Why Cybersecurity needs to be a topic of boardroom agenda

Raj Kumar
Why Cybersecurity needs to be a topic of boardroom agenda

• Set management direction and gain support
• Understand business risk
• Protect brand and reputation
• Meet Legal and regulatory requirements
• Implement security awareness
• Allocate Budget and resources
• Establish organisation structure
• Foster collaboration between business units and technology team
• Develop strategic response to cyber threats
Impact of cyber threats on business profitability

• Information security is what keeps valuable information asset ‘free of danger’ or threat

• Businesses need to:
  • Know what are the threat and vulnerabilities that can affect their business
  • Treat and manage the risk to information and physical asset
  • Ensure confidentiality, integrity and availability is preserved
  • Avoid, prevent, detect and recover from incidents
  • Securing people, processes and technology that are used
  • Protect the interest of customers, shareholders and partners
  • Business case to convince the senior management to invest and allocate resources for security management
Why Cyber security a must for business

• To protect brand and reputation
• To protect customer’s confidential information
• To ensure accuracy and correctness of information
• To ensure availability of information and system
• To meet legal and regulatory requirements
• To raise customer and third party confidence
• To understand risks and manage incidents
• To ensure business continuity and manage crisis
Core elements of cybersecurity for businesses

**People**
- Staff
- Management
- Suppliers
- Shareholders
- Customers
- Contractors
- Consultants
- Regulators

**Process**
- Policies
- Procedures
- Business Processes
- Work flow
- Best Practices
- Guidelines

**Technology**
- Cabling, data/voice network equipment, Telco services
- Mobile devices, desktop computers, and servers, data storage devices
- OS and application software
- Documents
- Locks
- Barriers
- CCTV
- Card Access
Definition: Resilience and Cyber - Resilience

Resilience
ITU-T SG17 defines resilience as the "Ability to recover from security compromises or attacks."
Complementing this focus, a recent ITU report on 'Resilient Pathways' defines resilience as "The ability of a system or a sector to withstand, recover, adapt, and potentially transform in the face of stressors such as those caused by climate change impacts".

b. Cyber - security
This concept refers to the discipline of ensuring that ICT systems are protected by attacks and incidents, whether malicious or accidental, threatening the integrity of data, their availability or confidentiality, including attempts to illegally 'exfiltrate' sensitive data or information out of the boundaries of an organisation.

c. Data protection
This notion refers to the tools and processes used to store data relevant to a certain ICT system or environment, as well as recover lost data in case of an incident - be it fraudulent, accidental or caused by a natural disaster.
Definition: Resilience and Cyber - Resilience

Cyber Resilience is the subset of business resilience

Source: EY-global-information-security-survey-2016-pdf
Ensuring resilience

A brainstorming session on board principles with the World Economic Forum Working Group on Cyber Resilience
Cyber Risk Framework

Source: WEF IT Partnering Cyber Resilience Guidelines 2012
**From the board room**

<table>
<thead>
<tr>
<th>Dark Gray</th>
<th>Light Blue</th>
<th>Orange</th>
</tr>
</thead>
<tbody>
<tr>
<td>We need to develop a coherent cyber resilience strategy</td>
<td>We need to know what our critical information assets are</td>
<td>We need a cyber smart workforce and partner network</td>
</tr>
<tr>
<td>We need to embed good practices across our organization</td>
<td>We need to communicate and understand more effectively across the organization</td>
<td>We need to understand how we will respond and recover from attack more effectively</td>
</tr>
</tbody>
</table>
Ensuring resilience

Cyber Risks
- Cyber Extortion
- Concerted Cyber Attack
- Large Scale Data Breach
- System Infiltration

Threat Agents
- Hacktivists
- Insiders
- Cyber Criminals
- Corporations
- Cyber Terrors
- Nation States
- Individuals

Threats
- Phishing
- Denial of Service
- Ransomware
- Malicious Code
- Web Based Attacks
- Botnets
- Spam
- Exploit Kits
- Data Breaches
- Physical
- Insider
- Information Leakage
- Identity Theft
- Cyber Espionage

Pillars of Resilience
- Anticipate
- Withstand
- Recover
- Evolve
3 high-level components of cyber resilience

**Sense**

- Ability of organisation to detect cyber threats
  - Using cyber intelligence, analytics and active defence
  - Early warning of risk of disruption

**Resist**

- Determine how much risk an organisation can take across its ecosystem
  - 3 lines of defence
    - Executing controls on daily operations
    - Deploying monitoring function – internal controls, legal department, risk management
    - Internal audit

**React**

- If Sense fails, the organisation failed to see the threat coming, there is a breakdown in React (the controls were not strong enough)
  - Organisation need to be ready for disruption
  - Ready with incident response capabilities
  - Ready to manage crisis
  - Ready to preserve evidence
  - Investigate the breach to satisfy customers, regulators, investors, law enforcement and the public
  - Bring the business back to normal state
  - Learn from what happened and improve cyber resilience.

Source: EY-global-information-security-survey-2016-pdf
Ensuring resilience

Source: EY-global-information-security-survey-2016-pdf
Ensuring resilience

<table>
<thead>
<tr>
<th></th>
<th>Sense (See the threats coming)</th>
<th>Resist (The corporate shield)</th>
<th>React (Recover from disruption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where do organizations</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>place their priorities?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Where do organizations</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>make their investments?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Board and C-level</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>engagement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality of executive or</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>boardroom reporting</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
With regard to Critical Security Controls, CSC “...failure to implement all of the controls that apply to an organization’s environment constitutes a lack of reasonable security.”
Kamala Harris, Attorney General, CA
Breach Report 2016
ITU : I Thank U