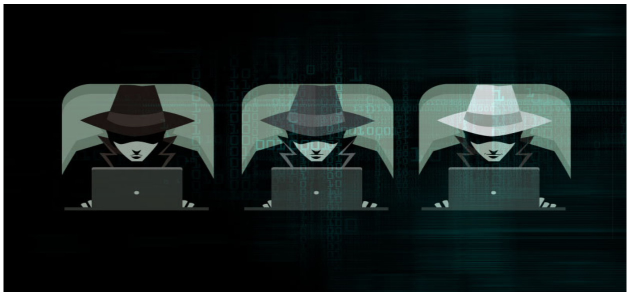
Talk Nerdy To Me

1

August 2019

THE GOOD, THE BAD, AND THE IN BETWEEN

Being A Hacker Is Almost A Dirty Word



The term “Hacker” was coined in the 1960s by individuals at the Massachusetts Institute of Technology (MIT) for people who creatively engineer. Creative engineering can involve almost anything; however, the term usually applied to those individuals who were connected to the computer engineering, mechanical engineering, or software development domains. If you were someone who could take two seemingly different things and make them work together in a creative way, you were a hacker.

Today, the term “Hacker” is viewed in a much different light and public opinion towards the creative genius that lead to someone being dubbed – Hacker, is no more. In today’s society, being a hacker is almost a dirty word; it’s something that conjures images of news bulletins, leaked data, monetary loss, and public manipulation. We’ve all seen the recent iterations of these transgressions displayed for full affect in the media – such and such state paid X for this ransomeware, such and such company was breached exposing everyone’s financial data, on and on and on. How often do you hear about hackers doing good? How often do you hear about hackers solving problems? How often do you see hackers saving companies from financial ruin?

Many organizations employ hackers or work with companies who employ hackers to test their infrastructure. These are the good guys/gals; the white hat hackers; the individuals focused on bettering society, security practices, themselves and others. These are the penetration testers, red team operators, security engineers, and reverse engineers. Most of these folks are highly passionate about their trade and see it as an opportunity to solve real world challenges while completing an extremely complex puzzle. They participate in bug bounty programs, collaborate with businesses directly to report and fix vulnerabilities, and offer their services for the betterment of the industry.

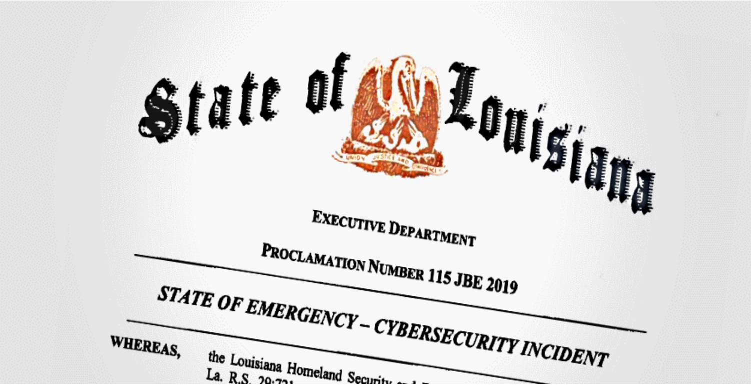
The black hat hackers are known in the hacker world as the unethical hackers and cybercriminals. These are the hackers we often hear about in the news today responsible for breaching company & customer data. These hackers are hacking for financial or political gain. They will use phishing scams and other tools to compromise user data. Once data is compromised it can be difficult to understand the extent of the damage caused.

The gray hat hacker is what most of the hacking world is made up of. These hackers typically don’t steal money and usually don’t target companies for data. Some may attack specific public figures for various reasons. These hackers typically don’t help people, and their skills are not as good as their white and black hat counterparts.

With the complex landscape of today’s business practices, it’s a best practice to follow a layered defense in-depth approach with regard to security. Preferred IT Group can help implement best practices for security in your company to help protect against those who would use their skills to cause your company harm. Call us today for a free network assessment.

Source: Jeremy Roe with Synack Inc.

Louisiana Declares State Of Emergecy After Ransomware Attack



State of Louisiana

EXECUTIVE DEPARTMENT

PROCLAMATION NUMBER 115 JBE 2019

STATE OF EMERGENCY – CYBERSECURITY INCIDENT

WHEREAS, the Louisiana Homeland Security

La. R.S. 29:721

Louisiana Governor John Bel Edwards has activated a state-wide state of emergency in response to a wave of ransomware infections that have hit multple school districts. The ransomware infections took place this week and have impacted the school districts of three North Louisiana parishes -- Sabine, Morehouse, and Ouachita. IT networks are down at all three school districts, and files have been encrypted and are inaccessible.

This is the second time that a state governor has activated a state emergency due to ransomware or any form of cyber-attack. The first time was in Colorado in February 2018, when the Colorado Department of Transportation was forced to shut down operations because of an infection with the SamSam ransomware. However, that state emergency activated additional state resources to help with traffic, road management, and transportation, and not with deploying cyber-security experts to help victims, like in Louisiana's case.

By signing the Emergency Declaration, the Louisiana governor is making available state resources to impacted schools. This includes assistance from cybersecurity experts from the Louisiana National Guard, Louisiana State Police, the Office of Technology Services, the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP), and others.

State officials hope that additional IT expertise will speed up the recovery process so schools can resume their activity and preparations for the upcoming school year.

Gov. Edwards was able to roll out a coordinated response for the ransomware infections at schools in the North Louisiana because he previously established a Cybersecurity Commission to assemble and coordinate response teams in the event of a cyber-attack.

He created this commission in December 2017, in the year when three ransomware outbreaks -- namely WannaCry, NotPetya, and Bad Rabbit -- had caused havoc across the globe, including in Louisiana.

"This is exactly why we established the Cyber Security Commission, focused on preparing for, responding to and preventing cybersecurity attacks, and we are well-positioned to assist local governments as they battle this current threat," Gov. Edwards said.

The state of emergency will remain in place until August 21, or until the recovery process at impacted school districts wraps up.

Gulf Coast neighbor Florida could have used a state of emergency declaration last month, as well, after three municipalities were hit by ransomware -- Riviera Beach (paid $600,000); Lake City (paid $500,000); and Key Biscayne (recovered from backups).

In recent months, US cities have been a prime target for ransomware gangs. Earlier today, some residents of Johannesburg, South Africa's biggest city and financial capital, have been left without electricity after a ransomware infection.

Source: zdnet.com

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 next Cyber Security Lunch and Learn in September!

www.preferreditgroup.com/beforethebreach

talk nerdy to me

	1			7	8			
	8			4		9		
		5	6				1	
1				6				5
	4		9	1	5		7	2
	6	7		8		4		
			3			1		
	7		8	9			2	3
					4			

PREFERRED IT EMPLOYEE SPOTLIGHT

Meet Scott Diehl! Scott is our Senior Systems Engineer and has been with Preferred IT Group for 5 years. Scott has been working in IT for 21 years! He has worked in various industries throughout his career, in Indiana, Chicago, Pittsburg, and California. Some of his most impressive certifications include Miscrosoft Server, VMWare 6 VCP-DCV, Red Hat RHCE5, and Datto DCAT.

Scott and his wife have a horse, two goats, a cat, and a dog. Scott loves to read, brew beer and watch the Steelers in his free time. He loves watching shows like Futurama and American Dad. Scott is our resident tea drinker in an office full of coffee people.

Scott is a huge asset to Preferred IT Group and we’re very thankful to have him!

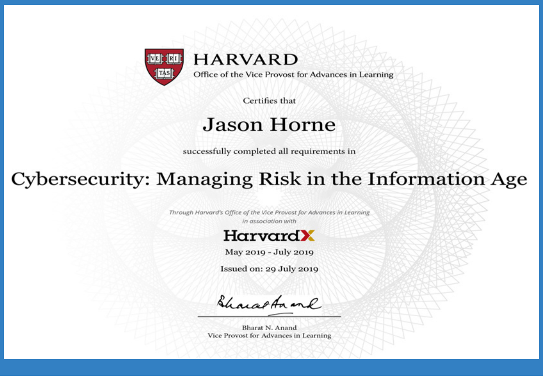
THE RISK MANAGMENT ASSOCIATION

Our CEO, Jason Horne, spoke this quarter at The Risk Management Association's meeting about cybersecurity and making it a part of company culture. He was joined by an agent with the Federal Bureau of Investigation Indianapolis Division who also spoke about cybersecurity and the emerging threats in the finance industry.

If you are a business owner or CEO, and want to make cybersecurity knowledge and prevention a part of your company's culture, join us next month for our free Before the Breach seminar.

HARVARD CERTIFIED

Congratulations are in order for our CEO, Jason Horne, for completing his Harvard course in Cybersecurity: Managing Risk in the Information Age. As CEO, he leads by example that it is important to always continue learning and educating yourself.



HARVARD
Office of the Vice Provost for Advances in Learning

Certifies that

Jason Horne

successfully completed all requirements in

Cybersecurity: Managing Risk in the Information Age

Through Harvard's Office of the Vice Provost for Advances in Learning
in association with

HarvardX
May 2019 - July 2019

Issued on: 29 July 2019

Bharat Anand

Bharat N. Anand
Vice Provost for Advances in Learning

preferred IT group

CONTACT US

Fort Wayne	Warsaw
260.440.7377	**574.306.4288**
Columbia City	Indianapolis
260.213.4266	**317.426.8180**

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.