EAB

Security Incident Response Tabletop Exercises

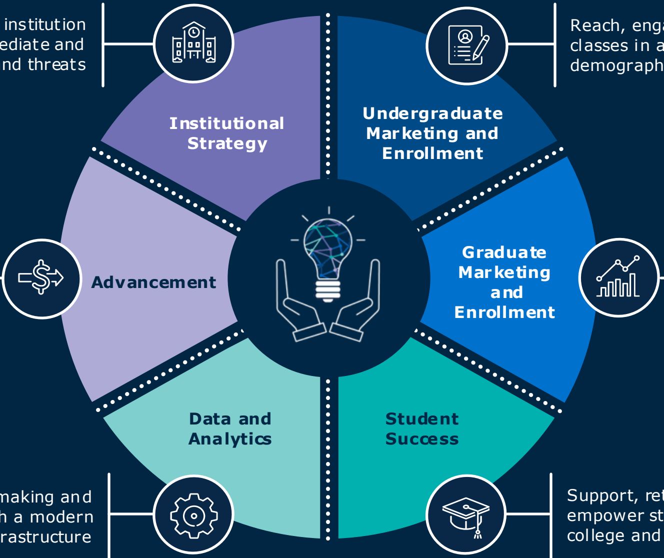
Mobilizing Crisis Leaders to Respond to Security Incident Emergencies

IT Forum

EAB

Education's Trusted Partner to Help Schools and Students Thrive

Insight-powered Solutions for Your Top Priorities and Toughest Challenges



Institutional Strategy

Future-proof your institution by addressing immediate and long-term opportunities and threats

Undergraduate Marketing and Enrollment

Reach, engage, and enroll future classes in a dynamic market with demographic headwinds

Advancement

Meet aspirational giving goals in an era of competing fundraising priorities and shifting donor interest

Graduate Marketing and Enrollment

Secure enrollments and revenue in an evolving graduate, online, and adult learner market

Data and Analytics

Improve decision-making and accelerate innovation with a modern data and analytics infrastructure

Student Success

Support, retain, and empower students in college and beyond

We partner with 2,800+ institutions to accelerate progress, deliver results, and enable lasting change.

95%+ of our partners return to us year after year because of results we achieve, together.

K12 • Community Colleges • Four-Year Colleges and Universities • Graduate, Professional, and Adult Programs • Employers

eab.com

1 **Why Conduct a Tabletop Exercise?**

2 Guidelines and Ground Rules: Preparing for a Security Incident Response Tabletop Exercise

3 Incident Response Prompt and Scenarios

4 Discussion: Lessons Learned and “After-Action”

What is a Tabletop Exercise?

Immersive

Provides rich, detailed description of a high-probability incident

Rigorous

Allow leaders to assess coordination, communication, and decision-making capabilities

Tabletop Exercise: Team-based simulation activities that allow leaders to practice staff and resource mobilization in response to a short-term incident

Cross-Functional

Can include a curated group of relevant stakeholders, from the president's cabinet to divisional leadership teams

Efficient

Requires only a few hours of time and can be completed with existing staff and resources

What is a Security Incident?

Key Cybersecurity Terminology

Security Event

An event where there is **potential for harm** to occur

- Ex: User received a phishing message and reported it to the security team

Security Incident

An event where there is **confirmed harm**

- *Not all security incidents rise to the level of security incident*
- Ex: User received a phishing message, opened the attached file, and installed ransomware

Use of Data Breach Terminology Can Open Institutions Up to Risk

!

- **Do not describe a security event or an incident as a data breach.** Misuse of the term could expose the institution to additional risk and obligations.
- The term *data breach*[1] has a very specific legal definition and each state is subject to different data breach laws.

[1] NIST defines a *data breach* as "An incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so."

Source: NIST, "Cybersecurity Basics Glossary", *NIST*, February 28, 2019; EAB interviews and analysis.

Setting the Table

Accelerating IT’s Response to Future Security Incidents

Why Tabletop Exercises Are Superior to Simply Distributing a Plan

Practice Readiness and Response

- Allow teams to rehearse high-stakes decisions in a low-stress setting
- Build collective problem-solving skills

Plan for the Unanticipated

- Raise novel questions that existing protocol doesn’t address
- Allow leaders to compare interpretation of current policy

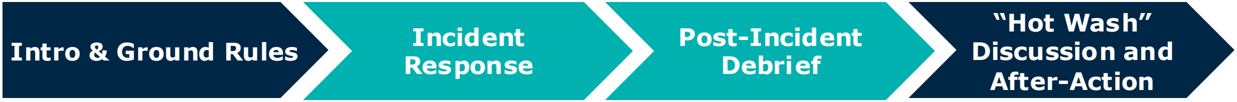
Evaluate Existing Protocols

- Identify if policies and plans rely on scarce resources or individual efforts
- Assess communication practices

Clarify Capabilities and Responsibilities

- Accelerate decision-making on who “owns” what
- Vet if teams and departments can deliver on execution

Components of Today’s Exercise



Intro & Ground Rules

- Review the purpose of the exercise
- Establish rules of engagement

Recommended time:
5-10 mins

Incident Response

- Introduction of the incident
- Facilitated response discussion

Recommended time:
30-40 mins

Post-Incident Debrief

- Facilitated discussion of existing protocol
- Identification of protocol vulnerabilities

Recommended time:
15-20 mins

“Hot Wash” Discussion and After-Action

- Review lessons learned and key takeaways
- Document challenges and concrete next steps

Recommended time:
20 mins

Total Recommended Time

90 minutes

ROADMAP

1 Why Conduct a Tabletop Exercise?

2 Guidelines and Ground Rules: Preparing for a Tabletop Exercise

3 Incident Response Prompt and Scenarios

4 Discussion: Lessons Learned and “After-Action”

Our Goals for Today

Learning Objectives for the Tabletop Exercise

Existing Protocol Review

1. Invoke all protocols in place
2. Identify when/why we should deviate from those protocols

Role Call

1. Highlight key roles that attendees play in incident response
2. Identify cross-team responsibilities

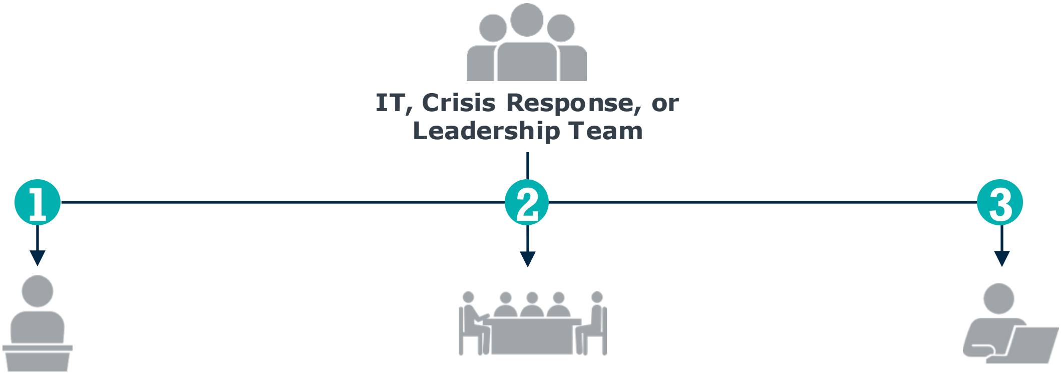
Vulnerability Analysis

1. Uncover vulnerabilities in current protocols
2. Remedy overreliance on individuals, resources, or systems that may not be available

Suggested Participants

Key IT/security function stakeholders and incident response/emergency management personnel in place

Attendee Roles



IT, Crisis Response, or Leadership Team

Facilitator

- Oversee the exercise
- Read the incident information, and ask targeted discussion questions throughout
- Keep the group on pace
- Ensure broad and representative participation

Participants

- Play themselves (unless otherwise specified)
- Respond to the incidents as if they're actually happening

Observer/Evaluator

- Take notes on quality of dialogue and decision-making, as well as group dynamics
- Share observations during after-action planning

Ground Rules

Tabletop Exercise Rules of Engagement

1 Even though it feels odd, try to behave as though this is really happening.

2 You'll inevitably want more information than is provided but work with what you have. Plan for possible contingencies and state your assumptions about what you believe to be true or what you do not know.

3 You **may not** use your smartphone to call, text, or research during the activity

4 Thinking out loud can sometimes keep others from thinking clearly. Try to take notes and only speak when you're ready to share, unless the whole group is at a loss and you must all brainstorm together to generate ideas.

5 Remember, a tabletop exercise is a "no-fault zone" where people can ask any question and admit uncertainty – it is a test of our plans, not of our leaders. There are no "hidden agendas" or trick questions in this exercise.

6 Any additional rules or questions?

ROADMAP

1 Why Conduct a Tabletop Exercise?

2 Guidelines and Ground Rules: Preparing for a Tabletop Exercise

3 **Incident Response Prompt and Scenarios**

4 Discussion: Lessons Learned and “After-Action”

Responding to a Security Event: Part A

Thursday, October 8 @ 2PM

A security analyst has reported to the CIO that data related to [INSTITUTION] and related credentials appears to have been posted to Twitter.

The CIO has followed up with the security analyst by phone and email, collecting screenshots and URLs from the original social media post.

The President has asked for an update by the end of the day.

Discussion Questions

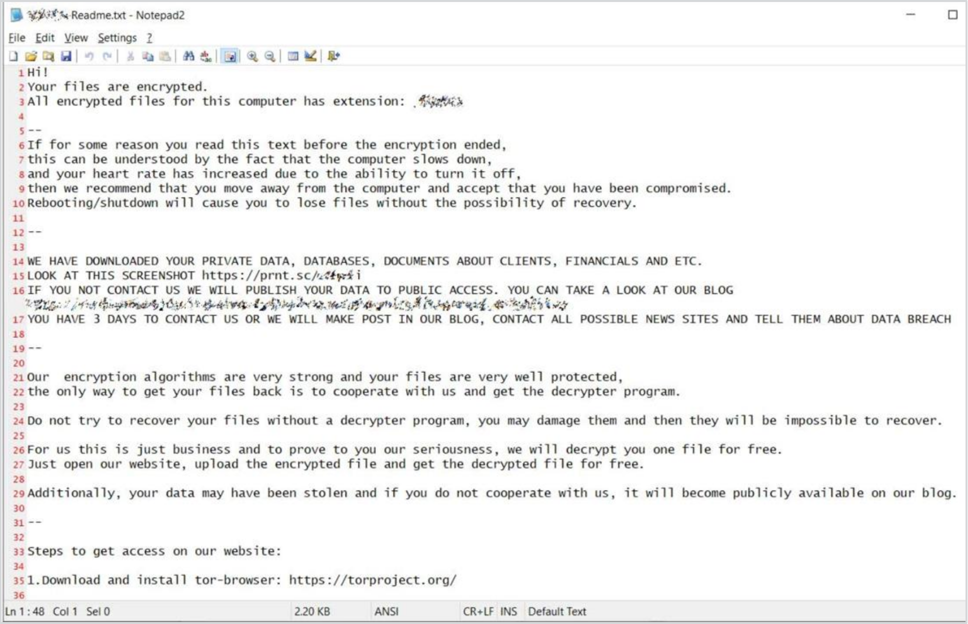
1. Is this a security incident?
2. Who needs to know about this?
3. What information do you need that you do not have?
4. What are the next steps?

Responding to Security Event: Part B

Thursday, October 8 @ 5PM

Multiple members of the security team have reported computer problems to the Service Desk.

Each ticket is reporting a similar situation: a message has popped up on their computer with a disturbing message.



```
Hi!
Your files are encrypted.
All encrypted files for this computer has extension: .[redacted]

--
If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compromised.
Rebooting/shutdown will cause you to lose files without the possibility of recovery.

--

WE HAVE DOWNLOADED YOUR PRIVATE DATA, DATABASES, DOCUMENTS ABOUT CLIENTS, FINANCIALS AND ETC.
LOOK AT THIS SCREENSHOT https://prnt.sc/[redacted]i
IF YOU NOT CONTACT US WE WILL PUBLISH YOUR DATA TO PUBLIC ACCESS. YOU CAN TAKE A LOOK AT OUR BLOG
[redacted]
YOU HAVE 3 DAYS TO CONTACT US OR WE WILL MAKE POST IN OUR BLOG, CONTACT ALL POSSIBLE NEWS SITES AND TELL THEM ABOUT DATA BREACH

--

Our  encryption algorithms are very strong and your files are very well protected,
the only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypter program, you may damage them and then they will be impossible to recover.

For us this is just business and to prove to you our seriousness, we will decrypt you one file for free.
Just open our website, upload the encrypted file and get the decrypted file for free.

Additionally, your data may have been stolen and if you do not cooperate with us, it will become publicly available on our blog.

--

Steps to get access on our website:

1.Download and install tor-browser: https://torproject.org/

```

Discussion Questions

1. Is this a security incident?
2. Who needs to know about this?
3. What information do you need that you do not have?
4. What are the next steps?

Responding to a Security Incident: Part C

Friday, October 9 @ 10AM

Late Thursday night into Friday morning, Information Security has received multiple alerts from its endpoint detection and response system.

Internal documents have been posted online by the same account. Some of these documents include data extracts showing name, DOB, SSN, address, and other information.

Multiple partners have contacted [INSTITUTION] management asking for more details.

There is increased pressure on [INSTITUTION] to make a public statement as The Chronicle and [LOCAL NEWS OUTLET] have asked for comment.

Discussion Questions

1. Who should be notified?
2. What are our next steps?
3. What information do we need that we have not acquired?

Responding to a Security Incident: Part D

Friday, October 9 @ 6PM

Information Security has confirmed the source of the leaked documents to have come from [COLLABORATION TOOL]; an unknown person was able to use a remote access tool to acquire these documents.

The remote access tool and malware has been removed from mailboxes to prevent reinfection.

All infected endpoints are reformatted and files are restored using backups from [DATA RECOVERY SYSTEM].

Discussion Questions

1 What additional clean-up needs to take place?

2 What partner outreach needs to occur and by whom?

3 Do we need a proactive incident communications strategy?

4 How do we prioritize the actions we have to take?

1. Why Conduct a Tabletop Exercise?

2. Guidelines and Ground Rules: Preparing for a Tabletop Exercise

3. Incident Response Prompt and Scenarios

4. **Discussion: Lessons Learned and "After-Action"**

“Hot Wash” Debrief on Lessons Learned

Four Key Questions to Consider

1. What worked well in this tabletop exercise?
2. What did we seem to struggle with in this tabletop exercise? What might be our areas for improvement?
3. What were the biggest discrepancies in our expectations or understandings?
4. What other perspectives were missing that should be included going forward?

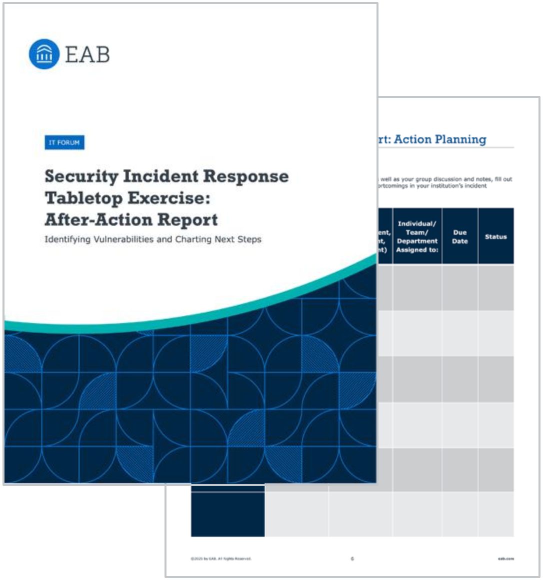
✓

Conducting a “Hot Wash” Debrief

- In a “round robin” format, allow every participant to share few minutes of thoughts, asking participants not to repeat one another.
- Once every participant has spoken, ask the facilitator and observer to share notes.
- Finally, time permitting, begin to identify specific shortcomings worth addressing (next slide).

Crafting an After-Action Report

Identifying Concrete Next Steps after the Debrief



EAB

IT FORUM

Security Incident Response Tabletop Exercise: After-Action Report

Identifying Vulnerabilities and Charting Next Steps

rt: Action Planning

well as your group discussion and notes, fill out
ortcomings in your institution's incident

ent, nt, nt)	Individual/ Team/ Department Assigned to:	Due Date	Status

©2025 by EAB. All Rights Reserved. 6 eab.com

Benefits of Creating an After-Action Report

- Outline vulnerabilities in existing policies and practices
- Highlight areas for improvement
- Articulate concrete next steps, and track progress as a team

Access the After-Action Report Template Here

1) For priority, use 3= most urgent, 2=important and timesensitive, and 1=relevant and would be helpful, but not urgent. Higher priority deficiencies could be those that most impact our educational and research missions, most endanger the health and safety of our community, or most violate regulations and laws. Lower priority deficiencies would be those that merely seek to confirm to best practices or industry standards or that would enhance the quality of the response.