CHECKLIST

Cyber Attacks

How to Protect Against Cyberattacks — and What to Do if You Are Attacked

Here's precautionary steps to prevent hackers from attacking your organization and a list of steps in case of an attack.

Cyberattacks are a major security issue, as hackers have exploited security weaknesses everywhere, from small businesses all the way through Fortune 500 corporations, with every industry at risk.

COVID-19 has made conditions worse. During the pandemic, more workers are accessing computer systems remotely (using personal devices) and individuals have been shown to be prone to phishing attacks involving COVID-19 themed email. Meanwhile, hackers have greater incentives to breach networks than ever: Total damages due to cybercrime are expected to reach $6 *trillion* worldwide in 2021.[1]

Although it's almost impossible to prevent all data breaches, organizations that guard against intrusions while also establishing post-attack protocols are best positioned to identify and respond to an attack. While all breaches may not be preventable, a well-prepared organization is better able to contain and minimize the impact of the breach.

Here are the checklists for preparation and response.

Preparing for a Cyberattack

□ **PLAN. Develop and maintain an incident response plan.** Planning needs to happen before an attack occurs. Key ingredients of a cyber incident response plan include a list of stakeholders and a plan for notifying them, along with instructions on how to investigate and escalate the issue. The actions outlined in a good incident response plan are also often supported by a cyber data breach policy, which provides the organization's driving set of principles.

□ **PROTECT. Defend the infrastructure and train the workforce.** Technical cyber controls like multifactor authentication, regular data backups, and firewalls are essential. With nearly 90% of all breaches caused by *human* error and a marked increase in working from home and COVID-19-related phishing attacks, *human* firewalls are important as well. Employees must be trained (and retrained) to recognize and report phishing and malware emails through an enterprise-wide reporting system. Keeping the organization safe dictates that cybersecurity is every employee's responsibility.

□ **DETECT. Be aware of the threat.** Employing endpoint detection and response software along with email filtering tools will help detect an intrusion. Periodically assessing vulnerabilities with network virus scans or penetration tests is especially critical for organizations with multiple locations and complex IT infrastructures.

Post-Breach Response and Recovery

□ **Document facts and actions.** Every cyberattack or data breach is unique, making it important to document key decisions and actions taken. As you begin to triage the situation and uncover what happened, keeping track of dates, times and details will help preserve evidence and move quickly into recovery.

□ **Contact and validate.** Engaging IT is the first step to validating whether you have sustained a cyberattack. Understanding who was affected, whether sensitive data was compromised and the impact will help inform plans to contain and mitigate the incident.

□ **Notify and leverage.** An insurance broker will help guide a successful recovery and claims process. Notifying the cyber insurance carrier via their breach response hotline is key to leveraging approved third-party breach response vendors that will aid you and help you avoid policy coverage issues down the road. The process usually involves retaining a privacy attorney, who will ensure compliance with federal and state regulations and engage response vendors and notify those affected by a breach.

□ **Contain and mitigate.** If breach response vendors are not immediately available, preserve evidence by disconnecting or isolating affected machines. Remember to avoid changing the state of the systems in question. If systems are on, leave them running, but disconnect from the network. If they are off, unplug them. Do not run programs and utilities or plug in storage devices and removable media without the help of an expert.

□ **Investigate and remediate.** Steps related to the forensic investigation, monitoring, remediation and recovery phases are often complex and technical — a privacy attorney or breach coach should dictate them. Remember that engaging a privacy attorney early may provide attorney-client privilege, which helps keep confidential communications secret in the face of legal demands for such communications.

Don’t Get Held for Ransom

When you partner with HUB, you’re surrounded by a team of experts who can help defend and protect your business. HUB gives you peace of mind — you know that your most-important assets are safe. For more information on how to help prevent a cyberattack and know what to do in case of one, contact a HUB cyber insurance specialist.

[1] Cybercrime Magazine, “Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021,” October 26, 2020