Talk Nerdy To Me

September 2019

CREATING A CYBERSECURITY CULTURE

Implementing An Effective Cybersecurity Strategy Is Critical

As news of cybersecurity threats and cyberattacks continue to dominate headlines, hackers continue exploiting vulnerabilities, foreign influences in elections and new forms of ransomware. This underscores the importance of preparing for these types of emerging threats. As a result, cyber risk management has become a fundamental component of our business operations. Understanding and mitigating this risk has become an essential skill.

No individual, government, or business is immune to a cyber-attack. C-level involvement is a critical part of implementing an effective cybersecurity strategy. But most do not know where to start. With a complex and shifting legal landscape, it's hard to understand where businesses need to comply. When organizations store and process data about their employees, business partners and customers they take on the risk of keeping that information safe. It is not possible to reduce your risk to zero, but we can take the necessary steps to reduce the harmful consequences of a data breach.

On May 5th, 2019, I began an online cybersecurity course offered by Harvard University. It is important that I stay up on the current technologies, but this was not a technology course. This was a business course focusing on the risks associated with technology. After completing the Harvard University course Managing Risk in the Information Age, I now have the framework to help businesses of all sizes start on creating a culture of cybersecurity.

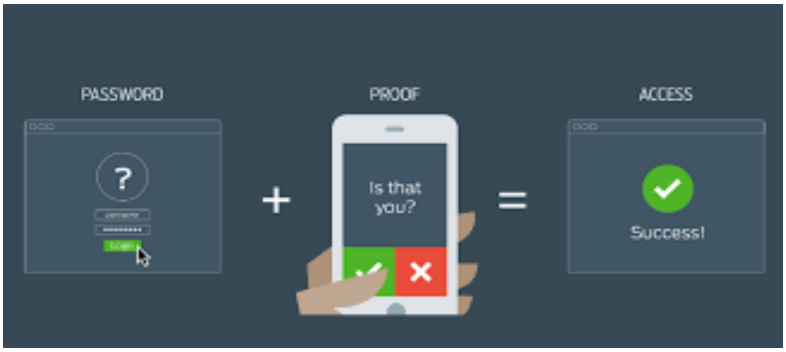
Working with peers from around the world over 8 weeks allowed me to design and develop a formal cyber risk strategy for Preferred IT Group. While we have all the technology and security systems in place, we still needed to formally add procedures and processes to ensure that we will respond accordingly in the event of a cyber-attack. Completing this course has allowed me to look at technology and the risks involved in a different way. I want to use my new-found knowledge to help businesses analyze and reduce those risks.

If you are a C-level employee or business owner looking to establish a culture of cybersecurity, contact Preferred IT Group to learn how we can help you establish your road map to reduce your risk and protect your business.

By: Jason Horne, CEO, Preferred IT Group

September 2019

Multifactor Authentication And Why It Is So Important



In today's world, passwords are just not enough. Passwords are a pretty laughable method of authentication and can be acquired easily from some simple phishing. That is why a lot of companies are pushing to use Multifactor Authentication, or MFA for short. Multifactor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) for logging onto a device, or program. Types of factors that are used are knowledge (something the user and only the user knows, such as a password), possession (something the user and only the user has, such as a hardware token or cell phone), and inherence (something the user and only the user is, such as a fingerprint).

Did you realize that you have most likely already used MFA in some form or another? For example, if you have swiped a bank card and entered a pin, or if you have logged into a website that sent a numeric code to your phone to gain access to an account. If you have done either of these, you have used MFA. In most cases MFA is very simple to use. In the typical scenario, you would first enter your username and password, then you would use an authenticator app, or a token to gain access. See, that isn't so bad!

So, what's the big deal? Why is it so important to use MFA? MFA helps protect you by adding an additional layer of security. It makes it more difficult for bad guys to log in as if they were you. Your information stays safe because a thief would have to steal your password and your phone/token to gain access to it. If you are using a phone instead of a token device you most likely have the extra layer of protection already because most phones are set up to use a password or fingerprint to unlock it.

The other big question we face is when to use an MFA? The answer is simple…use an MFA whenever possible. Especially when you are accessing sensitive data such as your primary email, your financial accounts, and your health records. But you must take the initiative to turn it on! Below is a list of some of the companies that have good authentication software.

- DUO Security
- Google Authenticator
- LastPass
- Ping Intelligent Identity Platform
- Authy
- RSA SecurID Access
- Google Security Key Enforcement
- Idaptive Next-Gen Access
- AuthPoint Multi-Factor Authentication
- RingCaptcha

Currently at Preferred IT Group, we use DUO Security as our MFA. We also have clients who use DUO. It is for organizations of all sizes. They secure access to your applications and data no matter where you or your users may be. We have found DUO to be user friendly and easy to work with.

We know that stopping all online crime is not realistic, but using an MFA will reduce your chances of having this happen to you. Please call us today to implement this extra security practice in your business.

BEFORE THE BREACH

HACKERS ARE HERE!

NEW SKILLS FOR A NEW FIGHT

- 1 in 5 businesses will suffer a cyber breach this year
- 81% of all breaches happen to small/medium sized businesses
- 66% of companies do NOT test their backups
- 60% of companies that lose their data will go out of business within 6 months
- 92% of malware is delivered via email
- 97% of breaches could have been prevented with today's technology

Want to learn more about how to protect your business?

Sign up TODAY for our FREE Cybersecurity Lunch and Learn

September 27th, 2019
12 PM to 4 PM
At Ruth's Chris Steak House
(Limited Seating)

RUTH'S CHRIS STEAK HOUSE

www.preferreditgroup.com/beforethebreach

talk nerdy to me

PREFERRED IT EMPLOYEE SPOTLIGHT

Meet Matt Hart! Matt started as an engineer with Preferred IT Group in April of 2018. He has been in the IT industry for 7 years. He is our Cisco certified engineer on staff, as well as having his CSSA and Datto DCAT certifications. During college, Matt was a part of Indiana Tech's Cyber Defense Team and went all the way to Nationals.

Matt is an avid curler and hockey fan. He is a board member of the Fort Wayne Curling Club. He also enjoys reading, playing board games with friends and playing video games. He has two dogs named Zeus and Freya.

Matt is a great addition to the Preferred IT Group team and we are pleased to have him!

Quarter 3 Leadership Team Offsite Meeting

Every quarter, our Leadership Team at Preferred IT Group has an offsite meeting to discuss issues and plan for the future. Once a year, we like to go somewhere fun! This year, we went to Tennessee and had a blast! The meeting was productive too...

MICROSOFT - END OF LIFE

There are only 4 months left until Microsoft deems Windows 7, Server 2008, and Exchange and Office 2010 end of life in January! Are your systems updated and ready for the change?

If it is important that your business be up to date and protected from virus, malware, and cybercriminals, call us today to find out how we can help!

If it's not important, well....we wish you the best of luck!

preferred IT group

CONTACT US

Fort Wayne
260.440.7377
Warsaw
574.306.4288
Columbia City
260.213.4266
Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.