Cyber risk is business risk. Small businesses can be attacked in the same way and by the same malicious actors as larger businesses, and yet small businesses simply do not have the same resources.

In that context, the newsletter is meant to provide quick insights and to aid awareness. The newsletter points out that phishing is where most compromises start. It mentions a multi-layered approach, and it mentions multi-factor authentication, or MFA as one important layer of defense. The observations and the advice are good. MFA is mentioned as part of a layered security approach, but have you ever wondered what the right layers are?

Years ago, I was sitting at my desk when one of those dreaded calls came. “The babysitter says everything is OK, but your six-year-old was hit by a car while riding a bike and is on the way to the hospital in an ambulance.” The caller had a strange approach to what “everything is OK” meant. I slammed the phone down and bolted out the door towards the elevator, knocking ~~a~~ departmental secretary to the floor. Suddenly I realized that I did not have my keys, wallet, or phone. I spun around and charged back into the office to grab my things and charged back towards the elevator. Things were going wrong, and I had no plan.

I had no plan, but I did have layers of child security. There was a bright, capable sitter. There was a helmet, there were phones, an ambulance, taxi cabs, a hospital, doctors, and insurance. My six-year-old survived and thrived.

Certainly, the layers of cyber security cannot be communicated in a one-page newsletter and reinventing the wheel for cyber could be quite a chore, but the point is that there are tools available to you. Those tools include the bright, capable people helping you build your business. They include your business practices and business partners like the Amalgamated Bank of Chicago. With the tools you have, you can build a plan.

Fortunately, the Center for Internet Security (CIS) has created a sharable, layered approach. CIS calls their approach the Critical Security Controls, and they have organized them in order of importance and by “Implementation Groups.” The implementation groups are levels of secure implementation ranging from Basic to Secure.

The CIS website has case studies, policy templates, helpful articles, and videos. Much of what CIS offers is free of charge. Some of the tools require a small annual investment. If your organization is ready to start building an effective cybersecurity program, CIS is a good place to start.

Building a cyber security program is like building a business. We must start where we are with the tools we have. Nobody can sell your business a box of success, and despite the cacophony of sales hype, there are no security tools that solve all the problems. Security is a process. Our business practices grow and evolve, and our cyber practices must keep pace because cyber risk is business risk.

Commercial Services Security Newsletter

April 2023 | CSN - Q1 - 2023

Raising the Security Level in Your Business

Businesses come in all shapes and sizes. Unfortunately, so do threats.

According to a 23 March report by Expert Insights, the biggest, most damaging and most widespread threat facing small businesses is phishing attacks. Phishing accounts for 90% of all breaches that organizations face, they've grown 65% over the last year, and they account for over $12 billion in business losses. Phishing attacks occur when an attacker pretends to be a trusted contact and entices a user to open the email.

Within the email, the attacker may include an attachment or link that downloads a malicious file or leads to a malicious site designed to collect credentials and other information. Collected information can lead them to areas containing high-value confidential information including account data.

Reducing Your Risk

Perhaps you currently outsource information technology security operations to a third-party service provider. For many small banks or credit unions, outsourcing information technology and security services may make sense, mostly due to a lack of expertise or perhaps cost.

Like any vendor, it requires close management and monitoring to ensure your interests are being met. Consider the following:

- *Are you sure that system vulnerabilities are being patched timely? How are you verifying this?*
- *Are you being notified of signs of potential probing and cyber-attacks?*
- *Do you require the vendor to undergo an independent audit and provide you with a certification?*
- *Where is the provider obtaining their threat-intelligence?*

Layered Security Approach

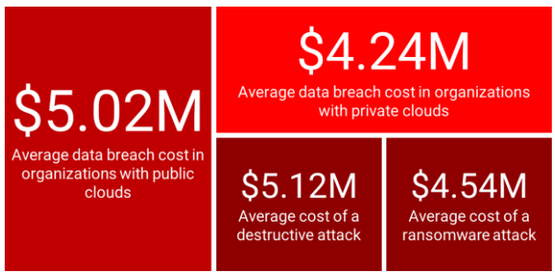
No security tool or measure is perfect, so you need to account for potential failures. Adding multi-factor authentication (MFA) when accessing your critical assets (e.g., customer records, employee data and healthcare information) is a baseline standard you should adopt.

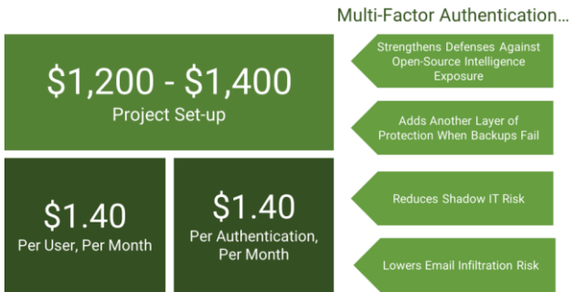
MFA requires more than one distinct authentication factor for successful authentication. The three possible authentication factors are:

1. *Something **YOU KNOW** (password or PIN),*
2. *Something **YOU HAVE** (badge or phone), and*
3. *Something **YOU ARE** (biometrics such as fingerprint, voice, or retina)*

Did You Know?

- The volume of phishing emails surged 569% and credential Phishing-related reports increased 478% in 2022.
- Half of US small and midsize businesses have no cybersecurity in place according to a 2022 study by UpCity.
- Implementing MFA can make you 99% less likely to get hacked according to Microsoft.
- Positive Technologies reports that 93% of corporate networks can successfully be penetrated by hackers, allowing them to deploy ransomware, trojans, spyware, or other malicious exploits.
- In 2022 malware attacks increased by 44%, with Emotet and Qakbot being two of the most prolific.





ROI comparison between the average loss associated with a cyber-incident and average setup use of Multi-Factor Authentication.

Cyber Insurance

MFA is fast becoming a cyber insurance requirement for all accounts, privileged and non-privileged, to protect on-site and remote access. Here's a quick guide to understanding the MFA insurance mandate. (IS Decisions)

In Summary

Amalgamated Bank of Chicago has other security recommendations that can help you incorporate additional layers of security to reduce your cyber-risks and keep your business profitable. Talk with your banking officer.

About the FS-ISAC

The Financial Services Information Sharing and Analysis Center is the only global cyber intelligence sharing community solely focused on financial services. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate, and respond to cyber threats. To learn more, visit fsisac.com.

