Talk Nerdy To Me

September 2021

Is Your Business Protected With Cyber Liability Insurance?

Many small businesses use computers to send, receive, or store electronic data. Important data may be contained in sales projections, tax records, contingency plans, and other company documents. If such information is lost, damaged, or stolen due to a security breach, it may be difficult and costly to restore.

A data breach can also trigger third-party claims or lawsuits if it involves personally identifiable information such as social security numbers, health records, and credit card numbers. Businesses can protect themselves against the costs associated with data breaches by purchasing a cyber liability policy.

What Is Cyber Liability Insurance?

Cyber liability insurance covers financial losses that result from data breaches and other cyber events. Many policies include both first-party and third-party coverages. First-party coverages pay out-of-pocket expenses that a firm directly incurs as a result of a breach. Third-party coverages apply to damages or settlements a business is obligated to pay as a result of claims or suits for injuries that result from the company's actions or failure to act. For instance, a client sues his therapist for negligence after a hacker breaches the therapist's computer system, steals the client's treatment records, and releases them online.

Who Needs Cyber Liability Insurance?

Businesses that create, store and manage electronic data online, such as customer contacts, customer sales, PII and credit card numbers, can benefit from cyber insurance. In addition, e-commerce businesses can benefit from cyber insurance, since downtime related to cyber incidents can cause a loss in sales and customers. Similarly, any business that stores customer information on a website can benefit from the liability coverage that cyber insurance policies provide.

What Is Covered And Not Covered By Cyber Insurance?

Depending on the price and type of policy, the customer can expect to be covered for extra expenditures resulting from the physical destruction or theft of information technology (IT) assets. Such expenditures typically include costs associated with meeting extortion demands from a ransomware attack; notifying customers when a security breach has occurred; paying legal fees levied as a result of privacy violations; hiring computer forensics experts to recover compromised data; restoring identities of customers whose PII was compromised; recovering data that has been altered or stolen; and repairing or replacing damaged or compromised computer systems.

Many cybersecurity policies exclude preventable security issues caused by humans, such as poor configuration management or the careless mishandling of digital assets. Other issues excluded by cybersecurity policies include preexisting or prior breaches or cyber events, such as incidents that occurred before the policy was purchased; cyber events initiated and caused by employees or insiders; infrastructure failures not caused by a purposeful cyber attack; failure to correct a known vulnerability, such as a company that knows that a vulnerability exists, fails to address it and is then compromised from that vulnerability; and the cost to improve technology systems, including security hardening in systems or applications.

It is important to protect yourself and your business from potential threats. Contact us today to schedule a Security Risk Assessment.

https://www.thebalancesmb.com/ and https://searchsecurity.techtarget.com/

Nigerian Threat Actors Solicit Employees to Deploy Ransomware for Cut of Profits

Researchers have discovered a Nigerian threat actor trying to turn an organization's employees into insider threats by soliciting them to deploy ransomware for a cut of the ransom profits. Researchers at Abnormal Security identified and blocked a number of emails sent earlier this month to some its customers that offered people $1 million in bitcoin to install DemonWare ransomware. The would-be attackers said they have ties to the DemonWare ransomware group, also known as Black Kingdom or DEMON, they said.

"In this latest campaign, the sender tells the employee that if they're able to deploy ransomware on a company computer or Windows server, then they would be paid $1 million in bitcoin, or 40% of the presumed $2.5 million ransom". "The employee is told they can launch the ransomware physically or remotely."

DemonWare, a Nigeria-based ransomware group, has been around for a few years. The group was last seen alongside numerous other threat actors launching a barrage of attacks targeting Microsoft Exchange's ProxyLogon set of vulnerabilities, CVE-2021-27065, which were discovered in March.

Accomplice-Based Campaign

The campaign begins with an initial email soliciting help from an employee to install ransomware while dangling the offer of payment if the person follows through. It also gives the recipient—who attackers later said they found via LinkedIn—a way to contact the sender of the email. Researchers from Abnormal Security did just that to find out more about the threat actor and the campaign. They sent a message back indicating that they had viewed the email and asked what they needed to do to help, they reported.

"A half hour later, the actor responded and reiterated what was included in the initial email, followed by a question about whether we'd be able to access our fake company's Windows server," researchers wrote. "Of course, our fictitious persona would have access to the server, so we responded that we could and asked how the actor would send the ransomware to us."

Researchers continued to communicate over five days with the threat actors as if they were willing to be a part of the scam. "Because we were able to engage with him, we were better able to understand his motivations and tactics," they wrote in the report.

Changing the Game

Upon being contacted, the threat actor sent researchers two links for an executable file that could be downloaded on the file-sharing sites WeTransfer or Mega.nz "The file was named "Walletconnect (1).exe" and based on an analysis of the file, we were able to confirm that it was, in fact, ransomware," researchers noted.

The threat actor showed flexibility in how much ransom he was willing to receive from the company, researchers said. While the original amount was $2.5 million in bitcoin, the threat actor quickly lowered that sum to $250,000 and then to $120,000 when researchers said that the fake company for which they worked had an annual revenue of $50 million.

"Throughout the conversation, the actor repeatedly tried to alleviate any hesitations we may have had by ensuring us that we wouldn't get caught, since the ransomware would encrypt everything on the system," researchers said. "According to the actor, this would include any CCTV (closed-circuit television) files that may be stored on the server."

Through initial findings from research done before they opened the chain of communication, they said that the actor with whom they communicated was likely Nigerian, "based on information found on a Naira (Nigerian currency) trading website and a Russian social media platform website," they said.

Social Engineering as Cybercrime Strategy

Overall, the experiment provided new insight and context regarding how West African threat actors—who are primarily located in Nigeria—"have perfected the use of social engineering in cybercrime activity," researchers said. Indeed, there long has been "a blurry line" between cyber-crime and social engineering, observed one security professional. "This is an example of how the two are intertwined," said Tim Erlin, vice president of strategy at Tripwire, of the campaign.

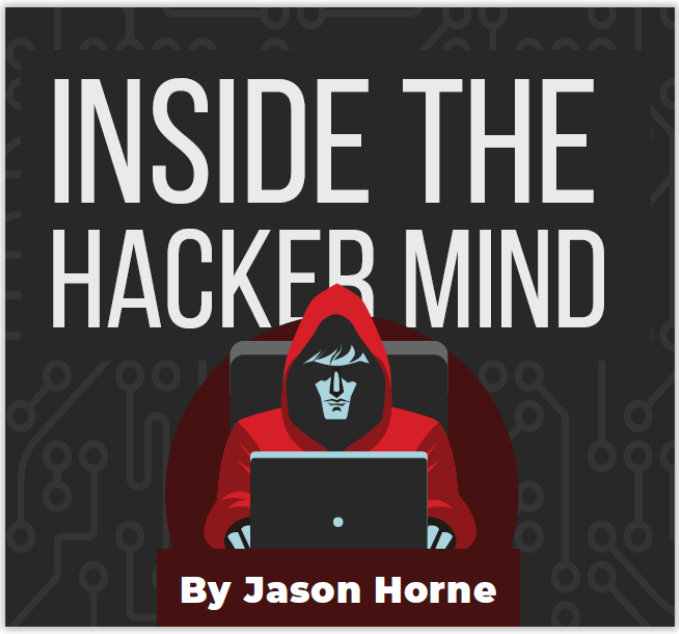
"As people become better at recognizing and avoiding phishing, it should be no surprise to see attackers adopt new tactics to accomplish their goals," he said in an email to Threatpost.

The campaign also sheds light on how attackers leverage the idea of a disgruntled insider to try to get them to do their dirty work for them—a concept that also isn't new, but can provide key insight into yet another way ransomware can find its way onto an organization's network, noted another security professional.

"It is always important that ransomware victims try their best to track down how the ransomware got into their environment," Roger Grimes, data-driven-defense analyst at KnowBe4. "It is an important step. If you do not figure out how hackers, malware and ransomware are getting in, you are not going to stop them or their repeated attempts."

https://threatpost.com/

Our CEO Is A Published Author



Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

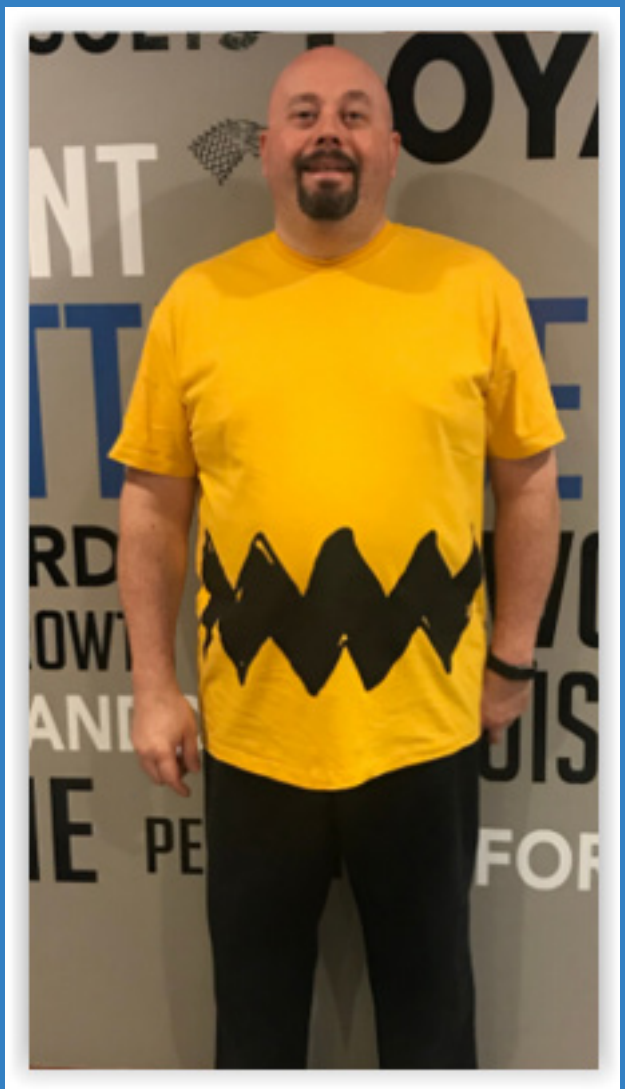
In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*

Happy Birthday Christopher!

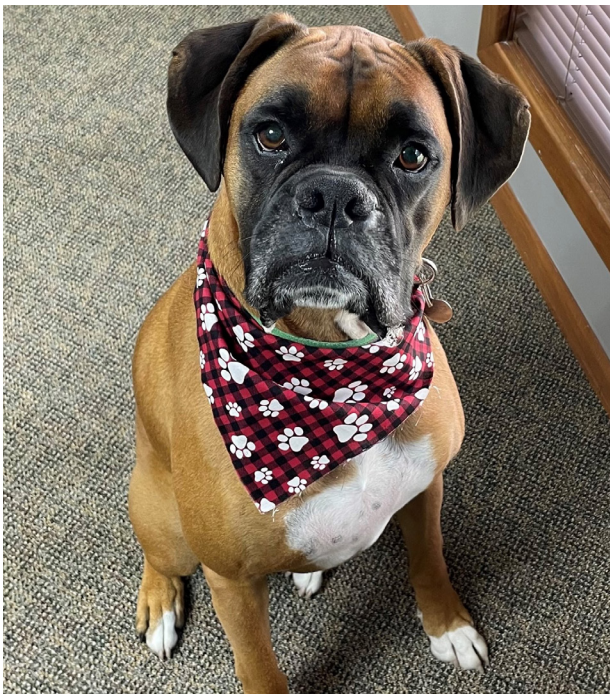
Thank you for everything you do!

Enjoy your birthday month!



Advantages To A Dog Friendly Workplace

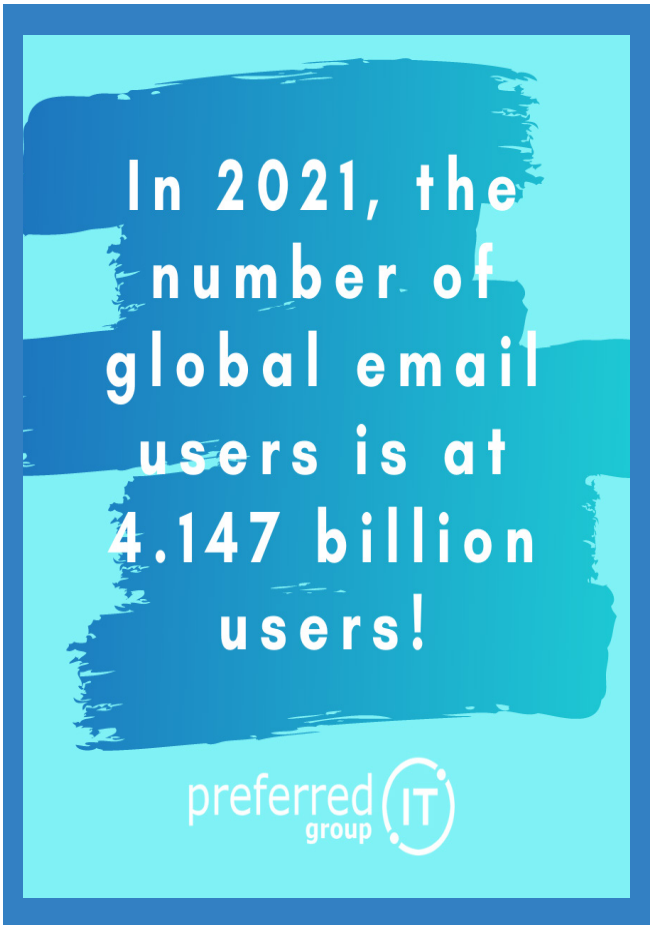
1. Office dogs help reduce employee stress.
2. Dogs boost office morale.
3. Dog-friendly workplaces promote productivity.
4. Office pups help improve communication.
5. Dogs encourage a healthier lifestyle in the office.
6. Dog-friendly office improve employee retention.
7. Dog-friendly workplaces appear more attractive to prospective employees.
8. Office dogs get socialized, rather than being left home alone.



We sure do love our office pup Sully!

https://www.lifelearn.com/

FUN FACT!



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.