Cyber Risk & Social Media

Presentation by Ricardo L. Saludo
Center for Strategy, Enterprise, and Intelligence

3enSEI
Cyber Risks & Social Media

Presentation by Ricardo L. Saludo
Center for Strategy, Enterprise, and Intelligence (CenSEI)
The Biggest Cyber Breaches

Business Hacks

Yahoo
• Date: 2013-14
• Impact: 3 billion user accounts
The Biggest Cyber Breaches

Business Hacks

Marriott International

• Date: 2014-18
• Impact: 500 million customers
The Biggest Cyber Breaches
Business Hacks

Adult Friend Finder

• **Date:** October 2016
• **Impact:** More than 412.2 million accounts
The Biggest Cyber Breaches

Business Hacks

eBay
• Date: May 2014
• Impact: 145 million users compromised
The Biggest Cyber Breaches

State Hacks

US Office of Personnel Management (OPM)

• **Date:** 2012-14

• **Impact:** Personal information of 22 million current and former federal employees
Stuxnet

- **Date:** Sometime in 2010, but origins date to 2005
- **Impact:** Meant to attack Iran's nuclear power program, but will also serve as a template for real-world intrusion and service disruption of power grids, water supplies or public transportation systems.
The Biggest Cyber Breaches

State Hacks

Wikileaks

• **Date:** July-November 2010

• **Impact:** Nearly half a million classified US military documents on the US war in Afghanistan leaked, plus 250,000 State Department cables since 1966.
The Paris G20 summit

Date: 2011

Impact: An email containing a PDF attachment infected with malware was sent around the French Ministry of Finance. The virus infected around 150 computers with access to confidential G20 data.
Sony's PlayStation Network

- **Date:** April 20, 2011
- **Impact:** 77 million PlayStation Network accounts hacked; estimated losses of $171 million while the site was down for a month.
Recent Philippine Cyber Hacks and Attacks

Commission on Elections

• **Date:** April 2016
• **Impact:** 55 million voters’ personal and biometric records stolen and posted online
Recent Philippine Cyber Hacks and Attacks

Two dozen Philippine companies hit by ransomware

• Date: 2017

• Impact: Damage was said to be "small to medium", infecting 30 per cent of servers and computers.
Wendy’s Philippines website hacked

• **Date:** April 2018

• **Impact:** More than 80,000 records including users’ personal data were exposed
Recent Philippine Cyber Hacks and Attacks

ABS-CBN UAAP shop site

• **Date:** Sept. 2018
• **Impact:** Two sites taken down after reported hacking with possible theft of payment information by a hacker in Irkutsk, Russia. ABS-CBN stock fell 3 percent.
Examples of Cyber Risk Events

Anthem, 2015

69 million to 80 million records compromised

In February 2015, Anthem, formerly known as WellPoint and the second-largest health insurer in the U.S., revealed its customer database had been breached. Stolen data included names, addresses, dates of birth, Social Security numbers and employment histories — Show more

The legal tussle between Apple and the U.S. Federal Bureau of Investigation (FBI) over access to the iPhone used by a shooter in last year’s San Bernardino attacks is now over after authorities announced they had accessed the device.

But the larger debate between technology firms and law enforcement authorities over data privacy and access remains. CNBC explains the case and why it was such a big deal.
An untamed beast

AON’s Global Risk Management Survey:

- 3 out of the Top 20 risks are technology related

- Many of the rest are caused by technology risks (e.g. supply chain failure) or direct consequences (e.g. damage to reputation)

- 2015 Global Cyber Impact Report (Ponemon Institute): 37% of surveyed companies have had significant security breaches in the last one year, averaging US2.1m

"Nine out of 10 respondents have validated our assessment that cyber risk is still not fully understood"
Cybercrime cost as a % of GDP (June 2014)

**G20 Countries**
- Australia (.08%)
- Brazil (.32%)
- Canada (.17%)
- China (.63%)
- European Union (.41%)
- France (.11%)
- Germany (1.60%)
- India (.21%)
- Japan (.02%)
- Mexico (.17%)
- Russia (.10%)
- Saudi Arabia (.17%)
- Turkey (.07%)
- United Kingdom (.16%)
- United States (.64%)

**Other Countries**
- Argentina (n/a)
- Colombia (.14%)
- Indonesia (n/a)
- Ireland (.20%)
- Italy (.04%)
- Kenya (.01%)
- Korea (n/a)
- Malaysia (.18%)
- Netherlands (1.50%)
- New Zealand (.09%)
- Nigeria (.08%)
- Norway (.64%)
- Singapore (.41%)
- South Africa (.14%)
- United Arab Emirates (.11%)
- Vietnam (.13%)
- Zambia (.19%)
Are You and Your Organization Addressing Cyber Risk?
Let’s do a little survey

• Log on to www.menti.com
• Type the code for the given question, and click your answer.
• All replies are confidential.
What does ‘Cyber(space)’ mean?

‘... an interactive domain made up of digital networks that is used to store, modify and communicate information ... includes the internet, but also the other information systems that support our businesses, infrastructure and services.’

The UK Cyber Security Strategy Protecting and promoting the UK in a digital world, UK Government Cabinet Office (2011)

‘... the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Common usage of the term also refers to the virtual environment of information and interactions between people.’

Cyber Risk: Who Might Attack? & What Are They After?

- The classic cyber criminal (i.e., organized crime) or skilled individual hackers
  - Guarded data and personally identifiable information, including health records, for monetary gain

- The advanced persistent threat, directed by nation-states
  - Highly sensitive information, including PHI, infrastructural, or strategic information, to gain an economic or technological advantage

- “Hactivists”
  - Systemic disruption with political, social, or personal motive, often in the form of high profile protest
Malicious cyber activity components

- Loss of intellectual property and business confidential information
- Cybercrime, which costs the world hundreds of millions of dollars every year
- Loss of sensitive business information, including possible stock market manipulation
- Opportunity costs, including employment and service disruptions, and reduced trust for online activities
- Additional cost of securing networks, insurance and recovery from cyber attacks
- Reputational damage to the hacked company

The Economic Impact of Cybercrime and Cyber Espionage Report, Center for Strategic and International Studies July 2013
Cyber risk is different to normal risk...

- Risks associated with cyber activities are relatively new.
  Boards are unlikely to have a comprehensive understanding of the issues or have past experience of dealing with such risks.

- A lack of understanding of the issues often results in an inappropriate response, such as simply increasing levels of IT security.

- Requires a full understanding of the risks.
  Companies may be focusing their attention and spending on areas that do not reflect the greatest risks.

- Little information sharing on cyber attacks between organisations.
  Unlike other risks, there are active enemies directing their activities towards damaging companies.

- Boards should be aware.
  Strategy is increasingly dependent on technology so the stability of the company’s operations is at risk from cyber attack.

- Boards may need to be educated.
  ...and be fully informed and have a complete understanding of the cyber risks faced by the company.

- Robust cyber security needs to be combined with a properly structured control environment.
A SERIOUS ISSUE
64% of Chairs think their Board colleagues take cyber risk very seriously.

WHO OWNS THE RISK?
When asked who owns the cyber risk for their company, Audit Committee Chairs responded with a wide variety of roles.

20% CEO 28% CFO 25% HEAD OF IT

CYBER IS A BUSINESS RISK
56% of respondents said their strategic risk register includes a cyber risk category.

CYBER SAVVY BOARDS
Most Chairs think their Boards are qualified, to some extent, to manage innovation and risk in a digital age.

2% indicated their colleagues were 'barely qualified'
36% think they have 'good skills'
11% think they are well positioned for the digital age

TRAIN YOUR BOARD
75% of respondents had not undertaken any cyber or information security training in the last 12 months and 80% of respondents said none of their Board colleagues had undertaken any either.

Respondents who have done training
Respondents who have not done training
Other board members who have done training
Other board members who have not done training

KNOW YOUR KEY DATA ASSETS

Over a third of Chairs said the main Board has a very clear understanding of what their company’s main information and data assets are.

- Poor understanding (4%)
- Basic understanding (59%)
- Very clear understanding (34%)
- Don’t know (1%)
- N/A (2%)

WHO HAS YOUR KEY DATA ASSETS?

A quarter of respondents said the main Board has a poor understanding of where the company’s key information or data assets are shared with third parties (e.g. suppliers, advisors, customers and outsourcing partners).

UNDERSTAND THE THREAT

40% of Chairs said the main Board does not receive regular threat intelligence from their CIO or Head of Security.

THE IMPACT OF A CYBER ATTACK

Less than half of FTSE 350 Chairs think their main Board has a clear understanding of the potential impact of information and data asset losses.

INFORMATION SHARING

Nearly half of the respondents said their employees are encouraged to share information with other companies in order to combat cyber threats.
Categories of Cyber Business Risk

- **Censure and embarrassment**: This impacts the company’s brand through negative publicity, and can cause a major disruption to strategy. It is most relevant in highly visible industries such as retail, finance, media, or law and can be as a result of hacktivism. Regulated industries may also suffer additional negative publicity as a consequence of subsequent regulatory censure.

- **Sabotage or disruption of business operations**: This most commonly manifests itself as the disruption of services to customers, and sometimes involves blackmail or online businesses. There is also the possibility of cyber terrorism against industries such as energy and utilities, where control systems are connected to the internet.

- **Direct fraud**: Theft of money or digital content by electronic means is most relevant to financial services operations and those whose products can be copied online, such as media and software companies. Examples are the stealing of card numbers to withdraw cash, or copying music.

- **Cyber espionage**: The silent copying of information for commercial purposes is most relevant to industries with high research and development costs, such as high-tech manufacturing, aerospace and software. It can also affect companies competing for high-value contracts in areas like construction or mining. Companies involved in merger and acquisition activity are vulnerable. Typically not reported directly but is common and large-scale.

- **Client loss**: A reduction in revenue can result from customers abandoning and/or suing the company following a loss of service or confidential information. Sectors where companies store information on behalf of customers, such as IT or professional services, or any retail business, are most at risk from client loss.

Adapted from: Guidance Note on Cybercrime, ICA (2013)
A Taxonomy of Cybersecurity

Incentive
The motive to attack

Vulnerability
Can be technical (e.g., lack of a firewall) or human (e.g., employees being tricked by phishing emails)

Four types of target entity
- Public sector
- Private enterprise
- Individuals
- Critical national infrastructure (CNI)

Targets

Four groups of attackers
- Governments
- Enterprises
- Cybercriminals
- Cyberterrorists or 'hacktivists'

Capability
The ability to steal, hijack, impair, or damage

Assets
Data (such as IP, customer records, or classified national secrets)
Systems, which vary in criticality from low (informational Web sites) to high (nuclear monitoring systems)

Raising awareness of Cyber Risk

What is the current level and business impact of cyber risks?
(Is there a plan to address the identified risks?)

How comprehensive is the cyber incident response plan?
(How often is the plan tested?)

How is the executive leadership informed about the current level and business impact of cyber risks?

How many and what types of cyber incidents are detected in a normal week?
What is the threshold for notifying executive leadership?

How does the cybersecurity program apply industry standards and best practices?
Cyber risk vs. business risk

- Cyber liability is a top 5 business risk: 29%
- Cyber liability is a top 10 business risk: 29%
- Cyber liability is not in the top 10 of business risks: 28%
- Cyber liability is the number one or two business risk: 15%

Determining the level of cyber risk

- Formal risk assessment by third party: 22%
- Policy terms and conditions reviewed by a third-party specialist: 20%
- Formal risk assessment by in-house staff: 18%
- Informal or ad hoc risk assessment: 14%
- Formal risk assessment conducted by the insurer: 13%
- Maximum available from the insurance market: 12%
- Other: 2%

Adequacy of coverage

- Hired a third party to conduct an assessment or audit: 26%
- Completed an informal (ad hoc) internal assessment: 21%
- Did not do any type of assessment: 20%
- Intuition or gut feel: 18%
- Completed a formal internal assessment: 15%

Cyber Risk
So what about cyber security governance? Can it help?

Governance 101...

Management
This is about running your business and in IT terms it includes plan, build, run and maintain.

Governance
Is about ensuring the business is run properly and this involves the activities of evaluate, direct and monitor.
Cyber Risk Management

- Includes the utilization of organizational strategies
  - to preserve the integrity of information and corporate intangible assets
- As businesses continue to turn to virtual organizations, connected information systems, and outsourcing (offsite hosting/storage, contract employees, etc.) to drive business strategy, these new ways of doing business increase the vulnerabilities to corporate assets
- When a corporate network, connected to the outside world, becomes compromised, the resulting damage can be tremendous, damages and security breaches to one computer can potentially lead to meaningful financial losses throughout an entire networking community
- What will happen if your computer network goes down or is compromised?
  - What will be the consequences?
  - Have you considered the additional effects of losses to your network that could be incurred down the line?
  - The overall risk management efforts of a company must address these vulnerabilities and scenarios
- proactively

*Cyber Liability Coverage, InsureTrust (2015)*
Assessment of Cyber Risk (i)

• Initial assessment
  – Of the organization's risk profile, and whether it is vulnerable to attack, is crucial
  – Consider external advice as part of the assessment
  – Reports received from external advisors should be clearly written and easily understood by all.

• Risk assessment
  – Carried out across the whole organisation, to assess the overall risk and identify specific areas at greatest risk
  – Internal functions such as HR, finance, legal and marketing may not appreciate the extent to which critical information is at risk (possibly not aware of the potential impact of a cyber attack)

• Risk assessments need to concentrate on
  – Threat to the protection of information, including customer data, and focus on the potential consequences which include losses from a substantial interruption to online transactions
  – Potential for the destruction of corporate value should not be underestimated
Assessment of Cyber Risk (ii)

• Assessment should include
  – the risks of using third party providers and the company’s supply chain
  – Outsourcing can sometimes be a more secure option, but it requires thorough due diligence in advance
  – Service providers may hold a great deal of valuable company information, so adversaries can obtain information without the need to attack a company directly
  – It should be remembered that, whilst companies can outsource activities, the risks, and the consequences, remain with the company

• Risk reports and risk registers
  – provided to the board and audit committee should include full and comprehensive information
  – Reports should reflect a fuller understanding of the impact of a cyber attack, including the wider impact on future strategy
  – As with all information received by the board and board committees, the company secretary has a role in ensuring the quality and quantity of information provided on cyber risk
  – It is essential that the risk function ensures the risks identified are communicated and understood by all areas of the organisation that could be affected by the risks, and that the board’s priorities for mitigating cyber risks are communicated to all business areas
# Organisational Risk

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
<th>Potential Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design and structure—silos and knowledge distribution</td>
<td>Cybersecurity is structured in silos, preventing knowledge exchange.</td>
<td>Exposure to attacks because the majority of associates are unable to recognize attacks, cybercrime and cyberwarfare</td>
</tr>
<tr>
<td>Design and structure—overconfidence</td>
<td>Management misperception of factual state of cybersecurity</td>
<td>Underfunding, limited management attention, resulting exposure to attacks</td>
</tr>
<tr>
<td>Design and structure—interfaces</td>
<td>Deficiencies in cooperating to recognize and respond to attacks and breaches</td>
<td>Managing cybersecurity is fragmented, leaving gaps that may be exploited.</td>
</tr>
<tr>
<td>Governance, compliance and control—control deficiencies</td>
<td>Lack of governance and compliance provisions, insufficient cybersecurity controls</td>
<td>Insufficient preparation, recognition, investigation and response to attacks and breaches; increased rate of human error</td>
</tr>
<tr>
<td>Governance, compliance and control—overcontrol</td>
<td>Overly complex governance and compliance system, controls addressing even minute details</td>
<td>Rigid control structure creates opportunities for attacks and breaches.</td>
</tr>
<tr>
<td>Culture—trust</td>
<td>The culture of trust partially or completely negates cybercrime and cyberwarfare.</td>
<td>Implicit or explicit trust may be exploited in social and technical attacks.</td>
</tr>
<tr>
<td>Culture—vigilance</td>
<td>Individual vigilance is reduced in the context of governance, compliance and control.</td>
<td>Attacks and breaches may not be recognized in a timely manner.</td>
</tr>
<tr>
<td>Culture—denial</td>
<td>Attractiveness in terms of attacks is denied a priori.</td>
<td>Factual attacks may not be recognized or misinterpreted.</td>
</tr>
</tbody>
</table>
# Social Risk

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
<th>Potential Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>People—skills</td>
<td>People have insufficient skills to understand and enact cybersecurity.</td>
<td>Cybersecurity concepts and actions cannot be fully implemented, leading to an increased risk of attacks and breaches.</td>
</tr>
<tr>
<td>People—rules</td>
<td>People are reluctant to accept and internalize cybersecurity rules.</td>
<td>Deficiencies, growing number of vulnerabilities and threats, more attack opportunities.</td>
</tr>
<tr>
<td>People—compliance</td>
<td>People inadvertently or deliberately commit or allow security breaches.</td>
<td>Attacks induced by people-based weaknesses, collusion or internal attacks, corrupt practices, infiltration.</td>
</tr>
<tr>
<td>Culture—leadership and responsibility</td>
<td>Personal responsibility may be diminished (or exaggerated) as a function of the prevailing style of leadership, e.g., quasi-military vs. laissez-faire</td>
<td>The under- or overemphasis on personal responsibility may lead to dysfunctional behavior and a corresponding increase in the risk of attacks or breaches.</td>
</tr>
<tr>
<td>Culture—societal context</td>
<td>Societal context adverse to, or largely ignorant of, cybersecurity and cyberwarfare</td>
<td>Society at large, or general culture is not conducive to individual adoption of cybersecurity thinking.</td>
</tr>
<tr>
<td>Culture—human error</td>
<td>High error potential or frequency due to various factors</td>
<td>Attacks or breaches are more frequent due to human error.</td>
</tr>
<tr>
<td>Human factors—complexity</td>
<td>Cybersecurity is too complex and therefore dysfunctional.</td>
<td>Failures of flaws and increased attack/breach potential.</td>
</tr>
<tr>
<td>Human factors—convenience</td>
<td>People disregard or abandon cybersecurity in favor of convenience.</td>
<td>Convenience-based misuse or inadequate use of IT and systems, with resulting vulnerabilities and threats.</td>
</tr>
<tr>
<td>Human factors—discontinuities</td>
<td>Individual (management) disposition toward negating aspects of cybersecurity</td>
<td>Ignorance, prejudice, short-termism, storming, bounded rationality and other factors increase the risk of attacks/breaches.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
<th>Potential Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human factors—discontinuities</td>
<td>Individual (management) disposition toward negating aspects of cybersecurity</td>
<td>Ignorance, prejudice, short-termism, storming, bounded rationality and other factors increase the risk of attacks/breaches.</td>
</tr>
<tr>
<td>Emergence—habitual behavior</td>
<td>Strong habits in people prevent improvements/implementation of cybersecurity.</td>
<td>Behavior patterns do not match the desired behavior patterns, thus increasing the security risk.</td>
</tr>
<tr>
<td>Emergence—paradigm shifts</td>
<td>Societal/cultural paradigms of IT use shift</td>
<td>Fundamental changes to the way in which IT is used increase the security risk.</td>
</tr>
<tr>
<td>Emergence—interpretive bias</td>
<td>Processes in cybersecurity are misinterpreted or not fully understood</td>
<td>Erroneous interpretation increases the number of vulnerabilities and threats.</td>
</tr>
</tbody>
</table>

---

**CRMS Global**  
Center for Risk Management & Sustainability  
**IFC**  
International Finance Corporation  
**World Bank Group**  
**cENSEI**  
**ERMA**  
Enterprise Risk Management Academy
## Technical Risk

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
<th>Potential Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Architecture—de-perimeterization</strong></td>
<td>Significant parts of the IT architecture are de-perimeterized.</td>
<td>Decentralized, mobile and home environments are more vulnerable and less amenable to organizational control.</td>
</tr>
<tr>
<td><strong>Architecture—third party</strong></td>
<td>Parts of the IT architecture are operated by third parties (Platform as a Service [PaaS], Infrastructure as a Service [IaaS]).</td>
<td>Cybersecurity shifts to a contractual basis (indirect control only), potentially increasing the risk of attacks and breaches.</td>
</tr>
<tr>
<td><strong>Architecture—exposed areas</strong></td>
<td>Parts of the overall architecture have a high risk/exposure to attacks and breaches.</td>
<td>Attacks focus on exposed areas (e.g., legacy, unpatched, dual persona use)</td>
</tr>
<tr>
<td><strong>Application layer—cloud/Software as a Service [SaaS]</strong></td>
<td>Critical applications are operated in the cloud and/or contracted as SaaS.</td>
<td>High risk of vendor side vulnerabilities and related attacks (see also Infrastructure—networks)</td>
</tr>
<tr>
<td><strong>Application layer—zero-day</strong></td>
<td>Zero-day exploits exist for critical applications.</td>
<td>High risk of targeted attacks using zero-day points of entry</td>
</tr>
<tr>
<td><strong>Application layer—malware</strong></td>
<td>Applications are altered or corrupted by various types of malware.</td>
<td>High risk of temporary or permanent open attack vectors and related impacts (see previous)</td>
</tr>
<tr>
<td><strong>Operating system layer—legacy</strong></td>
<td>Legacy versions of operating systems are needed for certain applications.</td>
<td>High risk of vulnerabilities arising from expired support/lock of patches for legacy operating systems, often favored as attack vector</td>
</tr>
<tr>
<td><strong>Operating system layer—zero-day</strong></td>
<td>Zero-day exploits exist for operating systems.</td>
<td>High risk of attacks using zero-day points of entry</td>
</tr>
<tr>
<td><strong>Operating system layer—security model</strong></td>
<td>Operating system security model inadequate for cybersecurity.</td>
<td>Gaps or weaknesses in the security model prevent secure configuration, high risk of known weaknesses being exploited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
<th>Potential Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure—networks</strong></td>
<td>Topology (wide area network [WAN]/LAN/metropolitan area network [MAN]) weaknesses and structural vulnerabilities</td>
<td>Parts of the combined network topology are susceptible to attacks and breaches; see also components and firmware.</td>
</tr>
<tr>
<td><strong>Infrastructure—components and firmware</strong></td>
<td>Network components and firmware contain vulnerabilities, patching may be infrequent, legacy component use</td>
<td>High risk of attacks based on known weaknesses in component firmware, often indirectly</td>
</tr>
<tr>
<td><strong>Infrastructure—hardware</strong></td>
<td>Hardware modification (including vendor-side)</td>
<td>Risk of attacks based on replaced or modified hardware, including cyberwarfare</td>
</tr>
<tr>
<td><strong>Technical infrastructure—embedded systems</strong></td>
<td>Vulnerabilities in embedded systems, hardware or software modification</td>
<td>High risk of attacks based on known weaknesses in embedded systems; modified embedded components may be used in cyberwarfare</td>
</tr>
<tr>
<td><strong>Technical infrastructure—management systems</strong></td>
<td>Vulnerabilities in control and management systems (e.g., SCADA)</td>
<td>High risk of attacks based on known weaknesses in control and management systems; APTs may be used in cyberwarfare</td>
</tr>
</tbody>
</table>
Cyber Risk Management Concepts (i)

• Incorporate cyber risks into existing risk management and governance processes
  – Cybersecurity is about more than implementing a checklist of requirements - Cybersecurity is managing cyber risks to an ongoing and acceptable level
• Begin cyber risk management discussions with your leadership team
  – Communicate regularly with those accountable for managing cyber risks
  – Enhance your awareness of current risks affecting your organization and associated business impact
• Implement industry standards and best practices
  – Don’t rely on compliance
  – A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems
  – It informs processes of new threats and enables timely response and recovery
• Evaluate and manage specific cyber risks
  – Identifying critical assets and associated impacts from cyber threats is essential to understanding an organization’s risk exposure – e.g. financial, competitive, reputational or regulatory
  – Risk assessment results are essential for identifying and prioritizing specific protective measures, allocating resources, informing long-term investments, and developing policies and strategies to manage cyber risks
• Provide oversight and review
  – Executives are responsible for managing and overseeing enterprise risk management
  – Cyber oversight activities include the regular evaluation of cybersecurity budgets, IT acquisition plans, IT outsourcing, cloud services, incident reports, risk assessment results, entity-level policies etc.
• Develop and test incident response plans and procedures
  – Even a well-defended organization will experience an incident at some point
  – When you have a breach, a CEO should be prepared to answer 'What is our Plan B?'
  – Cyber incident response plans should be exercised regularly

• Coordinate cyber incident response planning across the enterprise
  – Early response actions can limit or even prevent possible damage and require coordination
  • with your organization’s leaders and stakeholders
  – This includes your Chief Information Officer, Chief Information Security Officer, Chief Security Officer, business leaders, continuity planners, system operators, general counsel, public affairs, and human resources
  – Integrate cyber incident response policies and procedures with existing disaster recovery and business continuity plans

• Maintain awareness of cyber threats
  – Situational awareness of an organization’s cyber risk environment involves timely detection of cyber incidents, along with the awareness of current threats and vulnerabilities specific to that organization and associated business impacts
  – Analyzing, aggregating, and integrating risk data from various sources and participating in threat information sharing with partners helps organizations identify and respond to incidents quickly and helps organizations to ensure that protective efforts are commensurate with the risks

Questions for Boards and CEOs

Protection of key digital assets is critical

- How confident are you that your digital assets are properly managed and are safe from cyber threats?
- Are you clear on who the key actors are to be engaged?
- Do you have a full picture of the potential risks to reputation, brand value, and impact on business sustainability and reputation, etc.?

Explore who might compromise your digital assets and why is critical

- Do you receive regular intelligence from the CIO/CISO on attackers, methods, and motivations?
- Do you encourage technical staff to exchange information with other companies in the same sector to benchmark, learn and identify?

Proactive management of cyber risk at board level is critical

- Are key information assets assessed for vulnerability?
- Is cyber risk responsibility allocated appropriately?
Corporate Governance of Cyber Risk

Board
Make protecting your digital assets a board priority and responsibility

Regular digital/cyber risk reports
All board members
Request assurance

Assurance findings
Refine cyber stance

Business
Implement a digital/cyber risk management regime

CEO, CIO, CTO, CISO etc.

Corporate governance
Provide assurance that the digital/cyber risk management is effective

Non-executive directors, audit and risk committee heads

Cyber Risk Management – A Board Level Responsibility, Department for Business Innovation and Skills (2012)
Cyber Governance …

- Is both preventive and corrective
- Determines the processes, procedures and structures needed to deal with actual incidents
- Cyber governance principles and provisions must be reasonably flexible
  - Allow for the fact that attacks are often unconventional
  - Generally against the rules, and most often designed to circumvent exactly those procedures and common understandings within the enterprise that keep the business
Cyber Governance

Third Line – Internal Audit
- Internal controls testing
- Cybersecurity compliance
- Formal risk acceptances
- Investigation/forensics

Second Line – Risk Management
- Threats, vulnerabilities, risk
- Formal risk evaluation
- Business impact analysis (BIA)
- Emerging risk

First Line – Management
- Control self-assessments (CSAs)
- Attack/breach penetration testing
- Functional/technical testing
- Social/behavioural testing
- Regular management review
Cyber Risk Governance Framework

• The foundation of a cyber resilient organization is a cyber risk governance framework that is
  –Built into the larger enterprise-wide risk management framework
  –Covers the organization’s day-to-day activities

• Cyber resilient organizations are those that have
  –Cyber risk expertise within their senior management ranks and their boards
  –A detailed action plan to respond to cyber events (e.g., attacks, system breaches, etc.)
Cyber Risk Governance

An effective risk governance framework should include:
- a cyber risk governance committee
- a cyber risk oversight committee, and
- a cyber risk operations team

Each of these should have clear accountabilities, responsibilities, operating processes, and reporting lines.
Cyber Risk Governance Roles

Executive management
- Cyber Risk Oversight Committee
- Cyber Risk Governance Committee
- Cyber Risk Operations Team

Assesses existing and emerging cyber threats, and the effectiveness of response to threats – it directly oversees the cyber risk operations team

Who?
- IT team
- Business support teams
- Business teams

Works directly with the executive management team to develop the cyber risk strategy, and informs and seeks input from the board

Who?
- Chief Operating Officer
- Chief Risk Officer
- Head of security
- Heads of business lines and certain functional areas (such as business continuity planning, legal, risk, compliance, and regulatory)

Who?
- Managers with operational experience in fraud, networks, information security, and corporate security
- Security operations centre
Cyber Risk Governance Responsibilities

Executive Management
- Cyber Risk Oversight Committee
- Cyber Risk Governance Committee
- Cyber Risk Operations Team

Responsibilities
- Assessing the active risks the organization faces
- Evaluating the effectiveness of the cyber risk operations team
- Identifying emerging threats and strengthening internal controls to improve protection of information assets
- Determining how business changes affect the firm's cyber perimeter, e.g., new service offerings, suppliers, vendors, or business partners
- Monitoring the status of updates and configuration changes to critical systems
- Monitoring metrics that provide visibility on the performance of key elements of the cybersecurity program
- Overseeing employee training programs
- Reviewing new regulatory and compliance requirements

Responsibilities
- Collaborating with executive management to develop the cyber risk strategy
- Identifying critical information assets
- Setting the budget for cyber risk management and ensuring appropriate investment in related cyber risk awareness training
- Monitoring the firm's cyber risk position and reporting to executive management and the board
- Reviewing reports from the cyber risk oversight committee and cyber risk operations team to help prioritize emerging threats
- Reassessing cyber risk strategy periodically to adapt to changes in the risk landscape

Other Responsibilities
- Serving as the first line of defense for detecting and responding to cyber events
- Compiling real-time intelligence from all the groups that monitor cyber threats
- Producing reports for the cyber risk oversight and governance committees on number and type of cyber events, origin and duration of events, targeted assets, attempted frauds, cyber risk mitigation enhancements, and comparison of events to industry trends
Cyber Risk Oversight Principles

Principle 1: Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue

Principle 2: Directors should understand the legal implications of cyber risks as they relate to their company’s specific circumstances

Principle 3: 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

Principle 4: Directors should set an expectation that management establish an enterprise-wide cyber-risk management framework with adequate staffing and budget

Principle 5: 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
Cyber Governance Lifecycle Considerations
The PRECIOUS Way To Cyber Security

• Priorities and Strategies Setting
• Risk Evaluation
• Cyber Risk Management Program
• Implementation and Organization
• Upgrading and Strengthening
The Social Media Game

- Goals
- Audience
- Message
- Enablers
In dealing with people, let us

ENLIGHTEN

• Engage
• Nonpartisan
• Listen
• Investigate
• Gratitude
• Humility
• Truth
• Empathy
• Nationhood
Salamat Kaayo!
Thank you!
Salamat!

Your Proven Partner in Strategy and Learning

CenSEI designs and delivers strategies, knowledge, and solutions for more potent direction and performance of your organization.

(632) 531 1182 or (+63) 919 395 9215