Ransomware Resiliency Checklist: What to Do When There's a Breach

AUDITBOARD

Ransomware Resiliency Checklist: What to Do When There's a Breach

Despite your organization's best ransomware prevention efforts, you may be unable to prevent a cyberattack from succeeding. In 2021, the FBI's Internet Crime Complaint Center received 3,729 complaints involving ransomware, an increase of 51% from the prior year. Those attacks in 2021 exacted a heavy toll, with adjusted losses of $49.2 million.

Moreover, the Cybersecurity & Infrastructure Security Agency reports that ransomware gangs have increased their influence by focusing their efforts on targeting the cloud, attacking industrial processes, and launching attacks on holidays and weekends.

A breach response plan, legal counsel, and a robust communication plan, among other tools and tactics, can make the difference between returning your business to normal quickly, or prolonging the impact of ransomware far beyond the initial attack. This seven-step checklist breaks down what InfoSec professionals can do to minimize the damage in the event of a ransomware attack.

Ransomware Resiliency Checklist

As the threat grows unabated, limiting the depth and severity of an attack often depends on your company's response efforts. Here's a checklist to follow from the moment you find out an attacker has breached your defenses.

A breach response plan, legal counsel, and a robust communication plan, among other tools and tactics, can make the difference between returning your business to normal quickly, or prolonging the impact of ransomware far beyond the initial attack.

1. Activate your breach response plan.

A breach response plan can minimize the damage associated with an attack and the time it takes to return to business as usual. A comprehensive plan envisions each step in an attack and ensures those involved in the response effort understand and execute their assigned responsibilities. For example, the plan should identify who has responsibility for isolating the threat, restoring access to IT assets, and notifying key stakeholders, including employees, customers, regulators, and law enforcement. In order to ensure your organization is up to date with its breach response, it is a best practice to perform a tabletop exercise with all key stakeholders at least once a year.

2. Engage legal counsel.

If your organization has a legal department or you retain outside legal counsel, notify them of the breach as soon as it is uncovered. Regulatory scrutiny and litigation can follow an attack; therefore, engaging legal counsel quickly can ensure they play an integral role early in the process.

3. Contact law enforcement.

The Federal Bureau of Investigation, the Cybersecurity & Infrastructure Security Agency, and the U.S. Secret Service each play a role in ransomware incidents. While law enforcement may lack the resources to provide onsite assistance, they can provide guidance on how to mitigate the impact and whether to communicate with the attackers. If your organization has ransomware insurance, notifying law enforcement may be a requirement to receive coverage.

4. Perform due diligence.

Performing due diligence on the type of ransomware before committing to payment is a crucial step for your organization to take. Some governments are considering whether to require due diligence prior to payment. While the payment of ransomware is not illegal, there is a possibility that the group receiving payment has links to criminal activity, and payment of the ransomware could expose the organization to the risk of potential prosecution down the road.

5. Paying or denying the ransom demand.

When faced with a ransom demand, some organizations refuse to make a payment of any amount, while others arrange for a quick payment. Your legal department, insurance company, and law enforcement contacts can share their perspective on paying a ransom. But ultimately, that decision rests with the C-Suite and the board of directors. To make a fully informed decision, those involved should possess a detailed understanding of the attack, the impact on the organization, due diligence on the type of attack, and the potential ramifications of paying the ransom.

6. Communicate with key stakeholders.

Your organization must walk a fine line between disclosing too little or too much regarding a breach. For example, revealing more than is required to customers by regulators can increase the likelihood of losing their business and triggering lawsuits. Alternatively, disclosing too little to business partners can leave them feeling exposed and result in the loss of trust. You want

your stakeholders to be aware of the event and the actions your organization has taken, along with proposed changes to prevent an attack in the future. Without disclosing this type of information, they may feel in the dark and as though your organization is hiding information. And keep in mind the need to comply with breach notification requirements that can range from 72 hours, as is the case with the General Data Protection Regulation, to 60 days with the Health Insurance Portability and Accountability Act.

7. Document and act upon the lessons learned.

Every attack provides a window into your organization's security strengths and weaknesses. Set aside time to analyze the attack, including how the attacker breached your company's defenses, how long they remained undetected, and how long it took your organization to recover. These observations can then provide the basis for a remediation plan to help prevent a similar attack from succeeding in the future.

A well-designed breach response plan can provide a roadmap to help your business recover from an attack and typically includes many of the tasks included in this checklist. If you have yet to develop a breach response plan, or you've not updated it recently, now is the time to do so. When an attack happens, instead of spending time developing a plan in real-time, your organization can dedicate its time to executing a well-thought plan. It is crucial to test the plan at least annually to make sure all key stakeholders are aware of their role and identify gaps in the plan. After all, practice makes perfect. While you cannot prevent every attack, you can control how you respond.

A well-designed breach response plan can provide a roadmap to help your business recover from an attack and typically includes many of the tasks included in this checklist.