IMAGEQUEST℠ YOUR MONTHLY IQ

December 2018
IQ Newsletter 01

> ***Every carrier has what it calls a 'cyber policy,' but none of them cover the same things. You can have a $50,000 'cyber' policy that covers a network penetration situation but not a phishing loss.***
>
> *– Joe Davis, Director of Cyber Liability for Houchens Insurance Group*

HIG Houchens Insurance Group™
Nobody Works Harder.™
https://www.higusa.com

Milton Bartley

Jay Mallory

IMAGEQUEST℠

Your Managed IT, Cybersecurity & IT Compliance Experts

CYBERINSURANCE: ARE YOU COVERED?

Maybe - or maybe not

Here's a nightmare for every business owner, large and small: Criminals penetrate your computer network and steal your money or your data.

But you've got insurance for that, right? Unfortunately, maybe not, said Joe Davis, Esq., Director of Cyber Liability for Houchens Insurance Group.

While the past year saw significant improvements in cyber policies, new companies have entered the market with offerings labeled "cyber insurance" but offering limited coverage.

"Every carrier has what it calls a 'cyber policy,' but none of them cover the same things," Davis said. "You can have a $50,000 'cyber' policy that covers a network penetration situation but not a phishing loss. Or you can have a $1 million 'cyber' policy that not only covers a breach but also covers business income, contingent business income, credit monitoring for your clients in case of a breach, things like that."

One liability insurance buyers may overlook is attorney's fees, Davis said.

"In most cases where attackers get to your data, you're going to need an attorney to navigate through state and federal privacy laws," Davis said. "And you will be exposed to class action lawsuits that you will have to defend as well. You have to have an attorney at the start of most breaches that actually got to any information."

Ongoing risk means premium rates will continue to increase through 2019 and beyond, Davis said. That's because ongoing cyber attacks mean a bad outcome is more likely to happen.

"This is the only risk, from an insurance standpoint, where there is a legitimate

continued on P.02

MEET OUR TEAM: STEPHEN BRATCHER

STEPHEN BRATCHER is a Senior Systems Administrator for ImageQuest. His duties include setting up and imaging systems for new clients or replacing systems for existing clients. He also provides Tier 2 support to our customers on more complex issues.

Stephen majored in computer science at Tennessee State, focusing on programming. But he had jobs in IT Support and hardware, including an internship with the City of Memphis in desktop support. He found he preferred helping people solve problems to programming.

Stephen finished his computer science degree (including the programming requirements), then earned an MBA while working his first tech support job at Gaylord Entertainment. He accumulated considerable experience in support and systems administration elsewhere before joining us in 2016.

Stephen said he enjoys working at ImageQuest because he prefers an environment where everyone collaborates.

"I'm not ashamed to say I don't know, how do you do this? That's the only way you're going to learn," he said. "And I'm willing, if someone has an issue, to say, hey, have you got time for me to show you how to do this?"

The collaboration also means "the person that answers your call usually can resolve your issue," he said. "It's not like a larger organization, where the first person you talk to just takes your information and refers your ticket up the chain."

The ImageQuest team is fun to work with, and the challenges varied. Stephen also likes that "everyone is constantly trying to make sure our customers are running efficiently. We resolve issues a lot faster based on how closely we work together," he said.

You can view a video of Stephen ***https://www.imagequest.com/Meet-Stephen/.***

continued from P.01

bad actor every day trying to break into your system," Davis said. "You have fire coverage; you have accident coverage; you have all these other coverages that are in there and could happen – if there's an accident.

"But nobody's out there actively trying to run into your car; nobody's out there actively trying to burn your house down."

Davis spoke with ImageQuest about what cyber insurance trends materialized in 2018.

IQ: What trends have you seen in cyber claims?

Joe: Social Engineering is still the number one claim, followed by Ransomware. Social Engineering is the use of "spearphishing" emails. But I also see an uptick in Business Income losses and Contingent Business Income losses. (Contingent Business Income losses include when a supplier shuts down – say, from a breach - and you cannot quickly or easily replace their offering in your supply chain.)

IQ: Is there a ballpark loss figure from these claims?

Joe: It's hard to ballpark these losses because circumstances are different on every claim. I would expect a payout for a cyber incident to top $110,000 for most small businesses.

IQ: What are some examples of losses companies experienced due to breaches and attacks in 2018? (Examples are from Davis.)

- A law firm manager accepted a position with a competitor. The first firm immediately terminated the manager. An investigation of the manager's computer and email revealed the former employee stole hundreds of pages of proprietary materials. Costs to resolve the theft included computer forensics and attorney fees.
- The accounting office for a Large Electrical Contractor received a phishing email requesting payment on a fraudulent $20,000 invoice. The accounting office "paid" via wire transfer – and the money disappeared. Additional costs, in that case, included attorney fees and computer forensics to make sure no malware had been installed on the contractor's system.
- A ransomware attack disabled approximately 50 workstations for a Plumbing Supply Company, halting business transactions and bringing the company to a near standstill. The attack required the company to pay for digital forensics, incident response services, public relations, and attorney fees.
- An employee of a Public College had a laptop stolen from their vehicle. The college had to retain legal counsel and a forensics team to determine the scope of the breach. Also, the college had to notify students and parents, and increase marketing costs to smooth public perception and rebuild trust in the school.

IQ: What can business owners do today to their organizations from a cyber breach?

Joe: *First, get a risk assessment.* That's key to determining what information you have and what security you have in place to protect it. I recommend you use an independent – and experienced - third-party, such as ImageQuest, to handle this.

Second, train your employees on best security practices. The best security in the world cannot defend against an employee sending a wire transfer or clicking on a fraudulent email link. Proper training is the only way to protect your business.

Third, have a breach – or incident – response plan in place and back up your data regularly. Again, if you are unable to complete this in-house, or worry that your plan is incomplete, hire an experienced third-party IT provider, such as ImageQuest, to develop or review your plans to reduce the chance of an oversight.

Fourth, have the correct cyber insurance policy in place! I run into businesses every day that think they have cyber coverage. Once I review their coverage, nine times out of 10, they are not covered correctly.

HOW TO AVOID COMPLIANCE FATIGUE

Last month we discussed "Breach Fatigue," a malaise which leads one to ignore news about data breaches instead of taking action to update passwords, etc.

"Compliance Fatigue" is a related malady, in which those tasked with meeting regulatory standards and passing regulatory audits grow weary of all the hoops through which they must jump.

"Indeed the number of compliance frameworks … amount to an alphabet soup that could make an IT manager's eyes glaze over before even starting to look at the fine print," CSO Magazine wrote in 2015.

We encounter many regulated customers who believe they can manage IT Compliance internally – only to have the effort bog down.

Internal projects to handle risk assessment, response plan development, and documentation writing projects get shelved when organizations get busy with pressing daily business needs. The costs to achieve compliance balloon and frustration is high.

A third-party solution can be a better investment. The compliance experience an outside provider brings to your situation means a clear-eyed look at all your risks, even the sacred cows, and knowledge that can get your organization audit-ready for regulators – and customers.

Additionally, a third-party vendor may provide cost-saving solutions that help you achieve both IT compliance and security goals. IT Compliance and IT Security are not the same things, but they can achieve similar goals – which is to improve your security posture with your data.

Increasingly, an organization that meets compliance standards and maintains a best-in-class security posture enjoys competitive advantages, as the world increasingly demands robust data protection and privacy from vendors.

If you are struggling to meet your regulatory IT framework, give us a call. We have solutions and experience that will help!

IMPROVE YOUR TECH IQ

Worried about ransomware? You should review the preventative measures offered by a site called NoMoreRansom.org.

Developed by the National High Tech Crime Unit of The Netherlands police, Europol's European Cybercrime Centre and McAfee, the website's goal is to help victims of ransomware retrieve their encrypted data without having to pay criminals.

One section labeled "Crypto Sheriff," allows victims to upload the ransomware note, the email, website URL, onion and/or bitcoin address or actual files on a system, to get the malware identified and possibly gain a key to unencrypt the files.

The decryption tools have been supplied by companies such as Trend Micro, Intel Security, and Kaspersky Labs.

The site also offers prevention advice, ranging from the technical ("Disable smb v1") to the practical ("Trust no one. Literally.")

The address is ***https://www.nomoreransom.org/en***

NO MORE RANSOM!

MEET A CYBER CRIMINAL

Photo by Matthew Griffiths/
Wikimedia Commons

This being the holiday season, we thought we'd feature a cybercriminal who is now considered a hacker for the Good Guys (and gals.)

Kevin Mitnick rose to fame in the 1980s and '90s as the "World's Most Wanted Hacker." He was convicted in federal court in 1988 for stealing computer programs and breaking into corporate networks. After completing his one-year sentence (in solitary confinement, he has said), Mitnick was arrested in 1995 for "electronically" attacking "numerous corporate and communications in California, Colorado and North Carolina." The feds said he also damaged systems and stole proprietary information.

In 1999 he pled guilty to 14 counts of wire fraud and other charges and was sentenced to 46 months in prison plus three years probation.

Mitnick claimed he never profited financially from the stolen data. His admirers claimed his punishment was excessive compared to the monetary losses his victims suffered. Books and movies were produced about his life, but only added further to the controversy over his hacking and punishment.

Today Mitnick works for the KnowBe4 security company as its Chief Hacking Officer and is a published author of three computer security books. His focus is social engineering.

In an excerpt from one of his books, Mitnick refers to Robert Cialdini's six principles of influence that allow phishing and spearphishing, the two main social engineering tactics of hackers, to succeed. They include the power of doing/returning a favor, small commitments, time pressure and social proof (everyone else is doing it.)

Mitnick has also made appearances in the media as an information security expert and testified before the U.S. Senate.

WELCOME NEW CLIENT!

Trinity Benefit Advisors is a full-service employee benefits consulting and brokerage firm.

The privately held firm, founded in 2006, partnered in 2017 with Russ Blakely & Associates to form the largest independent benefits firm in eastern Tennessee.

The combined company works to give its clients best practices, current technology, and expertise to provide top service, tools, and guidance.

Trinity specifically works with companies of all sizes to develop benefits strategies and more to align with each customer's needs and long-term goals and objectives.

Its services include benefit plan modeling, risk financing & funding alternatives, health & wellness initiatives, employee education, strategic benefit planning, and HR technology tools.

The company strives to work closely with its customers' carriers and vendors, to help clients maximize cost savings and build a framework for sound business decisions.

Recently, Trinity Benefit Advisors sought guidance to ensure its technology and practices met IT Compliance regulations, particularly for HIPAA.

"We needed an expert who could ensure that not only were we compliant, but also ensure that we were following current best practices for IT Compliance," Trinity Communications Manager Katie Dotson said.

After some research, Trinity found ImageQuest, which came highly recommended from multiple sources, Dotson said.

ImageQuest's initial work to date has given the team at Trinity Benefits Advisors "greater confidence that we're able to stand behind our Best-in-Class service."

Trinity
Benefit Advisors

MEET TRINITY BENEFIT ADVISORS

About: Employee Benefits Consulting and Brokerage

Founded: 2006

Headquarters: Knoxville, Tenn.

Employees: 37

Websites: www.trinityben.com & www.rbabenefits.com

"We needed an expert who could ensure that not only were we compliant, but also ensure that we were following current best practices for IT Compliance," Trinity Communications Manager Katie Dotson said.

From Our Customers

"Thanks, Kim, your team is amazing."

"Fast response time. Fast resolution time."

"Damian and Eric(k) were very responsive and able to correct my issue quickly. Thanks, guys!"

"DeMarcus is wonderful. He is very polite and extremely patient. He is truly an asset for ImageQuest! He should get a raise."

"Mr. Adams is very professional and knowledgeable. I appreciate his assistance."

"Quick attention to our question, and prompt scheduling of a phone call to discuss with our stakeholders. Thank you!"

"Easy to work with – understood my lame explanations of the issues and easily figured out what has changed and fixed it!"

"Marvelous, Stephen, thank you!"

"Angela was very helpful in answering my questions in layman('s) terms."

"It was fast and friendly."

You can read more comments at imagequest.com/reviews. Thank YOU to our clients who shared their positive feedback about our help. We appreciate it! If you are not having this experience with your Technology Vendor, maybe you should give us a call!

DO YOU KNOW A COMPANY LOOKING FOR IT SUPPORT?

WHAT WOULD MAKE A GOOD REFERRAL?

A great referral for us is a company in any professional industry with at least 20 computers – or any organization with a regulatory compliance standard they must follow.

HOW DO I SUBMIT A LEAD?

You can submit your referral by emailing us at leads@imagequest.com, or by calling Milton Bartley or Jay Mallory at 888.979.2679. You can get more details at ***https://www.imagequest.com/referral-program/***