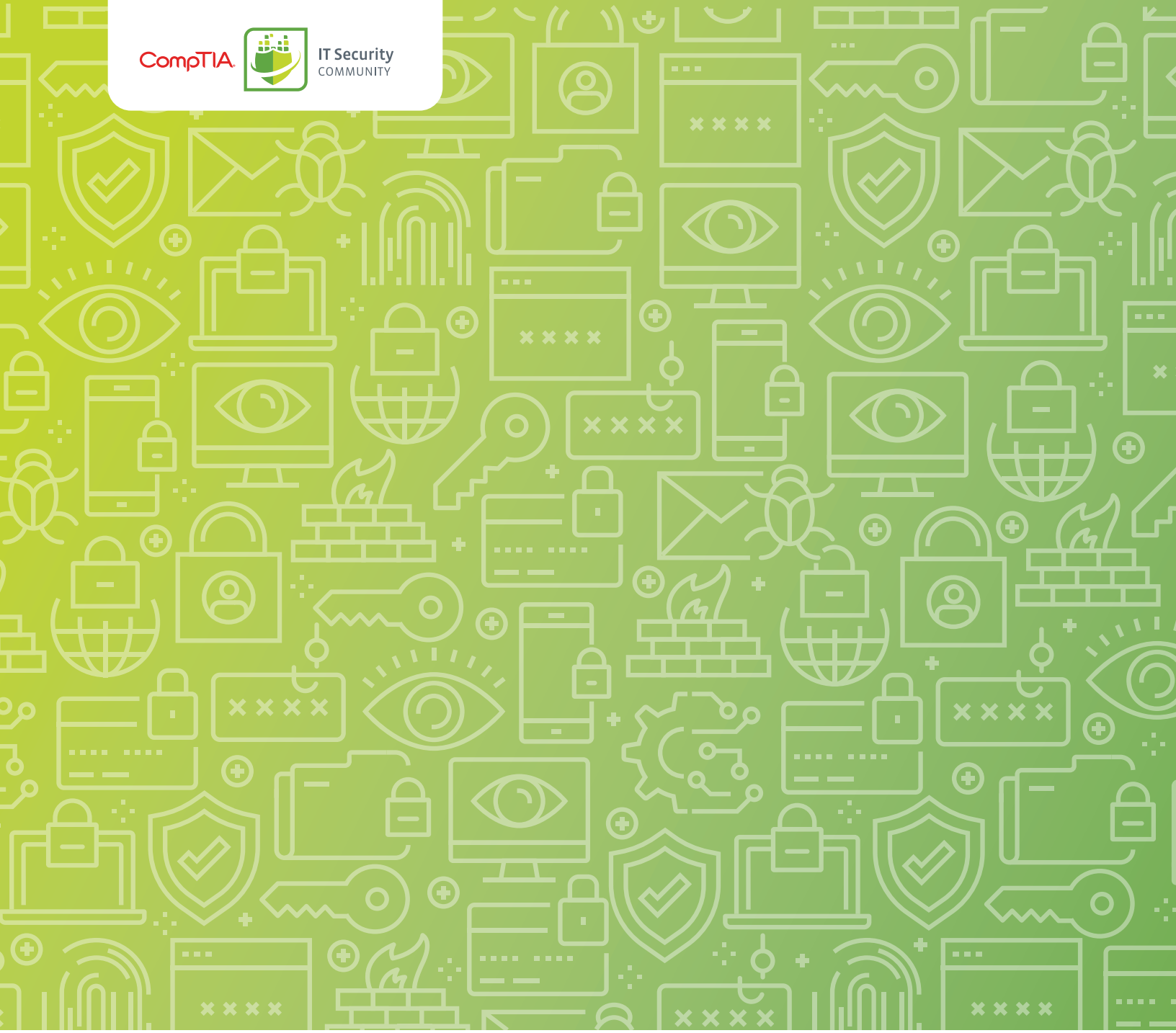


CompTIA IT Security Community Data Breach Response Planning Guide

INTRODUCTION

The same things that make you valuable to your client as a managed service provider make you a target for a security breach. Your expertise in storing, accessing and maintaining sensitive information draws the attention of cybercriminals. Your connections to multiple platforms, vendors and clients are enticing for bad actors looking for one-stop shops for their own black market supplies: credit card information, social security numbers, personal information, internal contacts and other sensitive information.

Unfortunately, far too many managed service providers have found themselves to be not only enticing victims, but also fruitful targets. Be it a lack of preparedness, human error or technical insufficiencies, information technology companies have struggled to meet the data security challenges we now face.

CompTIA's IT Security Community has created this tool to help guide you as you prepare a data breach response plan. The tips you'll find here range from the big picture (preplanning and testing) to the details (keeping related notes of an incident separate from day-to-day business), but are all designed to take fear of the unknown out of the equation. Even if you already have robust data security policies and a clearly defined data breach response plan, you may find a new idea or recommendation to further improve your posture. By sharing this planning guide with team members, you reinforce the idea that data security is not a passive, one-and-done activity. It's every day. It's a mindset. It must become embedded into your culture.

Luckily, there are some proven methods of training, planning and activating the proper support teams that will help you prevent what you can and respond appropriately to limit the impact of a security breach. This guide follows the structure of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) and highlights where in the CSF you can find more information. Please note that the NIST CSF is a framework, not a standard. The recommendations and concepts within the framework can be applied globally to any compliance standard or alternate security framework with which you may already be familiar. Of course, your plan should cover more than is shared here. Use this planning guide to get you started, highlight areas you may have missed and help you through them.

DATA BREACH RESPONSE: PREPLANNING

NIST CSF Identify & Protect Pillars

Defining your approach to data security is best accomplished at a time when you are not in an emergency or immediately following an incident. The IT Security Community strongly recommends building your data breach response plan in accordance with applicable regulatory compliance governing your location, industry or services. When building (or improving) your data breach response plan, start by identifying plausible incidents and considering how you would manage those scenarios that could happen based on the data you store, transmit and process.

1 Consider plausible scenarios. Avoid creating lengthy or complicated scenarios. Identify simple scenarios and define clear guidance for response.

- Examples of scenarios:
  What happens if we find something illegal on a client's computer?
  How do we ensure terminated employees lose access to sensitive data?
  What if there's a propagating worm, a DOS attack, a data breach or a disaster?
- Define categories of importance in your scenarios, such as low, mid, high, probable, variable, etc. Remember: Not everything can be the highest-level emergency.
- Include defined indicators of compromise, which is how you know that an incident is a breach. For example, if you see X, initiate the incident response team (IRT). This activity helps establish your risk threshold and identifies early indicators of an incident. In turn, this allows team members to act quickly and confidently when they see something out of the ordinary.
- Be aware of how deep your data goes, i.e., do you have protected health information (PHI), personally identifiable information (PII), etc., on your employees or clients?
- Practice these scenarios as if they are really happening and figure out how you would execute the plan. Afterward, identify areas that were cumbersome and improve the process.

2 Identify your incident response team (IRT). This internal team should cover all aspects of your business, including network engineers, techs, HR, legal, and PR and marketing staff.

- Establish a staging approach to the IRT. Identify roles and responsibilities for initial identification of an abnormality and elevation of a possible breach.

3 As part of the plan, conduct regular backups at the identified risk tolerance level and be sure to test them. Hackers have been known to turn these automated processes off.

4 External support is critical to managing an incident. Your insurance carrier and legal counsel will be among your best allies, as long as you have taken the time to clearly define coverage, liabilities and the role of counsel.

→ **Confirm and review insurance coverage.**

- Have a cyber liability insurance policy, not just basic liability or technical errors and omissions.
- Make sure your insurance policy will cover the various plausible scenarios identified so you won't be left liable. Vet all the details of your coverage including trigger dates, exclusions and the details of any bad actor clauses.
- Many insurance companies offer services such as a "breach coach" to help you through an incident. Ask about this benefit with your carrier. You will have enough on your mind during an incident so determine your support ahead of time.

→ **Involve your legal counsel. Engage counsel on all security contracts from the start to protect yourself with attorney privilege at all times.**

- Ensure your attorney has been approved by your insurance, i.e., they will cover attorney fees up to a certain amount, which may be less than what your attorney is charging.
- Open dialogue among yourself, your insurance carrier and your attorney improves your relationship with these support functions and provides clarity of roles.
- In an incident, bring in legal counsel immediately. As soon as you identify this is significant enough to bring in the IRT, decide if you're going to need external counsel. Make sure you have an attorney familiar with cyber incident management and related regulations.

5 Identify emergency contacts.

→ **Regulators**

- Keep in mind, laws vary from state to state, and country to country for those clients who operate regionally, nationally and globally.

→ **Law enforcement**

→ **Forensics recovery**

- Unless your technical staff is properly trained and certified in forensics, attempts they make to investigate an incident may taint critical evidence. Prepare for this by identifying options for forensics specialists to determine if an incident you have identified is indeed a breach.

→ **Vendor partners, clients and other business partners**

6 Be aware of compliance notification laws.

→ **Regarding the rules and regulations covering data, know which compliance rules apply to your notification laws. There are some that require notification within hours. Your chief compliance officer should identify which clients to notify and when, i.e., in real time, within 24 hours, etc. Failure to comply could have legal implications.**

WHAT IS DATA COMPLIANCE?

Data compliance consists of the processes that ensure adherence to both business rules (government department, university, industry or agency), as well as legal, regulatory and accreditation requirements when it comes to handling consumer data.

Regulations help companies secure their information, and non-compliance with these regulations can result in severe fines, or worse, a data breach. Here are some examples of regulations and resources to help you understand what applies to your company:

2019 New York SHIELD Act
nysenate.gov/legislation/bills/2019/s5575

American Institute of Certified Public Accountants (AICPA)
aicpa.org

California Consumer Privacy Act (CCPA)
leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Center for Internet Security Controls (CIS Controls)
cisecurity.org/controls

Children's Online Privacy Protection Rule (COPPA)
coppa.org

Control Objectives for Information and Related Technologies (COBIT)
isaca.org/cobit/pages/default.aspx

Federal Information Security Modernization Act of 2014 (FISMA)
cisa.gov/federal-information-security-modernization-act

The Federal Risk and Authorization Management Program (FedRAMP)
fedramp.gov

Gramm-Leach-Bliley Act (GLBA)
ftc.gov/tips-advice/business-center/privacy-and-security

General Data Protection Regulation (GDPR)
ec.europa.eu/info/law/law-topic/data-protection_en

Health Insurance Portability and Accountability Act (HIPAA) / HITECH Omnibus Rule
hhs.gov

International Organization for Standardization (ISO)
iso.org

National Institute of Standards and Technology (NIST)
nist.gov

NERC Critical Infrastructure Protection Standards (NERC CIP Standards)
nerc.com

Payment Card Industry Data Security Standard (PCI-DSS)
pcisecuritystandards.org

Sarbanes-Oxley Act (SOX)
soxlaw.com

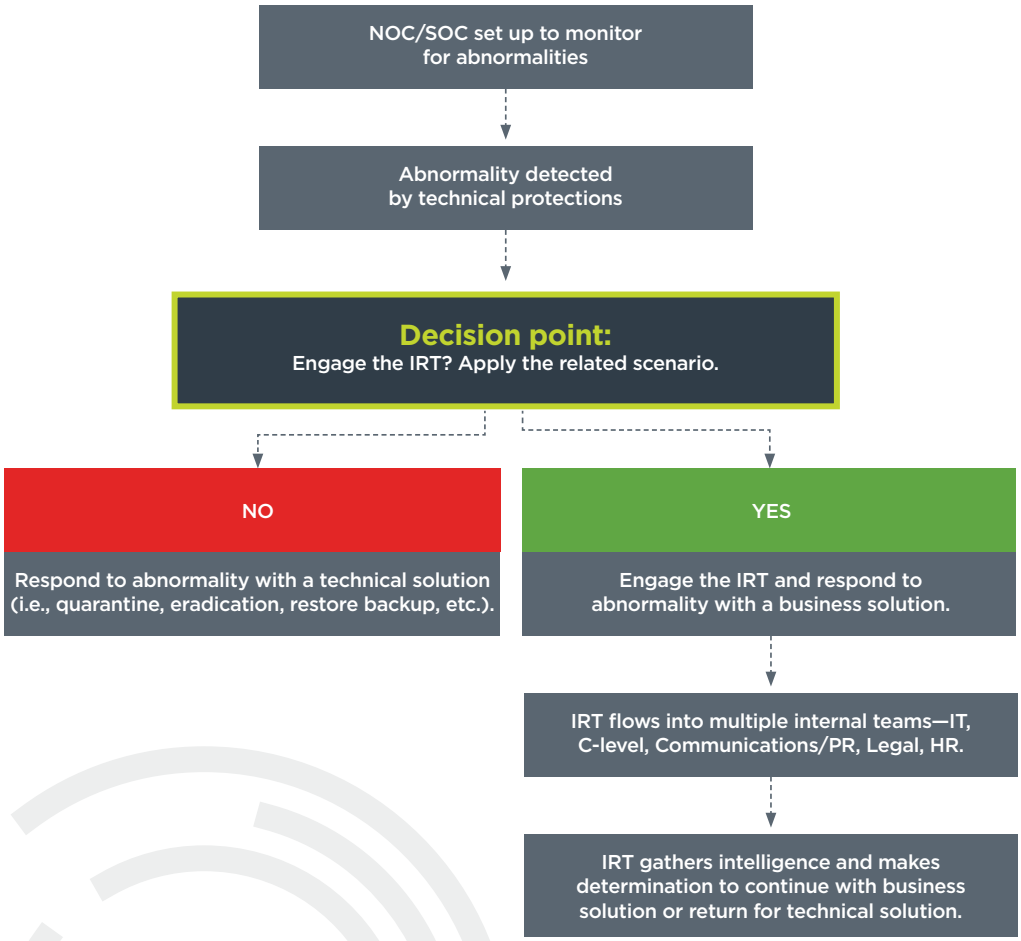
The Family Educational Rights and Privacy Act of 1974 (FERPA)
www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

THE INCIDENT: DETECTION AND PROTECTION

NIST CSF Detect & Protect Pillars

In most cases, an incident starts at the technical level when something is flagged as unusual. It could be at your network operations center (NOC) or your security operations center (SOC), or even at your frontline tech level. That abnormality gets raised to the next-level manager who will decide whether or not to activate the IRT. This manager should have the experience to determine that the incident is a breach and the authority to activate the IRT. Once that happens, it's no longer a technical issue, it's now a business issue. Keep in mind, not every incident is a probable breach, but you must be able to demonstrate how you made that determination. You cannot activate the IRT for every incident.

When Do We Engage the Incident Response Team (IRT)?*



*This decision tree is an example. Be sure to take any specific compliance regulation into account when defining your decision tree for engaging the IRT.

Your IRT is now engaged.

1. **Clamp down communications and immediately. Inadvertent admissions of fault can lead to unforeseen legal ramifications.**
2. **Follow the plan in place for that specific incident/scenario. If you've taken the time to identify and practice scenarios, you can activate your plan.**
3. **Bring together the core IRT members to gather intelligence. It's OK for members to drop off if they don't need to be involved after initial intelligence gathering.**
4. **Learn where the fault lies early on.**

- Sometimes, despite all your best efforts, the fault lies with a client.
- Make sure your managed services agreement spells out what incident response services are included or excluded. Particularly with clients who don't take your advice, break cybersecurity rules, or are dragged into a client's problem, determine if you are you going to charge for your services.

4 TIPS TO HELP YOUR INCIDENT RESPONSE TEAM SUCCEED

1

Give everyone a fresh notebook as part of the IRT "emergency kit" to keep notes specifically for this incident. Notes are discoverable evidence so this precaution will help keep this incident separate from team members' regular job duties.

2

Have general counsel get outside counsel with expertise in that area involved ASAP to protect attorney-client privilege. However, know when it's important enough to do this because it will add substantial cost.

3

Prepare for intensive focus and regular meetings for the IRT during an emergency period. One suggestion could be to have an open conference bridge manned at all times. As the incident is managed, the IRT can meet less or cut down to crucial members only.

4

Establish a meeting cadence for the IRT team to make certain nothing falls through the cracks. This will start off hourly and move to daily, every other day and then weekly until the incident is resolved.

THE RESPONSE: COMMUNICATION AND RECOVERY

NIST CSF Respond & Recover Pillars

The big question facing a business now is: When do you start communicating outside the IRT? Generally, you'll want to follow the plan for the scenario with compliance regulations playing a big role. Get legal advice to help you before you say something that may be costly. Use these guidelines to start communicating and recovering.

1 Save all internal communications.

- Maintain clear communication with your attorney and insurance, as well as your IRT team.
- Label your messages to be easily discoverable later.
- Keep items that are under attorney client-privilege separate from other communication.

2 Engage your insurance carrier.

- Depending on the scenario, get your insurance involved right away to figure out who will pay for everything. Insurance companies have cyber response and forensics teams they can draw upon. In certain scenarios, such as ransomware, PHI or PII compromise, you will likely want to engage your insurance with a claim.
- You may be asked to write an incident letter, i.e., "It happened to us" to help post-incident analysis and encourage information-sharing related to incident.
- Log all the time spent on the incident by members of the response team. Your insurance carrier will want this information for the errors and omission (E&O) estimation.

3 Plan your external communications strategy.

- Maintaining your other clients during this time is just as important as ever. You must make certain business as usual isn't interrupted with other clients and that proper precautions or lessons learned are implemented immediately and communicated to all parties.
- Be careful when talking to clients impacted by a breach prior to talking to an attorney. If you or one of your vendors may be at fault, you'll want to be careful what you say—even to your own clients. It could potentially be used against you if legal action is taken by your client. Have all external verbal and written documentation and communication approved by your attorney and insurance company.
    - In a ransomware situation, know when to notify potentially impacted clients. They will likely have actions to take, such as contacting their own insurance and attorney. If law enforcement is required, they will get involved. The insurance companies will take over once the incident has been contained.

- **Determine what can and should be said to various audiences—associates, clients, business partners, employees and the public. Stick to your key messages.**
    - Prepare a statement for employees to make certain everyone is on the same page. For example: "One of our clients was hit with ransomware. We are working with them, as well as the proper authorities, and will communicate back with the team as soon as possible."
    - Prepare a statement for press (just in case). For example: "We are being completely transparent with our clients, the state authorities and the FBI. We are working together to prevent this from happening to other businesses in the future. At this time, because of the ongoing investigation, we cannot provide any further details." Regarding public inquiry and the press, be conscious of who may appear to be at fault. The communication will change depending on if it's your fault (or your vendor or a secure-by-design flaw) as opposed to a client error.
    - Once your official statements are prepared and distributed, keep an open line of communication—consider a 24/7 hotline for a couple days—for the clients and customers impacted.

With honest forethought, clear scenarios, solid security design, and continual training and practice, managing the inevitable breach of sensitive data is possible. The IT Security Community strongly encourages every technology business to develop, maintain and execute its own strong data breach response plan to help combat cyberattacks.

IT Security COMMUNITY

Join your peers and get access to more cybersecurity resources and information by joining CompTIA's IT Security Community.

COMMON DATA SECURITY BREACH DEFINITIONS

Breach – an incident that has been confirmed

CIRT – Computer Incident Response Team

CSF – Cyber Security Framework

DOS – Denial of Service

Framework – a body of knowledge to help frame an approach to a practice but leaves the specifics to the practitioner

Incident – an indication that data may have been lost, stolen, accessed or acquired without authorization

NIST – National Institute of Standards and Technology

NOC – Network Operations Center

PHI – Protected Health Information

PII – Personally Identifiable Information (protected by law)

Ransomware – the malicious encryption of data which is held for ransom

SOC – Security Operations Center

Standard – a body of knowledge that defines a specific approach or methodology