Cybersecurity for Small to Medium-Size Businesses

Tabletop Exercise Leader's Guide

October 2023

Payments Innovation Alliance®

Table of Contents

Introduction

Background

Cybersecurity is the practice of protecting and recovering computer systems, networks, devices, and data from unauthorized access, damage or disruption. It involves measures like risk assessment, prevention, detection, response, education, and compliance to safeguard against cyberthreats. Effective cybersecurity programs require ongoing monitoring, updating, and collaboration with multiple stakeholders within and outside of the business.

According to the IBM "Cost of a Data Breach Report 2023," the global average cost of a data breach in 2023 was $4.45 million, 15% more than in 2020.[1]

Cyberattacks are increasingly targeting small and medium-sized organizations. According to Accenture's "Cost of Cybercrime Study," 43% of cyberattacks are aimed at SMBs, but only 14% are prepared to defend themselves.[2] Cybercriminals target small businesses because they are easier targets to penetrate.

These attacks are pervasive and may be conducted from anywhere: within your organization, your third-party provider's system or outside the United States. Criminal networks are increasingly sophisticated and evolve with emerging technology such as social engineering and may use artificial intelligence to circumvent traditional data security controls.

As the world has become digitally interconnected and more information is stored in the cloud with multiple users, it is increasingly important that companies remain vigilant in protecting data, computer systems, intellectual property, trade secrets, networks, devices and programs.

The U.S. National Cyber Security Alliance found that 60% of small companies are unable to sustain their businesses over six months after cyberattack. According to the Ponemon Institute, the average price for small businesses to clean up after their businesses have been hacked stands at $690,000, and for middle-market companies, it's over $1 million.[3]

There is no federal law that generally applies to data breach disclosure in the United States, although there are laws and rules that apply to specific entities, such as under the HIPAA Breach Notification Rule. Most importantly, there are data breach laws in all 50 states that minimally include three requirements:

- Notify those affected.
- Inform the government.
- Pay some type of fine or penalty.

---

1. *Cost of a data breach 2023: Financial industry impacts (securityintelligence.com)*

2. *Cost of Cybercrime Study (Accenture)*

3. *Sixty percent of small companies that suffer a cyberattack are out of business within six months. – The Denver Post*

Introduction

Background

A cyberattack could harm a company's reputation (e.g., negative media coverage, lack of customer confidence) and financial conditions (e.g., loss of customers/revenue, stock valuation, cost to recover from the cyberattack, regulatory fines).

Small and mid-sized businesses – defined as companies with 100 to 1,000 employees – spend an average of $955,429 to restore normal business in the wake of successful attacks. The average cost of a data breach involving theft of assets totaled $879,583. The cost of returning to business-as-usual for small and mid-sized businesses is greater than the amount of money taken in a cyberattack.[4]

Although such incidents rarely make the headlines, the majority of attacks target small and mid-sized businesses, and according to the National Cyber Security Alliance, some 60% of small companies go out of business within six months of a breach.[5]

Businesses of all sizes must ensure that all staff understand cybersecurity threats and how to mitigate them. This concern can be addressed through regular training and a cybersecurity response plan.

4. *Twenty Eye-Opening Cybercrime Statistics (securityintelligence.com)*

5. *Prepared Statement of the Federal Trade Commission on Small Business Cybersecurity: Federal Resources and Coordination, Before the Committee on Small Business, United States House of Representatives (ftc.gov)*

Introduction

Types of Cyberattacks

There are generally eight types of cyberattacks[6], as described below.

1. **Phishing Attacks:** Phishing is a form of social engineering where attackers impersonate legitimate entities and individuals to trick victims into providing sensitive information such as login credentials or personal or company data. Phishing may also be used to trick victims into sending money to the attacker under the guise that it is a legitimate transaction.
2. **Malware Attacks:** Malware is malicious software designed to disrupt, damage, or gain unauthorized access to a computer system. Malware can infect computers and networks through email attachments, infected websites or compromised software. Common malware include viruses, worms, Trojan viruses, spyware and ransomware.
3. **SQL Injection Attacks:** SQL injection attacks inject malicious SQL code into an application, allowing the attacker to view or modify a database that uses SQL. SQL is a standard programming language for database creation and manipulation. Attackers exploit security vulnerabilities in an application's software to inject malicious SQL code that allows attackers to spoof identities, tamper with, gather or destroy data or make the attacker the database server administrator.
4. **Ransomware Attacks:** Ransomware is a type of malware designed to deny a user or organization access to files on their computer by encrypting the victim's files. Attackers demand a ransom payment in exchange for the decryption key or restoring access to the systems. Attackers will often threaten to publish the victim's sensitive data or permanently block access to it unless a ransom is paid.
5. **Social Engineering Attacks:** Social engineering is the use of deception to manipulate individuals into sensitive information that may be used for fraudulent purposes, including getting the victim to take certain actions. Social engineering attacks can include impersonating a trusted individual or company, using pretexts to gain access to computer systems or exploiting human errors by creating a sense of urgency to perform a specific action, such as sending money to the attacker.
6. **Password Attacks:** Password attacks use technology to gain unauthorized access to the victim's accounts by cracking, guessing or stealing passwords. Common methods include brute force attacks, where a computer program tries possible passwords, or dictionary attacks, where the attacker uses a list of common passwords to guess the correct password.
7. **Insider Threats:** Insider threats are when employees or vendors within a company use their access privileges to gain unauthorized access to sensitive information or misuse information. Insiders may use their access to steal data, initiate unauthorized transactions, disable or destroy systems or give sensitive information to other bad actors.
8. **Zero-day Attacks:** Attackers exploit software vulnerabilities before a fix or patch for the previously unknown or recently discovered vulnerability is available from the software developer. Zero-day attacks refer to the software developer and users having "zero days" to prevent the attack, leaving the victim with little time to defend against the attacker.

---

6. *The Importance of Cybersecurity in Today's Digital Landscape (linkedin.com)*

Tabletop Exercise

Objectives of a Tabletop Exercise

One of the first possible steps for a business to address cybersecurity resilience is to conduct a tabletop exercise. A tabletop exercise is a role-playing activity in which participants respond to scenarios presented by one or more facilitators, referred to as the leader. A tabletop exercise both educates the participants on how to respond to a cyberattack and informs the company on areas where its cybersecurity response plan can be enhanced.

The leaders present a scenario that can be used to gauge an organization's readiness. Expect that the tabletop exercise will not be perfect the first or second time – cybersecurity is not static, and participants will learn through discussion. The overarching goal is for the team to uncover opportunities for remediating issues and creating an action plan while there is not a real, immediate cybersecurity threat.

The objectives of the tabletop exercise are to:

1. **Increase organizational preparedness**, response, and recovery efforts related to cyberattacks.
2. **Advance the understanding** of management and key internal and external stakeholders. External stakeholders may include cybersecurity companies, cyber insurance providers and law enforcement.
3. **Provide actionable approaches** for leadership to direct and bolster the organization's resilience.
4. **Identify enhancements** requiring attention from company leadership.
5. **Establish a framework for compliance** by understanding what laws, regulations and rules apply and implementing programs to address the company's obligations. Compliance with industry standards, such as SOC 2, can be addressed as part of the tabletop exercise and used to demonstrate to regulators and business partners that the company maintains a reasonably designed cybersecurity program.

Tabletop Exercise

Tabletop Exercise Kit

The Tabletop Exercise Kit is intended for small to medium-sized companies to conduct a two to three hour cybersecurity tabletop exercise to foster understanding and discussions to prepare for a cybersecurity incident.

The kit includes:

Leader's Guide:
This "Tabletop Exercise Leader's Guide" ("Guide") is for facilitators (rather than participants) and covers planning, conducting, and evaluating the exercise and responses. The Guide provides a framework that can be adaptable to nearly any cybersecurity threat. It includes helpful tips and suggestions for conducting the exercise and excludes legal advice or a comprehensive list of resources and regulations.

Cybersecurity Scenario(s):
The cybersecurity incident exercise is conducted through a set of facts outlined in a scenario. The scenario can be used in whole or in part and can be customized by the company as appropriate.

The scenario is designed to avoid adding additional facts that would change the discussion about questions previously discussed in prior sections. Participants should be able to move linearly through the scenario without the need to revisit or recall facts from previous sections.

Participant Workbook:
Each scenario has a corresponding workbook with two worksheets, as illustrated below.

Worksheet #1	
Section/Suggested Time Limit	**Questions for participants to address during the exercise**

Worksheet #1 asks participants to provide written responses to the question within the suggested time limit.

Worksheet #2	
Section	**Participants observations during the tabletop exercise**

Participants should be encouraged to provide observations, document issues, and capture questions that arise during the exercise using *Worksheet #2*.

Leader's Guide for Evaluating the Exercise:
This document provides general guidance for the Tabletop Exercise Leader to consider during the evaluation phase. It is intended to facilitate a discussion.

Tabletop Exercise

Tabletop Exercise Roles

Typical roles in a tabletop exercise include:

1. **Leader** who (a) defines the scenario, participants and allocated length of time for the exercise; (b) facilitates the exercise, including providing scenario updates and answering questions during the exercise; (c) conducts the post-exercise evaluation; and (d) leads/supports the action plan.

2. **Participants** who have an active role and perform in their regular roles and responsibilities during the exercise (e.g., discuss or initiate actions in response to the scenario) and during the post-exercise evaluation.

3. **Scribes** who are assigned to observe and document exercise activities and discussions. Their notes will be necessary during the post-exercise evaluation.

4. **Observers** who do not directly participate in the exercise, but may be consulted or ask or answer relevant questions (optional).

Helpful Tips for Exercise Leader and Participants

Tabletop Exercise Leader

The leader sets the tone and content for the tabletop exercise and does not need to be a cybersecurity expert. A company should scale the tabletop exercise that is most appropriate to the organization.

Best practice: **Apply a risk lens to your customization. Consider the most likely and painful threats to your business.**

The following tips are provided to help the leader plan, conduct and evaluate the exercise and create an action plan.

1. Planning the Exercise

- Start with a tabletop exercise scenario that is simple and appropriate for your company (refer to the scenario documents that are part of this kit).
- Set realistic expectations. The tabletop exercise will not be perfect, especially the first few times it is conducted.
- Identify who will participate in the exercise. Participants should generally play their actual roles. Participants may include both internal and external resources which are generally considered to be part of your Cybersecurity Response Team. The term "Cybersecurity Response Team" may be used in the tabletop exercise documents. This refers to the internal and external resources that would be called upon for an actual cybersecurity event. At your option, participants may be assigned a different role to encourage new thinking and an appreciation of other job functions.
- Determine the length of time for conducting the exercise. The scenarios included in the kit provide recommended the length of time for each section, generally between two to three hours.

2. Conducting the Exercise

- Inform the participants about the purpose of the exercise and expectations (see Tabletop Exercise Participant section).
- Emphasize that this is a simulation, and quick reactions are fine.
- Foster a supportive environment that will allow participants to learn.
- Insert the security classification in the workbook (e.g., confidential, highly confidential).
- Provide the participants with the workbook.
- Direct participants through the scenario and exercise. Read the scenario to the participants as they move through each section. Display the scenario section so participants can re-read the scenario facts.
- Time each scenario section and stop the discussion when the time provided in the workbook has expired.

Helpful Tips for Exercise Leader and Participants

Tabletop Exercise Leader

2. Conducting the Exercise, continued

- Answer questions during the exercise if participants are unsure about the facts. The leader should feel free to make reasonable assumptions about facts not presented yet stick to the scenario as closely as possible.
- Address any disagreements among participants about how specific issues should be addressed.
- Follow the scenario timeline provided to ensure the completion of the entire exercise.
- Create a "parking lot" of issues needing further discussion to be addressed after the exercise. Not every issue will be resolved during the tabletop exercise.
- Encourage multiple viewpoints because many of the issues raised are complex and may be addressed in various ways.
- Look for gaps in your team (e.g., participants' roles represented).
- Collect the worksheets at the end of the exercise.

3. Evaluating the Exercise

- Evaluate the exercise only after the scenario has been entirely played out. Ideally, the evaluation is conducted within two weeks of the exercise.
- Consolidate the participant's responses provided in Worksheets #1 and #2.
- Review the "Leader's Guide for Evaluating the Exercise" to prepare for the post-exercise evaluation session.
- Conduct a debrief on what worked/didn't work to support an improvement action plan. Facilitate a discussion using the consolidated responses. Additional subject matter experts and stakeholders may be included in the discussion as appropriate.
- Acknowledge there may be differences of opinion in the "correct" course of action.
- Capture recommendations and action/remediation plan.

Best practice: **Conduct another exercise with a different scenario and/or participants to improve your company's cybersecurity readiness.**

Helpful Tips for Exercise Leader and Participants

Tabletop Exercise Leader

4. Creating an Action/Remediation Plan

- Assign responsibilities for developing an action plan to address gaps or issues.
- Incorporate lessons learned into your Incident Response Plan and other policy and procedure documents.
- Secure electronic or hard copy documents related to deficiencies, remediations, Incident Response Plan, or other confidential intellectual property so that it is accessible by only authorized individuals.
- Use this as an opportunity to evolve and be better prepared in the future.

5. Summarizing Results

The exercise result should be a detailed report with a summary of the major findings, takeaways, discussion points from the exercise, and resources linked to the specific challenges identified during the event. Examples of key findings are provided below.

Example #1: Public Communication and Engagement: Identified existing plans, procedures, and mechanisms in place for communicating during a cybersecurity event. To improve the efficiency of these communications, participants noted the benefits of developing more formal protocols and agreements and establishing backup communication channels.

Example #2: External Stakeholder Coordination and Engagement: To enhance existing emergency plans, policies, and procedures, the company will benefit from increased coordination with external stakeholders, such as the Department of Homeland Security. These external stakeholders can provide useful guidance and resources supporting cyber incident preparedness, response, and recovery efforts.

Example #3: Cyber Partnerships: In addition to improving overall security preparedness, identify third-party vendors dedicated to guiding response actions in the event of a cyberattack on the company.

Tabletop Exercise Participants

Participants play an essential role in the success of the exercise. The following tips are participant expectations, which the leader should share with participants before the exercise starts.

- Stay in character during the exercise.
- Participate, observe and take notes about what worked and didn't work and log decisions made.
- Maintain confidentiality of any related cybersecurity activities (e.g., scenario, results, action/remediation plan, incident plan).

Conclusion

Cybersecurity is a concern of all businesses as cyberattacks become more frequent. Small to medium-sized businesses are particularly vulnerable. The responsibility for mitigating and responding to a cyberattack is not just the responsibility of the IT department; it is everyone's responsibility within your company.

Conducting and evaluating various scenarios through tabletop exercises and developing procedures for responding to unwanted attacks to data and assets are important measures for staying in business.

Payments Innovation Alliance – Cybersecurity Response Project Team

The Payments Innovation Alliance is a membership program that shapes the future of the payments industry and develops thought leadership relevant to financial service institutions. The Alliance established the Cybersecurity Response Project Team to help organizations understand evolving threats related to potential cyberattacks.

These resources may be downloaded and shared with employees, colleagues, and clients as appropriate. If you'd like more information on the Payments Innovation Alliance, including the work we have done and how your organization can get involved, please visit nacha.org/payments-innovation-alliance.