The Ten Commandments for Cyber Resilience

Present by Jude Pereira
[Managing Director]
Do I really need to automate provisioning? Only few people join/leave in a month!!

What solution areas should I target first? Which application?

Which product would work best for me?

Not sure if I have right policies and process to automate via an IAM system

All vendors say they can do. Who is best for me?
AGENDA ......

- Role of a CISO
- Introducing CYBER RESILIENCE
- CYBER RESILIENCE Frameworks
- The TEN Commandments for CYBER RESILIENCE
Role of CISO & Mindset
IBM’s 2016 Chief Information Security Officer Study revealed the changing role of the CISO

<table>
<thead>
<tr>
<th>How they differ</th>
<th>Influencers</th>
<th>Protectors</th>
<th>Responders</th>
</tr>
</thead>
<tbody>
<tr>
<td>have a dedicated CISO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>have a security/risk committee</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>have information security as a board topic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>use a standard set of security metrics to track their progress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>focused on improving enterprise communication/collaboration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>focused on providing education and awareness</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security challenges are a complex, four-dimensional puzzle ...

... that requires a new approach
Introducing CYBER RESILIENCE
“... the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents...”

• Cyber resilience involves a change in mindset whereby you look to identify how secure the business needs to be in order to survive.
BARRIERS TO CYBER RESILIENCE?

• Lack of awareness (board level down)
• Silo thinking (“it’s an IT problem”)
• Narrow focus on regulatory compliance, not risk
• Confusion about what “good” looks like
• Cyber resilience demands a “whole system” view (technology and people)
  o Cyber resilience has to be part of your organisational culture...
RISKS TO VALUE

• Loss of corporate reputation and customer trust
• Financial loss and reduced productivity
• Regulatory fines
• Reduced competitive advantage through IP theft
• (Damaged personal reputations)
CYBER RESILIENCE FRAMEWORKS
Cyber Resilience Review and the Framework

Relationship between DHS' Cyber Resilience Review and the NIST Cybersecurity Framework *CRR to NIST CSF crosswalk available*

- **Identify Services**
  - Identify and prioritize services

- **Create Asset Inventory**
  - Identify assets, align assets to services, and inventory assets

- **Protect & Sustain Assets**
  - Establish risk management, resilience requirements, control objectives, and controls

- **Disruption Management**
  - Establish continuity requirements for assets and develop service continuity plan

- **Cyber Exercise**
  - Define objectives for cyber exercise, perform exercises, and evaluate results

**Process Management and Improvement**
Cyber Resilience Assessment Framework
## Cybersecurity Resilience Maturity Framework

<table>
<thead>
<tr>
<th>Maturity Descriptor</th>
<th>Employment of Security Controls</th>
<th>Security Tailored to Mission</th>
<th>Participate in Information Sharing (threat/vul.)</th>
<th>Response to Cyber Threats</th>
<th>Resilience to Cyber Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 5: Resilient</td>
<td>Augment CSC Based on Mission</td>
<td>Mission Assurance Focused</td>
<td>Real Time Response to Inputs</td>
<td>Anticipate Threats</td>
<td>Operate Through Sophisticated Attack</td>
</tr>
<tr>
<td>Level 4: Dynamic</td>
<td>Augment CSC Based on Mission</td>
<td>Mission Focused</td>
<td>Real Time Response to Inputs</td>
<td>Rapid Reaction To Threats</td>
<td>Able to respond to Sophisticated Attack</td>
</tr>
<tr>
<td>Level 3: Managed</td>
<td>CSC Integrated and Continuously Monitored</td>
<td>Partially Mission Focused</td>
<td>Respond to Information Inputs</td>
<td>Respond to Attacks After the Fact</td>
<td>Protection against Unsophisticated Attack</td>
</tr>
<tr>
<td>Level 2: Performed</td>
<td>Foundational/ Critical Security Controls (CSC) Implemented</td>
<td>Mission Agnostic</td>
<td>Inconsistent Response to Information Inputs</td>
<td>Respond to Attacks After the Fact</td>
<td>Some Protection Against Unsophisticated Attacks</td>
</tr>
<tr>
<td>Level 1: No Resilience</td>
<td>Inconsistent Deployment of Security Controls</td>
<td>None</td>
<td>None</td>
<td>No Response</td>
<td>Susceptible to Unsophisticated Attacks</td>
</tr>
</tbody>
</table>

**Step 1: Implement CSC Baseline**

**Step 2: Address Sophisticated Attacks**
Cyber Resilience Controls

1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software
4) Continuous Vulnerability Assessment and Remediation
5) Controlled Use of Administrative Privileges
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports
10) Data Recovery Capability
11) Secure Configurations for Network Devices
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Security Skills Assessment and Appropriate Training to Fill Gaps
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises
TEN Commandments for CYBER RESILIENCE
Ten Commands For Cyber Resilience

01. Make security personal to your business – understand your business and how security can be built into IT.

02. Baseline your security regularly to understand your state of readiness, so that you can interpret the symptoms that can lead to a security incident.

03. Get executive and board engagement – The human element of Cyber Risk is likely to be higher outside your IT department than within it. With executive leadership buy-in, you can make your security culture all-inclusive.

04. What is your resilience plan? Security incidents happen every day. How do you identify the important incidents and ensure the business remains effective and up-and-running under all circumstances?

05. Education – from board to new hire, it’s essential that everyone understands that they are responsible and accountable. They need to know what part they play in the bigger picture.
06 Do the basics well – leverage government and industry guidelines. This includes aspects such as patching and good user-level access management.

07 Plan for today and scale for the future – for example, BYOD is here to stay. Hence, we must stop applying quick fixes to such issues, unless they are aligned to a longer-term strategy.

08 Start small, but think big. Information protection is a long-term project, but we need to start where we will add the most business value and then continue to expand where there is further, long-term business value. This can include, for example, the supply chain and how we interact with our wider network of vendors and partners. The key here is to think big but have a maturity plan, which must be linked to strategic business value and growth.

09 Be accountable – understand what the regulatory, legislative and peer-to-peer controls are that you need to adhere to. Make sure you have a clearly defined owner for each of these and an executive sponsor.

10 Don’t wait for it to happen – test your processes, procedures and people regularly. Make sure you have clearly defined lifecycles that reflect changes in business strategy, technology use and culture. Make sure your strategy is current and effective for the business and the risks.
Summary of Cyber Resilience
"It is not the answer that enlightens, but the question."

"The most important thing is not to stop questioning."

Any Questions?