Cyber Attack: What to Do After a Security Breach

Home

Understanding Different Types of Cyber Attacks

Unfortunately, any small business could face the risk of a data breach or cyber attack. Regardless of how big or small your business is, if your data, important documents or customer information is exposed, recovering from the aftermath could be difficult.

There are many types of cyber attacks. Some of the most common include:

- Phishing: a type of social engineering scam that attempts to fraudulently obtain sensitive information using email.
- Ransomware: malicious software designed to block access to a computer system until a sum of money (or ransom) is paid, or some other action is completed.
- Baiting: infecting a computer with malware after tricking someone into downloading free music or movies.

Steps to Take After Business Data Breach

If your business is the victim of a data breach and you're wondering what to do after a cyber attack, consider the following steps to help minimize the damage:

1. Contain the Breach

While you may be tempted to delete everything after a data breach occurs, preserving evidence is critical to assessing how the breach happened and who was responsible. The very first step you should take after a breach is to determine which servers have been compromised and to contain them as quickly as possible to ensure that other servers or devices won't also be infected.

Here are a few immediate things you can do to attempt to contain a data breach:

- Disconnect your internet
- Disable remote access
- Maintain your firewall settings
- Install any pending security updates or patches
- Change passwords

You should change all affected or vulnerable passwords immediately. Create new, strong passwords for each account, and refrain from reusing the same passwords on multiple accounts. That way, if a data breach happens again in the future, the damage may be limited.

2. Assess the Breach

If you are one victim of a broader attack that's affected multiple businesses, follow updates from trusted sources charged with monitoring the situation to make sure you know what to do next. Whether you're part of a broader attack or the sole victim, you'll also need to determine the cause of the breach within your specific facility so you can work to help prevent the same kind of attack from happening again. Ask yourself:

- Who has access to the servers that were infected?
- Which network connections were active when the breach occurred?
- How was the attack initiated?

You may be able to pinpoint how the breach was initiated by checking your security data logs through your firewall or email providers, your antivirus program, or your Intrusion Detection System. If you have difficulty determining the source and scope of the breach, consider hiring a qualified cyber investigator - it may be worth the investment to help protect yourself moving forward.

Identify those affected by the breach

You'll also need to find out who may have been affected by the breach, including employees, customers, and third-party vendors. Assess how severe the data breach was by determining what information was accessed or targeted, such as birthdays, mailing addresses, email accounts and credit card numbers.

Educate your staff about data breach protocols

Your employees should be aware of your business's policies regarding data breaches. After discovering the cause of the breach, adjust and communicate your security protocols to help ensure the same type of incident doesn't occur again. Consider restricting your employees' access to data based on their job roles. You should also regularly train your employees about how to prepare for a data breach or avoid a data breach in the first place.

3. Manage the Fallout

Notify managers and employees of the breach

Communicate with your staff to let them know what happened. Define clear authorisations for team members to communication on the issue both internally and externally. Remaining on the same page with your team is crucial while your business is recovering from a data breach. You may need to consult with legal counsel to figure out the best way to let your customers know about the breach.

If you have cyber liability insurance, notify your carrier

Cyber liability insurance is designed to help you recover from a data breach or cyber security attack. Contact your carrier as soon as possible to see how they can help assist you with what to do after a cyber attack. If you don't have a cyber liability insurance policy, AmTrust's appointed agents can assist you in the process of selecting cyber liability coverage that could help with costs associated with addressing future cyber incidents as well as identifying potential cyber exposures.

Notify customers

Emphasize your willingness to be transparent with your customers by considering a special action hotline specifically to address questions from affected individuals. Communication can be key to maintaining positive, professional relationships with your patrons.

A data breach can be stressful, but as long as you take the right steps, your business will be better prepared to recover successfully. Moving forward, conduct frequent security checks to help reduce the likelihood of an incident occurring again in the future.

Cyber Fraud Risks

Cyber fraudsters have targeted remote desktop sharing applications to compromise these systems and to gain access to other shared applications.

Teleworking Tips to Protect the Organization

- Restrict access to remote meetings, conference calls or virtual classrooms, including the use of passwords, if possible.
- Do not share links to remote meetings, conference calls or virtual classrooms on open websites or open social media profiles.
- Never open attachments or click links within emails from senders you do not recognize.

Other Cyber Fraud Prevention Recommendations

The FBI has provided the following additional tips that can help protect individuals and businesses from being victimized by cyber fraudsters:

- Do not open attachments or click links within emails received from senders you do not recognize – if you do, report it to your IT department immediately so they can make sure malware not been activated and released.
- Do not provide usernames, passwords, birth dates, social security numbers, financial data or other personal information in response to an email or phone call.
- Avoid using the same password for multiple accounts. Follow these tips to create a strong password.

Make sure your businesses takes time to review and update information security policies, business continuity plans and data breach response plans, and regularly communicates with employees about them.

How to Report Cyber Crimes

If you discover you are the victim of a fraudulent incident:

- Contact your IT/security department, if you have one
- Immediately contact your financial institution to request a recall of funds
- Contact your employer to report irregularities with payroll deposits
- Report the attack to the Internet Crime Complaint Center (IC3). They'll forward it to federal, state, local, or international law enforcement. Also, contact your credit card company. Tell them if you're disputing unauthorized charges made by scammers on your card or if you suspect your card number was compromised.
- If you or your organization is the victim of a network intrusion, data breach, or ransomware attack, contact your nearest FBI field office or report it at tips.fbi.gov.
- You could also become a victim of identity (ID) theft. Visit IdentityTheft.gov to learn how to minimize your risk.

Protect Your Business from Future Cyber Attacks with Cyber Liability Insurance

Cyber liability insurance for small businesses provides a variety of services to address the modern day risks and threats of business identity theft and data breaches. For more information about cyber liability coverage contact us.

This material is for informational purposes only and is not legal or business advice. Neither AmTrust Financial Services, Inc. nor any of its subsidiaries or affiliates represents or warrants that the information contained herein is appropriate or suitable for any specific business or legal purpose. Readers seeking resolution of specific questions should consult their business and/or legal advisors. Coverages may vary by location. Contact your local RSM for more information.