Cybersecurity First Aid Kit:

Four Steps to Recognize, React and Recover from a Breach

HIGHLIGHTS

Monitoring internal controls can catch early signs of a cybersecurity incident.

Forensic analysis helps determine the full extent of compromised files.

Ongoing cybersecurity adjustments can address vulnerabilities before a breach occurs.

RISK ADVISORY
WHITEPAPER

CBIZ®

Cybersecurity First Aid Kit

A company's electronic data hold value for more than that company and its related parties. Information stored electronically, such as intellectual property, health records, customers' credit card information, employee and customer personally identifiable information and Social Security numbers, have proven to be appealing targets for hackers.

When unauthorized users penetrate public and private networks, they can disrupt, modify or even destroy companies' electronic data, which can lead to devastating consequences for that company.

As technology advances, more organized and sophisticated cyberattacks are becoming increasingly prevalent and threatening. Many companies are investing in security measures intended to prevent attacks, but few have shifted their mindset to accept that data breaches in today's society are inevitable.

Having a proactive cybersecurity strategy is a company's best defense against a breach because it helps identify the access points so the company can respond quickly to minimize the consequences that come from unauthorized access to data. Companies need to have a plan in place that helps them recognize when an incident is occurring, react quickly to stop the breach and recover in a way that addresses both the short- and long-term problems that result from unauthorized access.

As technology advances, more organized and sophisticated cyberattacks are becoming increasingly prevalent and threatening to companies.

This cybersecurity "first aid kit" should be part of companies' overall process to oversee and control their networks and electronic devices.

Step 1: Identify the Problem

As in any trauma situation, identifying the source of the incident is paramount to minimizing the damage the incident could cause. Internal controls will have a large role in indicating where a breach may be happening. Monitoring logs and access to networks is especially critical because this is where signs of a breach will likely turn up. Large file transfers that do not regularly occur could be a sign of a security incident, as could the slowing down of a usually large bandwidth.

This occurred with a not-for-profit client of CBIZ. The client noticed their normally fast bandwidth had slowed almost to a stop and asked for help in identifying the cause. Our team worked with the FBI and discovered that cybercriminals were using the not-for-profits' servers as a conduit for illegally moving movies, games and music overseas. The FBI uncovered traces of these files within the organization's servers.

Step 2: Stop the Breach

A company's incident response plan to unauthorized access should be able to cut off the access point, slow down and stop the intruder and preserve the environment that has been compromised. This can be accomplished through proactive monitoring, user training and a layered security approach.

Forensic analysis will likely be required to determine the full range of files compromised. If a company does not have the means to do a full forensic analysis internally, it should enlist the help of an outside provider experienced with cybersecurity risk mitigation. A third-party provider can ensure that unauthorized users no longer have access to a company's electronic data and assist the company in taking the appropriate steps to prevent a similar event from occurring in the future.

Step 3: Notify Affected Parties

No matter what was accessed, companies will likely need to distribute information about the breach. It is also rare to find a breach that does not involve additional regulatory requirements related to disseminating information about what happened.

Many states have breach notification laws, and companies will need to consider which notification laws would apply to their case. Most breach notifications follow a simplistic format.

For compromised financial records, companies will generally be required to provide a service to monitor credit reports and other information related to financial security for the individuals affected by the breach. This service would have to be provided for one to two years, depending on the severity of the incident.

If credit card information was part of the breach, the company will have to notify cardholders and provide them with a service to monitor credit reports. The company will also be subject to payment card industry data security standard (PCI DSS) oversight.

Many states have breach notification laws, and companies will need to consider which would apply to their case.

PCI DSS has four tiers of monitoring, with the first being the most stringent. Companies subject to Tier 1 PCI DSS monitoring will have to provide due diligence to demonstrate that the environment around the credit card information is secure. A company that has credit card data that have been breached is automatically held to the highest tier (Tier 1) requirements.

Compromised healthcare records will have to follow Health Insurance Portability and Accountability Act (HIPAA) regulations for breach notification. Compromised entities must notify the affected individuals and the Secretary of Health within 60 days of the breach. The organization may also have to notify media outlets, depending on the type of breach.

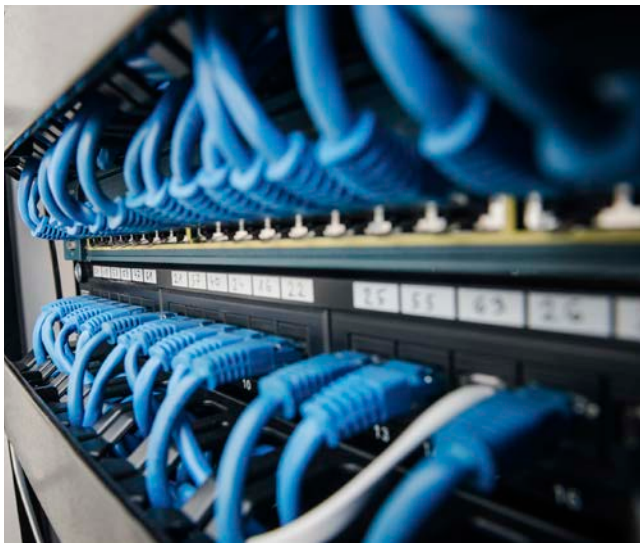
It is highly recommended that the company's external counsel be part of the notification drafting process. If the company carries cyberliability insurance, the insurance company will also need to be included as part of the immediate cybersecurity incident recovery.

Step 4: Repair the Damage

The regulatory environment surrounding the compromised data may require long-term corrections to be implemented. Both HIPAA and the PCI DSS will ask for monitoring and due diligence related to the security of their respective records.

First priority goes toward fixing the problems that led to the breach, which should be easy to identify because this information will likely be required as part of the breach notification.

Companies that tie breaches back to their third-party and vendor relationships should work with that company to understand what they are doing to prevent a similar event from occurring in the future and what their company can do to better secure data transferred between the two entities.



Recommended Cybersecurity Control Activities

- Segregating cyber risk management tasks
- Logging and reviewing administrator changes
- System update testing and approval
- Mobile device encryption
- Unique user ID and complex password for wireless access
- Real-time notification of back-up failures
- Annual service organization control audits
- Quarterly reports of cybersecurity control activities

If the breach occurred through wireless access to the network, companies may want to consider strengthening encryption for wireless access, issuing unique user IDs and making passwords for access more complex. Breaches that resulted from lost or stolen devices may necessitate companies create a policy on when to remotely wipe devices.

Changes should not stop with the immediate problem that needs to be addressed. Cybersecurity is an ongoing process.

Periodic cyber risk assessments can help identify emerging sources of vulnerability before they become targets of an attack. They can also assist with prioritizing your cyber risk procedures.

Not every piece of data needs to be secured on the same level; it is not cost effective or reasonable, so companies should identify the information that holds the most value for their company or is subject to regulatory requirements. Consider intellectual property, financial information and other personally identifiable data and what can be done to secure these areas.

Cybersecurity First Aid Kit

Vendor security practices need to be considered during the routine cyber risk assessment as well. Companies often share information with their vendors and third parties electronically, and this exchange has been shown to be vulnerable to cybersecurity incidents.

When meeting with a new vendor or third party, companies should include that vendor's cybersecurity protocols in the conversation. If a vendor's cybersecurity approach is not well-developed, then data exchanged with that vendor are more vulnerable to risk. The company should consider implementing controls to compensate.

Social engineering exercises are also recommended. In many cases, companies' weakest security link is protection against internal threats. An organization's cybersecurity awareness can help reduce the threat of someone within the organization accidentally or intentionally allowing unauthorized access to valuable information. Employees at all levels should be aware of some of the common unauthorized entry points to the organization's electronic data and what they can do to prevent a breach from occurring.

Once the primary vulnerabilities and risks have been ranked, companies need to implement robust control activities to ensure that the organization operates as it should and high-value data are protected. Cybersecurity-related activities should include logical/physical access controls, change management procedures, network monitoring, vulnerability assessments and penetration testing, mobile device strategy, incident response planning, anti-virus monitoring and user training. The more control activities in place, the more likely it is that risks will be mitigated.

The Best Defense is a Good Offense

The current environment indicates that companies should not consider unauthorized access to data an "if"; rather they should approach it as a "when." Having a proactive, robust plan in place can help minimize the potential damage from a breach and get your organization back on track more quickly in the wake of a disruptive event. Don't go at it alone.

Five Ways to Be Proactive with Cybersecurity

1. Accept that security will be compromised
2. Consider cyberliability in all activities
3. Focus on critical information assets
4. Be prepared to respond
5. Get the basics right