International principles for boards of directors and cyber security

Received (in revised form): 21st July, 2020

Larry Clinton
President and CEO, Internet Security Alliance, USA

Larry Clinton is president of the Internet Security Alliance (ISA), a multi-sector association focused on cyber security thought leadership, policy advocacy and best practices. In addition to teaching master classes for NACD, Larry teaches a graduate course on cyber security at the Wharton School and trains the staff of the Federal Reserve Bank on cyber. He is the former chair of the IT Sector Coordinating Council and advises the Center for Audit Quality on cyber issues. He has been a featured spokesman in virtually all major media outlets, testifies often before US Congress and has briefed NATO. Larry is author of the Cyber Security Social Contract which was the basis for President Obama's Executive Order and endorsed by the House GOP a task force on cyber security. He is the principal author of the NACD Director's Handbook on Cyber-Risk Oversight and has twice been named to NACD's Corporate 100.

Internet Security Alliance, 2500 Wilson Blvd, #245 Arlington, VA 22201, USA
E-mail: lclinton@isalliance.org

Abstract As threats emanating from poor cyber security have grown, calls for boards of directors to become more involved as have also grown. The exact role of the board, as opposed to management, in this new field has been murky, however, and effective steps at the board level have not previously been clearly defined. The Internet Security Alliance (ISA), in conjunction with organisations representing corporate board members and governments on four continents, conducted grounded research involving hundreds of directors, senior management government and academic responders. The ISA research generated a series of open source cyber risk handbooks. The handbooks articulated a common set of five core principles and practical steps to implement them. This paper discusses these principles, which include items boards need to be aware of in their own operations, as well as delineating the board's role in setting expectations for management. Although the core principles were supported by all participating organisations, adaptations were required to reflect differences in culture, board structure and law. The principles depart in significant ways from many commonly held assumptions about addressing cyber risk. For example, the very first principle is that boards need to conceptualise cyber security not as an 'IT issue' but as a broader risk management issue. Other principles urge boards to understand their unique legal obligations and access appropriate expertise. Boards are also urged to consider restructuring their cyber security management teams away from their current IT focus and urge management to adopt new cyber risk assessment techniques conceptualising cyber risk in empirical and economic terms. Although not part of the ISA research, the paper reports on an independent assessment PwC conducted on use of the handbooks. PwC's 'Global Information Security Survey' reported use of the handbooks generated higher budgets, better risk management, closer alignment between cyber security and business goals and helped generate a culture of security

KEYWORDS: cyber security, effective, principles, boards, international

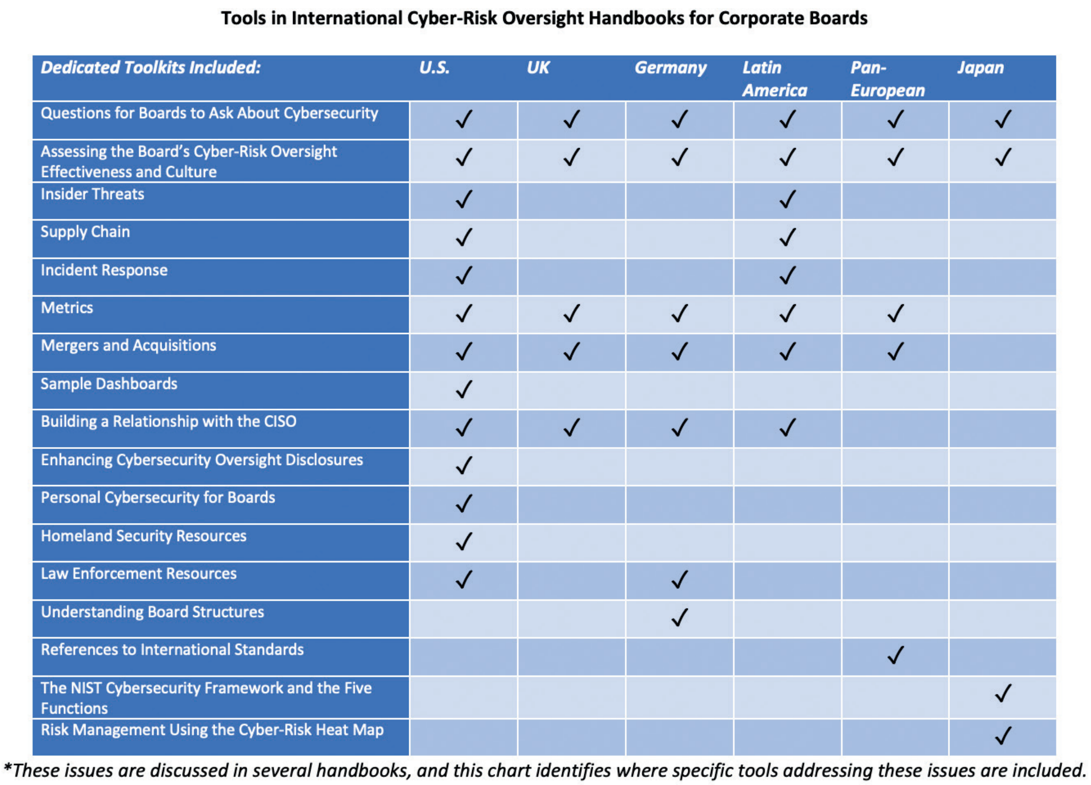
BACKGROUND AND METHODOLOGY

Since the earliest days of cyber security as a major policy issue two decades ago, there have been calls for boards of directors to be more involved. Early initiatives to involve directors were largely ineffective, however, as board members initially had difficulty appreciating cyber threats as more than a marginal cost of doing business, akin to pilfering or the technical 'Y2K' disruptions at the turn of the century.

Over time, however, leading directors and the organisations representing them increasingly realised the extent of the cyber threat and solidified the link between the economic imperatives of digital transformation and the downside risks of such business development represented by the lack of cyber security.

In 2013 the National Association of Corporate Directors (NACD), together with AIG, formed a relationship with the ISA and launched a project to clarify the messaging about the cyber threat from a director's, as opposed to a strict information technology (IT) practitioner's, perspective. A central theme of this effort was to embed cyber security issues in the business context boards appreciate, such as innovation, growth, profitability, strategic partnerships or mergers and acquisitions, as opposed to focusing exclusively on operational issues such as technical vulnerabilities and standards.

The core product of this effort was the publication in 2014 of the first Cyber-Risk Oversight Handbook[1] for corporate boards (see Figure 1). The handbook was immediately well received by both industry and government. It was the first private-sector publication endorsed by the US Department of Homeland Security, and the second edition[2] was also endorsed by the US Department of Justice. In addition, the



Tools in International Cyber-Risk Oversight Handbooks for Corporate Boards

Dedicated Toolkits Included:	*U.S.*	*UK*	*Germany*	*Latin America*	*Pan-European*	*Japan*
Questions for Boards to Ask About Cybersecurity	✓	✓	✓	✓	✓	✓
Assessing the Board's Cyber-Risk Oversight Effectiveness and Culture	✓	✓	✓	✓	✓	✓
Insider Threats	✓			✓		
Supply Chain	✓			✓		
Incident Response	✓			✓		
Metrics	✓	✓	✓	✓	✓	
Mergers and Acquisitions	✓	✓	✓	✓	✓	
Sample Dashboards	✓					
Building a Relationship with the CISO	✓	✓	✓	✓		
Enhancing Cybersecurity Oversight Disclosures	✓					
Personal Cybersecurity for Boards	✓					
Homeland Security Resources	✓					
Law Enforcement Resources	✓		✓			
Understanding Board Structures			✓			
References to International Standards					✓	
The NIST Cybersecurity Framework and the Five Functions						✓
Risk Management Using the Cyber-Risk Heat Map						✓

These issues are discussed in several handbooks, and this chart identifies where specific tools addressing these issues are included.

Figure 1: Tools in international editions of the Cyber-Risk Oversight Handbook for corporate boards
Source: Author

handbook quickly became one of the most popular publications in the history of the NACD.

PricewaterhouseCoopers (PwC) assessed the utility of the handbook in their annual 'Global Information Security Survey'[3] and reported that boards were in fact using the handbook and associated its use with higher cyber security budgets, better cyber risk management, closer alignment of cyber security with overall business goals and helping to create a culture of security within the organisations that adopted it.[4]

Based on the success of the initial handbook and its 2017 revision, industry associations and government entities around the world have now collaborated with ISA to develop versions of the handbook adapted to their unique cultures and requirements.

As of this writing, there are seven adapted versions of the handbook that have been published in the past three years which were created using the process described below. The handbooks are now available on four continents and in five languages. The ISA has been tasked with preparing all these handbooks in conjunction with regional and national partners, including the National Association of Corporate Directors, the US Department of Homeland Security, the US Department of Justice, the German Federal Office of Information Security (BSI), the Cybersecurity Council of Germany, the European Confederation of Directors Associations, the Japanese Business Federation and the Organization of American States. An Indian edition is under development with the Communication Multimedia and Infrastructure Association of India and is scheduled for publication in late 2020. All the handbooks are available on an open-source basis at no charge to any consumer.

METHODOLOGY

The process used to develop these handbooks was grounded in research primarily generated through focus groups. The groups were populated with cyber security experts generated through the partner organisations. Prior to the outreach process, ISA, working in partnership with the NACD, researched the existing literature on cyber security and boards of directors. Based on this literature and input from the ISA board and NACD membership and staff, an initial draft handbook was developed. This draft, based on the literature review, was deemed useful to help structure and focus the discussions with other participants in the process.

Following the development of the initial literature-based draft, ten in-person workshops were conducted covering four continents: North America, South America, Europe and Asia. These were then supplemented by 15 international webinars. Sessions generally included 10–15 participants, although in some cases as many as 40 individuals would participate in a session. In each region a draft handbook was created by ISA and its regional partner, based on the input, comments and suggestions from the sessions. The adapted drafts based on the sessions were then circulated to all participants in the region's sessions. Participants were encouraged to make in-line written comments/suggestions to whatever degree they felt appropriate. ISA stressed in all sessions that the intent was to allow the participants to 'make the handbook yours — for you and your colleagues' use'. Session participants were also encouraged to circulate the drafts to interested colleagues who may want to participate in the process. ISA was tasked with taking the final written comments and integrating them into the text. The regional partner was given final editorial sign-off to assure that the final handbook represented the needs and views of their region's participants.

Over 600 cyber experts generated by indigenous business, government and academic entities participated in developing the handbooks, either by participation in the workshops or webinars or by providing written comments to the drafts that were generated by the sessions.

Special attention was given to assure that individuals who sit on corporate boards were recruited for these groupings (as boards are the target audience), but all workshops and webinars as well as written review were available to management and academic personae as well. The ISA board of directors, which consists of 25 cyber security experts representing virtually all critical industry sectors, served as the technical authority and 'red team' for the handbooks. The result of this process is the closest thing currently available to a de facto standard of board of directors' theory and practice for cyber security internationally.

ANALYSIS: WHAT BOARDS INTERNATIONALLY SEEM TO AGREE ON REGARDING CYBER SECURITY

One of the most impressive findings of this process was that the participants from all areas involved in the programmes came to broad, nearly unanimous agreement on five key principles as to what should guide board process for cyber security (see Figure 2). Although there were slight modifications in some of the terminology used in the various handbooks, five consensus core principles are the foundation of all of the handbooks and can be summarised as:

- *Principle 1*: Cyber security is not an IT issue; it is an enterprise-wide risk management issue;
- *Principle 2*: Directors should understand the unique legal implications of cyber risks as they relate to their company's specific circumstances;
- *Principle 3*: Boards should have adequate access to cyber security expertise, and discussions about cyber risk management should be given regular and adequate time;
- *Principle 4*: Directors should set the expectation that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget;
- *Principle 5*: Board management discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate or transfer, such as through insurance, as well as specific plans associated with each approach.

It is noteworthy that all five of these principles were supported by all the organisations collaborating on developing these handbooks, despite a number of distinctions in the structures and composition of the boards in various regions. For example, in the US there is a fairly consistent structure of one independent board with oversight responsibility over management — and implicitly labour. In parts of Europe, particularly in Germany, there is a dual-board structure with both a supervisory board and a labour board. Some German companies are mandated to have boards while others use a voluntary board. As a result, principle 1 in the German edition advises to assess if they have a primarily supervisory function or a more direct management function. Japan, similarly, has a structure in which many boards are more heavily weighted in terms of management than the US independent oversight model. In contrast, in Latin America there is very often a substantial family constitution to the boards, which may dramatically affect both culture and oversight. Notwithstanding the variations in cultural board structures, the dominant role of a board of directors — even if heavily influenced by management — is vision, oversight and strategy.

Nonetheless, despite the varying structures, all conditions wound up supporting nearly identical versions of the five core principles.

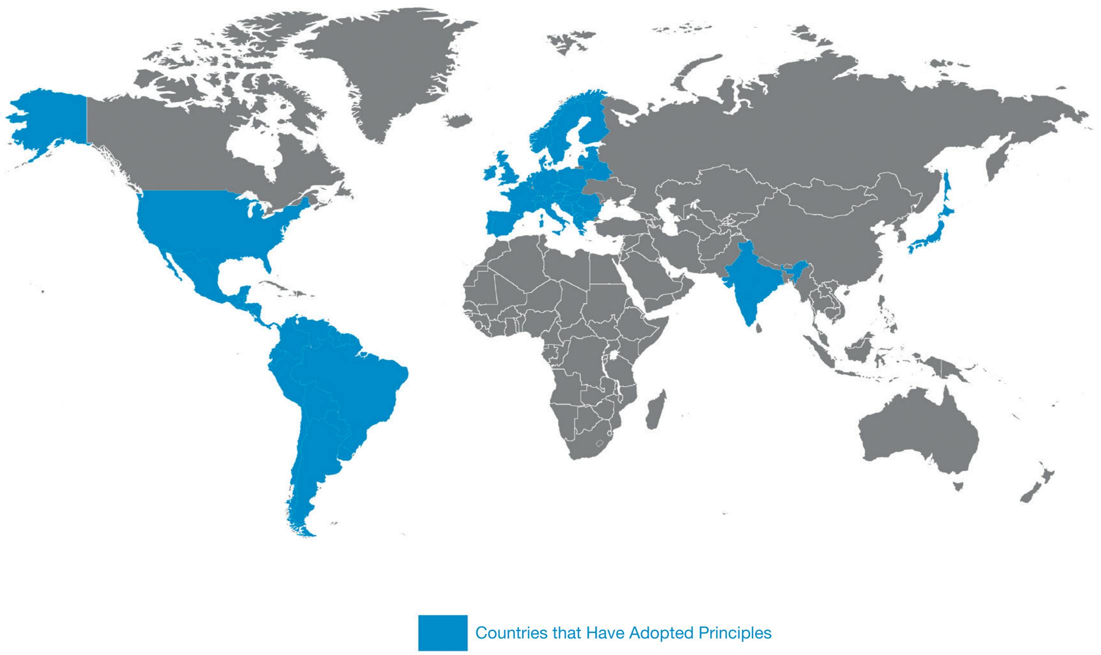


Figure 2: Adoption of corporate board principles on cyber security worldwide
Source: Author

Principle 1

Principle 1 is arguably the most comprehensive and foundational of all the principles, as it describes how cyber security ought to be understood in the full organisational context irrespective of the variations of board structure. Principle 1 describes an enterprise-wide 'top-down' model for cyber security as opposed to the traditional 'bottom-up' model. Ironically, in most organisations (including government) the understanding — the vision — of the cyber security issue has been allowed to bubble up from down in the IT department, and for the most part, the IT group, however structured, has been largely responsible for cyber policy and security.

In this reconceptualisation, cyber security is not thought of primarily as a technical issue, the management of which is based in the IT function, but rather as an overarching strategic business function wherein the entire enterprise — including but unnecessarily managed by IT — must be involved and to some degree take ownership of cyber security.

Whereas cyber security was until fairly recently thought of as a marginal cost of doing business, this modern conceptualisation sees the key business issue for the digital age as the tension between the economic imperatives of digital transformation and the potentially catastrophic risk from inadequate cybersecurity.

All the handbooks recognise that modern businesses, in order to service and compete in the digital age, need to make potentially risky technological decisions such as what and how to deploy the cloud, artificial intelligence (AI), Voice over Internet Protocol (VoIP), mobile devices, etc. Modern enterprises must also assess the risk–reward calculus of digital business practices such as extended vendor and partnership relationships, mobile employee structures, 'bring your own device' policies and long international supply chains. In the digital age, all these elements can have massive pro-growth and profit potential, yet also risk massive loss of proprietary or personal data as well as critical IP and reputational loss.

These are not decisions that are well addressed by the organisation's technical experts but must instead be approached in a more comprehensive and economically based process emanating from the top of the organisation. How the organisation thinks about its mission, its goals and its responsibilities needs to emanate from the top down.

Principle 1 also delineates, especially for traditional supervisory board structures, the role of the independent board from that of management. This is a distinction that is often missed in much cyber security discussion, which too often casually lumps boards and senior management together. It is, of course, true that effectively addressing cyber security for an enterprise will require the board to be working with management. The handbooks make clear it is not the board's job to conduct cyber risk management — management does cyber risk management.

Of course, there is an important role — roles, in fact — for the board to play in addressing organisational cyber threats. It is the board that is responsible for the vision of the organisation including assessing risk, based on data provided primarily through management determining the organisation's risk appetite and overseeing management in their implementation of the organisation's strategy.

Principle 2

Principle 2 is essentially a good governance reminder that says directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances. Part of the import of this principle is that, unlike many regulatory regimes, the legal and regulatory landscape with respect to cyber security, including public disclosure, privacy and data protection, information sharing and infrastructure protection requirements, is complex and constantly evolving. Boards should stay informed about the current compliance and liability issues faced by their organisations and, potentially, by board members on an individual or collective basis.

Principle 2 is also one of the areas wherein the various handbooks were written with discrete locations and regions involved, naturally including some of the widest variance in terms of specifics, and will require the most constant updating as practice and case law continually refines the requirements.

For example, the US handbook has been updated to include substantial detail about new advisories from the Securities and Exchange Commission and the evolution of state laws, especially California. The European editions naturally focus a good deal more attention on the General Data Protection Regulation (GDPR) and related issues, as well as other EU policy guidance such as the European Commission's certification regime and the NIS Directive. The German edition adds a section on the German Federal Data Protection Act. The Japanese version highlights the Tokyo Stock Exchange's Governance Code and other conditions regarding Japanese security standards.

Amid all the turmoil and complexity of the emerging cyber security requirements, however, the key takeaway for boards in all regions is that while compliance with legal obligations is critical, especially given potential liability by board members, compliance must not be equated with security. An organisation can be full in compliance with all regulations and still be subject to significant cyberattacks.

Principle 3

While principle 2 probably has the most variance in principle advice among any of the adapted versions, principle 3 probably has the least. The message for virtually all regions is clear: cyber security is not a simple issue that can be 'outsourced' to lower-level management.

As the cyber threat has grown, the responsibility (and expectations) of board members also has grown. Directors need to do more than simply understand that threats exist and receive reports from management. They need to employ the same principles of inquiry and constructive challenge that are standard features of board management discussions about strategy and company performance. Cyber literacy can be considered similar to financial literacy. Not everyone on the board is an auditor, but everyone should be able to read a financial statement and understand the financial language of business.

Many boards need to fundamentally alter the way they are addressing cyber security. Cyber security is not an appendage issue that should be tacked on to a few minutes on a board agenda. Cyber needs to be an inherent element of business development and operation, and few organisations have adequate in-house expertise to address cyber security comprehensively.

Principle 4

Principles 4 and 5 of the handbooks differ in some respects from the first three principles, in that the first three principles focus on what the board should be doing itself, while principles 4 and 5 focus more on what the board should be expecting from management. In order for boards to engage in effective oversight, it is important to fully understand the responsibilities that management has in addressing the organisation's cyber security. As technology has become more integral to business strategy, management has taken on the role of deploying, managing and protecting new technological capabilities across the organisation. Technology now integrates modern organisations, whether workers are across the hall or halfway around the world. But the existing reporting structures and decision-making processes at many companies are legacies of a siloed operating model, where each department and business unit makes decisions and manages risk relatively independently and without fully taking into account the digital interdependency that is a fact of modern business.

As a result, while identifying and continually assessing technical frameworks as a fundamental element of cyber security, boards need to also work with management to structure the organisation so that cybersecurity is understood and addressed on an enterprise-wide basis — not just IT.

Directors should seek assurances that management is taking an appropriate enterprise-wide approach to cyber security. Specifically, boards should assess whether management has established both an enterprise-wide technical framework as well as a management framework that will facilitate effective governance of cyber risk. An integrated risk model should consider cyber risk not as unique or separate from other business risks, but rather as part of a comprehensive risk management plan. Having an integrated approach to risk allows businesses to more effectively address cyber security risk across the entire enterprise.

While all the regions, with some modification in terminology, embraced the core element of principle 4, there was some interesting divergence among the regions in terms of how they interpreted this advice. The US handbook, which is the lengthiest and most detailed of all the treatments, provides a wide array of suggestions regarding technical frameworks that ought to be considered, citing the National Institute of Standards and Technology (NIST) Framework as well as the Center for Internet Security, ISO and others. The European and Latin American models largely follow this menu of options, citing unique models developed in this region. In contrast, the Japanese framework uniquely stresses the NIST Framework.

With respect to creating an enterprise-wide management framework, again the US was the most expansive, citing multiple frameworks stressing that control over the function ought to be assigned to a superior non-tech executive (eg CFO, CRO or COO), with the Europeans and Japanese and Latin Americans following similar themes. Meanwhile, the Europeans strongly resisted this advice as too directive and embraced the principle but were far less prescriptive regarding detailed advice.

Notwithstanding the variations, all treatments called for management to provide boards with clear and identifiable structures, both technical and managerial, that can implement a true enterprise-wide approach to cyber security.

Principle 5

Principle 5 is the culmination of the framework embodied in all the handbooks. If an organisation is going to understand cyber risk as an enterprise-wide issue and establish governance, technical and management structures to address it as part of its strategic digital transformation system, then it must systematically assess its cyber risks. This means management needs to present the board with a clear outline of what cyber risks it will accept (eg by placing its data in the cloud), reject (eg by refusing to work with insecure vendors), mitigate (eg by establishing/enhancing employee training) or transfer (eg by purchasing cyber insurance).

No organisation can do everything to eliminate all cyber risk. Indeed, cyber risk cannot be eliminated; rather, it needs to be managed. If cyber risk is to be managed as part of the business's digital transformation strategy, then these decisions must be made through a systematic, comprehensive, empirical, economics-based cyber risk assessment programme.

There was little variance among the treatments in principle 5 in any of the regions or countries. The issue is not should cyber risk be addressed in this fashion; the questions is how to do it.

Traditional risk assessment approaches have had difficulty fulfilling these requirements. Historically, cyber risk assessments tended to follow long checklists of highly technical information or control requirements — often 500 or more.

These methods have historically been qualitative assessments and have not assessed cyber risk through economic terms.[5] Quantitative economic assessments of cyber risk, however, have matured to the point where cyber risks can now be quantitatively assessed. Accordingly, just as other disciplines financially model major risks such as market, credit, insurance and strategic risks, cyber risks can now be modelled quantitatively to improve risk management performance.

Fortunately, as the cyber risk management field has evolved, the market has begun to develop tools and practices that are moving toward enabling cyber risk to be assessed in empirical and economic terms. Factor analysis of cyber risk and the x-analytics methodology are among the leading examples of these modern analytic methods and are referenced in the US, German, UK, Latin American and pan-European versions of the handbooks.

References

1. Clinton, L. (2020), 'Cyber-Risk Oversight: Directors Handbook Series', Internet Security Alliance, available at https://isalliance.org/isa-publications/cyber-risk-oversight-handbook/ (accessed 30th October, 2020).
2. Clinton, L. (2017), 'Cyber-Risk Oversight: Directors Handbook Series', Internet Security Alliance, available at https://regents.universityofcalifornia.edu/regmeet/july18/b4attach1.pdf (accessed 30th October, 2020).
3. PwC (2018), 'Global State of Information Security Survey 2018', available at https://www.pwc.co.uk/issues/cyber-security-services/insights/global-state-of-information-security-survey.html (accessed 30th October, 2020).
4. *Ibid*., note 1.
5. Jones, J. (2019), 'Understanding Cyber Risk Quantification: A Buyer's Guide', FAIR Institute, available at https://cdn2.hubspot.net/hubfs/1616664/CRQ%20Buyers%20Guide%20by%20Jack%20Jones.pdf (accessed 30th October, 2020).