November 27, 2015

PERSPECTIVES PAPER

Guiding Principles for Cybersecurity Oversight

The Global Network of Director Institutes (GNDI), founded in 2012, brings together member-based director associations from around the world with the aim of furthering good corporate governance. Together, the member institutes comprising GNDI represent more than 100,000 directors from a wide range of organisations. This paper describes the global perspective of GNDI on the role of the board in cybersecurity oversight.

A Global Issue Calling for Global Solutions

With the digitalization of the economy, an increasing number of companies in a wide range of industries are relying on information technology (IT) for their day-to-day operations. From manufacturers to retailers to airlines, organizations that never thought of themselves as "IT companies" are learning the promise and perils of the digital world. And of all perils, the greatest may well be cybercrime.

Attacks on the information assets of companies are occurring on a widespread and massive scale today, often crossing national borders. Worldwide, recovery from hacks and other internet crimes are costing the private sector more than $400 billion per year, estimates the London-based insurer Lloyds.[1] Furthermore, in addition to the cost of recovery, there are the costs of prevention: the technology research firm Gartner predicts a total of $77 billion in business cybersecurity spending for 2015 alone.[2]

[1] http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/
[2] http://www.securityweek.com/global-cybersecurity-spending-reach-769-billion-2015-gartner

Not surprisingly, a number of global organisations have tackled the problem of cybercrime. These include not only long-established organisations such as the Organisation for Economic Cooperation and Development (OECD) and the United Nations General Assembly (UN) but also relatively new global organisations such as the World Summit on the Information Society (WSIS), the Internet Governance Forum (IGF), and NATO Cooperative Cyber Defence Centre of Excellence, which has gathered a comprehensive collection of cybersecurity guidance from nearly 100 national sources[3] offering advanced cybersecurity oversight solutions for a worldwide audience.

In recognition of the global dimension of this problem, GNDI hosted a Cybersecurity Summit in early 2015[4], setting off a board-level global dialogue that continues to this day. This brief paper reports on some of our current thinking, intended to supplement rather than replace the authorities cited here.

What Can the Board Do?

When it comes to cybernetics there is no security, rendering "cybersecurity" an oxymoron as countless pundits have noted. Nonetheless, given its aspirational value, the term persists. Boards want to ensure the highest level of security possible for their systems as they oversee them—but how? The ultimate goal of any board's oversight will be what the MITRE Corporation has called "cyber resilience." MITRE, a not-for-profit organisation in the United States that operates federally funded research and development centres, defines cyber resilience as "the ability of an enterprise to anticipate, withstand, recover from, and evolve to improve capabilities in the face of adverse conditions, stresses or attacks on the supporting resources it needs to function." The oversight of any management area, including cybersecurity and disaster recovery, occurs within a larger governance system. The elements of such a system include

[3] https://ccdcoe.org/cyber-security-strategy-documents.html
[4] http://blog.nacdonline.org/2015/04/global-cyber-summit-sends-message-to-boardrooms/

systems for oversight, accountability, and control, with attention to risk tolerance as well as enhancement (or preservation) of value, as noted in the GNDI perspective paper on Guiding Principles of Good Governance (May 2015).[5]

Building on GNDI's earlier paper on governance, Part 1 of this paper seeks to identify principles for the cybersecurity oversight in the new environment. In addition, in Part 2, this brief guide to cybersecurity governance will summarize key cybersecurity developments in the countries and regions spanned by the GNDI membership.

PART 1: General Guidance

The role of the corporate board (supported by committees) in any domain outside its own operations is rightly described as "oversight." This occurs when a body vested with authority observes (or "oversees") matters--such as *people, processes, and technology*--and makes judgments on their adequacy, taking actions to ensure any needed improvements. It is worth underscoring the fact that oversight does not mean management: It is unnecessary for directors to delve into in-depth details or technical aspects that are more relevant to executives and operational-level personnel. Nonetheless, directors need to be familiar with the general effectiveness of the people, processes, and technology within the entities entrusted to their care. The board of directors needs to understand the big picture – the essential components of the entity they are overseeing and how they can oversee it effectively.

People

For example with respect to ***people,*** the board's oversight focuses on the persons reporting to the board. As such the board is typically accountable for decisions relating

[5] ""Effective governance structures allow organisations to manage their affairs with proper *oversight* and *accountability*, to *create value* over the short, medium and long term through sound investment and innovation, and provide *accountability and control systems* commensurate with the risks involved." To see this paper, go to GNDI.org and click on Papers.

to evaluation and compensation (and when necessary, hiring and firing) of the CEO, senior managers, and the external auditor or other board consultants. More broadly, boards oversee the entire pool of corporate talent. Extending these principles to cybersecurity, ***GNDI would urge boards to consider placing cybersecurity as a specific accountability of one of the officers reporting to the board (whatever the officer's title), and as such consider cybersecurity needs as part of the key functions needing officer-level attention.*** The executive having this accountability would report directly to the CEO. In addition, the board should consider meeting with the executives responsible for cybersecurity at the next level or levels down. Finally, the board can ensure that there is cybersecurity training for all employees to mitigate the risks of internal cybercrime.

Processes

With respect to ***processes***, the board is typically responsible for the oversight of the organisation's internal control environment, defined by the well-regarded COSO initiative as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in …operations… reporting, [and] compliance…"[6] Extending this definition to cybersecurity, ***GNDI would suggest that boards inform themselves of specific operational, reporting, and compliance aspects of cybersecurity, using (and as needed adapting or supplementing) at least one recognized framework to do so***. Recognized international frameworks include:

- Control Objectives for Information and Related Technology (COBIT) from ISACA,
- ISO 27000 standards from the International Organisation for Standardisation (based in Geneva, Switzerland),

[6] Internal Control: Integrated Framework (2013). http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf

- Framework for Improving Critical Infrastructure Cybersecurity from the National Institute of Standards and Technology (NIST), under the U.S. Department of Commerce, and[7]
- Information Technology Infrastructure Library (ITI), developed and owned by AXELOS in the United Kingdom

In addition to these general standards, there are specific industry standards for cybersecurity, notably:

- HIPAA or HITRUST (for health-care industry)
- PCI-DSS for credit card acceptance (retail industry, finance industry)

Fundamentally, the board's approach should be no different to any other area of potential or actual risk. Risk appetite/tolerance must be determined, specific risks must be identified and finally actions must be taken to avoid, mitigate, or transfer risks (e.g. through insurance). And, as in the case of risk in general, cyber risk needs to be overseen by the full board, with support from appropriate committees as the board may assign. Committee help can be critical. While cybersecurity should never be assigned entirely to a single committee, (lest it become marginalized at the board level), the board cannot be expected to oversee this area effectively without some additional committee support. The important point here is that directors and boards need to treat cyber-security as an integrated component of enterprise-wide risk-management.

This is a key theme in a recent publication developed by the international insurer AIG and the Internet Security Alliance, in association with the National Association of

[7] For a comparison of these standards, see http://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf

Corporate Directors (U.S.). Their Cyber-Risk Oversight Handbook proposes a five-point approach that has been adopted by others, including the Institute of Directors in New Zealand (IoD-NZ). Here are the five points (with introductory headings courtesy of the IoD-NZ):

1. ***Take a holistic approach.*** *Directors should approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.*

2. ***Understand the legislative environment.*** *Directors should understand the legal implications of cyber risk as they apply to the company's specific circumstances.*

3. ***Access expertise and put cybersecurity on the board agenda***
Boards should have adequate access to cybersecurity expertise and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda

4. ***Establish a framework*** *Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.*
5. ***Categorise the risks.*** *Board-management discussions about cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.*

Any oversight process should include both defence and response to ensure business continuity. Regarding the latter, the Cyber-Risk handbook recommends considering the following questions:

1. How will management respond to a cyberattack? Is there a validated corporate incident response plan? Under what circumstances will law enforcement and other relevant government entities be notified?
2. For significant breaches, is our communication adequate as information is obtained regarding the nature and type of breach, the data impacted, and ramifications to the company and the response plan?
3. Are we adequately exercising our cyber-preparedness and response plan?
4. What constitutes a material cybersecurity breach? How will those events be disclosed to investors?

Technology

Finally, with respect to ***technology,*** there is less standard guidance on the nature of board oversight here, but a growing number of boards are taking a greater interest in it. To help enable oversight of the challenges of information technology, including digitalization and cybersecurity, in an effective way, GNDI recommends that ***boards consider adding a member with some knowledge of information technology (including digitalization and cybersecurity).*** This is particularly important for boards of companies where IT is a core competence.

If the board has more pressing needs for expertise and cannot expand by adding an additional director, GNDI recommends the use of outside expertise to help the board assess the current state of cybersecurity in the organisation served.

"Fourth Estate"

Yet these three oversight areas, while important, are not enough. Cybersecurity is emerging as a kind of "fourth estate" for governance, outside the traditional borders of oversight, accountability, and control. As a recent paper from Gartner states, "[a] proliferation of technologies in the form of devices, things, access methods, applications

and other services that are *not manageable and controllable in the traditional sense* creates new risk vectors. This is exacerbated by the autonomy that digital business gives to the business, *invalidating the traditional, centralized control model on which most security programs are based*. As a result, new risks need to be treated differently." (Emphasis added.)

To build the cyber resilience recommended at the outset of this paper, technology should be built into the DNA of business operations and thus become part of directors' assessment of enterprise risk (the holistic approach suggested in this paper). This permits the board to combine tried and true systems of oversight with emerging techniques developed daily in response to new threats and opportunities. Finally, the board itself must be resilient and learning from global partners is one good way to maintain currency in this dynamic field.

One important aspect of cyber resilience is to avoid getting locked into any single approach. As such, these global principles for cybersecurity oversight are not intended to be prescriptive. Factors that may influence cybersecurity oversight include the organisation's industry, locations, regulatory environment, and culture. Nor are these principles to be considered a substitute for the relevant laws, regulations and standards with which organisations must comply.

GNDI recommends that the board stay current with emerging advice from a variety of sources such as those cited in the following section.

Part 2: Current Developments and Resources in GNDI Jurisdictions

GNDI member institutes tend to have a relatively high awareness of cybersecurity. A Global Cybersecurity Index prepared by ABI research with the Swiss-based International Telecommunication Union gives 29 rankings and most members of GNDI rank in the top five.

GLOBAL NETWORK OF DIRECTOR INSTITUTES

GNDI member institutes around the world regularly provide their members the tools and information they need to cope with emerging cybersecurity challenges. These resources typically include information about government initiatives and public-private partnerships. The following section provides some relevant highlights.

Australia. The Australian government has been proactive in fighting cybersecurity hand in hand with the private sector. The Australian Cyber Security Centre joins capabilities across Defence, the Attorney-General's department, the Australian Security Intelligence Organisation, the Australian Federal Police, and the Australian Crime Commission.[8] As such, "it creates a hub for even greater collaboration and information sharing with the private sector, state and territory governments and international partners to combat the full breadth of cyber threats." Other developments include a report on cyber resilience by the Australian Securities and Investments Commission, and proposed mandating breach notification requirements.

Brazil. The private sector in Brazil has been seeking ways to mitigate the threat of cybercrime. For example, the Igarapé Institute has published a white paper on Deconstructing Cyber Security in Brazil, and cyber security experts have gone on record with a variety of solutions.[9]

Civil society has created a Cyber Manifest[10] in Brazil, which "seeks to galvanize support and create a shared vision of how we might better protect Brazil from cyber-attacks and raise awareness and understanding." The initiative, supported by several people and

8 http://www.asd.gov.au/infosec/acsc.htm
9 "http://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf. See also http://www.financierworldwide.com/do-liability-in-data-privacy-and-cyber-security-situations-in-latin-america/#.VhWdqPlVhBd.
10 http://www.cyber-manifesto.org/wp-content/uploads/2014/06/cyber_manifesto_english.pdf

businesses[11], focus on four main areas: 1) Cyber Savvy Leaders; 2) Zero tolerance; 3) Fill the Cyber Skill Shortage; and 4) Turn people into the first line of defence.
Besides that, the government has sanctioned a couple of laws regarding internet, cybersecurity and privacy issues:

- Laws 12,735/12 and 12,737/12[12], which "amend and revise the Brazilian Penal Code, defining crimes committed in the digital environment and via access to information technology devices, and the counterfeiting of cards, criminalizing the behaviours with penalties of between 1 to 5 years' imprisonment and a fine"; and
- The Civil Rights Framework for the Internet Act (Law 12.965/14).[13], which "governs the use of the Internet in Brazil, through forecasting principles, guarantees, rights and duties to those who use the network as well as the determination of guidelines for government action".

Canada. The Canadian government has adopted Canada's Cyber Security Strategy which aims to protect Canadians from cyber threats. The main objectives of the Strategy are to secure government systems and work with others to secure systems outside of government. In addition, the federal government is collaborating with the U.S. government on a Cybersecurity Action Plan**.** Public Safety Canada and the U.S. Department of Homeland Security (DHS) are pursuing a coordinated approach to "enhance the cybersecurity of our nations through increased integration of …national cybersecurity activities and improved collaboration with the private sector." **[14]**

Europe. The European Commission has a program called the Digital Agenda for Europe, with a cybersecurity component.[15] The needs of the region have given rise to an

11 http://www.cyber-manifesto.org/#apoio
12 http://www.bkbg.com.br/direito-de-internet-publicadas-leis-que-tipificam-crimes-informaticos/?lang=en
13 https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf
14 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/cybrscrt-ctn-plan-eng.pdf
15 https://ec.europa.eu/digital-agenda/en/cybersecurity

Organisation for Security and Cooperation in Europe (OSCE). Also, the region was the site of a major Global Conference on Cyberspace that included a strong focus on cybersecurity.[16] Each nation within Europe has cybersecurity initiatives, some of them multilateral within and outside Europe. For example, the Cyber-Security Council of Germany has formed an alliance with the Internet Security Alliance, based in the United States.[17]

The Gulf States. As noted in an April 2015 study earlier this year, "[t]he Internet is one of the fastest growing areas of infrastructure development in the union of the Cooperation Council for the Arab States of the Gulf commonly referred to as Gulf Cooperation Council (GCC)." The paper commends Qatar and Oman for having developed technical, organisational, and legal measures to address cybercrime and notes a broader need to develop these safeguards. [18] [i] In May 2015, the GCC and the U.S. announced a joint initiative to combat cybercrime. In particular, the U.S. agreed to "provide GCC member states with additional security assistance, set up military cybersecurity exercises and national policy workshops, and improve information-sharing."[19][ii]

Hong Kong. In Hong Kong, the main sources of guidance [and assistance] include the following:

- The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), established in 2001 and managed by the Hong Kong Productivity Council, coordinates computer security incident response for local enterprises and Internet Users. It maintains an exchange of information with other CERTs and acts as a point of contact on cross-border security incidents.

[16] For Conference proceedings see a https://www.gccs2015.com/key-documents
[17] http://www.isalliance.org/publications/EU%20ISA%20CSCG%20Position%20Paper.pdf
[18] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594624
[19] https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015

- The Cyber Security and Technology Crime Bureau (CSTCB), upgraded in 2015 to become a separate bureau within the Hong Kong Police Force, is responsible for handling cyber security issues and carrying out technology crime investigations, computer forensic examinations and prevention of technology crime.
- The Cyber Security Information Portal (CSIP), launched by the Hong Kong Government's Office of the Government Chief Information Officer in early 2015, provides practical advice and step-by-step guidelines for general users, small and medium enterprises, and schools.
- The Office of the Privacy Commissioner for Personal Data (PCPD) puts out guidance on safe handling of personal data. Although Hong Kong as yet does not have at law a mandatory data breach notification requirement, the PCPD published Guidance on Data Breach Handling and the Giving of Breach Notifications in June 2010, which provides data users with practical steps in handling data breaches and to mitigate the loss and damage caused to the data subjects involved.
- The Hong Kong Monetary Authority (HKMA) recently on 15 September 2015 issued a circular on "Cyber Security Risk Management" (the Circular). The Circular provides general guidance to authorised institutions (AIs), which are banks, restricted licensed banks and deposit taking companies regulated by the HKMA, on cyber security risk management and highlights risks which in the view of the HKMA warrant special attention in light of recent incidents and trends. The circular could be seen as a reflection of the HKMA's concern that conventional risk management controls and philosophies practised by financial institutions need to be adjusted in order to meet the emerging challenges.
- The Hong Kong Institute of Directors has been organizing training courses and events on cybersecurity to raise the awareness among directors on the subject matter. The content material focuses on the oversight role that directors have to perform, including the questions they should ask of management vis-à-vis cybersecurity.

Malaysia. Ranking only behind the United States and Canada for commitment to cybersecurity, Malaysia's National Cyber Security Policy was formulated based on a National Cyber Security Framework that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects. The Malaysian Computer Emergency Response Team (MyCERT) works with law enforcement agencies such as the Royal Malaysian Police, Securities Commission, and Bank Negara Malaysia and also has close collaborations with Internet service providers, a number of computer security initiatives worldwide.

Mauritius. A look at the cyber wellness profile of Mauritius gives an overview of the country's levels of cybersecurity development based on, amongst other things, legal, technical and policy measures.

Legal

Mauritius has adopted legislation designed to challenge and combat the increasing risks which accompany dissemination of data and information. One of such initiatives includes the adoption of the Computer Misuse and Cybercrime Act 2003 which provides for the repression of criminal activities perpetrated through computer systems.

Technical

The National Computer Emergency Response Team of Mauritius (CERT-MU) operates under the National Computer Board, a statutory body under the aegis of Ministry of Technology, Communication and Innovation. The CERT-MU handles and co-ordinates cyber security incidents, prevents occurrence and recurrence of cyber incidents by developing incentives for cyber security compliance, and interacts with government agencies, the industry, the research community, and others to analyse cyber threats and vulnerabilities, disseminate reasoned and actionable cyber security information such as mitigations to the public.

Policy

Mauritius has adopted a National Cyber Security Strategy (2014-2019) which was developed by the National Computer Board along with other stakeholders and that sets out the guidelines, measures and action plans that will provide reasonable assurance of resilience and security to respond effectively to cyber threats and support national missions and economic stability. The implementation of the strategy is planned over a period of 5 years from 2014 to 2019.

The strategy also gives an insight into the Government's approach and strategy to protect the cyberspace in the country.

The strategic guidelines are:

- To secure our Cyberspace and establish a front line of defense against Cybercrime
- To enhance our resilience to Cyber Attacks and be able to defend against the full spectrum of threats
- To develop an efficient collaborative model between the authorities and the business community for the purpose of advancing National Cyber Security and Cyber Defense
- To improve the Cyber Expertise and the comprehensive Cyber Security Awareness of the society at all levels.

With the Internet's pervasive reach to businesses, governments and home users, cyber threats are not only continuing to evolve, but new techniques are also being adopted. Cyber criminals continue to devise new ways to monetise victims while espionage is being carried out by nation-state hackers to steal information. In addition, the growing popularity of the "Internet of Things" (e.g., mobile devices, applications, social networks, and interconnected gadgets and devices) makes the threat landscape a moving target. New threats arise with emerging technologies like Near Field

Communications being integrated into mobile platforms. Innovative uses of GPS services to connect our digital and physical lives present new opportunities for cyber criminals to compromise our security and privacy. Mauritius recognises that the development of a national cyber security strategy will help in managing deliberate and unintentional disturbances in the cyber space as well as respond to and recover from them[20].

From a regulatory perspective, it is to be noted that the Mauritius Financial Services Commission, which is the regulator for financial services (other than banking), and for global business regularly issues investor alerts including those which relate to cybercrime and cybersecurity, for example, on fraudulent correspondence and on phishing.

New Zealand. In 2015 the Institute of Directors in New Zealand (IoD) produced a Cyber-risk Practice Guide, based on the 5 principles of cyber-risk oversight developed by the NACD. The guide aims to help boards monitor cyber-risk, develop strategies for seeking assurance and to oversee management. The IoD website has a range of resources regarding the board's role in cyber-risk and technology governance.

The New Zealand Government's National Cyber Policy Office (NCPO) leads the Connect Smart initiative, a public private partnership of government agencies, non-government organisations, and private businesses. The Connect Smart website encourages taking proactive steps to protect against cyber threats and includes resources to help boards.

There are currently no mandatory requirements for reporting cyber incidents in New Zealand. Cyber incidents relating to critical national infrastructure are reported on a voluntary basis to the New Zealand National Cyber Security Centre (NSCS).

[20] http://cert-mu.govmu.org/English/Events/Pages/National-Cyber-Security-Strategy-Validation-Workshop.aspx

Pakistan. The fight against cybercrime in Pakistan occurs largely through a National Response Centre for Cyber Crime (NR3C) – Federal Investigation Agency, a law enforcement agency dedicated to fight cybercrime. The mission of the NR3C is to "achieve excellence by promoting culture of merit, enforcing technology based law, extending continuous professional training, ensuring effective internal accountability, encouraging use of technology and possessing an efficient feedback mechanism.

In order to mitigate the risks associated with Internet Banking and safeguard the interests of customers, State Bank of Pakistan has issued on October 21, 2015, 'Regulations for the Security of Internet Banking' under Sections (3) and (15) of the Payment Systems and Electronic Fund Transfers Act, 2007. These regulations outline minimum set of operational, administrative, technical and physical safeguards to secure Internet Banking offered by the banks in Pakistan and will be effective April 1, 2016.

These regulations would help banks in Pakistan to develop a formal Internet Banking Security Framework containing administrative, technical and physical safeguards based on best international practices. The major components of the framework would be Security Risk Assessment (of threats, vulnerabilities to systems and customers information), Security Controls Implementation based on the Security Risk Assessment and Security Controls Monitoring. Further the framework should clearly define the roles and responsibilities of Board of Directors (BODs), senior management and employees with regard to its approval, development and implementation.

This Framework and any reviews thereafter should be duly approved by the BODs. The BODs should also review the Security Risk Assessment document and any reviews conducted thereafter. Among the authentication controls, the banks shall implement at least Two Factor Authentication (2FA) such as Passwords (1 factor) and One time

tokens, Dongles etc. (2nd factor) and shall also implement additional layered security programs for high value transactions processed through Internet Banking.

Singapore. The Cyber Security Agency of Singapore (CSA), Singapore's national body overseeing cybersecurity strategy, education, outreach, and industry development, has forged new partnerships to boost cyber security capabilities as part of its ongoing efforts to strengthen Singapore's cyber security posture and stay ahead of a rapidly evolving cyber security landscape.[21]

South Africa. In South Africa we currently have the Cybercrimes and Cybersecurity Bill ("the Bill"), which is out for public comment until 30 November 2015.In creating the Bill, the South African Government has drafted various policies, strategies and reviewed existing laws to determine its adequacy in dealing with the cyber challenges within the country. The Electronic Communication and Transactions endeavours to deal with electronic restrictions and the Protection of Personal Information Act deals with protection of personal information, however these and other legislations don't specifically deal with cybersecurity and the NCPF will be well received when it comes into effect. The King III Report on Governance speaks to IT governance but does not deal in detail with the critical exposures of cybersecurity.

Switzerland. Known for its global banking institutions, Switzerland has been a target for cyber threats partly because of its global banking institutions. Therefore it is not surprising that the central agency for cybersecurity in Switzerland, Reporting and Analysis Centre for Information Assurance, known as MELANI (an abbreviation **for** *Melde- und Analysestelle Informationssicherung*) has been urging pushing private sector organisations to boost security since its founding more than a decade ago. The information Security Society of Switzerland, a professional association has been part of

[21] https://www.csa.gov.sg/

the solution as well. As mentioned earlier the International Organisation for Standardisation, source of a leading standard for information security, is based in Switzerland.

Thailand. In Thailand, the issue of cybersecurity oversight as well as IT oversight is relatively new for the majority of board of directors. Institutions in Thailand are working to encourage private sectors' awareness and make it an important agenda item. One such institution is Electronic Transactions Development Agency (ETDA) intended to encourage confidence in electronic transactions and increase awareness of cybersecurity and related IT issues through knowledge dissemination. The agency plays an important role in developing and improving legislation on electronic transactions and cybercrimes. Thailand's first legislation on cybersecurity is on its way. Recent (2015) legislative initiatives in Thailand include the tabling of the Computer-related Crime Bill (amendment) and the Cybersecurity Bill and Personal Data Protection Bill. Under these initiatives, a National Cybersecurity Committee would be established to determine approaches and measures for responding to and tackling cyber threats.

Thai IOD also understands the importance of making Thai directors aware of their role in cybersecurity and IT oversight. For this reason, it dedicated a recent director forum to the issue of IT governance, including cybersecurity. Thai IOD and ETDA also work in collaboration to raise awareness on the issue. We have recently jointly developed a director training course to begin in 2016 focusing on board oversight role in IT, called Driving Company Success with IT Governance, in which the issue of cybersecurity is included.

United Kingdom. The UK's Centre for the Protection of National Infrastructure works in close collaboration with nation's technical authority for information assurance, known as CESG (for the Communications-Electronics Security Group). CESG advises organisations on how to protect their information and information systems against

current cyber threats. The CESG's 10 Cyber Security Steps is used by some two thirds of the FTSE350. In addition, the CESG has published a paper on "Common Cyber Attacks: Reducing the Impact," including practical advice on understanding why an organisation is targeted. In an interview with the BBC in October 2015, Oliver Parry, a senior economic adviser at the Institute of Directors, stated: "The risks need to be reviewed regularly by the board of directors, who must ensure they know where the potential threats are coming from and are prepared in case the worst happens. The CESG states "We believe understanding the cyber environment and adopting the 10 Steps are effective means in protecting your organisation from these attacks."

United States. In the United States the main sources of high-level guidance include the following:

- *National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity* (NIST Framework) widely used as a basis for cybersecurity-oriented discussions and decision making at all levels of the corporation, from front-line managers to the board.[22] It identifies five concurrent and continuous functions: identify, protect, detect, respond, recover.[23]
- *The United States Department of Homeland Security (DHS)* has at least two major programs: 1)*The DHS Critical Infrastructure Cyber Community ("C Cubed") Voluntary Program*, [24] under the Department of Homeland Security, recommends that organisational leaders gain an overview of (and know how to communicate) the cyber threat, understand risk, discuss the state of existing company security plans, identify priorities and plans, and use government resources such as those available from the Department of Homeland Security (namely DHS Enhanced Cybersecurity Services, DHS Cyber Information Sharing

22 http://www.nist.gov/cyberframework/
23 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
24 U.S. Department of Homeland Security, Critical Infrastructure Cyber Community ("C Cubed") Voluntary Program, www.us-cert.gov/ccubedvp.

and Collaboration Program); and 2)*The United States Computer Emergency Readiness Team (US-CERT)* is a part of the National Cybersecurity Communications and Integration Center (NCCIC). It maintains lists of resources specifically aligned to the five NIST areas cited above (at note 9): identify, protect, detect, respond, recover.[25]

- *The Cyber Threat Intelligence Integration Center* (CTIIC), formed in February 2015, will "serve as the national cyber threat intelligence center to 'connect the dots' within government regarding malicious foreign cyber threats to the nation."[26][iii]
- *The National Association of Corporate Directors (NACD),* in conjunction with AIG and the Internet Security Alliance (ISA), has produced a Cyber-Risk Oversight Handbook with five steps, namely: approach cybersecurity as an enterprise-wide risk management issue, understand legal implications of cyber risks, ensure adequate board access to cybersecurity expertise and devote regular and adequate time on the board agenda; approve a framework that includes adequate budget for cybersecurity; and decide what risks to avoid, accept, mitigate, or transfer through insurance, while setting specific plans associated with each approach.[27] In addition, NACD maintains a cybersecurity toolkit.[28] Finally, NACD runs frequent panels on cybersecurity that yield new ideas.[29]New frontiers are yet to emerge through dialogue.
- *The Institute of Internal Auditors Research Foundation (IIARF*), a global organisation based in the United States, has published *Cyber Security: What*

25 https://www.us-cert.gov/ccubedvp/getting-started-business
26 https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015
27 http://www.nacdonline.org/cyber
28 http://blog.nacdonline.org/tag/cybersecurity/
29 For example, at the October 2015 Global Board Leader's Summit, Nick Donofrio, former IBM VP for Innovation and Technology, and a director of NACD and the MITRE Corp. emphasized the importance of keeping up with the changing techniques of the attackers. http://blog.nacdonline.org/2015/10/cyber-experts-offer-six-tips-for-director-oversight/

Directors Should Ask, with more detailed guidance based on these principles, including ten action steps and six areas for questioning.[30]

GNDI Conclusion

Clearly, cybersecurity is an enterprise-risk challenge that knows no global boundaries. Information sharing within and between the private and public sectors is occurring on a global level with positive results. This brief paper constitutes one such collaboration. As a collective of the pre-eminent governance associations around the world, GNDI plays an important role in providing leadership on governance issues for directors of all organisations to achieve a positive impact for companies, the economy, and society. This paper on cybersecurity oversight, like other GNDI perspective papers, has been developed as part of a commitment to this goal and to guide boards in good governance beyond legislative mandates.

[30] https://na.theiia.org/special-promotion/PublicDocuments/GRC-Cybersecurity-Research-Report.pdf