Tabletop Exercises

Scenarios to Help Prepare Your Cybersecurity Response

RoundTable TECHNOLOGY

Introduction

This has been adapted for use by nonprofits and small businesses by Joshua Peskay and Kim Snyder of RoundTable Technology.

The original content is from the Center for Internet Security - Six Tabletop Exercises to Help Prepare Your Cybersecurity Team.

What are Tabletop exercises?

Tabletop exercises are meant to help organizations consider different risk scenarios and prepare for potential cyber threats. These are discussion-based exercises where team members meet in an informal setting to discuss roles during an emergency and our responses to a particular emergency situation.

A facilitator guides participants through a discussion of one or more challenging scenarios that our organization may face.

Why do Tabletops?

Tabletops are an opportunity for organizational stakeholders to review and discuss the actions to take in specific emergency scenarios. Well-facilitated tabletops enable organizational stakeholders to gain insights before an emergency happens. This is an opportunity to test preparedness and response capabilities in an informal, low-stress environment.

Tabletops are used to clarify roles and responsibilities and to identify additional mitigation and preparedness needs.

Tabletop exercises are not tests or fire drills and are not meant to provide an evaluative result or to provide grounds to criticize any person or team. There is no “pass” or “fail” for a tabletop exercise.

Getting Started

The objectives of a tabletop are to:

- Provide a safe space for team members to openly discuss preparedness and response capabilities to the scenarios presented.
- Identify gaps or other weaknesses in our response capabilities and in our decision-making process
- Identify gaps or other weaknesses in our current practices that could be improved to reduce the likelihood and/or severity of a crisis

Learning is the primary goal for a tabletop exercise.

How to Run a Tabletop - Getting Started

Each of the exercises featured in this white paper can be completed in as little as 15-20 minutes, making them a convenient tool for putting your team in a response mindset. In addition, each scenario will list the processes that are tested, threat actors that are identified, and the assets that are impacted.

Implementing tabletops is a three phase process that can be broken down into **Plan, Do and Improve.**

How To Use

Plan

1. Clarify what objectives you are hoping to achieve from conducting a tabletop(s). Is the purpose of the tabletop to get a general understanding of organizational readiness and gaps, or is it to address a specific situation?
2. Identify who will facilitate the tabletop and which tabletop scenarios you will be addressing.
3. Identify the stakeholders who will be involved in the tabletop. Your selection of stakeholders may vary depending on the scenario that you are addressing.

Do

1. Designate a Facilitator and identify members from business units to participate. We recommend the IDOARRT Meeting Design [1] as a format for running the tabletop. Prior to the tabletop, outline each of these points:

    - Intention - What is the goal of doing the tabletop?
    - Desired Outcome(s) - What specific results do you want from the tabletop?
    - Agenda - What activities will be conducted during the tabletop?
    - Roles - Who is responsible for what during the tabletop?
    - Rules - What ground rules will ensure a safe, productive tabletop?
    - Time - How long will it take?

2. Implement a selected tabletop exercise.

    - Read the scenario aloud to the group and ensure a common understanding.
    - Facilitate a conversation about how your organization would handle the scenario.
    - Use the "questions to ask" section of the tabletops to facilitate discussion

3. The Facilitator records the findings from the exercise(s). This includes gaps, lessons learned, and areas for investigation.

How To Use (con't)

Improve

- Address gaps by developing a short- and long-term Incident Response Plan.
- Identify who will be responsible for addressing different aspects of the Incident Response Plan. Be as specific as possible about tasks and set due dates.
- Schedule a date for an accountability check-in.
- Schedule a date (annually, perhaps) to perform your next tabletop

[1] Hyper Island Toolbox, IDOARRT Meeting Design

The Exercises


Exercise 1 - The Quick Fix


Exercise 2 - Phishing for Dollars


Exercise 3 - Compromised Email Account


Exercise 4 - Photogenic Malware


Exercise 5 - The Known Unknown


Exercise 6 - The Cloud Compromise


Exercise 7 - Financial Break-in

Exercise 8 - Double Whammy


Exercise 9 - The Deepfaked Special Guest (Disinformation Campaign)


Exercise 10 - DDoS via bot

Exercise 11 - Free Wi-Fi Gets Quite Costly


Exercise 12 - A Visit from the Anti-Science Doxxers


Exercise 13 - The Compromised Sendee


Exercise 14 - Cleaned-out Border Crossing


Exercise 15 - Connecting the OSINT Dots


Exercise 16 - The Open Vault


Exercise 17 - The Bamboozled Bookkeeper


Exercise 18 - The Holiday Buffalo Jump (specific to IT Service Providers)


Exercise 19 - The Third-Party Leak (the hackers did everything at Zombo Com)


Exercise 20 - The Deep State Deep Fake

Exercise 1

The Quick Fix

SCENARIO: Jolene, your network administrator, is overworked and underpaid. Her bags are packed and ready for a family vacation to Disney World when she is tasked with deploying a critical patch. In order to make her flight, Jolene quickly deploys the patch before leaving for her trip. Next, Sue, the on-call service desk technician, begins receiving calls that nobody can log in. It turns out that no testing was done for the recently-installed critical patch and it has caused the networking to fail on all impacted computers.

What is your response?

Discussion questions:

- What is Sue's response in this scenario?
- Does your on-call technician have the expertise to handle this incident? If not, are there defined escalation processes?
- Does your organization have a formal change control policy?
- Are your employees trained on proper change control?
- Does your organization have disciplinary procedures in place for when an employee fails to follow established policies?
- Does your organization have the ability to "roll back" patches in the event of unanticipated negative impacts?

Processes tested: Patch Management
Threat actor: Insider
Asset(s) impacted: Internal Network

RoundTable TECHNOLOGY

Exercise 2

Phishing for Dollars

SCENARIO: Arjun, your new finance admin, receives a phishing email that spoofs the Executive Director's email (the email appears to come from the Executive Director). The email requests that Arjun purchase $800 in Amazon gift cards and send them via email immediately for a fundraising event. Arjun complies with the request and purchases the gift cards, emailing them to the sender of the fraudulent phishing email.

What is your response?

Discussion questions:

- What is your response in this scenario?
- Have you configured SPF, DKIM and DMARC records to mitigate this type of threat?
- Do you have cyber liability insurance? If so, do you know if it covers this type of event?
- Have your employees been training on cybersecurity awareness, including phishing and social engineering?
- Was there a financial procedure in place to protect against this kind of attack?
- Does your organization have disciplinary procedures in place for when an employee fails to follow established policies?

Processes tested: Security Awareness, Policies and Procedures for financial transactions
Threat actor: Outside attacker
Asset(s) impacted: Email and finance

RoundTable TECHNOLOGY

Compromised Email Account

SCENARIO: Your Chief Financial Officer (CFO) reports strange behavior of his email account to the IT department. After investigating, the support engineer discovers that the CFO's email account has been compromised by a hacker. The hacker has set up blind forwarding of all the CFO's email to the hacker's account and has been sending emails from the CFO to employees and board members of the organization.

What is your response?

Discussion questions:

- What is your response in this scenario?
- Can you determine how long ago the breach started?
- Can you determine what information was compromised?
- Did the CFO have Two-Factor Authentication (2FA) enabled on their email account? What about other employees?
- Can you determine if the CFO's email account was used by the hacker to compromise other accounts?
- Do you have cyber liability insurance? If so, do you know if it covers this type of event? Can you get cybersecurity help from your insurer?
- Have your employees been training on cybersecurity awareness, including phishing and social engineering?
- What, if anything, do you tell your board members? Other constituents? How/when do you notify them?
- Do you have communication templates in place for this type of situation?

Processes tested: Security Awareness, Email Security, Detection and Response
Threat actor: Outside attacker
Asset(s) impacted: Email and finance

RoundTable TECHNOLOGY

Exercise 4

Photogenic Malware

SCENARIO: Javier, a photographer within your organization, uses organization USB flash drives to store and transport photographs and video files. In the course of doing this, he took a few personal photographs that he then loaded onto his home computer by inserting the USB drive into his home computer's USB slot. Unbeknownst to Javier, the USB drive got infected with malware while connected to his personal computer. When Javier later brought the USB drive to work and inserted it into his work computer, it infected his work computer with malware which then began spreading to other computers on the organization network. The malware encrypted critical network files and demanded a ransom of $900 in Bitcoin to decrypt the files.

What is your response?

Discussion questions:

- How would your organization identify and respond to malware infecting your system through this vector?
- How would your organization handle the ransom request? Would you have another means of restoring the files encrypted by the malware?
- How long will recovery take?

What is the process for identifying the infection vector?

Discussion questions:

- What other devices could present similar threats?
- What should management do?
- How can you prevent this from occurring again?
- Does your organization have training and policies in place to prevent this?
- Do policies apply to all storage devices?

Processes tested: Detection ability/User awareness
Threat actor: Accidental insider
Asset(s) impacted: Organization data

RoundTable TECHNOLOGY

The Known Unknown

SCENARIO: A nation-state hacking group threatens to target your organization following a series of articles exposing human rights violations by their government. You do not know the nature of the attack they are planning. How can you improve your posture to best protect your organization?

What is your response?

Discussion questions:

- What are the potential threat vectors?
- Have you considered which attack vectors have been the most common over the past month?
- Are there other methods you can use to prioritize threats?
- Have you checked your patch management status?
- Can you increase monitoring of your IDS and IPS (Intrusion Detection and Intrusion Protection Services)
- If you don't have the resources to do so, is there another organization that could be called upon to assist?
- What organizations or companies could assist you with analyzing any malware that is identified?
- How do you alert your help desk?
- Do you have a way of notifying the entire organization of the current threat (bulletin board, etc.)?
- Does your Incident Response Plan account for these types of situations?

Processes tested: Preparation
Threat actor: Nation State
Asset(s) impacted: Unknown

RoundTable TECHNOLOGY

Exercise 6

The Cloud Compromise

SCENARIO: Your organization's development department frequently uses Dropbox to store large amounts of donor data, some of which may be considered sensitive. You have recently learned that Dropbox has been publicly compromised and large amounts of donor data have been exposed, including names, addresses, emails, gifts and interests. All user passwords and data stored in Dropbox infrastructure also may have been compromised.

What is your response?

Discussion questions:

- How will you determine what information was compromised?
- Does your organization have current policies that consider 3rd party cloud storage?
- Should your organization still be held accountable for the data breach?
- What actions and procedures would be different if this was a data breach on your own local area network?
- What should management do?
- What, if anything, do you tell your constituents?
- How/when do you notify them?
- Do you have communication templates in place for this type of situation?

Processes tested: Incident response
Threat actor: External threat
Asset(s) impacted: Cloud Data

RoundTable TECHNOLOGY

Exercise 7

Financial Break-In

SCENARIO: A routine financial audit reveals that several people receiving paychecks are not, and have never been, on payroll. A system review indicates they were added to the payroll approximately one month prior, at the same time, via a computer in the financial department.

What is your response?

INJECT: You confirm the computer in the payroll department was used to make the additions. Approximately two weeks prior to the addition of new personnel, there was a physical break-in to the finance department in which several laptops without sensitive data were taken.

OPTIONAL INJECT: Further review indicates that all employees are paying a new "fee" of $20 each paycheck and that money is being siphoned to an off-shore bank account.

Having this additional information, how do you proceed?

Discussion questions:

- What actions could you take after the initial break in?
- Do you have the capability to audit your physical security system?
- Who would/should be notified?
- Would you be able to assess the damages associated from the break in?
- Would you be able to find out what credentials may have been stored on the laptop?
- How would you notify your employees of the incident?
- How do you contain the incident?
- Optional Inject question: How do you compensate the employees?

Processes tested: Incident Response
Threat actor: External threat
Asset(s) impacted: HR/Financial data

RoundTable TECHNOLOGY

Double Whammy

SCENARIO: Your organization is located within a flood zone. Winter weather combined with warming temperatures has caused flooding throughout the area. Local authorities have declared a state of emergency. In the midst of managing the flooding, a ransomware attack occurs on your facility, making computer systems inoperable.

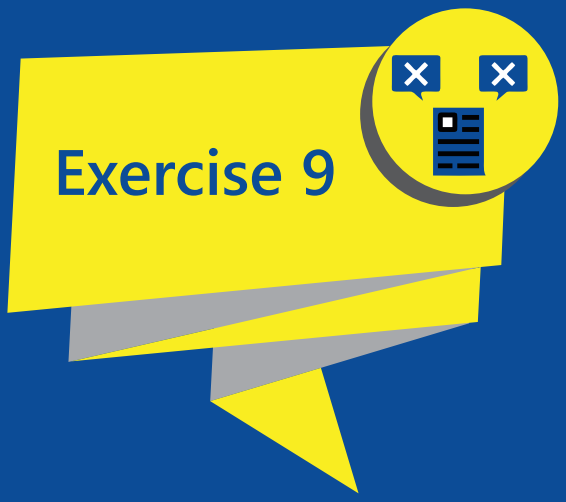
What is your response?

Discussion questions:

- Do you have a COOP (Continuity of Operations Plan) or DRP (Disaster Recovery Plan)?
    - o If so, do you carry out an annual simulation to ensure the COOP or DRP is sufficient and running smoothly?
- Do you have an Incident Response Plan (IRP) that specifically details ransomware steps?
- What steps will you take if restoring from backup is not an option?
- Does your IRP only take into account the financial implications of a cybersecurity incident, or does it consider the severity of the situation as well?
- Do you have a plan in place for how to acquire bitcoin?
- Have you considered that a targeted ransomware attack may require more bitcoin than is easily accessible on the market?
- Do you have a backup for completing Emergency Operations Center (EOC) processes without a computer system?
- Can you route emergency communications/processes through a neighboring entity?
- Who do you need to notify, and how will you do so?
- Consider that increased phone traffic may be congesting the lines.

Processes tested: Emergency response
Threat actor: External threat
Asset(s) impacted: Emergency Operations Center Processes

RoundTable TECHNOLOGY



The Deepfaked Special Guest

(Disinformation Campaign)

SCENARIO: Jackie, a new videography intern with Campaign Momentum Group (CMP), was thrilled to film a special event about dark money and politics featuring rising star Senate candidate, Lauren Tish, a few weeks before election day. The event ran late, so Jackie immediately uploaded the rough video to the CMP shared Dropbox account when she got home. The credentials for the Dropbox account are stored in her computer's Chrome browser. By the next morning, the event was all over the internet, along with the hashtag #TishFake. In the video Tish could be heard saying "Of course pharma helps pay for this. And since no one expects it, I can fake it." The video seemed off, but Tish's voice was clear. How would leadership explain this exploit for such a high stakes ally? Analysis quickly revealed that deep fake audio had been generated and inserted into the video. After reviewing with Dropbox, it was determined that someone had been logging into the shared Dropbox account from nearby Boston. More research revealed this was likely a former roommate of Jackie's who had grabbed the Dropbox password. Her former roommate was a 4Chan user and was seeking to boost his 4chan reputation by getting a hold of a candid Tish video so close to the election. The audio edits were surprisingly easy, and then once the roommate dropped his remake into the group, it was less than an hour before #TishFake got bot-propelled into a trending topic.

What is your response?

Discussion questions:

- What is your response in this scenario?
- Is there a password manager in place and is access to that controlled?
- Why is Dropbox a Shared Account? Why not use individual accounts with 2FA enforced (trying to save money?)
- What is an intern's level of access?
- Does each person -- employee or intern -- have a unique login if they need access to key systems?
- Is there a way to know the range of people who may have once had or still have access to Dropbox?
- What is the intern's responsibility in this situation?
- Is there a way of tracing provenance for raw video, audio files?
- Are there policies for using the organization's content repositories from personal, non-work-issued computers?
- Do staff understand how deepfake and other potentially malicious technologies can be deployed?

Processes tested: Incident response, Crisis PR/Communications
Threat actor: Internal-external threat
Asset(s) impacted: Cloud (Dropbox)

RoundTable TECHNOLOGY

Exercise 10

DDoS via bot

SCENARIO: Early morning, November 3rd, 2020. Election day. George tried to login to CMS to update the blog and found the site was inaccessible. The site had been tested earlier, multiple times, and on multiple devices and everything had checked out. But now it was just shy of 1am and the site would not load and kept displaying the same message - Error 503. The server was down. After a few phone calls and repeated attempts, George woke Julie, the web developer. A few hours later she reported that it looked like they had been hit with a Distributed Denial of Service (DDoS) attack. There had been a spike in service right around midnight. The sheer volume of traffic could only be explained by a coordinated botnet flooding the site with traffic and data requests, bringing the server to a halt. The website host reported that they were working on the situation, but at present there was nothing they could do to bring the website online until the DDoS stopped.

What is your response?

Discussion questions:

- Has the organization evaluated WAF (Web Application Firewalls) such as CloudFlare (Project Galileo)
- Is there any sort of Response Team at RepUs to ensure an organized, efficient response?
- Is there a process for escalating this incident - have all of the right internal and external contacts been contacted?
- Was there a monitoring system that could have identified this ahead of the site coming down?
- Do we have any sort of server backup plan? Is there a failover established, especially as a way to plan for crucial dates and events?
- Had all website updates and patches been installed?
- Was a website Penetration Test been conducted, and had the web team addressed all identified vulnerabilities?
- Is the website continuously monitored and reviewed for vulnerability to new forms of malicious attack?

Processes tested: Incident Response, Resiliency
Threat actor: External threat
Asset(s) impacted: Website

RoundTable TECHNOLOGY

Free Wi-Fi Gets Quite Costly

SCENARIO: Jason had been running late all day - he got to the airport for his pre-dawn flight late, the report that was due yesterday was still unfinished. It's easy to imagine his relief when he heard that the plane was unexpectedly delayed and Houston has free wifi. Even though Jason was wary of public wifi, he figured he could log on quickly, pull his document down for local editing and then get out. What he didn't realize was that the public wifi with the name "Free Airport Wi-Fi" was actually run by a hacker, who only needed a few seconds to have full access and grab Jason's network credentials. That's all the hacker needed to access the company's cloud drive and encrypt everything on it. Jason was 30,000 feet and finishing off the off-line version of the report by the time his colleagues down on terra firma were finding themselves locked out of their files with only a bitcoin ransomware message.

What is your response?

Discussion questions:

- What is your response in this scenario?
- Do you have an Incident Response Plan (IRP) that specifically details ransomware steps?
- Was a 3rd party backup system in place, and if so, had it been tested?
- Since all files are inaccessible, what steps will you take if restoring from backup is not an option?
- Does your IRP only take into account the financial implications of a cybersecurity incident, or does it consider the severity of the situation as well?
- Do you have a plan in place for how to acquire bitcoin?
- Have you considered that a targeted ransomware attack may require more bitcoin than is easily accessible on the market?

Processes tested: Incident Response, Resiliency
Threat actor: External threat
Asset(s) impacted: Cloud/Organizational Data

RoundTable TECHNOLOGY

Exercise 12

A Visit from the Anti-Science Doxxers

SCENARIO: You had really grown protective of Maxine, the researcher who had spearheaded the study that you hoped would put an end to the supposed "science" around the coal resurgence. You both knew that the push for coal had been nothing but well-funded political theater. You had been thinking how fortunate that Maxine wrapped up before the US Energy Summit. So, you were not at all prepared for the call that came in from her at 6am on the morning of the Summit. Her private information - home address, personal phone, the names of her children - was circulating on the web. She had started receiving calls during the night. You looked for yourself, comments about Maxine, about your organization, littered your organization's public Facebook page - in the hundreds, maybe even thousands. Your Twitter accounts showed tens of thousands of notifications. You learned that one caller threatened to find Maxine's youngest child at school, another said he was right outside waiting for her. She called the police who arrived 20 minutes later to a dead animal placed on the front door mat along with several lumps of coal. The police were there when she called you. She was calling to let you know so that you could take care of things for the organization.

What is your response?

Discussion questions:

- Were there any standard privacy or security practices in place?
- Do your staff know what public/private records are available online?
- Is there a policy of reviewing terms of service and performing opt-outs where possible?
- Do Self Care plans exist for staff who are involved with potentially risky or controversial projects?
- What is the proper incident response protocol for this type of attack?
- Is there a process for escalating this incident - have the proper security and governmental contacts been notified?

Processes tested: Incident Response, Resiliency
Threat actor: External threat
Asset(s) impacted: Privacy

RoundTable TECHNOLOGY

Exercise 13

The Compromised Sendee

SCENARIO: You woke up from your sleep in a state. You were pretty sure that the special reporter knew to keep her identity and whereabouts under cover, at least until after the Copenhagen event. But the email you got from her a few hours ago just didn't seem right. You checked. It was from the right account, the one she used only for this project, and only you and a few others even knew about it. It just didn't sound like her. You knew you should have called but it was late, so you sent the latest version of the research without calling first as you normally might have, especially given that the email just didn't quite sound like her. You checked your email again. Nothing back from her, but it had gone out and the report with all of the damning information was in there. There it was in "sent." You try calling and she doesn't pick up.

What is your response?

Discussion questions:

- What should you do right away?
- How do you attempt to get a hold of this reporter without further risking her safety?
- What processes are in place if you suspect something malicious has happened?
- What about your own email account do you need to check? What do you need to change?
- How would you find out if the document had been intercepted? How could you have prevented the information from getting out?
- What further tests should you run on your own devices?

Processes tested: Incident Response, Resiliency
Threat actor: External threat
Asset(s) impacted: Cloud/Personal data, devices

RoundTable TECHNOLOGY

Exercise 14

Cleaned-out Border Crossing

SCENARIO: The border crossing at Rantau Panjang was usually fairly uneventful, especially now that the flooding was over. Your passport and necessary papers were in order, everything seemed fine until your one-word answer to the question to the armed guard about your profession, "Journalist." You were told to sit down and hand over your electronic devices. You pulled your phone from a pocket immediately, with a smile, in the hopes that the guard wouldn't ask you to open your bags and handover your laptop. A few minutes later, he was back, he couldn't unlock the phone "give me your password" and then "You got a computer?" That contained reports, some of which needed redaction, and lists of your contacts.

What is your response?

Discussion questions:

- With so much private, confidential information on your devices, what do you do?
- How do you comply with the demands of the border agent while maintaining your own safety and the confidentiality of your professional contacts?
- How could your devices have been more protected?
- What plans does your organization have for travel in potentially high risk areas?
- Are there backups in the event that the devices are not returned to you?
- With your phone taken, how would you alert your colleagues at the home office about what had happened?
- Is there anything they can do from their end to further protect sensitive information?

Processes tested: Preparedness, protection, planning, resiliency
Threat actor: External threat
Asset(s) impacted: Data, devices

RoundTable TECHNOLOGY

Exercise 15

Connecting the OSINT Dots

SCENARIO: Sanjay and Gerald were relieved. The fruits of their labor would finally culminate in a indisputable report of the facts - "Who is Funding Oil Politics in Indonesia?". On the verge of release, it was not too soon to start laying groundwork, so Gerald naturally asked Global Energy Fact Finders (GEFF) to start promoting the report on its Twitter feed. With barely a mention of its author, Sanjay's energy activist group posted a few of the more telling images - a set of diagrams clearly delineating sources of dark-money influence. What neither Gerald nor Sanjay were aware of was that Indonesian powers-that-be had been following both of them closely through open source intelligence service. The near simultaneous social media posts would be key in tying the GEFF report with Sanjay's group, considered too radical by many professional circles. Exposing this connection would surely hurt both the reputation of the report and its sponsoring organization. It was hoped that the threat of a ransom demand and exposure would put an end to the report's release to the public. This connection also provided the Indonesian government with motivation to jail Sanjay on some minor infraction, and put an end to his relentless sniffing around.

What is your response?

Discussion questions:

- How could this have been prevented/mitigated?
- Does the organization have a system for classifying information - public, internal, restricted, top secret?
- How would both Sanjay and Gerald have known how to use a classification system if it existed?
- Were Sanjay or Gerald (and any others working on sensitive information) aware of the capabilities of OSINT?
- Had social media policies been clearly articulated and socialized to all staff and collaborators with the organization?
- Was Sanjay aware that posting the charts that he selected on Instagram would constitute a risk, both to himself and to the organization?

Processes tested: Policy, protection, planning
Threat actor: External
Asset(s) impacted: Work product/assets

RoundTable TECHNOLOGY

Exercise 16

The Open Vault

SCENARIO: One of your company's newer web developers, Jake, calls his direct manager, Sara, to report that he got an email about a login to his 1Password account from Poznan, Poland a couple weeks ago. He acknowledges that he should have reported it when it first happened but he didn't think it was anything serious. But Jake got another notification of a login the previous night from Sydney, Australia. Sara learns that Jake's 1Password credentials were similar to a password he used frequently and that he had not set up 2FA for his 1Password account. Jake had been providing maintenance for several high profile client projects -- one was a website for a political advocacy organization campaigning on a very contentious ballot measure on immigration. The organization's website is used to gather supporter and volunteer data. No clients have reported anything suspicious yet.

What is your response?

Discussion questions:

- Does Sara have a clear policy instructing her on what she should do with this information?
- Does the organization have an Incident Response Plan (IRP) that details actions to take next?
- What steps would you take to figure out what client sites might be compromised?
- How would you determine whether any client website projects, such as whether the candidate website, had been attacked and/or used for malicious purposes?
- What policies exist to guide all levels of employees regarding password policies?
    - o 2FA?
    - o Saving passwords on computers?
- How would you determine if and who to notify?
    - o How will you do so?
- Does your cyber liability insurer provide services to help with a response?
    - o Do you have their claim information readily accessible?

Processes tested: Employee awareness, Emergency response
Threat actor: Internal (misconfiguration) / External (exploit)
Asset(s) impacted: Password vault, client web properties

RoundTable TECHNOLOGY

The Bamboozled Bookkeeper

SCENARIO: Your bookkeeper reports strange behavior of his email account to the IT department. After investigating, the support engineer discovers that the bookkeeper's email account has been compromised by a hacker. The hacker has set up blind forwarding of all the bookkeeper's email to the hacker's account and has been sending emails from the bookkeeper to employees and customers of the organization.

What is your response?

Discussion questions:

- What is your first response?
- Do you have an incident response plan and/or checklist for responding to a situation of this type?
- Can you determine how long ago the compromise happened?
- Can you determine what information was compromised?
- Did the bookkeeper have Two-Factor Authentication (2FA) enabled on their email account? What about other employees?
- Can you determine if the bookkeeper's email account was used by the hacker to compromise other accounts?
- Do you have cyber liability insurance? If so, do you know if it covers this type of event? Can you get cybersecurity help from your insurer?
- Have your employees been training on cybersecurity awareness, including phishing and social engineering?
- Do you have documentation of your bookkeeper taking this training?
- What, if anything, do you tell your clients?
- Partners? Contractors?
- How/when do you notify them?
- Do you have communication templates in place for this type of situation?

Processes tested:
Threat actor:
Asset(s) impacted:

RoundTable TECHNOLOGY

Exercise 18

The Holiday Buffalo Jump

(specific to IT Service Providers)

SCENARIO: It's Sunday morning, November 29th, 2020. Everyone except a few Tier 1 helpdesk personnel is enjoying the last day of the Thanksgiving holiday. At around 11AM, senior engineers on call start seeing their phones light up. Some customers have called in saying they can't access their workstations. The Tier 1 helpdesk can't get into the PSA or the RMM systems. As the hours pass, more customers call in saying both servers and workstations are inaccessible. By 3:00 PM, you have determined that attackers have compromised both your PSA and your RMM and have locked you out of both systems. Many, possibly all workstations and servers in the RMM environment are locked with ransomware, but you can't tell how many because you can't access the RMM yet. At 4:30 PM, the attackers get in touch. The attackers provide proof that they have exfiltrated data from the compromised environments and threaten to publish to the dark web if the ransom isn't paid. The attackers are asking for $600,000 to unlock everything and delete the exfiltrated data.

What is your response?

Discussion questions:

- What is your first response?
- Are you, in any way, prepared for this situation?
- Do you have an incident response plan for this situation? Do you know where it is?
- Do you have cyber liability insurance? If so, do you know if it covers this type of event? Can you get an incident response team from your insurer?
- What do you tell your clients? Do you have a means of communicating with your clients outside of your PSA?
- How will you regain control of your PSA and RMM?
- Will you consider paying the ransom? Are you aware of the legal implications of paying the ransom? Do you have financial and technical means for paying?
- Can you estimate, even roughly, how long it will take to get client environments back online if you don't pay ransom?
- If you perform bare metal restores, will you try to retain any forensic evidence?
- Do you have communication templates in place for this type of situation?

Processes tested:
Threat actor:
Asset(s) impacted:

RoundTable TECHNOLOGY

Exercise 19

The Third-Party Leak

SCENARIO: You get the following email from your CRM vendor, **Zombo.**

In June of 2020, Zombo discovered and stopped an attack.
Prior to our locking the cybercriminal out, the cybercriminal exfiltrated a subset of data from our environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data was our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

What This Means for Your Organization Specifically
A copy of your Zombo CRM data was part of this incident. The cybercriminal did not gain access to credit card numbers, bank account information, usernames, passwords, or social security numbers stored in your database because they were encrypted. None of your data was lost or corrupted as a result of this incident.

What is your response?

Discussion questions:

- What is your first response upon getting this email?
- Do you have an incident response plan that can be put into action for this situation?
- How can you determine what information was part of this breach? How can you determine which clients were affected?
- Do you know what your legal notification requirements are for your affected customers?
- Do you have cyber liability insurance for this type of incident? Do you know what support your insurer can provide? Legal? Incident Response? PR?
- What, if anything, do you tell your clients? How/when do you notify them? Do you have communication templates in place for this type of situation?
- Given the information breached, how can you mitigate future risk of this information being used by attackers against you and/or your clients?

Processes tested:
Threat actor:
Asset(s) impacted:

RoundTable TECHNOLOGY

Exercise 20

The Deep State Deep Fake

SCENARIO: Dena Digital is a digital strategy consultancy that specializes in helping progressive organizations with campaigns, such as fundraising, but also contentious ballot measures across the United States. Dena Marks, the CEO of Dena Digital, is a charismatic leader who is frequently interviewed on podcasts and radio programs. Dena was recently interviewed harshly criticizing a congresswoman who is an outspoken follower of the deep state conspiracy group K-ANON. Dena is travelling internationally and, earlier in the week, had tweeted about how excited she was to be attending an upcoming digital conference in Sweden. Sam, a senior developer at Dena's Digital, notices a missed call and voicemail from Dena's mobile number when he turns on his phone in the morning. Sam listens to the voicemail from Dena,

"Sam, this is Dena. I got locked out of my Gmail account and can't get to my email or Google Drive. By the time you get this voicemail I'll be in conference sessions, so you won't be able to reach me. Can you please email my Google account password to my personal email as soon as you get this? My personal email is dena.digital@protonmail.com. Please do this as soon as you get this message. Thanks a ton!"

Sam immediately complies with the request, but when he doesn't hear back from Dena after several hours, he decides to give her a call. Sam gets her voicemail and leaves a message asking her to confirm that she got the passwords. A few hours later, Sam tries to login to the agency's Google Ads account, but gets a message that he does not have access to the Google Ads account. As he is investigating this, he gets a phone call from a frantic sounding Dena saying she never left such a voicemail and wasn't locked out of her account, but that now she is locked out of her accounts.

What is your response?

Discussion questions:

- Did you provide security awareness training to all personnel? Within the past year? Did this training cover social engineering? Did this training cover new and emerging threats such as deep fake audio?
- Do you have a policy governing acceptable information sharing on social media?
- Was 2FA enforced for all agency Google accounts? Was SMS discouraged or disabled as a 2FA option?
- Do you have an Incident Response Plan (IRP) that identifies a response team and a checklist of actions with contact information for needed resources?
- What policies exist about acceptable methods of sharing passwords and other restricted information?
- Does your cyber liability insurer provide services to help with a response? Do you have their claim information readily accessible?

RoundTable TECHNOLOGY

Additional (free) CIS Resources

CIS Benchmarks: https://www.cisecurity.org/cis-benchmarks/

CIS Controls: https://www.cisecurity.org/controls/

CIS-CAT Lite: https://learn.cisecurity.org/cis-cat-landing-page

Sample Remediation Kit: https://learn.cisecurity.org/remediation-kits

Webinar: CIS-CAT Pro Demo: https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-webinar/

Additional Resources Recommended by RoundTable

Incident Response Report Form: RoundTable Incident Response form

Backups vs. Business Continuity eBook: Datto - Backups vs. Business Continuity ebook

Field Guide for Incident Responders: Digital Guardian - Field Guide to Incident Response

RoundTable Webinar Recording: - What now? Incident Response webinar recording

Recovery Time Calculator: Datto - Recovery Time Calculator

Ready.gov: www.ready.gov/workplace-plans

American Red Cross: Readiness Rating

Preparatory Steps

List out some or all of the reasonable preparatory steps you can take to better prepare yourself for these scenarios. A couple of examples included:

Action	Time	Responsible	Outcome
Enforce 2FA on Email and Password Manager accounts	2hrs	Joshua	All ORG email and password managers protected by 2FA
Review Cyber Liability insurance	2hrs	Kim	Determine all resources available from cyber insurance provider and add information (including procedure and contact) to ORG incident response plan.