

Cyber Risk Assessments and Tabletops

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

Framework for Cybersecurity

- In 2018, the National Institute of Standards and Technology (NIST) issued a 'Framework for Improving Critical Infrastructure Cybersecurity.' It was designed to help improve cybersecurity risk management.
- It can be a guide or model to international cooperations on how to strengthen their cybersecurity in critical infrastructure as well as other sectors and communities.
- The framework consists of three parts:
  - The Framework Core,
  - The Implementation Tiers, and
  - The Framework Profiles.

(c) 2023 Lexeprint Inc. All Rights Reserved



Trending Threats and Vulnerabilities Today

- Cloud breaches and cloud migration - 45% data breaches occur in the cloud.
  - Companies that experienced a breach during a cloud migration project had a 25.7% higher cost than the average, $5.63 million per breach.
- Ransomware – 41% of data breaches are caused by ransomware, and 17% of all cyber attacks.
- Remote Work – The average cost of a data breach cost $1 million greater where remote work was a factor, averaging at $4.90 million per breach.
- In recent years the U.S. has faced major national security threats from foreign actors leveraging cybersecurity.
  - Supply chain disruption like SolarWinds
  - Critical infrastructure
  - Undermining institutions

**IBM Cost of a Data Breach Report 2022*

(c) 2023 Lexeprint Inc. All Rights Reserved.



Initial Attack Vectors

- Initial Attack Vectors refer to the methods a hacker uses to illegally access a network or computer.
- The highest average total cost of initial attack vectors include:
  - (1) Phishing ($4.91);
  - (2) Business email compromise ($4.89 million);
  - (3) Vulnerability in third-party software ($4.55 million);
  - (4) Stolen or compromised credentials ($4.50 million); &
  - (5) Malicious insider ($4.15 million).*

** IBM Cost of a Data Breach Report 2022*

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-ND.

What is a Cyber Risk Assessment?

- The NIST defined cyber risk assessments as:
  - "*risks assessments that are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.*"
- This assessment is used to inform decision-makers and support proper risk responses. It also helps to provide an executive summary to help executives and directors make informed decisions about security.
- According an ABA survey, only 35% of respondents report that their firm has had a full security assessment performed by a third party.

(c) 2023 Lexeprint Inc. All Rights Reserved



Difference between Risk, Vulnerability, and Threat

- While these terms are often used in the same contexts, it is important to understand how they differ:
- Risk
  - The probability and impact of an attack or incident.
- Vulnerability
  - A weakness in a system or network that is targeted and exploited by a malicious actor.
- Threat
  - Potential harm caused by an attacker.

(c) 2023 Lexeprint Inc. All Rights Reserved


This Photo by Unknown Author is licensed under CC BY-NC-ND

What Cybersecurity Risk Assessments Help Answer

- Some of the key questions cybersecurity risk assessments can answer include:
  - What are our organization's most important information technology assets?
  - What data breach would majorly impact our business, whether from malware, cyber-attack, or human error? Think customer information.
  - What are the relevant threats and threat sources to our organization?
  - What are the internal and external vulnerabilities?

(c) 2023 Lexeprint Inc. All Rights Reserved



What is a Tabletop

- Cyber Risk Assessments can take the form of audits, workshops, or tabletops.
- A cybersecurity tabletop is a simulated or hypothetical cyber event that tests an organization's ability to respond to a cyber incident.
- Tabletops generally include stakeholders from departments and teams across an organization, including IT, legal, HR, and senior management.
- Tabletops are used to test an organization's existing cyber risk management and identify weak points or gaps.
  - The risks identified through a tabletop are not only technical; they also identify legal and regulatory risks.
- Resource: Tabletop.ai

(c) 2023 Lexeprint Inc. All Rights Reserved.



Why Should Your Law Firm Do a Tabletop?

- Ensure Sensitive Information is Protected
  - Tabletop exercises provide a critical opportunity for law firms to measure their cybersecurity risk management as a business but also as the custodian of highly sensitive client information.
- Better Counsel
  - By participating in this exercise, attorneys can not only protect their business but also gain valuable experience and knowledge in incident response, which can help them provide better legal advice to clients.
- Mitigate Technical and Regulatory Threats
  - Participating in a tabletop allows organizations to receive actionable mitigation strategies and demonstrate compliance and active risk management to regulators and other stakeholders.

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA-NC

Why Should Your Law Firm Do a Tabletop? (cont.)

- Training and awareness
  - The exercises can also serve as a training and education opportunity for attorneys and staff, raising awareness of the importance of cybersecurity and data protection and promoting a culture of security within the firm.
- Competitive Edge
  - Finally, conducting cybersecurity tabletop exercises can help law firms differentiate themselves from competitors by demonstrating their proactive approach to cybersecurity, which can be a significant factor in client retention and acquisition.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Key Takeaway: Why You *Should* Perform Cyber Risk Assessments

Implementing assessment and mitigation solutions that consider both technical risk and leverage regulatory requirements can help lead to:

- Reduction of long-term costs,
- Cyber security risk assessment template for future assessments,
- Avoidance of data breaches,
- Avoidance of regulatory issues,
- Avoidance of data loss.

(c) 2023 Lexeprint Inc. All Rights Reserved



Additional Strategies for Cyber Risk Mitigation

This Photo by Unknown author is licensed under CC BY-SA-NC.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Defense-in-Depth

- Defense-in-Depth (DiD), also known as the "castle approach," is a cybersecurity method of layering defensive mechanisms to protect valuable data and information.
- The layered approach strengthens the security of the system and covers different attack vectors.
- Common security elements found in a DiD:
    - Network Security Controls
    - Antivirus Software
    - Analyzing Data Integrity
    - Behavioral Analysis

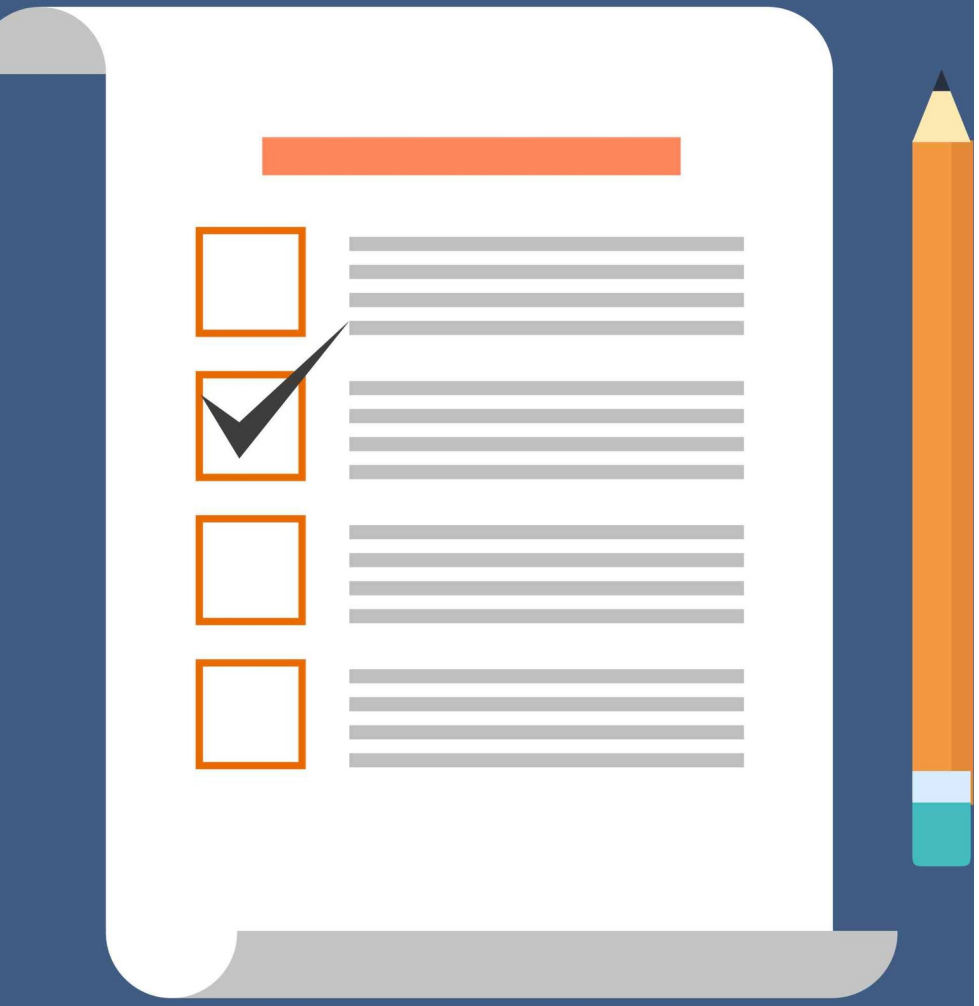
(c) 2023 Lexeprint Inc. All Rights Reserved


This Photo by Unknown author is licensed under CC BY-NC-ND.

Third-Party Vendor Management

- Vet your vendors for risks and track the news for potential vulnerabilities.
- Use experienced technology companies have groups dedicated to third-party vetting and should be used, and while this may increase costs in the short run, it will pay off in the long run.
- Hire security consultants during the contract negotiation process and take advantage of services that can help them rate the risks of their potential vendors.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Incident Response Plan

- Engage all key areas (business, legal, marketing, insurance, HR, IT).
- Develop a cross-functional incident response plan and team.
- Retain outside technical, legal, and PR experts for the inevitable cyber incident and identify points of contact within law enforcement before a cyber-attack.
- Test it!

(c) 2023 Lexeprint Inc. All Rights Reserved.



Cybersecurity Insurance

- Assess the full range of risks and costs from disruption of services, data leaks, data ransoms, and extortion schemes.
- Verify and validate that key partners have coverage -- a vendor that is hacked can lead to your organization being compromised.
- Ensure that coverages map to the cybersecurity controls, process, vendors, and protocols in any IR plan.
- Stay abreast of the market -- cyber insurance is still evolving, and coverage and pricing are in progress.
- Policies and available products must be continuously reviewed for gaps.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Technical Risk Management

Regularly Update Permissions

- Recurring events when permissions within the company are re-evaluated can limit access to important data and limit the entry ways hackers may use to breach the data.
- This strategy may be most beneficial when employees resign, get promoted, or take leave of absence.

Maintain Records of Data Access

- By tracking data access, irregularities may become apparent in defining when an account may be compromised, files are no longer accessible, or data has been changed.
- Tools including the User and Entity Behavioral Analysis (UEBA) may be a useful device to discover any activity that is unusual.

(c) 2023 Lexeprint Inc. All Rights Reserved.



(c) 2023 Lexeprint Inc. All Rights Reserved.