How to Prepare for and Respond to Information Security Breaches

White paper

cbts

Consult Build Transform Support

Introduction

There's a good chance that someday, if you're working as a security practitioner, you'll be involved in the investigation and response of a breach or intrusion. The feelings of dread and confusion that accompany these circumstances are common for those faced with this scenario. But what if instead of feeling hopeless, you felt prepared? Perhaps a little startled, but ready to respond with confidence?

In this whitepaper, we aim to highlight both the essential practices required to be prepared to investigate an intrusion, as well as the high-level steps necessary to conduct an effective investigation and restore the organization to a "clean" state. The practices described here come from a tried-and-true resource: The National Institute of Standards and Technology's Special Publication on the subject, 800-61r2.

Step 1: Get Prepared

You'll find responding to a breach without a plan is, at best, chaotic, and at worst, disastrous; potentially causing more damage to the business than the intruder. Documenting your business' incident response plan is key to an effective recovery, giving all staff and stakeholders a clear idea of their roles and responsibilities when an incident has been declared.

What should go into this plan? At minimum, the following should be described:

- What constitutes a breach or intrusion to the organization? What conditions must be satisfied?
- Who is responsible for leading the response effort? Who else from the organization will be participating, and in what fashion?
- What phases make up an investigation? How does the team know when one phase ends and the next begins? When is the effort complete?
- What communication processes are followed during each phase of the response? What tools will be used for communication?
- When should law enforcement be contacted? How? What does LE coordination look like?
- What details are shared with third parties (employees, shareholders, customers, or the public), when, and how?

Step 2: Detecting and Analyzing an Intruder

Ideally, your network should be instrumented to provide your security team with sufficient visibility to know (with relative certainty) that an intruder is operating in the environment. Perhaps your endpoint or network defenses generated an alert; or, your security team discovered an anomaly by examining activity from other infrastructure–servers, workstations, applications, or network devices.

Or, perhaps a third party notified you of this anomalous activity or the theft of data. You might not have much to go on, but it's clear that you need to investigate.

Is it a human attacker? Or a piece of malware operating independently? What are they after? Did they successfully achieve their goal yet?

While the temptation may crop up to block the traffic, disable the stolen account, or shut off the compromised machine, the modern breach cannot be solved so easily. On the contrary, removing the attacker's tools or access too early could alert them and force them to change their tactics, making them even harder to track. You could even lose valuable forensic data if you shut down a compromised machine–many of the attacker's tools may be stored in volatile memory.

Instead, careful analysis must be performed to fully understand the scope of the intrusion. How did the attacker enter the network? How many machines have been compromised? Are they still active in the network? What data did they steal? What tools did they use? Every piece of information you find about the attacker–an account they used, a machine they touched, a piece of code they ran–will help you as you examine your environment to find additional indicators of compromise and fill in the blanks about their operation.

It is essential to complete this investigation, using data you find from investigating known compromised machines to uncover more attacker activity, in a cycle, until you've mapped out as much as you are able with the data you have. Answering these questions will be the most time-consuming piece of the investigation, and it is essential to exhaustively catalog the attacker's operation until you are sure you have all of it covered.

It should be noted that every incident, every attack, every investigation is different and will require a different calculus on when to call the detection and analysis cycle complete and move on to containment. Sometimes, with simpler, less sophisticated attacks, you may be done gathering data on the attacker after a few hours. Sometimes it may be days or weeks.

If all of this sounds quite intense, and you don't have the skillset to investigate effectively, we recommend using a third-party incident response firm with experience in performing this kind of work.

Step 3: Contain, Eradicate, and Recover

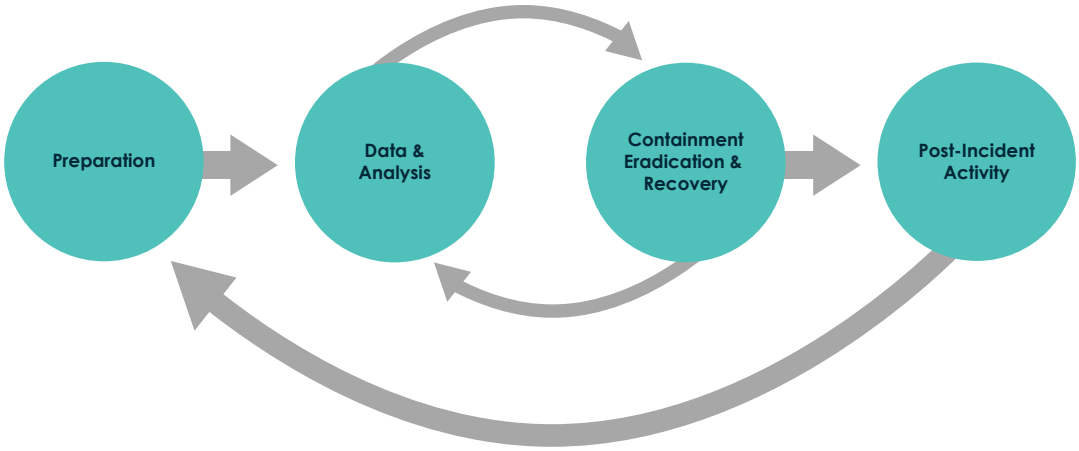
Once you've developed a comprehensive list of all affected hosts, accounts, and applications, it's time to contain the attacker–allowing them no further access to advance their goals. Note that containment activities will differ depending on the nature of the attack. There may be times that containment activities uncover additional intelligence or compromised systems, and revisiting the detection and analysis phases may be necessary.

After isolating the attacker, eradicating their presence on the network involves removing their access, tools, and artifacts. This is typically a carefully coordinated operation, involving a variety of IT operations and security personnel acting in concert.

Recovery of impacted assets follows removal of the intruder. This may involve changing passwords on affected accounts, reimaging compromised machines, and addressing gaps in security controls that allowed the intrusion to occur. It's also essential to monitor the environment during each phase to ensure the intruder has been successfully stopped. Expect each of these steps to take days, maybe even weeks, especially during the organization's first investigation and response.

Step 4: Assess Your Learnings

After the smoke has cleared, it's healthy to look back at the effort and learn some lessons. There's plenty to review–starting with how the breach occurred. What was the root cause? What controls, defenses, policies, and processes would have stopped or reduced the effectiveness of the attack? Was an alert or notification about the attack dismissed or disregarded? What monitoring would have allowed the attack to be detected earlier? Were there gaps in the incident response plan? Did each phase of the response go as envisioned? What metrics help quantify the effectiveness of the effort, and how can those be improved during the next investigation?



Additional Resources

Given the modern threat landscape, every organization must be prepared to respond to a security breach. Whether developing your incident response plan, improving your visibility through security monitoring, adopting stronger security controls, or formalizing a security and risk program, businesses should turn to the experts where gaps exist.

CBTS recommends partnering with a trusted incident response provider to assist in these efforts, especially if your organization has no prior history of performing this function internally. A third party brings expertise and objectivity that are paramount to conducting a sound forensic investigation. We work with services providers in the space and can help gather your requirements and connecting you with a provider that meets your needs.

CBTS Security experts can assist in all areas of maturing your incident response practice. Our consulting group can help assess your readiness to respond to a breach, and our product specialists can help collect your requirements and find best-of-breed solutions to complete your security strategy.

Learn More About CBTS Security Offerings:

Penetration Testing

Network Vulnerability Assessment

Disaster Recovery and Data Protection

Security Program

Managed Patching

Call 1.866.587.2287 for a free consultation to answer your questions today.