PAPER

Malwarebytes

How to create a successful cybersecurity plan

Along the edge of subway tracks in the UK is a sign that says, "Mind the gap," warning passengers to watch out for the space between the station platform and the train. Business owners might consider these words as well when they think about the gaps in their own security. When a plan for protecting data hasn't been fully realized, it's easy for safety precautions to slip through the cracks.

And that's why it's important to have a cybersecurity plan.

As breaches become the new norm, having a cybersecurity plan becomes not just a matter of saving face, but of saving money, data, and valuable employee resources. Each year, thousands of breaches take place around the world, resulting in the theft of over 1 billion records of personal identifiable information. According to the Ponemon Institute's 2018 Cost of a Data Breach Study, the average total cost of a data breach is $3.86 million.

> "The sustainability of the business hinges on what every employee does, both internally and externally. A single individual's actions can result in data being compromised throughout the business, from intellectual property to financial data."
>
> Davis Truong, Enterprise Architect
> Malwarebytes

Getting started

Cybersecurity policies can range in size from a single one-sheet overview for user awareness to a 50-page document that covers everything from keeping a clean desk to network security. The SANS Institute offers templates for creating such policies, if you're looking at developing a more robust plan.

Ideally, a company's cybersecurity plan should be documented, reviewed, and maintained on a regular basis. Realistically, many small and medium-sized businesses don't have the manpower. Even creating a short guide that covers the most important areas goes a long way in keeping your business protected.

Compliance

Taking a look at the cybersecurity regulations put forth by the federal government or by your industry is a helpful roadmap for developing a cybersecurity plan. First and foremost, you need to make sure you're operating within the law. For example, if you're a business entity that deals with protected health information, you must have certain administrative, physical, and technical safeguards in place. The HIPAA Security Rule requires organizations, their business associates, and even their subcontractors to maintain and implement written policies and procedures for protecting data and technology.

Infrastructure

A well-thought-out cybersecurity plan outlines which systems should be in place to guard critical data against attacks. These systems, or the infrastructure, tell IT and other administrative staff how they will protect the company's data and who will be responsible for protecting it.

Your cybersecurity plan should include information on controls such as:

- Which security programs will be implemented (Example: In a layered security environment, endpoints will be protected with antivirus, firewall, anti-malware, and anti-exploit software.)
- How updates and patches will be applied in order to limit the attack surface and plug up application vulnerabilities (Example: Set frequency for browser, OS, and other Internet-facing application updates.)
- How data will be backed up (Example: Automated backup to an encrypted cloud server with multi-factor authentication.)

In addition, your plan should clearly identify roles and responsibilities. That includes:

- Who is responsible for the plan's maintenance
- Who is responsible for enforcing the plan
- Who will train users on security awareness
- Who responds to and resolves security incidents and how
- Which users have which admin rights and controls

Employees

The most critical step in establishing a successful cybersecurity plan is documenting and distributing the acceptable use conditions for employees. Why? No matter how strong defenses are, users can introduce threats to your company's networks by falling for phishing scams, posting secure information on social media, or giving away credentials. According to the 2014 IBM Cyber Security Intelligence Index, over 95% of all threat incidents investigated involved human error.

Your cybersecurity plan should clearly communicate best practices for users in order to limit the potential for attacks and ameliorate damage. They should also allow employees the appropriate degree of freedom they need to be productive. Acceptable use guidelines might include:

- How to detect social engineering tactics and other scams
- What is acceptable Internet usage
- How remote workers should access the network
- How social media use will be regulated
- What password management systems might be utilized
- How to report security incidents

In addition, the employee plan should also cover what happens when users fail to comply with guidelines. For example, an employee found to be responsible for a breach might be required to repeat training if it was due to negligence, or terminated if the breach was an inside job.

Next steps

Establishing and documenting a cybersecurity plan is just the first step in keeping your business secure. Once the plan has been created, you'll need to come up with a strategy for deploying it, maintaining it, training users, and making them accountable.

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796