Oversight of Cybersecurity Matters in the Boardroom: Emerging Standards, Questions to Ask, and Best Practices

Stephanie Ziertenn
Associate Counsel
Federal Reserve Bank of Boston
Cybersecurity Landscape

Major Data Breaches (e.g., OPM, IRS)

Data Breach Notification Laws

Derivative Suits

Federal Legislation

Enforcement Actions (e.g., FTC, SEC)
Cybersecurity Risk Environment

Risks & Vulnerabilities

- External Cyber Attack
- Insider Threats (Intentional or Inadvertent)
- Employees
- Third Party Service Providers

Mitigants

- Cyber Risk Management & Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience
Legal Framework: Directors’ Duty of Care

Corporate Law
Duty of Care, Loyalty, and Good Faith

Business Judgment Rule: Act on an informed basis to oversee and manage risks

Cybersecurity Information and Reporting: Basic knowledge of technical landscape, risks, response plan

Other considerations, including: Applicability of authorizing statutes and financial regulation
- e.g., FDIC, Fed, and OCC - Relevant expectations and guidance.
## The Context for Becoming (and Staying) Informed

| Enterprise Wide Risk Management: Cybersecurity as part of enterprise-wide risk management |
| Cyber Risk Implications: Understand the legal, operational, and financial implications of cyber risks related to organization’s mission |
| Access Expertise: Access to cybersecurity expertise, regular discussions, and updates |
| Require a Framework: Expectations that management establishes an enterprise-wide risk management framework with staffing and budget |
| Risk Decisions: Accept, mitigate, transfer |
Director Oversight of Cybersecurity Questions to Ask

Enterprise Wide Risk Management

• How frequently are “health checks” completed by auditors.

Cyber risk implications:

• What are the **top five risks the organization** has related to cybersecurity, what are the critical data/systems?
• How are **employees made aware** of their roles?
• What types of **connections** does my firm have (and how are they managed)?
• What risks are associated with **third party providers**; how are they managed?
• What is the data breach, what is the **incident response plan** (and is it robust enough)?
• Has institution tested recovery of critical systems (i.e. **resiliency**)?
• What **data breach laws** apply?
• What major **cyber attack attempts have been made** against the organization?
• Does the organization gather, analyze, and leverage **threat and vulnerability information** from multiple sources?
Director Oversight of Cybersecurity Questions to Ask

Require a Framework*

- Does the organization use a security framework?
- How is security governance managed within the organization?
- Does the budget align with similarly situated entities?

Accessing Expertise

- How often do we meet with Chief Security Officer?
- What reports are provided on the cyber events and trends?
- Has management established relationships with appropriate national and local authorities who are responsible for cybersecurity or cyber-crime responses?

Risk decisions

- What risks were avoided and accepted?
- Is cyber insurance an option and if so sufficient?

*For example, written security standards and practices covering the identification and classification of data, where and how data is stored, access to data, anticipated exposure, and breach response protocol.
## On-going Practices to Support Director Oversight

<table>
<thead>
<tr>
<th>Practice</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well informed and knowledgeable about, and act in a deliberate manner in the oversight of, the organization’s cybersecurity program.</td>
<td>✓</td>
</tr>
<tr>
<td>Appoint one or more qualified officers to be responsible for the organization’s cybersecurity program</td>
<td>✓</td>
</tr>
<tr>
<td>Preserve and cultivate expertise of one or more IT/cyber-savvy board member(s) (identify director(s) monitor and report to the board on cybersecurity matters)</td>
<td>✓</td>
</tr>
<tr>
<td>Have access to, and leverage as needed, internal and/or external cybersecurity expertise</td>
<td>✓</td>
</tr>
<tr>
<td>Be aware of best practices and leading industry “standards”</td>
<td>✓</td>
</tr>
<tr>
<td>Engage internal and/or external auditors to assess the organization’s program from time-to-time</td>
<td>✓</td>
</tr>
<tr>
<td>Review, discuss, and be periodically updated on the organization’s cybersecurity program</td>
<td>✓</td>
</tr>
</tbody>
</table>
Legislative Developments: Information Sharing under the Cybersecurity Act of 2015

Authorizes organizations to engage in activities to combat cyber threats:

- Sharing of information related to cyber threats (but generally no personal information; use of information is limited)
- Monitoring information systems
- Conducting defensive measure (but not hack backs)

Protections under the Act

- Liability protections
- Sharing protections (e.g., not subject to FOIA, no anti-trust violations for sharing)

Current Sunset: December 18, 2025