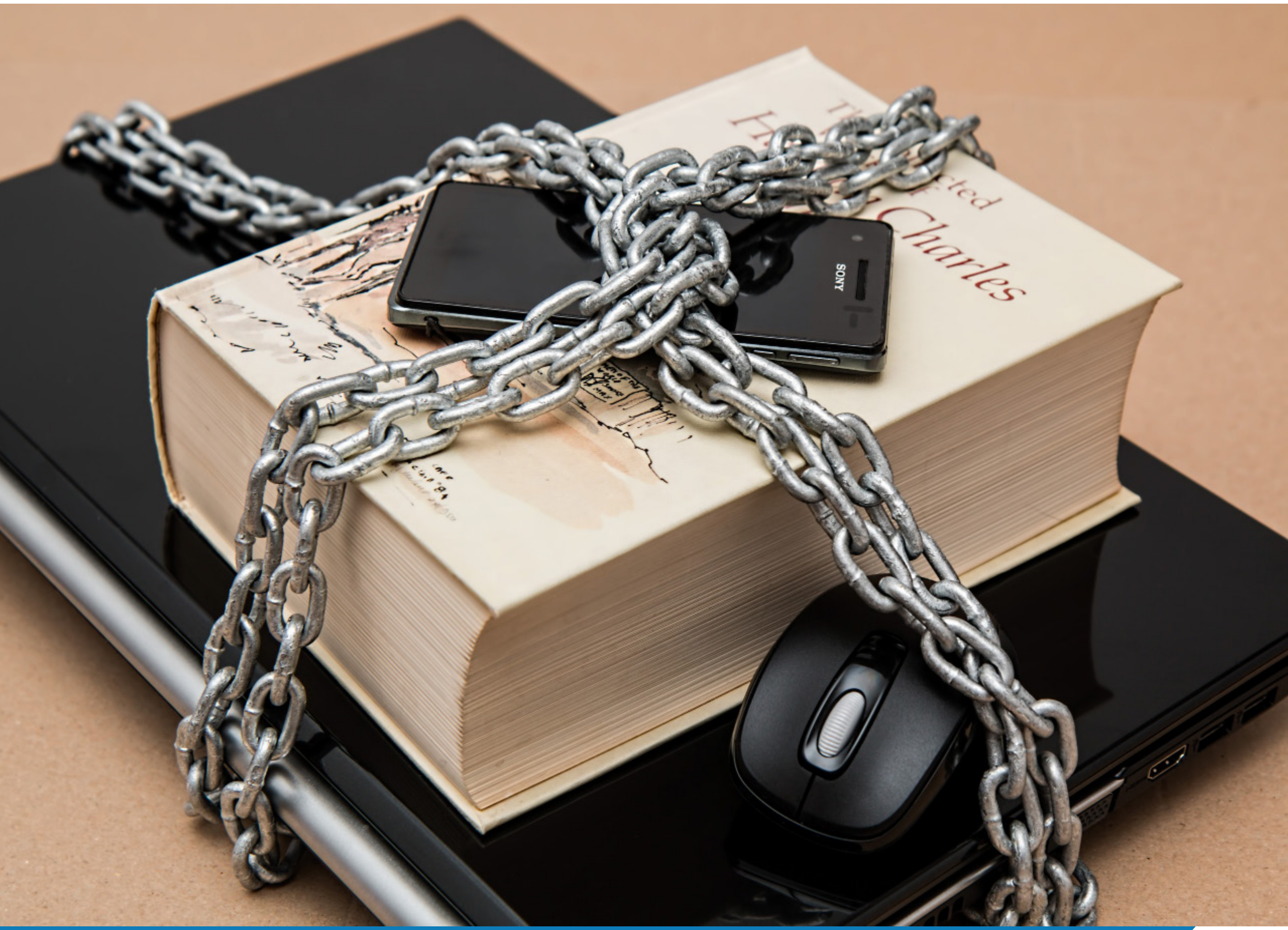
CAIN ELLSWORTH
& COMPANY, LLP
Beyond the Numbers...



What you need to know about Cyber Threat and Cyber Defense

Cyber security is a constant battle on both an individual and corporate level. If you aren’t vigilant about cybersecurity, it could cost you. In fact, The National Computer Security Survey, which was conducted by the U.S. Department of Justice’s Bureau of Justice Statistics, determined that “approximately 68% of the victims of cyber theft sustained monetary loss of $10,000 or more.” CSO (from IDG) states that “the average ransomware attack costs a company $5 million.” That’s especially concerning when you consider the fact that 42 percent of companies report experiencing some form of ransom attack.

Cyber Defense Isn’t Just an IT Concern

Still, when you mention “cyber crime,” “cyber threats,” or “cybersecurity,” many executives are quick to dismiss the issue. They assume their IT department will handle the problem, leaving their hands free for other work.

By the same token, individuals often assume cyber threats are thwarted by the various computer programs and apps they use, both at work and in their own personal lives. But these are both serious misunderstandings of the current state of security.

While most IT departments and software developers are doing everything they can to protect both businesses and individuals from cyber threats, the current level of cyber crime is so high that defense simply must be a group effort.

To put it bluntly, there’s no way to stick your head in the sand and pretend that cyber threats aren’t an issue for everyone – because they absolutely are.

Here are some of the best defense strategies against cyber threats.

1) Password Security

81% of breaches are caused by poor password security. Obvious, but all too common issues are using the same password across multiple sites, using easily guessed passwords and storing passwords in an insecure manner.

There are available tools you can use for password management such as LastPass or Dashlane. These products enable you to securely store your passwords across multiple devices such as your computer, phone and tablet.

They also help in generating new random passwords when registering for any new online account.
Passwords are not easily guessed nor is the same password used across multiple sites.
These products also enable you to securely share login credentials with your colleagues or family members.

2) Anti-Virus Software

There are a lot of ways that your computers can be corrupted; computer viruses, malware, ransomware and spyware are a few examples. While there are a lot of threats there are also many ways to stay protected. Consider protecting your computers with a suite of security tools such as Kaspersky Internet Security or Bitdefender Total Security.

A security suite is ideal because it can protect against many different types of threats.
Make sure to protect all devices connected to your network or accessing sensitive data, this can include mobile phones, tablets, remote laptop computers, and even wifi-devices.

3) Outdated Software

Almost all computer software comes with its own protection against cyber security threats, but these protections only work if they are updated with the most recent patches and fixes. Oftentimes, your program may prompt for automatic updates. Other times, however, this may require an action on your part. Regardless, make sure all software is updated.

4) Backup Your Data

Always maintain proper backups of your data. Ideally, you'd keep one backup of your data on-site and one off-site. Consider using a service like Dropbox or Google Drive to centralize and maintain backups of your files. These services are great for centralizing files across all employees and devices while also being able to maintain local backups of your files.

However, please be aware that online storage for revisions and deletions may be limited, so be sure to check with the servicer provider. You may also want to consider vendors that focus just on data backup like Carbonite.

5) Internal Security Policies

A significant vulnerability that companies face is their own employees and simple human error.

Consider who has access to what data and assess if they really need access to that data. Limit access to sensitive data where possible.

Implement proper procedures and train employees on handling sensitive data. Procedures should address how to properly verify identities when discussing data with customers or vendors, or modifying data, or modifying access to data.

Also consider limiting employees ability to connect their personal devices to your network. Viruses can certainly exist on devices like personal computers and flash drives.

Conclusion

It’s not our intention to scare you with this information, but just to make sure you’re aware of the possible implications of cyber security threats.

Because cyber crime is on the rise and can cause such serious harm for both individuals and businesses, it’s absolutely essential that you protect yourself with the proper defense techniques.

You should also remember to only trust your data to qualified experts who also implement their own security techniques to ensure your information stays safe and confidential.

If you have any additional questions about cyber threats or defense strategies, please contact us for advice. We’re also happy to outline the security systems we use to keep client information safe.

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