Cyber Risk

BEYOND THE FIREWALL

5 Ways to Protect Your Cyber Space

HYLANT

hylant.com

INTRODUCTION
PROTECT YOUR SPACE

Cyberattacks are in the news daily. Not only is the frequency increasing, but so is the loss severity. That's why cyber underwriters, when deciding to insure an organization, are looking more closely at what the organization is doing to protect its systems and data.

Most organizations are familiar with preventive steps such as securing firewalls and installing antivirus software to help safeguard their technology systems. However, companies sometimes overlook other *important ways to protect their cyber space*, such as the following.

ONE:
MULTIFACTOR AUTHENTICATION

Have you recently logged in to your bank account and then received a text or email asking you to copy and paste a code, answer a security question, or type some other type of secondary information into the login page? That's **multifactor authentication**, or MFA. It's a way your authorized system users can remotely log into your environment and prove they are who they say they are. MFA makes it much more difficult for threat actors to remotely log in.

If you don't have MFA in place, most insurance companies that offer cyber risk coverage are not going to insure you. The risk is simply too great. It's the equivalent of leaving the doors to your home not only unlocked when you leave for vacation, but also wide open.

TWO:
NETWORK SEGMENTATION

If an employee has login credentials to your network, can he or she see everything on your network? If so and a bad actor gains access to your systems through an email phishing scam or other way, **your entire cyber environment is now at risk**.

While there are ways to secure networks, most of the time it's not necessary that every user have access to every piece of the environment. **Network segmentation can be a powerful tool for limiting potential damage to your organization's systems and data.**

"Taking cybersecurity seriously cannot be something that only comes from the IT function. Every single employee has a hand in cybersecurity. Creating a culture of information security is critical. It must come from the top of the organization, and the C-suite must really believe it and live it."

THREE:
EMAIL FILTERING AND EMPLOYEE TRAINING

Your well-meaning employees are the most vulnerable part of your organization's network security program, thanks to phishing scams. The reality is that everybody is busy. All it takes is one click on one bad link, and someone has given away their credentials, which a threat actor can use to enter your network.

Applying strong email filtering programs is important. So is training your employees to identify phishing emails. Supplement the training with phishing testing that praises employees who correctly identify and report a suspected bad email (your test email). Provide further education for those who don't identify it and instead click on it ***(e.g., This was a phishing test--a potential scam. Here's how you could have identified it, and here's how to avoid that mistake in the future.)***.

FOUR:
ENCRYPTION

If you have sensitive data, whether it's personally identifiable information, commercial confidential information, or third-party information that you don't want made public**,** **encrypt it.** Encryption is the process of scrambling text or data and making it unreadable by anyone except its owner.

Even if your data is stolen or accessed, encrypted information won't be viewable by bad actors.

"Give your information security team a high-five. They do a tough job and don't get enough thanks. CEOs and CFOs get to sleep occasionally. CIOs never sleep."

FIVE:
SYSTEM BACKUPS

To avoid a ransomware situation, it's important to back up systems thoroughly and frequently. Store information offsite and, if possible, offline. Why offline?

Let's say you accidentally click a phishing email. Nothing seems to happen, but you've given away credentials to a threat actor who's laying low in the environment, moving laterally, and discovering where your backups are stored. **If they're stored on your network, the criminal can encrypt not only your network but also your backups.**

ONE MORE
IMPORTANT STEP

These are all good measures, but are they enough? Many business leaders believe they can "prevent" their way out of a cyber risk, that they can manage their risk down to zero. Unfortunately, that's just not possible. So then, what's left?

Preparation. Creating, testing, and regularly updating a cyber incident response plan can help your company recover more quickly and with less turmoil. If your company has a plan but hasn't reviewed and tested it in the last few months, we recommend you start immediately.

Need help? Contact a Hylant risk manager today.