SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

Does the Transit Industry Understand the Risks of Cybersecurity and are the Risks Being Appropriately Prioritized?

Scott Belcher, JD, MPP
Terri Belcher
James Grimes
Lusa Holmstrom
Andy Souders

Key Take-Aways for Board Members

- A cybersecurity breach can impact the financial viability, operational capability, and reputation of the organization.
- Every agency is at risk of a cybersecurity breach, regardless of size.
- Cybersecurity is an enterprise risk management issue, not solely a technology issue, and the Board should be regularly briefed on how the organization is managing all enterprise risks, including cybersecurity. As such, cybersecurity should be part of every board's agenda.
- The board has a fiduciary obligation to ensure the organization is cognizant of the threat posed by a cybersecurity breach, is aware of the organization's vulnerabilities, and has a plan to address them.
- The board should ensure that the organization has cybersecurity insurance or is capable of self-insuring against a cybersecurity breach.

Key Take-Aways for Executive Leadership

- A cybersecurity breach can impact the financial viability, operational capability, and reputation of the organization.
- Every agency is at risk of a cybersecurity breach, regardless of size.
- Cybersecurity is an enterprise risk management issue, not solely an IT issue.
- Executive leadership has a fiduciary obligation to ensure that the organization is cognizant of the threat posed by a cybersecurity breach, is aware of its vulnerabilities, has internal controls in place to manage them, and keeps the board apprised as part of every board meeting.
- Executive Leadership should encourage collaboration with other agencies through industry trade associations and other supporting organizations to become stronger together in the cybersecurity domain.
- Executive Leadership should ensure that the organization is following the recommendations set forth in the Transportation Security Administration (TSA), *Information Circular IC-2021-01, Enhancing Surface Transportation Cybersecurity TSA Circular for Surface Transportation,* specifically:
    - Designate a Cybersecurity Coordinator
    - Report Cybersecurity Incidents
    - Implement a Cybersecurity Incident Response Plan
    - Perform a Cybersecurity Vulnerability Assessment
- Executive Leadership should ensure that the organization has written cybersecurity policies and procedures in place and is following them.
- Executive Leadership should be aware of the role that their part of the organization must play in preventing and responding to a cybersecurity attack.
- Executive Leadership should ensure that the organization has cybersecurity insurance or is capable of self-insuring against a cybersecurity breach.
- Executive Leadership should be aware of any federal, state, or local cybersecurity requirements impacting the organization and ensure that the organization follows them.

- Executive Leadership should be aware of the cybersecurity resources available to the organization and avail themselves of them as appropriate.

Guidance for Technology Professionals

The objective of cybersecurity is to protect the entire infrastructure of an agency, encompassing both Information Technology (IT) and Operational Technology (OT) environments, from unauthorized access and malicious threats. Cyber resilience assumes that when an agency experiences a cyber event, it can sustain operations and recover rapidly, minimizing downtime and impact on customers. This includes developing effective response strategies and recovery plans to restore functionality and maintain continuity. Cybersecurity preparedness involves implementing proactive measures to identify, protect, and detect vulnerabilities and risks within an agency's infrastructure, including on-premise and cloud systems, agency operated hardware and software, and vendor operated hardware and software. As specifically addressed in the study and reported in Section IV Findings, the authors recommend the following:

Cyber Resilience

- **Cybersecurity Assessments** – Conduct regular cybersecurity assessments of preparedness and resilience to evaluate the Agency's preparedness and recovery capabilities. Use the findings to close critical gaps and drive continuous improvements in prevention, response processes, and recovery plans.

- **Disaster Response Planning and Testing** – Develop and maintain a comprehensive Disaster Response plan and business continuity strategies, and regularly test them through tabletop and partial data recovery exercises, ensuring critical systems and applications can be restored promptly with minimal disruption to operations.

- **Cybersecurity Incident Response (IR) and Testing** – Develop and maintain a comprehensive IR plan that aligns with agency recovery objectives. Integrate IR playbooks with pre-defined actions for various cyber scenarios, ensuring quick mobilization and coordination across teams during incidents and regularly test them through tabletop and partial data recovery exercises.

Cybersecurity Preparedness

- Continuous Employee Cybersecurity Training – Provide ongoing, role-specific training programs focused on phishing detection, secure practices, and awareness of emerging threats, ensuring personnel are equipped to recognize and respond to security risks.

- Comprehensive Log Management – Implement centralized logging mechanisms that aggregate, correlate, and analyze data from various sources in real time. Maintain backup protocols to secure essential logs for forensic investigations and compliance requirements.

- Vendor Management and Assessment – Execute continuous security assessments of third-party vendors, focusing on their compliance with security standards and adherence to risk management policies. Incorporate third-party risk management frameworks to evaluate vendor security postures systematically. Review existing contracts to ensure that vendors are maintaining adequate cybersecurity hygiene and address cases in which they are not. Ensure that all new contracts have cybersecurity provisions that require an appropriate level of cybersecurity hygiene and protections for the agency.

Although it was not specifically asked as part of the survey, the authors recommend the additional Cybersecurity Preparedness objectives to further reduce risk:

- **Multi-Factor Authentication (MFA)** – Enforce MFA for all critical systems, particularly those with privileged access, to mitigate risks associated with unauthorized access and credential theft.

- **Patch Management and Vulnerability Scanning** – Establish automated patch management to ensure timely application of patches and updates, addressing known vulnerabilities, and reducing the exploitable surface. Conduct regular internal and external vulnerability scans using advanced tools and manual analysis to identify and prioritize remediation actions.

- **Penetration Testing and Adversarial Simulation** – Implement a continuous penetration testing program that simulates real-world attack scenarios instead of a "one and done" annual approach. Try to mimic adversary tactics, techniques, and procedures to identify potential weaknesses in response protocols.

- **Network Segmentation of IT and OT Environments** – Architect and implement strict segmentation protocols within and between IT and OT networks to contain threats, prevent lateral movement, and safeguard critical operational assets.

- **Advanced Anti-Virus and Endpoint Detection and Response (EDR)** – Deploy anti-virus solutions with heuristic and behavioral capabilities to detect and prevent sophisticated threats. Integrate EDR tools to provide continuous endpoint monitoring, enabling proactive threat hunting and automated response to malicious activities.

- **Principle of Least Privilege (PoLP)** – Enforce PoLP by rigorously controlling access rights, ensuring users, systems, and applications only have permissions necessary for their functions, reducing attack vectors.