P&N
Postlethwaite & Netterville

Cybersecurity: It's a Lot, but is It Enough?

By Michael Richmond

If a hacker decided to launch a cyber attack against your organization, would they meet any resistance? Or would they be able to easily find and exploit vulnerabilities, gaining access to sensitive customer and employee information? How would your organization respond to the attack? How quickly would you know it had happened?

Many businesses are compromised without realizing that their sensitive data is in the hands of hackers until months after the initial attack.

With frequent headlines about high-profile breaches at well-known companies, you may be wondering if cybersecurity is something your company should be concerned about, too. The short answer is yes. A cyber attack is one of the greatest threats to any organization, not just multi-billion dollar brands. Hackers have the tools to easily and quickly target multiple organizations of any size. Businesses with fewer resources and defenses in place can easily fall victim to these wide-reaching attacks, making an organization like yours a more vulnerable target than the large corporations you hear about in the news. The risk to your business' reputation, client relationships, and revenue stream is very real.

With the ever-evolving tactics used by hackers, cybersecurity is not something that you set up and then forget about. It requires constant evaluation, monitoring, and education. Cyber attacks can cause damage in almost no time, and knowing how to identify and respond to the attack quickly is crucial. Many businesses are compromised without realizing that their sensitive data is in the hands of hackers until months after the initial attack. Don't fall into the trap of underestimating the value of cybersecurity until your business is victimized.

The following steps are some of the basic strategies to protect against cyber attacks:

- Consider any complex regulations that apply to your organization (PCI, HIPAA, HITECH, FISMA, GDPR, SOX). Manage compliance and track regulatory changes.
- Conduct an IT risk assessment every 24 months.
- Conduct penetration testing to identify vulnerabilities.
- Train employees to spot potential red flags, and re-train them with updated tactics repeatedly.
- Test employees with real-world scenarios at random, and require re-training for any employees who fall victim.
- Implement or update your written IT policy (including policies related to employees' personal devices).
- Manage and monitor your IT policy.

- Patch all software and ensure programs and devices are up-to-date for every user.
- Back up all data and create a recovery plan to address the risk of data corruption or loss.
- Manage anti-virus protection for all users.
- Require strong passwords that include a combination of uppercase and lowercase letters, numbers, and symbols. Require that employees change these passwords once a month.
- Implement necessary tools to identify breaches and recover any lost data.
- Have a plan in place to effectively respond to incidents.

It's a long list, but it's not all-encompassing. Fortunately, cybersecurity providers like P&N's Technology Services Group stay up-to-date with the latest threats and vulnerabilities. By partnering with a team of professionals who have the technical knowledge and experience to customize a protection strategy, monitor for threats, and respond in the event of a breach, you can get past the overwhelming details and focus on your business.