprietary assessment algorithm to measure an organization's breach exposure and breach protection levels. The BPI has two components. The first is the Breach Exposure Level, which helps to quantify the magnitude of the business impact to your organization should a data breach incident occur. This measure takes into account factors such as value of your brand, nature of your customer base, amount and sensitivity of the PII/PHI you maintain, and your regulatory and compliance environment. The second component is the Breach Protection Level, which measures your overall protection level



correlated with known data breach risk factors, and how well your organization has protected itself against these risks. This component measures the relative maturity of an organization's breach protection and overall privacy programs, processes, and procedures.

The Breach Protection Map (BPM) uses a "heat map" approach to provide an easy-to-understand visual analysis of the business' protection level. The map uses color-coded zones to help quickly expose any gaps between breach risks and the required level of protection as determined by your organization's BPI. The heat map helps your organization comprehend its exposure and protection levels at a glance, and it can also be used for benchmarking purposes.

http://www.idexpertscorp.com/breach/health-check/

Model-Based Security Risk Assessment

CORAS (Cost-of-Risk Analysis Software) is a method for conducting security risk analysis. CORAS provides a customized language for threat and risk modelling, and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis. In this respect CORAS is model-based. The Unified Modelling Language (UML) is typically used to model the target of the analysis. For documenting intermediate results and for presenting the overall conclusions, special CORAS diagrams which are inspired by UML are used. The CORAS method provides a computerized tool designed to support documenting, maintaining, and reporting analysis results through risk modelling.

In the CORAS method, a security risk analysis is conducted in seven steps:

- **Step 1**: The first step involves an introductory meeting. The main item on the agenda for this meeting is to get the representatives of the client to present their overall goals of the analysis and the target they wish to have analyzed. Hence, during the initial step the analysts will gather information based on the client's presentations and discussions.

- **Step 2**: The second step also involves a separate meeting with representatives of the client. However, this time the analysts will present their understanding of what they learned at the first meeting and from studying documentation that has been made available to them by the client. The second step also involves a rough, high-level security analysis. During this analysis, the first threats, vulnerabilities, threat scenarios, and unwanted incidents are identified. They will be used to help with directing and scoping the more detailed analysis still to come.

- **Step 3**: The third step involves a more refined description of the target to be analyzed, and also all assumptions and other preconditions being made. Step three is terminated once all this documentation has been approved by the client.

- **Step 4**: This step is organized as a workshop, drawn from people with expertise on the target of the analysis. The goal is to identify as many potential unwanted incidents as possible, as well as threats, vulnerabilities and threat scenarios.

- **Step 5**: The fifth step is also organized as a workshop, this time with the focus on estimating consequences and likelihood values for each of the identified unwanted incidents.

- **Step 6**: This step involves giving the client the first overall risk picture. This will typically trigger some adjustments and corrections.

- **Step 7**: The last step is devoted to treatment identification, as well as addressing cost-benefit issues of the treatments. This step is best organized as a workshop.

http://coras.sourceforge.net/

CERT Resiliency Management Model

1. Are security and business continuity activities coordinated in your organization, or are they performed in silos? Are they viewed as technical rather than business activities?

2. Can you actively manage operational resiliency, or do you typically react to disruptive events as they occur?

3. Do you know if the security and business continuity practices that you've implemented are effective? Do they support the achievement of the organization's strategic objectives and mission?

4. Can you measure the success of your security and business continuity activities? Can you consistently repeat and sustain that success over the long run?

5. Do you have a foundation from which to continuously improve your security and business continuity efforts?

If your organization cannot answer these questions with certainty, CERT's research in the field of resiliency management may help. CERT is developing tools, techniques, and methodologies that allow organizations to move their security and business continuity activities to the next level by focusing on actively managing operational resiliency to achieve the organization's mission. The cornerstone of the research is the development of the CERT ® Resiliency Management Model. The model is the foundation for a process-improvement approach to security and business continuity. It establishes an organization's resiliency management process: a collection of essential capabilities that an organization performs to ensure that its important assets – people, information, technology, and facilities – stay productive in supporting business processes and services. The model serves as a foundation from which an organization can measure its current competency, set improvement targets, and establish plans and actions to close any identified gaps. As a result, the organization repositions and repurposes its security and business continuity activities and takes on a process-improvement mindset that helps to keep these activities productive in the long run.

The CERT Resiliency Management Model doesn't replace your organization's best practices – it provides a process structure into which these practices can be inserted and managed. Using the resiliency management process definition as a guide, your organization can select the right practices to achieve the intended result and to ensure optimized resource deployment. In turn, your organization can measure the achievement of process goals to validate that the implemented practices are providing results.

http://www.cert.org/resiliency/

Chapter 6 Appendix – A Framework for Analyzing Financial Risk Transfer and Insurance

Capacity, Deductibles, Coinsurance, and Agent Access

Carrier	*Capacity Available*	*Deductible or Self-Insured Retention (SIR) (Minimum and Maximum)*	*Is Product Available to Retail Broker or to Wholesale Only?*
ACE Digital DNA	$15 million	Minimum deductible: $5,000	Available to all brokers licensed with ACE
ACE Privacy Protection	$25 million	Minimum retention: $5,000 Data breach fund retention: $0	Available to all brokers licensed with ACE
AIU	$25 million	Minimum retention: $5,000	Available to all licensed brokers appointed with AIU
AXIS-AXIS PRO	U.S. and Canada: $250,000 to $15 million Certain other foreign countries: UK £10 million CyberLiability Plus Programme Certain other foreign countries: UK £10 million TechPlus Liability Programme	U.S. and Canada: $2,000 – no maximum UK and certain other foreign countries: £2,500 minimum	Appointed retail brokers and wholesalers
Beazley	$20 million	Minimum normally $25,000 for third party and $100,000 for first party	Available to all brokers licensed with Beazley
Chubb	$25 million	Minimum deductible: $15,000	Available to all Chubb appointed retail brokers and wholesalers
CNA NetProtect	$10 million on all coverage; higher limits on a highly selective basis	Varies by risk	Standard CNA commissions
CNA NetProtect Essential	$2 million; up to $5 million on a highly selective basis	Minimum $1,000	Standard CNA commissions

Carrier	*Capacity Available*	*Deductible or Self-Insured Retention (SIR) (Minimum and Maximum)*	*Is Product Available to Retail Brokers or to Wholesale Only?*
Digital Risk Managers	$10 million (primary or excess)	Deductibles: First party: $25,000 minimum Third party: $25,000 minimum Maximum deductibles: N/A	Can be retail or wholesale. Only work with selected group of wholesalers. Product generally sold on a retail basis
Euclid Managers	$10 million (primary or excess)	Minimum deductible: $2,500	Retail or wholesale: product available on surplus-lines basis in most states
Evanston	$5 million	$2,500	Wholesalers only
Hiscox	Up to $10 million for small/ medium businesses. Up to $20 million for large companies for both first- and third-party covers	$2,500	Both
SafeBusiness	First party: $20,000 to $75,000* Third party: $250,000 to $1 million *Higher limits available upon request	Minimum deductibles: First party: $100 Third party: $1,000	Available to retailers and wholesalers where Safeonline has a signed business agreement
SafeCommerce	Up to $5 million online; higher coverage limits available upon request	Minimum deductible: $5,000	Available to retailers and wholesalers where Safeonline has a signed business agreement
Travelers Global Technology	CyberTech+: $25 million	Minimum deductible: $5,000	Retail or wholesale
Travelers Financial Institutions	Cyber+ for Financial Institutions Insurance: $5 million	Minimum deductible: $10,000	Retail or wholesale
Travelers Public Entity	Public Entity Cyber+ Liability Protection: $5 million	Minimum deductible: $1,000	Retail or wholesale
Zurich Financial Services	$10 million (primary or excess)	Minimum deductible: $2,500	Available to all licensed brokers appointed with Zurich

Project Leadership

The **Internet Security Alliance** (ISA) is a non-profit collaboration between the Electronic Industries Alliance (EIA) and Carnegie Mellon's CyLab and works closely with the CERT Coordination Center (CERT/CC), a leading, recognized center of Internet security expertise. The non-profit helps law firms and companies in the aerospace, defense, entertainment, financial, food service, manufacturing, and telecommunications sectors by standardizing best practices in Internet security and network survivability and by working with legislators and regulators to ensure that market incentives are at the forefront of public policy.

www.isalliance.org

The **American National Standards Institute** (ANSI) is a private non-profit organization whose mission is to enhance U.S. global competitiveness and the American quality of life by promoting, facilitating, and safeguarding the integrity of the voluntary standards and conformity assessment system. Its membership is comprised of businesses, professional societies and trade associations, standards developers, government agencies, and consumer and labor organizations. The Institute represents the diverse interests of more than 125,000 companies and organizations and 3.5 million professionals worldwide.

The Institute is the official U.S. representative to the International Organization for Standardization (ISO) and, via the U.S. National Committee, the International Electrotechnical Commission (IEC), and is a U.S. representative to the International Accreditation Forum (IAF).

www.ansi.org

Premium Sponsor

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

www.symantec.com

Partner Sponsors

- Direct Computer Resources, Inc.
- Phillips Nizer

Internet Security Alliance
2500 Wilson Boulevard, Arlington, VA 22201
T: 703.907.7799 | E: info@isalliance.org
www.isalliance.org

"Every company has embraced and realized the benefits of digitization, but have they calculated the risks along the way? Increasingly, security is becoming a top-of-mind topic among corporate leadership and ISA and ANSI have produced a document that cannot be ignored.

"This excellent guide for the C-suite puts forth the right questions to help organizations be proactive in managing their risk and exposure that is derived from their digital dependence. The guide goes on to offer mechanisms that organizations can use to develop the necessary policies, programs, and communications strategies required to ensure business continuity in a time of crisis."

– Melissa Hathaway, President, Hathaway Global Strategies, LLC; Senior Advisor, Harvard Kennedy School's Belfer Center; former Senior Advisor to the Director of National Intelligence and Cyber Coordination Executive; and former Acting Senior Director for Cyberspace, National Security Council

"Bridging the gap between the 50 questions offered in the 2008 publication *The Financial Impact of Cyber Risk* and C-level executives' need for answers, this document provides actionable recommendations for addressing well-articulated cybersecurity risks. Rather than focusing on technological tactics, this document outlines procedures for developing strategies that cross functional and departmental boundaries."

– Donald Deutsch, VP Standards Strategy and Architecture, Oracle

"As a CIO, I am constantly searching for tools that enrich the executive team's understanding of cybersecurity as an enterprise-wide responsibility to be addressed collaboratively on the basis of risk. This document is a rare example that succeeds in that and in also providing an actionable road map for developing a comprehensive cybersecurity program."

– Alan C. Levine, CIO,
John F. Kennedy Center for the Performing Arts

"This document clearly identifies a framework for any private or public entity that recognizes the current cybersecurity risks. Although it is presented as a 'framework,' it represents a significant body of knowledge that if followed will align any enterprise to today's risk profile."

– Richard F. Mangogna, President and CEO,
Mason Harriman Group (formerly DHS/CIO)

American National Standards Institute
25 West 43rd Street, New York, NY 10036
T: 212.642.4900 | E: info@ansi.org
www.ansi.org

"This document is brilliant, well written, and can be a very useful guide for non-profit entities, especially healthcare facilities with limited resources, to use in building a foundation to protect themselves from the dangers and consequences of cyber risk. This is a must-read for the executive team, board of directors, and stakeholders."

– Roberto J. Lagdameo, Director of Finance, Collington Episcopal Life Care Community, Inc.

"This booklet is a must-read for all C-level executives and board members. Not only does it enumerate clearly and concisely (in language that business people can easily understand) the scope of the cybersecurity issues challenging all enterprises today, it also offers a pragmatic framework within which these issues can be addressed, thereby allowing organizations both to minimize and mitigate their cyber risks."

– Dr. John Fox, President and CEO,
FFC Computer Services, Inc.

"Being meaningfully 'proactive' in the war against cyber threats is a direct function of how well you truly understand your total enterprise risk. This study guides you through the often uncomfortable horizontal – across the silos – questions every organization must ask to achieve that critical understanding."

– Christopher J. Steinbach, President and CEO,
The Newberry Group, Inc.

"The issue of cybersecurity has been a topic of serious discussion both within the Federal government and the private sector since the formation of the 1996 President's Commission on Infrastructure Protection. For years, a business case and action plan for meaningful cybersecurity were difficult if not impossible to define and execute with any semblance of consensus. In my opinion, this paper is a significant step in summarizing a way forward to both."

– Ron Dick, Former Director,
National Infrastructure Protection Center (NIPC)

"A must-read for all C-level executives! As a former CFO of a $800 million public company I thought cyber risk was an information technology issue. Don't make that same mistake."

– Bob Gregg, CEO,
ID Experts Corp