CAIN ELLSWORTH
& COMPANY, LLP
Beyond the Numbers...

A Proactive Approach to Cybersecurity Risk Management

A quick glance at the news shows that cyber threats are everywhere. Hackers are getting more sophisticated, and they're not limiting their victims. Businesses and organizations of all sizes - from mom-and-pop shops to mega-corporations and government agencies - have become targets.

A cyberattack can be devastating. It can cost your business a significant amount of money, harm your reputation, and disrupt your operations.

In 2017, Equifax experienced a massive data breach that exposed the personal information of 147 million people. The fallout was huge: they agreed to a settlement of up to $700 million to help those affected. That's not just pocket change; it's a financial hit any business would feel.

Then there's Heartland Payment Systems - a company that didn't realize for months that hackers had infiltrated their systems. By the time they caught on, over 100 million credit and debit card numbers had been stolen. The company's reputation took a nosedive. Their stock price plummeted by 77%, and they paid over $200 million in compensation. Eventually, they were acquired by a larger competitor.

The list of examples goes on and on. Whether it's a data breach, where someone breaks into your system to steal information, or a data leak, where sensitive info accidentally gets exposed, both can spell trouble. The good news is that you can help prevent these issues with strong cybersecurity practices.

Build a strong defense

A strong cybersecurity foundation is your first line of defense against threats. Begin by securing your internal network, starting with firewalls and encryption settings. While many routers include these protections, verify that your device uses the latest encryption standard and are updated with the latest firmware.

Ensure all devices connected to your network have reliable anti-malware and antivirus software installed. These will help to detect, prevent, and remove malicious software from your devices.

Even the best security setup is vulnerable if it's not kept up to date. Software updates aren't just about new features; they often patch critical security weaknesses that hackers actively exploit. Regularly updating all systems is a fundamental practice to protect against breaches.

Enforce password security

Provide employees with a password manager to help them create, store, and manage strong, unique passwords. Most password managers also enable users to securely share passwords with others when necessary.

Finally, ensure employees use multifactor authentication when available, so logging into secure sites requires a second form of verification.

Ensure remote devices are secure

When employees work remotely, they need to be especially careful. Their computers might also be used for non-work activities or shared with family members, increasing the risk of exposure to cyber threats. Ensure that all work devices have up-to-date antivirus and anti-malware software installed and establish clear guidelines for remote work.

Secure data disposal

One of the lesser-known ways that data is leaked is through discarded hardware that still contains sensitive information. To prevent this, ensure data is permanently deleted from devices using specialized data-wiping software. Simply deleting files from a drive isn't enough, as data can still be retrieved without proper destruction.

Educate your team

Your employees play a key role in protecting your business from cyber threats. Consider what happened to Mailchimp: cybercriminals successfully carried out a phishing attack by tricking an employee into revealing their credentials. This led to a data breach that compromised several hundred user accounts, including those of well-known businesses. With more thorough training on phishing scams and the use of multifactor authentication, this incident might have been avoided.

To prevent similar incidents, train your team on the importance of secure passwords, how to handle sensitive data, and the risks of unsecured networks. Keep them informed about the latest threats and phishing tactics, and regularly remind them of your security protocols.

Control access to information

In 2022, fintech company CashApp faced a costly leak of 8.2 million users' personal and financial information. Sadly, the leak came from within. After terminating an employee, the company failed to revoke the employee's access permissions, so they were able to download sensitive data from outside the company.

To prevent incidents like these, limit access to sensitive data based on each employee's role - giving them only the access necessary to do their job. Implement proper termination procedures to immediately revoke access when someone leaves the company. Regularly conduct user access reviews and continuously monitor user activity to spot any unusual behavior.

Manage third-party risks

Your security is only as strong as your weakest link, which might be a third-party vendor or partner. Consider what happened to Facebook in 2019. A third-party app developer had failed to password-protect their entire dataset, and this oversight left sensitive user information open for anyone to access and download. While Facebook wasn't directly responsible for the incident, it brought scrutiny to how they managed third-party access to user data.

This highlights the importance of evaluating the security practices of any third parties you work with, especially if those third parties have access to financial or medical data, which could expose your company to legal issues. Include clear security requirements in your contracts and regularly assess their compliance.

Have a plan for incidents

Even with strong defenses, cyber incidents can still happen. That's why it's wise to have a plan ready before anything goes wrong. Think of it as a fire drill for your company's cybersecurity.

To reate an effective response plan, establish a clear process for assessing the situation, neutralizing the threat, and recovering. Identify who contacts IT, who informs management, and who is responsible for communicating with clients and stakeholders. Beyond the immediate communication flow, your plan should also detail the steps necessary to contain the breach, restore systems from backups, and assess the extent of the damage.

Lastly, don't forget to test your plan. Conduct drills to see how well it holds up under pressure, and update it regularly to account for new vulnerabilities or changes in your business operations. This preparedness can make all the difference in how quickly you recover and how well you protect your business's reputation and assets.

Consider cyber insurance

Many insurance providers now offer cyber insurance designed to help your business recover from the financial losses caused by cyber incidents. However, it's important to shop around. Policies can vary widely, so be sure to understand any limitations a policy may have and choose one that best fits your needs.

Next Step

We share this information to help you strengthen your defenses against cybersecurity risks. Our goal is to support your business growth while minimizing potential threats that could impact your financial health. If you'd like to discuss additional strategies to bolster your defenses against financial risks, please contact our office.

About Cain Ellsworth.

Cain Ellsworth is not all things to all people. Instead, we specialize in serving small to medium businesses in banking, manufacturing, property and casualty insurance, plus a variety of other industries. And we dedicate significant resources to assure that we are well-informed in each of them.

Cain Ellsworth:

Sheldon, IA Office
1008 Third Avenue
PO Box 449
Sheldon, IA 51201

Sioux Falls, SD Office
5130 E 57th Street
Sioux Falls, SD 57108

IA - (712) 324-4614
SD - (605) 610-4611

sdykstra@cainellsworth.com

www.cainellsworth.com