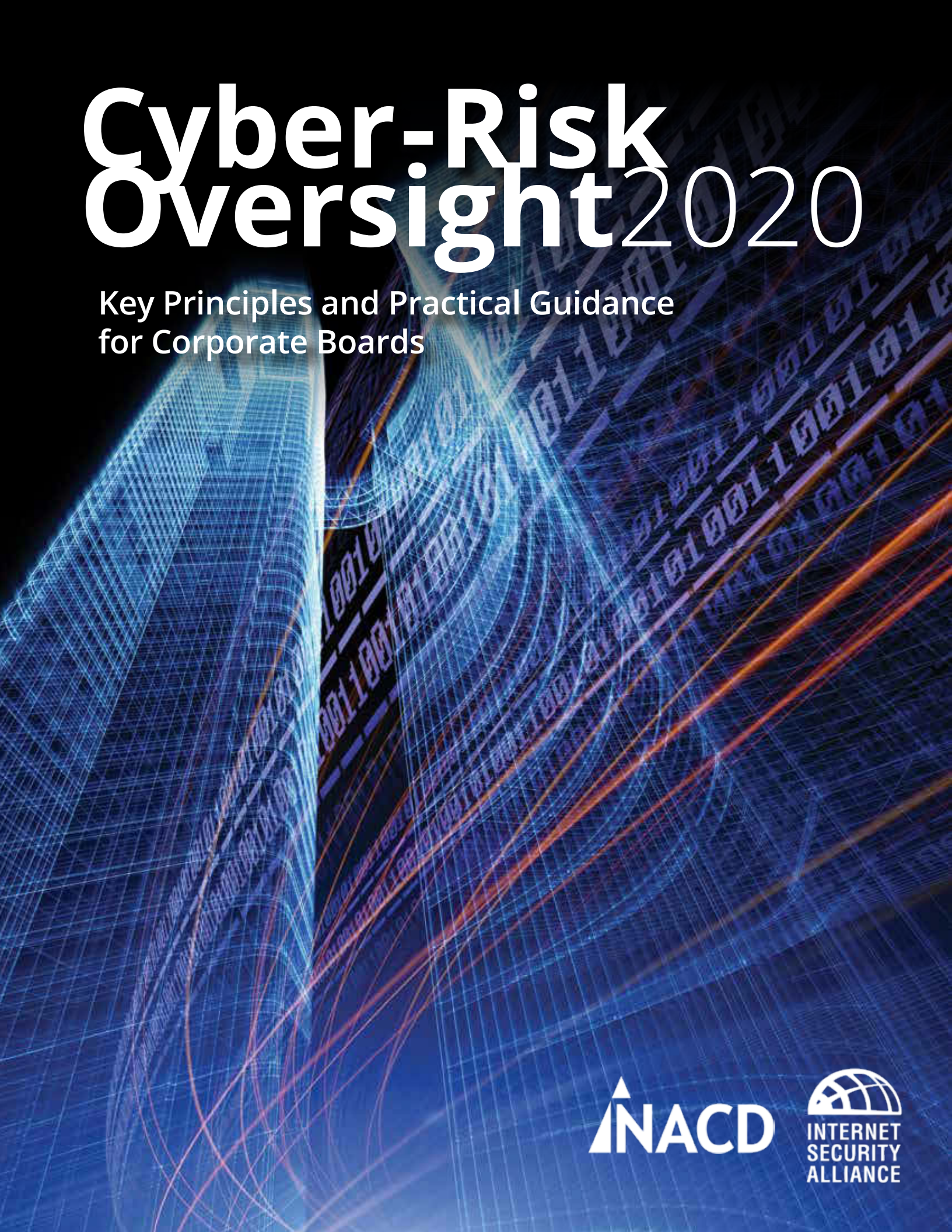
Cyber-Risk Oversight 2020

Key Principles and Practical Guidance for Corporate Boards



NACD

INTERNET SECURITY ALLIANCE

Tool D – Supply-Chain and Third-Party Risks

By Lisa Humbert, Operational Risk Officer of the Americas, Bank of Tokyo Mitsubishi, MUFG; and Tim McKnight, Chief Security Officer, SAP

OBJECTIVE OF THE TOOL:

Some of the biggest cybersecurity risks that enterprises must manage are their supply chain and third-party relationships. Many data breach incidents are caused by third-party vulnerabilities. As a result, the strength of an organization's cybersecurity often depends on the weakest link in its supply chain, which can directly affect the company's profitability and reputation. This Tool details questions that directors should be asking management to ensure adequate security measures are in place to address supply-chain and other third-party risks.

Below we have provided definitions for both Cyber Supply-Chain Risk Management and Third-Party Risk Management, and considerations for both disciplines. In some industries these functions overlap; however, the activities for each are distinct.

This Tool details questions, with considerations, that directors should be asking management to ensure that adequate security measures are in place to address Cyber Supply-Chain Risk Management and Third-Party Risk Management.

NIST defines cyber supply-chain risk management (C-SCRM) as "the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of [IT] product and service supply chains."[1]

Third-Party Risk Management (TPRM) is the standardized process companies use to monitor and manage risk associated with key partners and vendors.

Questions Directors Can Ask to Assess the Company's Approach to Cyber Supply-Chain Risk Management

1. How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks? Here are some items to consider:
   a. Risk and reward analysis, and accounting for cybersecurity management and Information Technology governance in the Total Cost of Ownership calculation
   b. Negotiation strategies inclusive of cybersecurity insurance provisions
   c. Implementation of service-level agreements inclusive of reporting, metrics, and ongoing monitoring requirements

CYBERSECURITY RISK IN THE SUPPLY CHAIN

- Each new supplier adds security vulnerability
- Cyber attackers often target third-parties
- Understanding what suppliers have data, where it is stored, and who has access to it
- Data quality checks and data flow mapping
- Supplier maturity within the FinTech community
- Contract negotiations and terminations
- Employee skill level
- Subcontractors
- Age of contracts
- Internal cybersecurity maturity
- End-to-end process management and oversight

[1] NIST, "Cyber Supply Chain Risk Management" on csrc.nist.gov.

2. What do we need to do to fully include cybersecurity in current supply-chain risk management? Here are some items to consider:
   a. Training supply-chain personnel to recognize cybersecurity risk and enabling mitigation activities
   b. Third-party due diligence throughout the proposal, selection, and onboarding processes
   c. Cybersecurity expertise leveraged during the negotiating and contracting process
3. How are cybersecurity requirements built into contracts and service-level agreements? How are they enforced? Contracts and service-level agreements can be written to include requirements for the following:
   a. Cybersecurity insurance provisions
   b. Personnel policies, such as background checks, training, etc.
   c. Access controls
   d. Encryption, backup, and recovery policies
   e. Secondary access to data
   f. Requirements around the use of subcontractors
   g. Countries where data will be stored
   h. Data-security standards and notification requirements for data breaches or other cyber incidents
   i. Incident-response plans
   j. Audits of cybersecurity practices and/or regular certifications of compliance
   k. Participation in testing and contingency activities
   l. Requirements for timely return/destruction of data at termination

CASE IN POINT

An Impact on the Consumer Experience

A US-based consumer reporting agency suffered a data breach that affected the personally identifiable information of more than 100 million Americans. Hackers penetrated the company's information system using known vulnerabilities in software, which was developed by a third-party software vendor and widely used. An external third party notified the public about vulnerabilities before the breach. The data breach was preventable had the company patched the vulnerability in the third-party software. The company was required to pay a multimillion-dollar data breach settlement.

Source: Lily Hay Newman, "All the Ways Equifax Epically Bungled Its Breach Response," *Wired*, September 24, 2017.

Major US Retailer Breached by Vulnerability in Third-Party Vendor's Security

A major US retailer suffered a data breach after hackers penetrated a third-party vendor's information systems to steal network credentials. Hackers then stole 70 million shoppers' information. The incident revealed that an organization's cybersecurity is as strong as the weakest link in its supply chain: in this case, a third-party refrigeration and HVAC services vendor.

At the time, the major retailer had passed Payment Card Industry (PCI) standard compliance audits, which highlighted the limits of the compliance approach to cybersecurity. "Just because you pass a PCI audit does not mean that you're secure," warned a security researcher at the time. A chief technology officer commented: "Compliance can give you a false sense of security."

Source: "Target Hackers Broke in Via HVAC Company," *Krebs on Security* (blog), February 14, 2014; John P. Mello Jr., "Target Breach Lesson: PCI Compliance Isn't Enough," *Tech News World*, March 18, 2014.

4. Do our vendor agreements provide adequate controls for legal risks and compliance requirements (e.g., FTC, HIPAA, GDPR, etc.)? Here are some items to consider:
   a. Access to confidential or proprietary data, personally identifiable information (PII), sensitive personal information (SPI), or handling of personal health information
   b. Data, used for regulatory, financial, or other internal reporting, provided by a third party
   c. Third-party compliance with laws, regulations, policies, and regulatory guidance
5. Are we indemnified against security incidents on the part of our suppliers/vendors? Here are some items to consider:
   a. Breach, incidents, and vulnerabilities
   b. Limitation of liability
   c. Intellectual property violations

Questions Directors Can Ask to Assess the Company's Approach to Third-Party Risk Management

1. What will need to be done to fully include cybersecurity in current third-party risk management? Here are some items to consider:
   a. Initial and ongoing monitoring of third-party compliance and the control environment
   b. Assessment process and cadence, designed to identify and remediate weaknesses and threats
   c. Skilled personnel assigned to monitoring and oversight of the third party

CASE IN POINT

Major Airline Responds Quickly to Third-Party Vulnerability

In 2018, a major airline revealed that some consumer information had been compromised via a vulnerability in a third-party, online-chat support service. In response to this breach, the airline launched a custom website outlining details of the breach and implemented a comprehensive communications campaign highlighting education and best practices. The airline also worked with partners to analyze the breach, including identifying whether the vulnerability had impacted any part of the airline's own website or its own computer systems. Once the airline had successfully managed the fallout from the breach, the airline filed a lawsuit against the third-party service, citing that the third-party vendor had failed to comply with a contractual promise to notify the airline immediately should a breach occur.

Source: Anna Convery-Pelletier, "The Delta Airlines Security Breach: A Case Study in How to Respond to a Data Breach," *Radware* (blog), October 24, 2018.

2. How are we monitoring compliance of operational and legal requirements? Here are some items to consider:
    - **a.** Reporting and testing
    - **b.** On-site and remote assessments
    - **c.** Periodic business reviews with the third party

3. Do we have the right skill set to conduct assessments, testing, and ongoing monitoring of our third-party population? Here are some items to consider:
    - **a.** Creating a risk-management framework, including defined roles and responsibilities
    - **b.** Adequate understanding of the products and services provided by the third party
    - **c.** Understanding of external regulatory guidance and impacts on the third-party products and services

4. How difficult/costly will it be to enhance monitoring of access points in the supplier network? Here are some items to consider:
    - **a.** Data protection need and availability
    - **b.** Multilayered assessment of data quality, and inflow/outflow
    - **c.** Access to supplier network

5. How difficult/costly will it be to establish and maintain a viable cybersecurity program for our third-party risk? Here are some items to consider:
    - **a.** Technology and infrastructure
    - **b.** Organizational staffing
    - **c.** Regular cross-functional stakeholder collaboration to ensure effective access controls

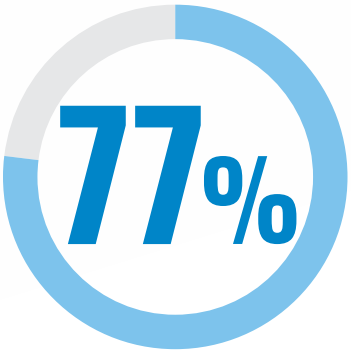
Why NACD?

NACD empowers more than 21,000 directors to lead with confidence in the boardroom. As the recognized authority on leading boardroom practices, NACD helps boards to strengthen investor's trust and the public's confidence in business by ensuring that today's directors are well prepared for tomorrow's challenges. NACD members can also take the next step to elevate their individual and board performance by becoming NACD Directorship Certified™.

OF DIRECTOR MEMBERS SAY THAT
NACD MEMBERSHIP HAS IMPROVED THEIR BOARDROOM IMPACT

NACD Directorship Certification®

NACD'S Directorship Certification distinguishes you as a director. The program is designed as a framework for continuous learning and equips certified individuals with the baseline knowledge, skills, and abilities they need to contribute to the boardroom dialogue on day one. The entire Certification experience, from registration through the exam, is available virtually and on your schedule.



OF ALL NEW, PUBLIC-COMPANY DIRECTORS
ARE SERVING ON THEIR FIRST PUBLIC-COMPANY BOARD

JOIN AND BECOME NACD DIRECTORSHIP CERTIFIED™.

Join@NACDonline.org • 571-367-3708 • NACDonline.org/Join

NACD