ADAMS BROWN
Technology Specialists

Responding to a Cybersecurity Incident

Despite employing the best preventive measures, a cybersecurity breach can still occur. It is essential to have a proactive strategy in place for such scenarios to minimize the potential damage and swiftly restore normal operations.

WHAT TO DO IF A BREACH OCCURS

In the event of a cyber breach, it's important to take immediate action to contain the damage and mitigate the impact. The following are some steps companies should take:

1. **Identify the extent of the breach.** Start by determining what data was accessed or stolen, who was affected and how the breach occurred.
2. **Contain the breach.** Once you know the extent of the breach, contain it to prevent further damage. You want to disconnect affected systems from the network to prevent the spread of malware or other malicious activity. But also consider changing passwords and possibly even notifying legal counsel and law enforcement.
3. **Contact your cyber insurance carrier.** If you carry cyber insurance, you'll want to reach out as soon as possible so the insurance company can begin its investigation and provide assistance to mitigate damage. Depending on your policy, they may be able to provide advice on how to respond, financial assistance to cover the costs of responding to the breach and legal representation if needed.

4. **Assess the damage.** What was the impact of the attack? Start by looking at who specifically was impacted including customers, employees or partners. But also consider things like lost revenue, the cost of repairing damage and the impact on the company's reputation.
5. **Notify appropriate parties.** If sensitive information is compromised, the business owner should notify those affected immediately. The notification should include details of the breach, the types of data that were compromised and what steps the business is taking to address the issue. This is where you can tell them what support, if any, you are providing to protect themselves from any potential risk.
6. **Preserve evidence.** You need to preserve evidence of the cyberattack, including logs, emails and other relevant information. This information can help during the investigation of the incident and the identification of the responsible parties.
7. **Investigate the attack.** You should aim to find out how the cyberattack occurred so you can determine how to prevent future cyberattacks.
8. **Prevent future attacks.** Implement measures to prevent future breaches, including more robust security measures, providing additional employee training, updating policies and procedures and conducting regular security audits.

Working through the magnitude of things that need to be done in the event of a cyberattack is why it's crucial to have a plan in place before it happens.

KNOW WHOM TO CALL UPON FOR HELP

In addition to a plan, you should have a ready-to-assemble team consisting of experts who can work together to help you respond quickly and effectively. Here are some of the key roles you should rely on:

- **Chief information security officer (CISO).** Regardless of the exact title, this person is responsible for the security of your information. They can help investigate the attack, mitigate damage and prevent future attacks.
- **Cybersecurity firm.** Hopefully, you have an existing relationship with a firm. If not, you will need to find one quickly. Count on them to provide expert advice and assistance in investigating the attack to limit damages. They can also play a large role in helping with a strategy to prevent future attacks.
- **Lawyer.** Rely on legal counsel to provide advice on the implications of the attack, such as notification requirements and potential liability.
- **Public relations specialist.** This could be an internal or external role, but this person(s) can help you communicate with the public in an accurate, timely and transparent way. They will make sure you are mindful of the relationships you need to preserve and handle any media narrative if it ends up in the news. They are experienced in crisis counseling and can provide counsel to protect your reputation.
- **Insurance company.** If you have cyber insurance, pull upon the resources available to make sure you're doing what is needed to get financial assistance for you and those impacted.

Your team will help you stay calm while acting quickly. They can help you communicate effectively with everyone involved, limit exposure and ensure you're better protected if a cyberattack happens again.

NOTIFICATION & REPORTING OF ANY ATTACKS

The necessity of notifying and reporting cyberattacks cannot be overstated. Affected parties must be promptly informed if their sensitive data has been compromised. This is where your team can help you with the right messaging to protect your company as well as those impacted.

The notification should be clear and comprehensive and cover items like:

- What happened
- What data was compromised
- What steps are you taking to protect customers, employees, partners and yourself
- What steps can they take to protect themselves

You must also clarify you are willing to answer any questions that people may have and how they go about asking them.

If you are offering something to help those affected people protect themselves, explain what it is and how they get it. This could be something like free credit monitoring, identity theft protection, discounts, etc. Rely on your insurance company here if any offer is covered in your policy.

Finally, be sure to apologize—a sincere apology goes a long way. Let people know that you are sorry this happened and that it's creating an inconvenience for them. It shows respect and helps repair relationships and restore trust.

A well-prepared response strategy is as crucial as a robust cybersecurity plan in the fight against the ever-evolving landscape of cyber threats.