TruStage™

Incident response

tabletop exercise & discussion guide

Cyber threats, such as ransomware, distributed denial-of-service (DDoS) attacks, and supply chain interruptions, have provided organizations an opportunity to reclaim and reinvigorate incident response planning. While there is no one correct way to develop and test your incident response plans; it is important to continuously improve the plan by incorporating lessons learned.

Tabletop exercises for incident plans use a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. These resources assist you to initiate discussions within your organization about your ability to address a variety of cyber threat scenarios.

Cyberattacks can cripple networks and jeopardize critical aspects of your organization. Incident response plans must emphasize speed and flexibility, so you are able to quickly adapt to rapid change.

Each exercise and scenario are customizable and should involve discussion questions to assist your key stakeholders with the ability to identify gaps and potential issues.

It is essential that your leadership and employees use fact-based information and tested alternatives to enable real-time decision making. This integrated, comprehensive approach will help you build long-term operational resilience and prepare the credit union organization for any future cyber disruption.

Clearly, there is a lot at risk when it comes to incident response planning.

Do you know what to do if you are a victim?

An incident response plan is a critical component in your ability to take the necessary actions to respond to data breaches efficiently.

Establish a core vision that is tailored to your credit union's specific business objectives and priorities. However, your focus must go beyond vision and theory; you need application.

Testing your incident response plan's level of resilience can be strengthened by identifying the potential events that could affect your business, grading risks according to the impact, and then implementing a strategy to mitigate and manage risks.

And your partners are crucial to the resilience of the credit union. Understanding how partner/vendors will respond and adapt to change will contribute to improved resilience.

Remember, a tabletop exercise isn't an exam. It should be a convincing simulation that lets your team practice working through your incident response plan and identifying needed changes in that plan.

The incident response tabletop exercise is built around the concept that your organization likely will be impacted by some sort of cyber incident and proactive preparation will help minimize the damage.

Incident planning checklist

Developing purpose statements is a really good way to begin. It can create clarity about what the event will entail.

It should include or sound like:

- To raise awareness and understand threats
- To review preparedness for a high impact events with focus on evaluating the critical functions and ability to ensure business continuity
- To provide an opportunity to discuss and explore key issues, using a structured scenario loosely based on real-life events
- To identify strengths and areas needing improvement with regards to a particular event/scenario
- Opportunity to practice a response so that in a live situation it is not the first time
- As a training mechanism to improve team member response capabilities
- To identify gaps in existing plans
- To identify characteristics unique to your organization; geographical, logistical, demographical, etc.

Setting expectations

A tabletop exercise is a facilitated discussion of a scripted scenario in an informal, stress-free environment that is based on current policies, plans, and procedures. The exercise should identify strengths and weaknesses, and/or achieves changes in policies and procedures. The success of the exercise depends largely on group participation.

- Key performance indicators/key success indicators or metrics for measuring results
- Funding limits – how much should a planning exercise cost
- How will recommended revisions to current plans, policies, and procedures be communicated
- Encourage open and honest dialogue and feedback throughout the exercise
- Participants should feel free to ask questions to one another and challenge each other's assumptions
- No one will be singled out or punished for what they say during the exercise
- Make a commitment to act on the lessons learned during the testing stages
- Set realistic follow up timelines

Tabletop exercise basics

This is where the fun begins, and planners can get creative. A few things that you should keep in mind as you start planning for your next incident response tabletop scenario, while the scenario is the centerpiece of the exercise it is not the only document you will prepare in advance of the event.

The exercise begins with a general setting, which establishes the stage for the hypothetical situation. In your exercise, the facilitator stimulates discussion by intelligence or situation updates. These updates describe major events that may be directed to individual players or participating departments, agencies, or organizations. Recipients of the updates then discuss the action(s) they might take in response to the situation/incident.

Cyber incident tabletop exercises are a true test of your credit union's cybersecurity readiness and incident response capabilities.

Through a simulation of a real-life cyber attack scenario, you will be able to evaluate and enhance your preparedness and response to a cybersecurity incident. The exercise will help identify existing gaps in your cyber incident response plan. It will also help build your team's familiarity with it, so they better understand their individual roles and responsibilities.

During the tabletop exercise, the facilitator utilizes key questions which focus on roles (how they would respond in a real situation), plans, coordination, the effect of decisions on other functions, and similar concerns to drive the discussion.

The scenario makes the difference by introducing key events that occur during the incident. Choosing the right scenario can make an otherwise mediocre exercise a memorable and valuable experience for the participants and the credit union.

Steps to a successful exercise

1. Review the list of supporting documents needed to test your incident plan.
2. Identify your exercise planning team – facilitator; participant; observer; and evaluator
3. Hold a objectives meeting. Gain agreement regarding exercise concept (scope, type, mission area[s], exercise program priorities to be addressed), exercise objectives, aligned core capabilities, and timeline.
4. Hold an initial planning meeting. Determine if you'll organize the exercise and discussion as a single group or use a multi-table format organized by functional area.
5. Develop the exercise by coordinating logistics and selecting the scenario.
6. Hold a final planning meeting to ensure all exercise elements are ready. Be sure to resolve any open planning issues.
7. Make documents available for each participant.
8. Conduct the exercise. Exercise conduct involves activities such as preparing for the exercise; managing the presentation, facilitation, and discussion; and conducting immediate exercise wrap-up activities.
9. Ensure the facilitator is responsible for keeping the discussion focused on the exercise objectives and making sure all issues are explored within the time allotted.
10. The end goal of the exercise is to produce an after-action report with recommendations for improving preparedness capabilities for your organization. The improvement plan should provide timelines for improvement recommendation implementation and assignment to responsible parties. This plan should be an ongoing effort by your organization.

Facilitator

- Engaging
- High energy
- Disciplined
- Good presenting and facilitating skills
- Comfortable with technology
- Ability to remain neutral

Participant

- Representation from all key functional areas
- Knowledgeable about their area and process
- Vocal and willing to participate
- Willing to step outside comfort zone
- Security officers and facility managers

Observer

- Passive role
- Attention to detail
- Ability to document thoughts and notes
- Good understanding of broader credit union operations

Evaluator

- Knowledgeable of CU goals and objectives
- Analytical
- Decision-makers
- Understands the guidelines set forth during planning

Key elements for your tabletop exercise

Setting your agenda

Each tabletop exercise is typically recommended to take approximately four hours to an entire day. The actual duration and agenda is scalable to the needs of your organization and to your exercise's objectives.

Most agendas will follow this order:

- Welcome / Session Introduction
- Threat introduction review & discussion
- Incident & aftermath review & discussion
- Incident response & recovery review & discussion
- Event evaluation discussion
- Closing & next steps
- Debrief

Selecting your tabletop scenario

Cyber threats come in many shapes and sizes and some of scenarios will be more applicable to your organization than others.

Implementing and facilitating a tabletop exercise can be accomplished yourself or by using a partner – such as your cyber insurance and risk management provider.

No matter your approach, you will have to select a scenario to get started. Some popular incident response tabletop exercise scenarios are:

- Ransomware
- Cyber extortion
- Insider threat
- Information stealing trojans
- Software vulnerability exploitation
- Cloud-based data breach
- Vendor supply chain compromise

Remember, in most cases, only the facilitator knows all the details ahead of time

Keep your scenarios real

- **Custom details**
  Tailor the scenario to your organization by using names of actual employees or job functions, the software your team uses, real third-party providers, etc. This will heighten the realism and help everyone grasp the potential consequences.
- **An unfolding threat**
  Throw in a series of developments and plot twists to reflect that, in a real-life incident, not all the facts upfront.
- **Unavailable personnel**
  At some point, reveal that whoever is in charge of your team (or a staff member or vendor with necessary expertise) is not available. This forces everyone to work on the problem on their own rather than just saying that they'll call someone else for guidance.
- **Outside pressure**
  Include questions from members, partners, the media, bad actors etc., in the mix to raise the tension and test the aspects of the communications component of your incident response plan.

Essential questions that should be used in any scenario

With any tabletop exercise or scenario that you use, structure the exercise so that participants can successfully participate through discussion of these questions:

- Does this qualify as an incident? Who will assist you in determining?
- When should I contact my insurance and risk management partners - TruStage™ and Beazley?
- What's your first step after realizing that something odd is happening?
- What security breach notification laws does your state or NCUA have in place? What notification obligations exists? What is the potential impact to your organization?

Considerations for non-IT priorities

What needs to be done from the standpoint of:

- Internal communications
- External communications
- Legal
- Risk management/insurance
- Contractual

- What information/evidence do you need to collect regarding the incident?
- How do you know what data was compromised/exfiltrated?
- How do you secure your systems?
- What cybersecurity incident escalation criteria is defined in your cyber incident response plan?
- Who else in your organization needs to be notified and what should be shared internally?
- How long will it take to recover your data from backup? Will it be necessary to implement workarounds and how long may it take?
- Do you have talking points ready for staff members who may get calls from members? When do you proactively notify customers of the problem?
- What deadlines from your service level agreements (SLAs) are at risk while your system is compromised?
- What is your organization's decision-making process regarding ransomware payments? Are ransomware policies/procedures including in your plan?
- What are your reporting requirements after the incident is over?

Scenario exercise
Ransomware

1

Short scenario

Day 1:
An Alert is issued regarding a new ransomware variant. It is reported that bad actors are using the ransomware to target financial institutions.

Day 2:
An employee received and mistakenly opened several emails on their work laptop which contained sensitive organizational information and access to several credit union data sources.

Day 4:
A few days later, the employee informs IT that they opened the emails and negligently provided sign-on information.

Day 6:
An increase in Domain Name System traffic outside of standard business hours is flagged by your organization's intrusion detection system and an alert is sent to your IT team.

Upon further investigation of the system logs, they discover that a significant amount of data was transferred to external IP addresses

Day 7:
As a member of the C-suite, you open your work computer one Monday morning and find that when you try to log in, you are greeted by an unfamiliar message demanding that you send a sum of money in cryptocurrency to an unknown party, who in exchange will unlock your devices and data.

Computers throughout your organization display a blank screen. A ransom message then appears demanding $1 million worth of Bitcoin for the decryption key and a warning that the key will expire unless payment is received within 48 hours.

Suggested discussion questions

- How does your incident response plan describe the actions that your organization should take at this time?
- Describe the training your employees receive on this plan.
- How can your organization be certain that your data has been stolen?
- What guidance does the plan include on assessing the severity of the incident?
- How will you contain/stop the spread?
- What redundant systems exist for when primary systems are compromised?
- Who can authorize use of alternate systems or procedures?
- How long can you perform manual or alternate processes on your critical systems?
- What is your organization's decision-making process regarding ransomware payments? If decided, how would you pay the demand?
- Discuss potential legal and reputational ramifications of paying or not paying the ransom.
- What additional resources outside of your organization would be necessary for responding to the cyber incident?
- What are you communicating? Describe your processes to respond to the media and inquiries about the incident.
- How would you preserve and reinforce your reputation?

Scenario twist

Day 10: A security blogger reports on a series of Dark Web posts that a well-known hacker group has shared data records from your organization – including employee social security numbers, bank account and routing number information. News outlets report on the cyber incident. Several contact your organization for comments on the potential ransomware infection and data breach.

Scenario exercise

Vendor supply chain compromise

2

Short scenario

A Service Provider is the victim of a cyber incident, leading to impacts on the managed services they provide to your organization.

Day 1:
A release announces that malicious actors executed cyber attacks against one of your third-party Service Providers and their downstream customers. The malicious actors leveraged a vulnerability in a popular Remote Monitoring and Management software. Once the malware was discovered, the software was shut down. The third-party provider is unable to provide services to customers worldwide, affecting the critical functions of entities across multiple sectors. Your organization is not impacted currently.

Two months later:
Several employees at your organization report they're unable to sign in to the network when they arrive in the morning. Your IT helpdesk is inundated with calls reporting the issue. Your IT department contacts the third-party Service Provider, but they are unable to reach any of your key contacts.

Two months + one day later:
During routine monitoring, your security team identifies suspicious network activity that is traced back to the third-party application. Employees are also unable to access your network. There is a significant impact to business-critical systems.

When you reach the Service Provider, it is discovered that the cyber attack months ago impacted their widely-used platform. It is suspected your systems unknowingly have had malware for several months and you could be affected by the malicious code. It is suggested that you take steps to identify the malicious code and eradicate it.

Suggested discussion questions

- How does your incident response plan describe the actions that your organization should take at this time?
- How are third-party vendors involved in your incident response plan?
- Does your service-level agreement include incident response activity?
- What guidance does the plan include on assessing the severity of the incident?
- Does this third-party vendor have access to your organization's network & data?
- How will you contain/stop the spread?
- What steps will you take to protect organizational data from theft/loss?
- What redundant systems exist for when primary systems are compromised?
- Does your plan define escalation criteria, notifications, and action steps?
- What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period? How long can you perform these processes?
- Discuss potential legal and reputational ramifications of the compromise and impact to your organization.
- What additional resources outside of your organization would be necessary for responding to the incident?
- What are you communicating? Describe your processes to respond to the media and member inquiries

Scenario twist

Approximately 25 members have contacted you that they are having difficulties connecting to your online banking application to make necessary transactions. Many have expressed significant concerns and have commented that they may be closing their accounts with your credit union. Unfortunately, you are not immediately sure if these situations are connected to the vendor issue.

Incident response tabletop exercise & discussion guide

It's great to have well-documented cyber incident response plans, playbooks and processes. But if nobody knows what's inside them, they're of little use to you.

Incident Response Tabletop Exercises help you rehearse your incident response strategies. They're a confirmation of the effectiveness of your plans, policies and processes, people, internal coordination, vendor and third-party coordination, communications, and decision-making abilities.

Most importantly, validating incident response plans and processes can significantly reduce the chances of poor decisions and missteps.

Recap: Tips for an effective tabletop exercise

- Gain leadership buy-in to the importance of the activity
- Tailor your tabletop exercise to your organization to create real-life situations
- Expand your participants beyond just technical staff
- Choose a top-notch facilitator – consider working with your insurance/risk management partners to assist with the exercise
- Test people can reliably perform in unexpected situations, not technology
- Keep the number of participants in line – not too many…not too limited
- Dedicate the exercise gets the time needed. Encourage participants to be all-in
- Ensure the exercise is conducted in a safe space – no pressure to win or lose, but rather understand what works and what doesn't
- Use insights gained to make improvements to your incident response plan

TruStage™ Cybersecurity Protection

With our best-of-class cyber solution, you can be confident that we carefully focus on arming you with the protection you need.

This exclusive TruStage & Beazley solution provides your credit union with premier insurance coverage along with insights and resources on risks, losses, and other protection needs with credit union specifics in mind.

In addition to resources within the TruStage Business Protection Resource Center, as a Beazley policyholder, you have direct access to cybersecurity resources and training at **www.BeazleyBreachSolutions.com** related to compliance & laws, safeguarding information, and preparing to respond to breach incidents.

Looking for additional insights?

- Access the **Business Protection Resource Center** (User ID & password required) for exclusive risk and compliance resources to assist with your loss control efforts.
- If you'd like to discuss this risk in more detail, simply connect with a TruStage™ Risk Consultant by contacting us at **riskconsultant@trustage.com** or at **800.637.2676**.

TruStage™