Steps to Take Within the First 48 Hours After a Data Breach

Shawn Waldman
CEO & Founder
Secure Cyber Defense

University *of* Dayton
Center for
Cybersecurity &
Data Intelligence

OHIO CYBER
RANGE INSTITUTE

Overview

When a company experiences a data breach, a common, critical mistake is not following their incident response plan or – worse yet – not having a plan in place to draw from. The first 48 hours after the discovery of a data breach are critical, and preplanning allows many vital tasks to be put immediately into action. This paper outlines the nine steps your team should be prepared to take in the event of a data breach.

About the Author

Shawn Waldman is the founder and CEO of Secure Cyber Defense LLC in Moraine, Ohio. He is a 20-year IT veteran and previously served in law enforcement. Secure Cyber Defense assists organizations in protecting assets from internal and external threats and aligning cybersecurity strategy with consumer needs. The company offers services, tools, and support for business by analyzing and monitoring digital environments for anomalies with cutting-edge solutions to identify, stop, and prevent cyber threats. Utilizing vulnerability assessments, intrusion prevention, and continuous monitoring services, they scale custom solutions to any size organization or budget.

For five years, Shawn was deeply involved with the FBI's Criminal Justice Information System compliance framework, and ultimately wrote the compliance-training curriculum for other agencies and vendors. Shawn and his company have provided expertise to clients in the law enforcement, government, healthcare, and financial services industries, helping them protect sensitive company and consumer data against outside threats.

Shawn is a subject matter expert when it comes to Cybersecurity compliance and speaks across the country on various topics related to cybersecurity, threat detection and awareness. Currently, Shawn's speaking, training, and writing expertise on cyber-related issues are in high demand.

University of Dayton
Center for Cybersecurity and Data Intelligence
937-229-1929
udaytoncyber@udayton.edu

Find more tools at **go.udayton.edu/cybersecurity**

Steps to Take Within the First 48 Hours After a Data Breach

Shawn Waldman
CEO & Founder
Secure Cyber Defense

When a company experiences a data breach, one critical mistake is not following their incident response plan or, worse yet, not having a plan in place. The first 48 hours after the discovery of a data breach are critical, and preplanning allows many vital tasks to be put immediately into action. “Often it’s not what happens in the first 48 hours of a data breach, it is what a company has done in advance to prepare and understand the actions to take when a data breach occurs,” says Shawn Waldman, CEO of Secure Cyber Defense.

When a data breach is discovered, a company’s incident response team, law enforcement, insurance providers, forensic team, IT team, lawyers and public relations teams should not be meeting for the first time. These are critical functions that must work efficiently together and have defined tasks and responsibilities to address how to restore critical business functions and when and how to communicate with employees, law enforcement and the public.

The first 48 hours are a chaotic time where emotions run high. Having a command center set up with defined roles and levels of authority is critical in calming executive teams, employees and even suppliers. A good training incident response team is a one-part advisor/calming force and another part cybersecurity and forensic experts who can act quickly to secure critical evidence and stop the spread of malware, further data theft or damage to critical systems.

As an experienced incident response team, we are often brought in during the critical first 48 hours. Many times, companies contact us because they did not have a contract with an incident response team, or their IT services company did not have the experience or team of experts to deploy. Living in this pressure cooker of alarm, highly charged emotions and sophisticated cyberattacks that are fast-moving has taught us several valuable lessons in how to counsel companies in developing their own incident response plans, particularly in the first 48 hours.

1. **If your company has purchased cyber insurance**, contact your insurance company immediately to determine the resources they plan to bring to mitigate the losses caused by the breach and to restore system functions. Often the reaction time from insurance providers and their network of incident response teams can be delayed which requires an initial incident response team focused on evidence gathering, containment and minimizing the further spread of the attack.

2. **Contact law enforcement** including the Secret Service if the loss is greater than $25,000. Local law enforcement and the Secret Service have a wide array of resources at their disposal to determine where the attack originated, compare similar threat patterns, and track the transfer of money and data. Law enforcement teams help to answer the critical who and where questions to determine appropriate actions.

3. **Put legal and PR teams into action** to determine what and when to communicate to board members, employees, partners and vendors, customers and government

regulators. All parties must be on the same page for what is to be shared, who has the responsibility for talking with the press, how to respond to customer questions, and where to channel information requests outside of an employee's specific responsibilities. Your legal team should advise you and the forensic team of the chain of custody requirements to ensure that it is found admissible in court. It is also important they review and address local, State, Federal and Industry laws and regulations so appropriate actions can be taken.

4. **Determine who is in charge** and who will be communicating with the incident response team. Establishing clear lines of communication and responsibilities is a critical step in the first 48 hours and beyond to help make efficient decisions and to reduce overlapping efforts. So, choose a response leader from the start and have them work with the structure of the internal and external experts.

5. **Affected devices should be taken offline** but NOT shut down or changed. In the case of virtual systems or machines or third-party vendors, a snapshot of what was occurring through those machines at the time of the breach is critical in understanding the entire IT network's activity at the time of the breach or cyberattack. The top priority is to stop the activity coming from outside the company and to protect the chain of evidence so the forensic team can determine the who, what type of attack, when the system was breached, and what data is the target of the attack or what they want from the attack.

6. **Implement an employee, partner and customer password reset** adding multi-factor authentication if not currently enabled. In many cases, passwords are the main goal of the cyber attack since they enable additional data access. Changing passwords will help shut down the spread of the breach particularly if it is found to be ongoing. This procedure should be applied to all accounts within the IT system whether they have been confirmed as compromised or not.

7. **Ensure that existing auditing and logging systems are operational.** If auditing and logging have been disabled, perhaps to cover the cybercriminal's trail, these should be restored since these systems are valuable in helping to understand if the breach is ongoing and when it can be safely determined that the breach has ended.

8. **Communicate what you can when you can**. During a breach, emotions run high particularly when normal business functions are shut down. It is human nature to want to understand what is going on and how long it might be until business operations are back in place. A crisis communications plan's goal is to give as much information as needed without raising expectations or causing panic. Employees are concerned about their jobs and paychecks, while board members are concerned about the financial health of the company as the mitigation process drags on.

9. **Document everything that takes place** to capture evidence and document key findings and facts to evaluate current cybersecurity practices, hardware, and equipment. Discussing what went wrong allows companies to craft a new approach to reduce the risk of a similar breach from happening again and to test vulnerabilities in other IT systems.

Keep in mind that while the first 48 hours is stressful, most organizations are impacted for months. According to IBM, on average, companies take about 197 days to identify and 69 days to contain a breach. Setting the stage early helps set the right tone in communication and builds confidence with a measured approach for recovering and restoring systems.