INTERNET
SECURITY
ALLIANCE

Sophisticated Management of Cyber Risk

Sponsored by:

AIG

Acknowledgements

The following professionals comprise the Internet Security Alliance's (ISA's) Board of Directors, without which, the work of ISA would not be possible. We would also like to acknowledge AIG, which is a member of ISA and which sponsored the workshops and publication of this case study white paper.

Internet Security Alliance Board of Directors

Fidelity Investments	**Timothy McKnight,** ISA Board Chairman; EVP Information Security and Risk
Raytheon Company	**Jeffrey Brown,** ISA Board First Vice Chairman; VP of Infrastructure Services and CISO
USAA	**Gary McAlum,** ISA Board Second Vice Chairman; SVP and CSO
Verizon	**Marcus Sachs,** VP of National Security Policy
BNY Mellon	**Thomas Quinn,** Managing Director and CISO
Lockheed Martin Corporation	(Lt. Gen., Ret. USAF) **Charlie Croom,** VP of Cyber Security Solutions
Northrop Grumman	**Russell Koste,** Director of Identity, Intelligence and Network Defense
Wells Fargo	**Rich Baich,** CISO
General Electric	**Larry Trittschuh,** Director of Global Information Security Operations
Carnegie Mellon University (CMU)	**Tim McNulty,** CyLab Associate VP for Government Relations
Dell SecureWorks	**Jeffrey Schilling,** Director for the Incident Response Practice
Tyco International	**Gene Fredriksen,** Senior Director and Global Information Security Officer
The Boeing Company	**Thomas Kelly,** Director of Information Security – Assessments and Vulnerabilities
SAIC	**Julie Taylor,** SVP Operations, Cyber Security Services and Solutions
Direct Computer Resources	**Joe Buonomo,** President & CEO
AVG Technologies	**Siobhan MacDermott,** Chief Policy Officer
National Association of Manufacturers (NAM)	**Brian Raymond,** Director of Tax, Technology and Domestic Economic Policy
Vodafone Group	**Richard Knowlton,** Group Corporate Security Director
Internet Security Alliance (ISA)	**Larry Clinton,** President & CEO

About the Internet Security Alliance:

The Internet Security Alliance (ISA) is a multi-sector trade association with membership from virtually every one of the designated critical industry sectors, including substantial participation from the aviation, banking, communications, defense, education, financial services, health care, insurance, manufacturing, security and technology industries.

ISA focuses exclusively on cybersecurity and cybersecurity related issues as is embodied in its mission, which is to create a sustainable system of cybersecurity by combining advanced technology with economics and public policy.

About Our Publication and Workshops Sponsor:

American International Group, Inc. (AIG) is a leading international insurance organization serving customers in more than 130 countries. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States.

Notice:

Material in this publication is for educational purposes. Neither the publisher nor the authors assume any liability for any errors or omissions or for how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. For legal advice or any other, please consult your personal lawyer or the appropriate professional.

The views expressed by the individuals in this publication do not necessarily reflect the views shared by the companies they are employed by (or the companies mentioned in this publication). The employment status and affiliations of authors with the companies referenced are subject to change.

THE EMERGENCE OF THE SOPHISTICATED THREAT

For many years, cyber attacks were thought to be the exclusive province of teenage hackers and academic nerds. Incursions had cutesy names like "Love Bug" and "BLASTER," and, while annoying, they tended to do little actual damage; most enterprises shrugged them off as either a petty cost of doing business, similar to low-level pilferage, or an obtuse issue best relegated to the geeks in information technology (IT) and not worthy of senior level attentions.

Those days are over.

In his February 12, 2013 State of the Union Address, President Obama declared that: America's "enemies are seeking the ability to sabotage our power grid, our financial institutions and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[1] The President's signature white paper on the issue, the "Cyberspace Policy Review," suggests the costs to American business could run close to one trillion dollars.[2]

In October, Defense Secretary Leon Panetta warned of increasingly sophisticated attacks being launched on private cyber systems and the need for greater awareness and attention to securing these systems.[3]

In February, *The New York Times* and *The Washington Post* reported the results of security firm Mandiant's findings that not only had these iconic institutions been compromised, but that the degree of sophistication of attacks had grown substantially.[4],[5],[6],[7] Indeed, Mandiant reported that the sophisticated attacks that had previously been confined to governments and major defense contractors have now spread broadly throughout the economy.[8]

[1] Obama, Barack H. "2013 State of the Union Address." Address. Capitol Building, Washington, D.C. 12 Feb. 2013. W*hitehouse.gov*. White House, 12 Feb. 2013. Web. 18 Mar. 2013. <www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address>.

[2] United States. Executive Office of the President. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." *Whitehouse.gov*. White House, 2009. Web. 1 May 2013. <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

[3] Panetta, Leon E. "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security." Address. 2012 BENS Eisenhower Award Dinner. New York City. *Defense.gov*. U.S. Department of Defense, 11 Oct. 2012. Web. 1 May 2013. <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.

[4] Perlroth, Nicole. "Hackers in China Attacked the Times for Last 4 Months." *NYTimes.com*. New York Times, 30 Jan. 2013. Web. 30 Apr. 2013. <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html>.

[5] Sanger, David E., David Barboza, and Nicole Perlroth. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *NYTimes.com*. New York Times, 18 Feb. 2013. Web. 30 Apr. 2013. <http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>.

[6] Wan, William, and Ellen Nakashima. "Report Ties Cyberattacks on U.S. Computers to Chinese Military." *WashingtonPost.com*. Washington Post, 19 Feb. 2013. Web. 1 May 2013. <http://www.washingtonpost.com/world/report-ties-100-plus-cyber-attacks-on-us-computers-to-chinese-military/2013/02/19/2700228e-7a6a-11e2-9a75-dab0201670da_story.html>.

[7] Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." Rep. *Mandiant.com* Mandiant, 18 Feb. 2013. Web. 1 May 2013. <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>.

[8] Ibid.

Unfortunately, the research shows that most enterprises are still attempting to fight these modern attacks with perimeter-based defenses like anti-virus and intrusion detection, which are no longer adequate to meet the modern cyber threats.[9]

Fortunately, while attack methods have continued to evolve, so too have defensive strategies.

THE RISE OF SOPHISTICATED DEFENSE

A series of studies has indicated that, while perfect security is not feasible, we are learning a good deal about how enterprises can better manage their cyber risk.[10],[11],[12] Although analysis of successful attacks has generated good data on how to combat them, this data has not been broadly integrated into business practice.[13] This research suggests that by combining modern organizational techniques with research-based technical procedures, organizations can mitigate damage from all but the most sophisticated of cyber threats (e.g., those launched by nation-states) and even these attacks can be better managed.

The major barriers to widespread adoption of these techniques are lack of awareness at senior corporate levels, and, as always, cost.[14],[15],[16],[17],[18]

In early 2012, AIG elected to sponsor an effort by the ISA and the Union of Concerned Cybersecurity Leaders (UCCL) to investigate how sophisticated and experienced firms are addressing their cyber threats. Operating in conjunction with a series of partner organizations including, the Financial Services ISAC, the Aerospace Industries Association (AIA) and the National Association of Manufacturers (NAM), a series of workshops were held in Washington, Silicon Valley and New York City. The goal of this effort was to analyze the risk management methods sophisticated firms in the defense industrial base, IT and financial services were and are using. In

[9] Ibid.

[10] Internet Security Alliance and American National Standards Institute. “The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask.” Rep. *ISAlliance.org*. Internet Security Alliance, 2008. Web. 30 Apr. 2013. <http://www.isalliance.org/isa-publications/>.

[11] Internet Security Alliance and American National Standards Institute. “The Financial Management of Cyber Risk: An Implementation Framework for CFOs.” Rep. *ISAlliance.org*. Internet Security Alliance, 2008. Web. 30 Apr. 2013. <http://www.isalliance.org/isa-publications/>.

[12] Verizon RISK Team, et al. “2012 Data Breach Investigations Report.” Rep. *Verizonenterprise.com*. Verizon, March 2012. Web. 30 Apr. 2013. <http://www.verizonbusiness.com/about/events/2012dbir/>.

[13] PricewaterhouseCoopers (PwC). “The Global State of Information Security Survey: 2011.” Survey. *PwC.com*. PricewaterhouseCoopers, 2010. Web. 1 May 2013. <http://www.pwc.com/en_GX/gx/psrc/pdf/findings_from_the_2011_global_state_of_info_security.pdf >.

[14] Westby, Jody. “Governance of Enterprise Security: CyLab 2012 Report – How Boards & Senior Executives are Managing Cyber Risks.” Rep. *Cylab.com*. Carnegie Mellon CyLab, 16 May 2012. Web. 30 Apr. 2013. <http://www.cylab.cmu.edu/outreach/governance.html>.

[15] PricewaterhouseCoopers. *The Global State of Information Security: 2008*. Rep. PricewaterhouseCoopers, 2007. Print.

[16] Brenner, Bill. "Business Partners with Shoddy Security; Cloud Providers with Dubious Risk Controls; What’s a CIO to Do?" *CIO Magazine*, 14 Oct. 2010.

[17] Baker, Stewart, Shaun Waterman, and George Ivanov. “In the Crossfire: Critical Infrastructure in the Age of Cyber War.” Rep. *McAfee.com*. McAfee, 2010. Web. 30 Apr. 2013. <http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf>.

[18] Domenici, Helen, and Afzal Bari. *The Price of Cybersecurity: Improvements Drive Steep Cost Curve*. Rep. Ponemon Institute-Bloomberg Government Study, 31 Jan. 2012. Print.

each case, highly sophisticated entities were asked to describe their cyber risk management processes and then engage with an invitation-only set of industry players to discuss the pros and cons of these approaches. Based on this work, a cost-friendly system of managing cyber risk could be developed and an easily accessible educational tool could be created to diffuse this information broadly in the business community.

More than 75 firms participated in the workshops and assisted in developing insights into how a useful risk management paradigm could be developed based on the real world experiences of these sophisticated companies that are living in the cyber attack world on a daily basis.

This report presents the preliminary findings of that effort. This report does not purport to be a large randomized sample of how enterprises are generally dealing with cyber threats. Rather, it describes how very sophisticated companies are adopting and adapting the research-based methods to their own day-to-day operations. Results drawn from these workshops suggest sophisticated companies are adopting at least three broad strategies to address cyber risk management:

1. Sophisticated entities are broadening their concept of cyber defense and treating it on an enterprise-wide, as opposed to IT-centric, basis including evaluating the financial risk and whether to retain or transfer some of the risk through cyber insurance;

2. Sophisticated entities are attempting to retain focus on the basics of good cyber hygiene and not simply following the mitigation strategy of the day; and

3. Sophisticated companies are adapting a series of research-based "mid-level" strategies to enhance their defenses on a systemic basis above and beyond doing the basics.

Organizing for Cyber Risk Management

As recently as 5 years ago, Carnegie Mellon University's (CMU) "Governance of Enterprise Security" report documented the "gap between IT and enterprise risk management," namely, that "senior executives are not involved in key areas related to governance of enterprise security." This CMU report further documented that only 17% of corporations had a cross-organizational privacy security team, less than half (47%) of organizations had a formal enterprise risk management plan, and one third of the 47% that had a plan did not include IT related risk in that plan.[19]

That same year, ISA initiated its program, chaired by AIG, to alter the perception of cyber security in the enterprise space from an "IT issue" to understanding cyber security as an enterprise-wide, risk management issue. That program produced two papers designed to alter the model of enterprise cyber risk management. The first, "The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask," is self-explanatory.[20] The second, "The Financial Management of Cyber

[19] Westby, Jody. "Governance of Enterprise Security: CyLab 2012 Report – How Boards & Senior Executives are Managing Cyber Risks." Rep. *Cylab.com*. Carnegie Mellon CyLab, 16 May 2012. Web. 30 Apr. 2013. <http://www.cylab.cmu.edu/outreach/governance.html>.

[20] Internet Security Alliance and American National Standards Institute. "The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask." Rep. *ISAlliance.org*. Internet Security Alliance, 2008. Web. 30 Apr. 2013. <http://www.isalliance.org/isa-publications/>.

Risk: An Implementation Framework for CFOs," described a six-step process that enterprises could adopt to implement more of an enterprise-wide risk model.[21]

By 2012, the trend toward viewing cyber in a broader enterprise risk context was clear. The 2012 CMU follow-up study found that whereas only 17% of firms had enterprise wide risk teams in 2008, by 2012, that number had grown to 72%.[22] The PricewaterhouseCoopers (PwC) "Global State of Information Security Survey" further validated this trend by documenting a 39% reduction in Chief Information Security Officers (CISO) reporting to the Chief Information Office (CIO) and a 15% increase in CISOs reporting to the Chief Financial Officer (CFO), a 36% increase reporting to the Chief Executive Officer (CEO), and a 15% increase in reporting to the Chief Operating Officer (COO). PwC concludes by commenting that across industries, "we see executive recognition that security's strategic value is being more closely aligned with business goals than IT."[23]

Workshop Example: One financial services participant stated that understanding the functional divisions and interdependencies within an organization are essential in order for a CISO to have success in developing an enterprise-wide security plan. In order to translate such a plan, the CISO also has to remove techno-babble and place the plan in a "so-what"/"if…then" context using real-life situations and scenarios such as what could happen in terms of cost if there is no plan and the systems and networks are down for realistic intervals (1 hr, 5 hours, 10 hours, etc.). This participant also stressed that relationship building amongst functional heads is imperative to success, that a CISO should become best friends with his/her Chief Risk Officer, Chief Compliance Officer, and Audit Executive.

This same participant stated that real life crises and incidents present great teaching opportunities, which a CISO can show a Board how such an event impacts the organization. For example, during Board meetings, a CISO should provide a demonstration on how easy it is to conduct credit card fraud through card forging, etc.

[21] Internet Security Alliance and American National Standards Institute. "The Financial Management of Cyber Risk: An Implementation Framework for CFOs." Rep. *ISAlliance.org*. ISA, 2008. Web. 30 Apr. 2013. <http://www.isalliance.org/isa-publications/>.

[22] Westby, Jody. "Governance of Enterprise Security: CyLab 2012 Report – How Boards & Senior Executives are Managing Cyber Risks." Rep. *Cylab.com*. Carnegie Mellon CyLab, 16 May 2012. Web. 30 Apr. 2013. <http://www.cylab.cmu.edu/outreach/governance.html>.

[23] PricewaterhouseCoopers. "Lost in Translation? Exploring the roots of miscommunication: strategies to ensure Information Security is on your Board's agenda." Rep. *PwC.com*. PricewaterhouseCoopers, 1 March 2011. Web. 1 May 2013. <http://download.pwc.com/ie/pubs/lost_in_translation.pdf>.

Citing:

PricewaterhouseCoopers. "The Global State of Information Security Survey: 2011." Survey. *PwC.com*. PricewaterhouseCoopers, 2010. Web. 1 May 2013. <http://www.pwc.com/en_GX/gx/psrc/pdf/findings_from_the_2011_global_state_of_info_security.pdf>.

Notwithstanding these positive trends, it is noteworthy that the more modern understanding of cyber security as an enterprise-wide imperative is far from universal even today. Despite an impressive increase in the percentage of companies adopting an enterprise-wide approach to cyber risk, CMU's data still shows that nearly 30% of companies still do not even have an interdepartmental team to address security and privacy.[24]

However, the one place where a gap did not exist was within the sophisticated companies participating in the AIG-sponsored workshops. Literally every one of the presenting companies for whom data could be collected reported dealing with cyber risk in a fashion consistent with the six step organization-wide model outlined in the "Financial Management of Cyber Risk" including:

* **Designating a cross-departmental Executive vested with strategic control of cyber systems.**

Workshop Example: One of the surveyed companies' CFO is very much involved in the company's risk management. Reporting to the Board and CEO, this company's CFO not only helps define the program's design requirements, but actively participates in cost-benefit analyses of program identified risks and risk management options. He/she also receives updates as to the cost impact of program implementation and provides an annual cost-benefit analysis of the program.

* **Establishing a cross-enterprise "Cyber Risk Team" to identify cyber risk.**

Workshop Example: In one company, the IT security team that is charged with identifying cyber risk consists of 10 people hailing from the company's different business lines and reports in to the company's CISO. This team's business line diversity helps ensure that different thoughts and priorities are represented when conducting the cyber risk identification, analysis, and contextualization that they are tasked with.

* **Having the "Cyber Risk Team" meet regularly.**

[24] Westby, Jody. "Governance of Enterprise Security: CyLab 2012 Report – How Boards & Senior Executives are Managing Cyber Risks." Report. *Cylab.com*. Carnegie Mellon CyLab, 16 May 2012. Web. 30 Apr. 2013. <http://www.cylab.cmu.edu/outreach/governance.html>.

*** Developing and adopting a cyber risk management plan.**

> ***Workshop Example:*** For one company, once it "heatmaps" its risk, its cross-departmental risk and compliance committee is able to recognize the top five risks that require further attention. These top five risks are then briefed before the company's top leadership, namely a higher level Integrated Risk Council, the CEO, the Board and appropriate Executive Committees. With respect to these prioritized five risks, the risk and compliance committee "treats" or develops a mitigation initiative (or initiatives) for each identified risk. In relaying these initiatives to leadership and other stakeholders, the risk and compliance committee describes them in non-technical terms and answers three key questions:
>
> (1) What is driving (the reason for) the initiative?
>
> (2) What is the initiative's objective(s)?; and
>
> (3) What is the expected outcome from the initiative?
>
> From this, an initiative "playbook" is created that, while not overly prescriptive, helps assure that the right people and decision-makers are appropriately involved at the right times.

*** Developing and adopting an enterprise-wide cyber risk budget.**

> ***Workshop Example:*** One company sends out and solicits cross-enterprise risk questionnaires to help its risk management team identify risks for the risk register and to quantify a particular risk's business impact and likelihood of occurring. These responses from across the enterprise help this team estimate how much time, effort and resources would be necessary to reduce the risk to a more tolerable level. Actuarial models, such as loss and availability models, help the company refine its risk quantification.

*** Regularly reviewing the plan, testing it and updating it.**

> ***Workshop Example:*** One of the companies surveyed utilizes what it terms the "shampoo model" of "lather, rinse, repeat" to manage its risk. Specifically, this company uses a 7-step, iterative risk management process. These 7 steps are:
>
> (1) Identify Top Risk Categories;
>
> (2) Identify Detailed Risks;
>
> (3) Populate Risk Register;
>
> (4) Validate with Risk Governance;
>
> (5) Approve Plans;
>
> (6) Track Progress; and
>
> (7) Refresh Risk "Heatmap."

MAINTAINING FOCUS ON GOOD CYBER HYGIENE

It has long been conventional wisdom in the cyber security field that 80% of cyber incursions could be prevented or substantially mitigated if enterprises would simply use good cyber hygiene.

Since 2008, Verizon and the U.S. Secret Service have been conducting forensic analysis of hundreds of cyber security breaches, examining tens of thousands of individual data points to see if this common wisdom would hold up.

In virtually every study, the common wisdom was proven wrong. The percentages of cyber events that could be stopped by simply employing well-known and comparatively inexpensive cyber security best practices is far higher than conventional wisdom suggested. The most recent Verizon-Secret Service study documents that as much as 97% of cyber events could have been prevented, or their damage mitigated, through the use of best practices.[25]

The best practices are not sexy new technologies, but fairly common sense ideas that need to become part of an enterprise's culture. The common practices are listed below:

- **Eliminate unnecessary data and keep tabs on what is left;**
- **Ensure essential controls are met and regularly audit in order to assure consistent implementation;**
- **Change default credentials;**
- **Avoid shared credentials;**
- **Implement a firewall or access control list (ACL) on remote access/administration services;**
- **Utilize IP blacklisting;**
- **Update anti-virus and other software consistently;**
- **Audit user accounts;**
- **Restrict and monitor privileged users;**
- **Monitor and filter outbound network traffic;**
- **Test applications and review codes;**
- **Monitor and mine event logs;**
- **Change the approach to event monitoring and log analysis;**
- **Define 'suspicious' and 'anomalous' (then look for whatever 'it' is);**
- **Increase awareness of social engineering;**
- **Train employees and customers to look for signs of tampering and fraud;**
- **Create an incident response plan;**
- **Engage in mock incident testing; and**
- **Secure business partner connections.**

[25] Verizon RISK Team, et al. "2012 Data Breach Investigations Report." Report. *Verizonenterprise.com*. Verizon, March 2012. Web. 30 Apr. 2013. <http://www.verizonbusiness.com/about/events/2012dbir/>.

While the growing number of cyber incidents pays ample testimony to the fact that many enterprises are still not following these common techniques, once again this gap was not apparent among the sophisticated companies participating in the ISA-AIG sponsored workshops.

As was the case with the organizational techniques described earlier, virtually 100% of the presenting companies at the ISA workshops described procedures consistent with the Verizon-Secret Service model.

Explanations and Examples

Eliminate unnecessary data and keep tabs on what is left: Research has demonstrated that a large number of security breaches have occurred by accessing information for which the target company had no legitimate business use. Organizations should establish reasonable data retention policies and hold only data for which there is a reasonable business need. Operating with clean data files can reduce risk and increase efficiency.

Ensure essential controls are met and regularly audit in order to assure consistent implementation: Organizations should identify a set of essential controls and ensure their implementation across the organization without exception. This process needs to be regularly evaluated by the risk management team so that more advanced controls will be implemented where needed to address more sophisticated attacks.

> ***Workshop Example:*** One company's Board of Directors reviews its corporate risk management program to ensure that, as implemented, risk and business objectives are adequately addressed. Throughout the year, the Board also reviews the program's oversight by other top corporate leaders and receives program updates and risk notifications. The Board's audit committee provides the risk management program with its annual audit requirements and apprises the rest of the Board of the audit results.

Change default credentials: When system/network administrators "stand-up" a new system, then there is a need to change the passwords. If organizations outsource this to a third party, the contractor must assure it fills this role. This process needs to be part of regular maintenance. "Don't assume staff or partners consistently will follow through on policies and procedures."[26]

Avoid shared credentials: "Along with changing default credentials, organizations should ensure that passwords are unique and not shared among users or used on different systems. The use of shared credentials [has] allowed quite a few breaches…. This was especially problematic for assets managed by a third party."[27]

[26] Verizon RISK Team, et al. "2011 Data Breach Investigations Report." Report. *Verizonenterprise.com*. Verizon, March 2011. Web. 30 Apr. 2013. <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf>.

[27] Verizon Enterprise Solutions RISK Team. "2009 Data Breach Investigations Report." Report. *Verizonenterprise.com*. Verizon, 2009. Web. 30 Apr. 2013. <http://www.verizonenterprise.com/resources/security/reports/2009_databreach_rp.pdf>.

Implement a firewall or access control list (ACL) on remote access/administration services: "In many instances, remote access services have been enabled and are Internet-facing." In addition, some organizations "will allow any device on the network to connect and remotely access any other device"; these practices, while convenient, increase risk. These services should be tied down so only specific IP addresses or networks can access them. It is especially important to limit access to sensitive systems within the network. "Tie down remote access services to specific management networks via access control lists."[28]

Utilize IP blacklisting: "[C]onsider blocking large address blocks/regions if they have no legitimate business purpose."[29]

Workshop Example 1: Rather than restrict employees web surfing on a blanket basis, one company initiated and deployed a website screening program. When an end user clicks on a known or suspected malicious site, it is blocked. If, however, the website is not categorized, the end user receives a pop up window asking him/her whether he/she wants to proceed and to acknowledge the risk that he/she is taking. After a specific time interval, this pop-up window reappears if the user remains on the site.

Workshop Example 2: During an exchange between one of the workshop participants and a Federal Bureau of Investigation (FBI) representative, it was suggested that as the FBI investigates new malware, it should share just the hash binary code (also known as the "hash value" or "malware hash") and not the hash signature, so that organizations could check to see if they were currently infected. This was suggested because according to the participant, it would seem to satisfy the FBI's need to keep certain information classified to conduct a proper investigation, while providing companies with enough information to isolate an identified threat.

Update anti-virus and other software consistently: Verizon found that for every vulnerability which was exploited by hacking and malware attacks in 2008, "the patch necessary to prevent the breach had been available for at least six months prior to the incident. In fact, all but one had been around for a year or more." Moreover, the problem is not that organizations aren't patching fast enough. "All of these organizations had patch cycles well below the six month mark." The problem throughout all five years of the Verizon studies has far more to do with scope than speed. "Organizations would find much more value if they divert resources from patching faster to patching more consistently and comprehensively."[30]

[28] Verizon RISK Team, et al. "2011 Data Breach Investigations Report." Report. *Verizonenterprise.com*. Verizon, March 2011. Web. 30 Apr. 2013. <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf>.

[29] Verizon RISK Team, et al. "2012 Data Breach Investigations Report." Rep. *Verizonenterprise.com*. Verizon, March 2012. Web. 30 Apr. 2013. <http://www.verizonbusiness.com/about/events/2012dbir/>.

[30] Verizon Enterprise Solutions RISK Team. "2009 Data Breach Investigations Report." Report. *Verizonenterprise.com*. Verizon, 2009. Web. 30 Apr. 2013. <http://www.verizonenterprise.com/resources/security/reports/2009_databreach_rp.pdf>.

Audit user accounts: Data consistently demonstrates the value of reviewing user accounts on a regular basis. “The review should consist of a formal process to confirm that active accounts are valid, necessary, properly configured, and given appropriate (preferably least) privileges.”[31]

Restrict and monitor privileged users: Organizations should not give users more privileges than they need. Moreover, it is important to ensure that users are properly supervised, that they understand the policies and expectations and adhere to them. “Privileged use should be logged and generate messages to management. Unplanned privileged use should generate alarms and be investigated.”[32]

Monitor and filter outbound network traffic: As the once uniquely sophisticated attacks become more common place, the ability to keep intruders outside of the perimeter is reduced. However, most breaches are not successful when the system is breached, but rather when data is captured and exits the system. “By monitoring, understanding, and controlling outbound traffic, an organization will greatly increase its chances of mitigating malicious activity.”[33]

Workshop Example: One of the companies developed a program to prevent data exfiltration that could result from cyber attacks. This program utilizes an outbound traffic-blocking strategy/mechanism that, in effect, “traps the thief in the vault” by blocking the outbound traffic to unauthorized, known malicious, or suspected command and control channels, IP addresses, URLs, etc.

Application testing and code review: Attackers are moving up the stack and targeting the application layer. Nearly half of the breaches Verizon found attributed to hacking or network intrusion involved SQL injection attacks, cross-site scripting, authentication bypass and exploitation. As these attacks multiply, so too must a company’s defenses respond. Web application scanning and testing would have found most of the problems that led to major breaches in the past year. In addition, regular reviews of architecture, privileges and source code are recommended. “Incorporating a Security Development Life-Cycle (SDLC) approach for application development is recommended as well.”[34]

Workshop Example: As part of its cyber security campaign, a company mapped its server assets, identified high-risk applications and undertook over 400 application reviews. In the next phase, this company plans on developing its vulnerability management processes into more established governance processes and reduce the over 200,000 identified vulnerabilities.

[31] Verizon RISK Team, et al. “2011 Data Breach Investigations Report.” Report. *Verizonenterprise.com*. Verizon, March 2011. Web. 30 Apr. 2013. <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf>.

[32] Ibid.

[33] Ibid.

[34] Ibid.

Monitor and mine event logs: It makes little sense to spend the time and effort to create event logs and then not use the data. Yet that is a fairly common situation. "All too often, evidence of events leading to breaches was available to the victim but this information was neither noticed nor acted upon. Processes that provide sensible, efficient, and effective monitoring and response are critical to protecting data." Whereas logging efforts on network, operating system, IDS and firewall logs may have been sufficient in earlier days this process now needs to be expanded to include remote access services, web applications, databases and other critical applications. These logs can help to formulate "a rich data set for detecting, preventing, and investigating breaches."[35]

Change the approach to event monitoring and log analysis: Research suggests that organizations would be better served to focus less on the "real-time" methods of detection, and more on the "this-week" methods. Shifting the compromise to discovery time frame from weeks and months to days could significantly reduce the damage from a breach. Ironically, this switch "need not be expensive; a simple script to count log lines/length and send an alert if out of tolerance can be quite effective. We are confident that this approach will reap benefits and save time, effort, and money."[36]

Workshop Example: During its "Organize for Success" security phase (security phase 1), one company set out first to understand its threat landscape; for its second security phase, the company's goals were more proactive, including real-time threat intelligence gathering and briefing; the development of "intel" driven programs; and the development of a team of "network hunters" tasked with finding network holes and vulnerabilities.

"Define 'suspicious' and 'anomalous' (then look for whatever 'it' is):" "This is admittedly vague, but—in truth— generalizing what this entails in order to prescribe something for everyone would counteract the point. Discover what is critical, identify what constitutes normal behavior, and then set focused mechanisms in place to look for and alert upon deviations from normality."[37]

Workshop Example: As part of its cyber risk management, one company utilizes the following 6-step, "end-to-end" process:

(1) Define risk;
(2) Identify potential risks;
(3) Contextualize these risks;
(4) Analyze these risks;
(5) Prioritize these risks; and
(6) Gap closure (also known as threat/risk mitigation).

[35] Ibid.

[36] Ibid.

[37] Ibid.

Increase awareness of social engineering: Educate employees about different methods of social engineering and the vectors from which these attacks could arise. In many cases, we see users “clicking links they shouldn’t and open[ing] attachments received from unidentified persons. Reward users for reporting suspicious e-mail and sites and create the incentives necessary for vigilance.”[38]

Workshop Example: After receiving leadership buy-in, one of the companies surveyed sent out a series of phishing emails to establish a baseline of click-through rates on such potentially hazardous emails. Once the committee established the baseline, an awareness campaign about the identification of phishing emails and the potential hazards of clicking on these emails was implemented. One year from the baseline and following the training, the committee tested again and found a 35-50% improvement in “click-throughs.”

Train employees and customers to look for signs of tampering and fraud: “Such awareness campaigns have been around in certain areas for some time, but ATM and Pay-at-the-Pump tampering/fraud seem to be increasing in number and scope. Organizations operating such devices should consider conducting regular examinations [of these systems]. Additionally, empower customers to help protect themselves as well as aiding the organization in spotting potential issues.”[39]

Workshop Example: As part of one company’s cyber awareness campaigns, employees were taught to look for fraudulent activities, and, in some cases, campaign administrators provided incentives such as monetary rewards for those that reported pernicious/suspicious activity.

Create an Incident Response Plan: “If and when a breach is suspected to have occurred, the victim organization must be ready to respond. An effective Incident Response Plan helps reduce the scale of a breach and ensures that evidence is collected in the proper manner.”[40]

Workshop Example: One of the companies surveyed had previously developed resiliency and disaster recovery plans geared toward natural disasters. To meet the changing business environment and increased cyber threats, this company began adapting these older plans so that they now constitute its IT Systems resiliency and disaster recovery plans.

[38] Ibid.

[39] Ibid.

[40] Ibid.

Engage in mock incident testing: "[W]e are talking about practice, because practice makes perfect. In order to operate efficiently, organizations should undergo routine IR training that covers response strategies, threat identification, threat classification, process definition, proper evidence handling, and mock scenarios."[41]

Workshop Example: In response to actual spear-phishing attacks, one of the companies surveyed developed and deployed a program to screen, but not necessarily restrict, incoming emails. First, the company baselined the click-through rates on pernicious emails that seemed to be forwarded from valid senders and contained appropriate subject lines. After the company took these measurements, it created an awareness campaign regarding spear-phishing, its dangers and how to recognize and respond to such threats.

Secure business partner connections: "Basic partner-facing security measures, in addition to security assessments, contractual agreements, and improved management of shared assets are all viewed as beneficial in managing partner-related risk."[42]

Workshop Example: In evaluating its risk, it was becoming clear to one company that its smaller supply chain vendors were now becoming increasingly targeted by ever more sophisticated attacks. In response, the company devised a security/risk questionnaire that its vendors now have to complete. In addition, this company began working with its existing vendors to develop programs to help thwart and/or mitigate these attacks.

Beyond Cyber Hygiene to Cyber Health

While sophisticated entities organize themselves to address cyber threats from a business-oriented, enterprise-wide basis, with a focus on fundamentals, they also go beyond the fundamentals and integrate a set of "mid-level" strategies to further protect their systems.

In the last few years, Australia's Defense Signals Directorate (DSD) and the U.S. National Security Agency (NSA) independently surveyed the techniques hackers used to successfully penetrate networks. NSA (in partnership with private experts) and DSD each came up with a list of measures that stop almost all attacks. DSD found that four risk reduction measures block most attacks. Agencies and companies implementing these measures saw risk fall by 85 percent or more.[43]

[41] Ibid.

[42] Verizon Enterprise Solutions RISK Team. "2009 Data Breach Investigations Report." Report. *Verizonenterprise.com*. Verizon, 2009. Web. 30 Apr. 2013. <http://www.verizonenterprise.com/resources/security/reports/2009_databreach_rp.pdf>.

[43] Lewis, James A. "Raising the Bar for Cybersecurity." Publication. *CSIS.org*. Center for Strategic and International Studies, 12 Feb. 2013. Web. 1 May 2013. <http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf>.

We categorize these techniques as "mid-level" protections because even this combination may not be sufficient to protect enterprises from ultra-sophisticated nation-state, or so-called "APT" (Advanced Persistent Threat) attacks. Addressing these attacks will be the subject of another paper to be published shortly by the Internet Security Alliance.

James Lewis of the Center for Strategic and International Studies does an excellent job summarizing the mid-level defenses identified by DSD and NSA in his 2013 paper "Raising the Bar for Cyber Security"[44] and suggests a fifth measure:

1. **Use application "whitelisting":** "Use application 'whitelisting' to help prevent malicious software and other unapproved programs from running – DSD regards this as the most important step companies can take. Rather than trying to identify and block malicious software, which creates the possibility that previously unknown attacks will not be stopped, using a "whitelist" means that only approved programs can run on a machine. This step eliminates much of the risk from malware."

2. **Patch software:** "Patch applications such as PDF readers, Microsoft Office, Java, Flash Player, and web browsers. These applications are in daily use in most companies. Patching closes off avenues that hackers will otherwise exploit. Software companies send patches to rectify or eliminate exploitable flaws or weaknesses in a system's design or operation found after it was sold (similar to a recall notice for an automobile). Often, patches are developed in response to the discovery of a successful hack. A failure to install the patches leaves systems vulnerable. Most companies already have some kind of patching system in place, but research suggests that even with these systems, 5 to 10 percent of computers will 'miss' a patch. This means that mitigation works if it is paired with automatic monitoring."

3. **Patch operating systems:** "Patch operating system vulnerabilities, for the same reasons discussed above. All operating systems have potential vulnerabilities; when software companies find and offer a fix, not using that fix leaves the users susceptible to criminals and foreign intelligence agencies, who expend considerable effort to find these 'holes' and exploit them."

4. **Minimize the number of users with administrative privileges:** "Minimize the number of users with administrative privileges, the highest level of authority to make changes or undertake actions on a network. Easy access to administrative privileges lets criminals who obtain them (and this is a frequent initial goal for most hackers) install malicious software and change settings to make it easier to exfiltrate data and to hide their criminal activities."

5. **Continuous monitoring for risk:** "Continuous monitoring does not mean a round-the-clock watch of a computer screen by a human being. This approach uses the built-in ability of computers to monitor and log performance. Some continuous monitoring systems generate data by comparing network performance and configuration to specific standards and known vulnerabilities…Continuous monitoring allows companies to observe the behavior of their networks and take rapid action to stop problems and is a critical complement to mitigation…It allows companies to automatically

[44] Ibid.

collect data on the behavior of their networks and generate quantifiable data that allows them to identify risks. It lets them verify that their security measures are working…."

> ***Workshop Example:*** At one company, the CISO is not only responsible for translating cyber risk program requirements into an executable program, but also assess the effectiveness of this program through the company's continuous monitoring capabilities. For immediate or realized risks, the company's operations/intelligence provides both information and intelligence as well as incident response.

CYBER INSURANCE: A FINANCIAL "BACKSTOP" FOR BREACHES

As even the adoption of mid-level techniques may not prevent some of the more sophisticated APT attacks, companies are realizing that investing in cyber insurance can provide a financial "backstop" in the event of a breach.

Many organizations are still unaware that cyber insurance is readily available in the market and that cyber exposures are not typically covered under traditional insurance policies. Expenses resulting from a breach can add up quickly, and cyber insurance is usually designed to cover:

Security and Privacy Liability: Covers third-party liability including legal defense costs/damages and regulatory actions/fines and penalties (where insurable by law).

Event Management: Covers the first-party costs for forensic investigations, legal consultations, and public relation expenses as well as costs for notifications, identity monitoring and other services to assist in managing and mitigating a cyber incident.

Network Business Interruption: Covers the first-party loss of income due to a material interruption caused by a network security failure.

Cyber Extortion: Covers the threat of intentional security attacks against a company by an outsider attempting to extort money, securities or other valuables including monies paid to end the threat and the cost of an investigation to determine the cause of the threat.

Not only are there more carriers offering insurance protection, but also a few that are leveraging their expertise to include loss prevention services as part of the policy to help companies stay ahead of the curve. These services are an additional layer to support the organization's own security efforts, and in the event of a breach, post-loss services are often available to provide guidance on how to handle the incident.

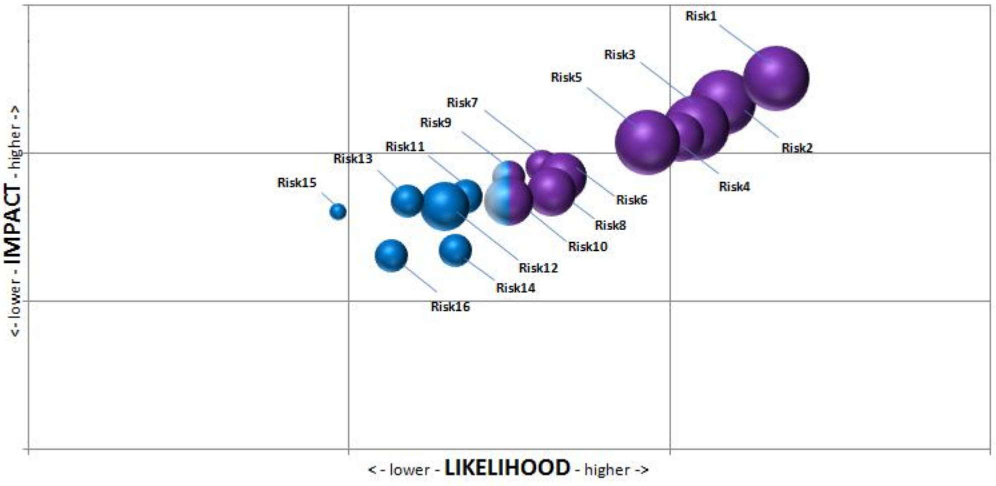
EXAMPLES OF BEST PRACTICE MODELS USED BY SOPHISTICATED ORGANIZATIONS

One Organization's Risk Categorization and Risk Prioritization Process:

While 80% of the attacks this company faces are simplistic, 20% of them are more sophisticated and include APT or APT-style attacks. Regardless, this company's risk and compliance committee evaluates both these simplistic and more advanced attacks/risks utilizing the process described below and separates them into three distinct, qualitative risk categories for risk prioritization and further management. The three categories are "High Priority Risks," "Priority Risks," and "Watch List Risks," with each category receiving different treatment:

> ***High Priority Risks:*** This company provides High Priority Risks with a detailed risk treatment plan and requires that these risk plans receive regular review and audits. Each High Priority Risk and its corresponding plan must be measured and updated quarterly.
>
> ***Priority Risks:*** This company develops risk treatment plans as well for risks categorized as Priority Risks, but the plans are less detailed than those for High Priority Risks. Moreover, Priority Risk measurements and updates occur semi-annually, rather than more frequent quarterly updates reserved for High Priority Risks.
>
> ***Watch List Risks:*** This company develops an even less detailed, or "snapshot," plan for risks categorized as Watch List Risks. While the risks themselves are reviewed annually, their snapshot plans are only reviewed and updated as needed.

Following risk categorization, heat maps are then generated. These heat maps not only depict an attack's risk category, but they also depict the estimated attack velocity and measure the attack's likelihood and potential impact along the axes. With respect to risk/attack impact estimation, this analysis also includes black swan or 100-year events analysis and the analyses of action plan costs, costs of action versus inaction and sequestration.

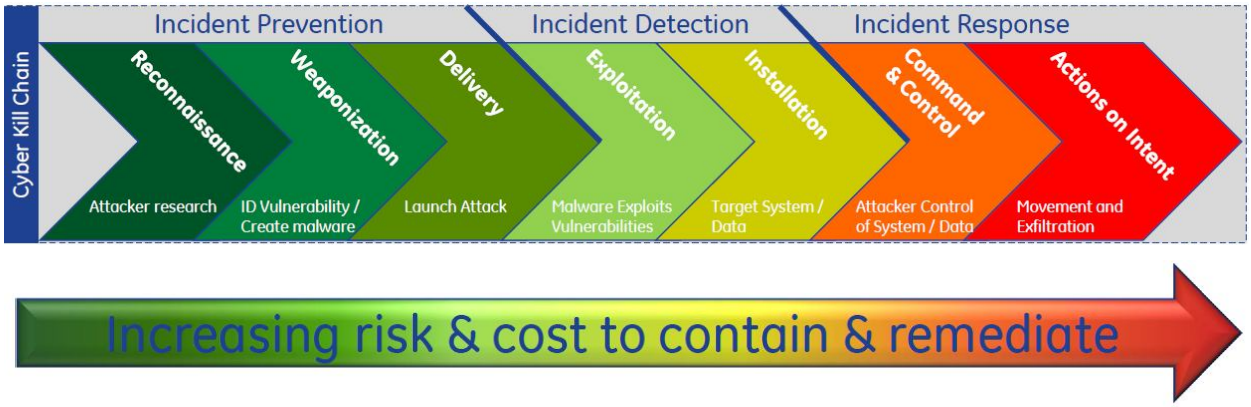


- Y Axis Indicates a Risk/Attack's Impact Magnitude
- X Axis Indicates a Risk/Attack's Likelihood
- Size of Bubble Indicates Rick/Attack Velocity (i.e., larger = faster)
- Bubble Color Indicates Risk Category (Purple is a High Priority Risk, Blue is a Priority Risk, and Mixed Purple and Blue is an Emerging Risk)

“Cyber Kill Chain” - Incident Contextualization for Incident Mitigation/Response

For immediate or realized risks, two of the participants, one from the financial services industry and one from the aerospace and defense industry, determine an appropriate response to a cyber incident depending on where the particular incident can be categorized along what they call the “Cyber Kill Chain.” The “Cyber Kill Chain” is a model which recognizes that, in order for most attacks to succeed, an adversary has to proceed through a series of seven steps within three attack phases. These three phases and seven steps are shown below:

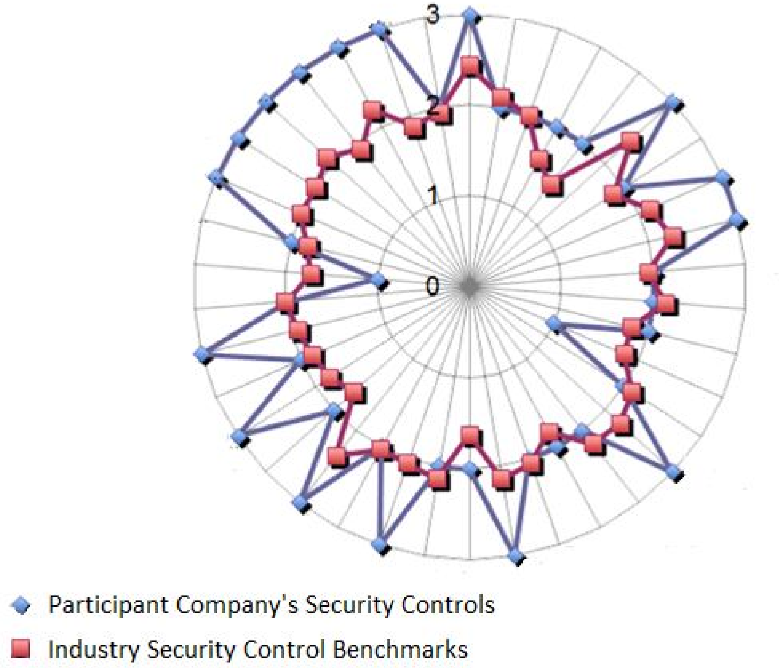
Phase 1: Pre-Compromise **Phase 2: Compromise** **Phase 3: Post-Compromise**



Examining incidents using this model allows the two companies to gauge how close to success the adversary is in achieving its objective as well as their costs to contain and remediate the attack. As the above arrow indicates, as a would-be attacker accomplishes more and more steps along this kill chain, a company’s risk and cost increase.

One Company’s Risk Mitigation Validation Process

As part of its risk mitigation validation process, one financial services participant company stated that not only did it conduct internal evaluations of its risk management/mitigation procedures and processes, but it also assessed these efforts against others in the financial services industry and other critical infrastructure sectors. To help it benchmark, this company looked to companies such as Microsoft, compared itself against various ISO standards, utilized the Resiliency Maturity Model and participated in activities such as the DHS Cyber Resiliency Assessment. The diagram on the next page is an example of a chart that this company utilizes comparing its security controls against that of the financial services industry.



The red square nodes above depict the industry baseline while the blue diamond nodes depict how the company's security controls compare. In terms of the numerical values, 0 means that there is no capability for a given control, 1 means that there is limited capability, 2 means that there is ongoing capability, and 3 means that there is forward looking capability.

Conclusion: Keeping Pace with Cyber Attack and Defense Methods Can Enhance Risk Management

While cyber attacks continue to advance, so do defensive strategies. Research suggests that more sophisticated companies, regardless of size, are continuing to evolve their cyber defenses. The more evolved strategies practiced by these companies tend to be characterized by understanding the cyber threat as an enterprise-wide risk management problem, and not just an "IT issue." These robust strategies virtually always include integrating cyber security with overall business processes, including the direct involvement of senior management. This broad perspective is accompanied by adoption of basic and "mid-level" operational tactics, which are research-based and have proven to be cost-effective.

Finally, overall risk management includes analysis of the needs and strategies involved in risk transfer and insurance solutions. These strategies are also continuing to evolve to become an integrated part of the enterprise risk management approach to corporate security, including new tools and methods offered by carriers that can augment and advance internal controls.