Workshop C (Business) Cybersecurity for Business Leaders
Making Sure your Company is Ahead of the Cyber Curve

James Turgal
James Turgal

Visionary leader with proven skill in developing a culture of leadership, driving solutions to global problems, while using intelligence and strategy to drive operations. A 20 year Senior Executive federal law enforcement official with expertise in directing and managing worldwide national security, cyber and criminal operations and investigations. Called upon by FBI and Intelligence Community officials to create solutions and implement change that is tangible and sustainable. Previously designated as the FBI's Chief Human Capital Officer, and selected as the Executive Assistant Director for the Information Technology Branch, responsible for all Enterprise Information Technology for the FBI's global operations.

**Current: Deloitte**

Managing Director

**Former: FBI**

Executive Assistant Director - *Responsible for all enterprise information technology covering FBI operations worldwide.*

Special Agent in Charge - *Directed all FBI investigative and security operations for counter-terrorism, counter-intelligence, cyber, criminal, foreign intelligence, counter-proliferation, economic espionage and International criminal operations in Mexico and South America.*
# Cybersecurity for Business Leaders

1. **Security Threat Landscape**

   **Objective:** Identify the impact adversaries could have on your organization.

   20 min

2. **Resilience and Response**

   **Objective:** Identify and match the success factor definitions to the appropriate area on the pinwheel.

   20 min

3. **Board Room Discussions**

   **Objective:** Discuss the top questions we see boards discussing. How many of the questions have been raised or discussed within your boardroom?

   20 min
## Security Threat Landscape

Who is my greatest threat and what are they going after?

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Financial theft / fraud</th>
<th>IP / data theft / data loss</th>
<th>Business disruption</th>
<th>Critical Infrastructure Destruction</th>
<th>Reputation damage</th>
<th>Regulatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organized Criminals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hactivists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nation states</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insiders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third parties</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individual hackers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **High Impact**
- **Moderate Impact**
- **Low Impact**
Cyber Resilience and Incident Response

After a threat is detected, how would I respond?

**Strengths**

- Educate executives on crisis communication plans and their associated responsibilities. Setting tone at the top of organizational hierarchies has cascading impacts.
- Carefully select CIR team members and confirm they have the requisite skills and experience to perform responsibilities outlined in the plan.
- Prevent your plans from becoming “shelf ware” by training your CIR team periodically.
- Involve business operations in Cyber Incident Response planning so that mission critical processes and systems are available when crises occur.

**Challenges/Gaps**

- Prepare ahead and incorporate relevant considerations into the CIR plan; Determining legal, regulatory, and compliance issues in the midst of a crisis is a bad place to be.
- Simple, flexible and distributed plans provide guidance to responsible parties throughout the organization. Understand where external help is needed and have contracts and capabilities in place beforehand.
- Organizations should embrace technologies that enable operational resiliency and proactive detection and response capabilities.
- Simulate realistic incidents regularly. By exercising the plan, organizations can build “muscle memory” and respond more effectively and consistently.
Top Questions Boards are Facing
How do I deal with the board?

- Do the board and C-suite demonstrate due diligence, ownership and effective management of cyber risk?
- As a technology or data entity, how does the organization protect both Information Technology and Operational Technology?
- Have we established an appropriate cyber risk escalation framework that includes BOD risk appetite and reporting thresholds?
- Is the IT infrastructure focused on, and investing in, the right things? Is resilience being built into the networks and data flow?
- How do our cyber security program and capabilities align to industry standards and peer organizations?
- Do we have an organization-wide cyber-focused mindset and cyber-conscious culture?
- What has management done to protect the organization against third-party cyber risks, both upstream and downstream from the organization?
- Can we rapidly contain damages and mobilize diverse response resources should a cyber-incident occur?
- How do we evaluate the effectiveness of our organization’s cyber security program?
- Are we helping to protect our industry, the nation and the world against cyber risks by taking a holistic approach to information sharing?

Status:
- Not yet Discussed
- Active Conversations
- Briefly Discussed
- Discussed and Resolved