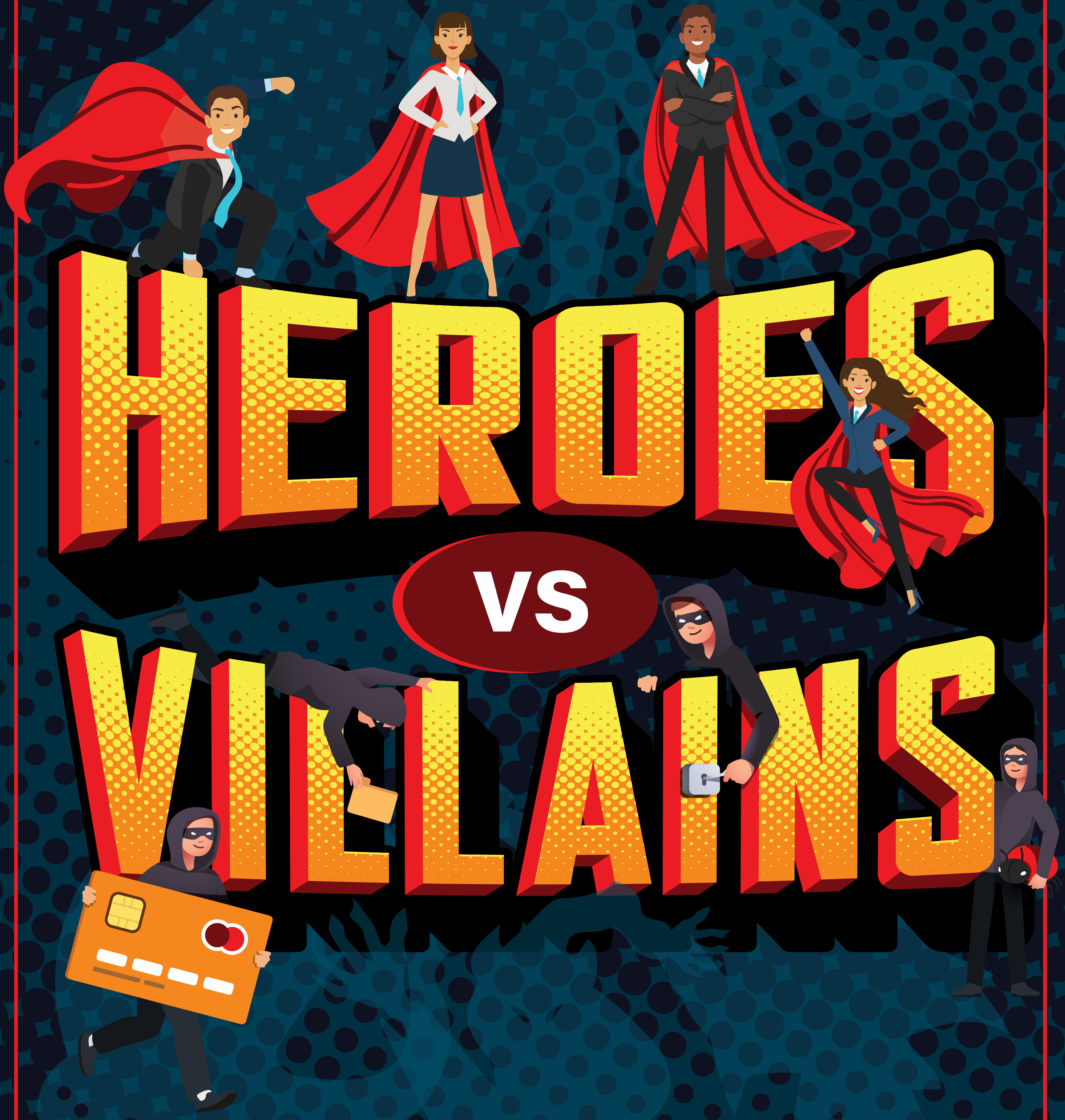
onestep
Secure IT Services



HEROES VS VILLAINS

The Latest Byte - Vol. 2 | 2022

One Step Secure IT’s quarterly newsletter, The Latest Byte, has arrived! And it’s Cybersecurity Awareness Month!

Cybersecurity Awareness Month is the perfect opportunity to ensure you are taking the necessary steps to protect your sensitive information from cyber criminals. The theme of The Latest Byte Newsletter this quarter is...

Heroes vs. Villains.

Our IT professionals are the heroes in our eyes—stopping the cyber-villains in their tracks!

Get ready for the showdown!

ONE STEP Q&A

YOUR FAVORITE...

HERO?

SPIDER-MAN
BATMAN XX
THE TICK
DOCTOR STRANGE
CAPTAIN AMERICA
STARLIGHT
SUPERMAN XXX
MR. INCREDIBLE
DEADPOOL
BLACK PANTHER
MY WIFE (FAVORITE ANSWER!)

VILLAIN?

JOKER XXXX
MAGNETO XX
VENOM
DARTH VADER
HOMELANDER
LEX LUTHER
TERMINATOR
BANE
DR. OCTOPUS
ULYSSES KLAUE

POWER?

SUPER STRENGTH
SUPER SPEED
HEALING POWERS
MAGIC POWERS
INVISIBILITY XXX
LEVITATION
FLIGHT
X-RAY VISION
TELEKINESIS
ABILITY-TO-ACQUIRE-ANY-POWER

See Yourself in Cyber

OCT

2022 CYBERSECURITY AWARENESS MONTH

As we enter the autumn season, we can look forward to cooler weather, pumpkin patches, and Cybersecurity Awareness Month!

October is a month to remind ourselves of the importance of the cybersecurity best practices that help us protect our sensitive information.

One Step Secure IT has signed on as a **Cybersecurity Awareness Month Champion.** The Cybersecurity Awareness Month Champions Program is a collaborative effort among businesses, government agencies, colleges and universities, associations, nonprofit organizations, and individuals committed to the 2022 Cybersecurity Awareness Month theme of **"See Yourself In Cyber."**

This year's theme reminds us that cybersecurity is an individual responsibility, and everyone plays a part in keeping an organization cyber-safe.

> *"We have a mission to help protect 1 million people. Education is an important part of that," One Step Secure IT Founder and CEO Scott Kreisberg said. "Cybersecurity begins with good personal cybersecurity hygiene and is something everyone—and I mean everyone—can constantly improve on."*

It seems that every year, technology is becoming a larger part of our lives—from smartphones to online school to remote work. The evolution of technology is moving fast, and cyber criminals are working hard to find ways to compromise technology and disrupt personal and business life.

Cybersecurity Awareness Month aims to highlight some of the emerging challenges that exist in cybersecurity today and provide straightforward, actionable guidance that anyone can follow to create a safe and secure digital world for themselves and their loved ones.

In 2022, Cybersecurity Awareness Month's primary focal areas revolve around four key fundamental cybersecurity best practices:

1. Recognizing and reporting that phishing is still one of the primary threat actions cyber criminals use today.
2. Understanding the benefits of using a password manager and dispelling existing myths around password manager security and ease of use.
3. Enabling multi-factor authentication on personal devices and business networks.
4. Installing updates regularly and turning on automated updates.

If you have any questions about cybersecurity or need further guidance, we are here to help. Feel free to schedule an appointment below to chat with one of our cybersecurity experts at **www.OneStepSecureIT.com/Contact** or call us at **(623) 227-1997.**

Cybersecurity education isn't limited to the month of October. Stay tuned as we release more resources on social media (@OneStepSecureIT) and our blog (www.OneStepSecureIT/Blog) in the upcoming weeks that you can use year-round!

Stay Safe & Cyber-Aware

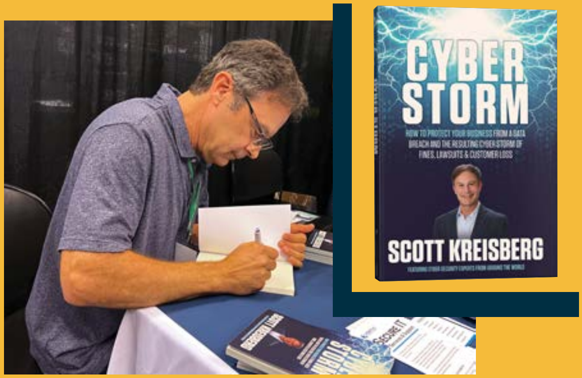
— this month and every month.

WHAT WE'VE BEEN UP TO!

Our One Step Secure IT team has been busy! We've been able to get out of the office, meet other IT and cybersecurity professionals, and share our knowledge with those looking to strengthen their security strategies.

ARIZONA TECHNOLOGY SUMMIT

Our team attended the 13th Annual Arizona Technology Summit, where One Step Secure IT Founder and CEO, **Scott Kreisberg** signed dozens of copies of his Amazon best-selling book, *Cyber Storm.*


CYBER STORM
HOW TO PROTECT YOUR BUSINESS FROM A DATA BREACH AND THE RESULTING CYBERSTORM OF FINES, LAWSUITS & CUSTOMER LOSS
SCOTT KREISBERG

"The Arizona Technology Summit was a great place to see what other IT professionals are up to. I enjoyed hearing how other cybersecurity professionals are adapting to the ever-changing threat landscape," **Tim Derrickson,** One Step's vCSO, said. "It's a must-go for anyone living in Phoenix who wants to learn about technologies being used to keep environments running smoothly and safely."

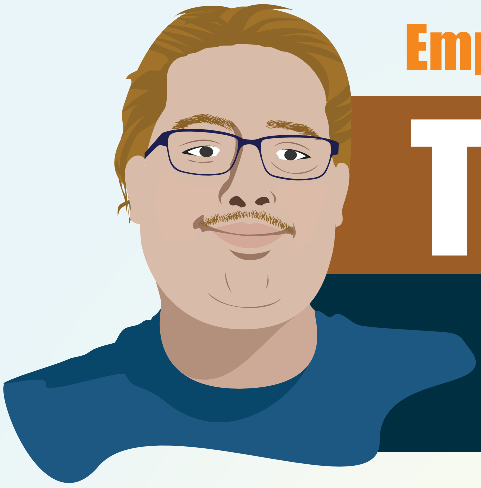
"The show's attendance and participation way exceeded my expectations. Clearly, cybersecurity is becoming a top-of-mind topic for all organizations now more than ever," **Kevin McAdam,** One Step's Chief Revenue Officer, said. "Our mission is to help protect 1 million people, and education is the primary barrier to that. That's why events like this are so important. They give us a chance to talk face to face and help bridge that gap."

SECURE IT ON THE GREEN

Over the past several years, the Doug Carr Memorial Fall Classic Golf Tournament has grown into the largest insurance industry charity golf tournament in the West. Since its inception in 2018, the event has generated over $275,000 in charitable contributions.

"The One Step Secure IT team had a great time playing golf and meeting other professionals...I'm glad we could make connections and support a worthwhile cause," said Josh Kreisberg, One Step Secure IT Technology Consultant.

The golf team (right to left): Josh Kreisberg (One Step), Chris Holub (CCV), Andrew Ward (One Step), and Luis Flores (Sunburst Pet Supplies)



Employee Spotlight

TRYSTAN HAYDEN

Trystan is **One Step Secure IT's Senior Network Administrator & Customer Consultant.** With 20 years of IT experience under his belt, he has graced the halls of One Step with his IT knowledge for the past 11 years. Let's learn more about this IT hero that keeps our clients cyber secured.

What do you enjoy about your role?

1) I am always learning something new.
2) I enjoy helping people solve problems and coming up with solutions for new and different problems.

When did you realize you enjoyed IT?

I was probably 13 or 14 when my parents bought our first computer. It came with a VHS tape on how to install the video card and the sound card. I found that very interesting and decided working with technology was something that would probably come easy and continue to be interesting in the future.

Misconceptions of Cybersecurity?

That you can set up security and then forget about it. You constantly need to be evolving and learning about new threats so you can protect yourself against them.

What do you enjoy outside of work?

Being outdoors, camping, hiking…I've walked an average of 5 miles every day this year. I also enjoy video games and concerts, mostly Punk.

Earliest memory using technology?

My earliest memory of the Internet involves being kicked off-line every time the phone rang. I absolutely do not miss that. At the age of 16 with my first paycheck, I bought high-speed Internet. Shortly after that, I had all my friends over because no one else had anything but dial-up in my neighborhood.

Recent IT challenge you had to troubleshoot?

The one that comes to mind is a Network-attached Storage (NAS) that had been infected with ransomware. Through shell commands on the NAS and a backup done a few days prior, I was able to restore everything on the NAS within a couple of hours.

How do you stay cyber-safe in your daily life?

For me, the most important thing to protect in my daily life is my personal information. Unlike at work, almost everything that I need to protect is on a smartphone as opposed to a computer. So when using my smartphone, I use Orbot as a proxy/VPN for internet security. I also use DuckDuckGo’s Android web browser and search engine because they do not store personal information or sell it.

Theories on the future of IT?

More and more breaches will occur due to IoT devices. Before buying your next device ask yourself, “Do I really need a SMART oven, belt, deodorant, toilet, or sandals?”

And before you ask, yes, those are all real things.

The Business of Cyber Crime

Paint a picture in your mind of a typical hacker...

I'm guessing you've got an image of a young male in a hoodie sitting in a darkened room, typing away at a computer keyboard. While that may be the case, it's more likely a group of individuals who run their cyber criminal operations as a business—aka organized crime. Think offices with cubicles and work from home (WFH) employees. Anytime there's a lot of money to be made, it's a given that organized crime will step in.

Many of you may remember The Godfather, written by Mario Puzo, originally published in 1969. This crime novel tells the story of one of five New York mafia families, the Corleone's. The Corleone family is fighting for survival after a failed assassination attempt on the head of the family, Don Vito Corleone (the Godfather), by one of the other families vying for control.

In a famous scene, his two sons, Sonny and Michael, and his top lieutenants gather to discuss what action to take in the wake of this egregious infraction. Michael, the younger son, suggests meeting with the head of the offending family, and his corrupt police Captain to broker a truce. However, he intends to shoot them both. When the elder son, Sonny, protests, Michael calmly says, "It's not personal Sonny, it's strictly business."

Cyber crime—it's strictly business. Big business. Cyber crime "companies" run just like other businesses. They post job openings on the Dark Web and interview new employees. They sell software like malicious code or malware to other hackers—just like a legitimate software company. They offer ransomware as a service "kits"—whereby they get a "cut" of the profits for all successful attacks—just like a franchise.

The question is, who are these organized crime actors?

In a May 2021 post published by the U.S. Department of Defense, the U.S. Deputy Assistant Director for Cyber Policy, Mieke Eoyang is quoted as telling the U.S. House Armed Services Committee during a hearing on cyber crime,

> "The line between nation-state and criminal actors is increasingly blurry as nation-states turn to criminal proxies as a tool of state power, then turn a blind eye to the cyber crime perpetrated by the same malicious actors," she said. "We have also seen some states allow their government hackers to moonlight as cyber criminals."

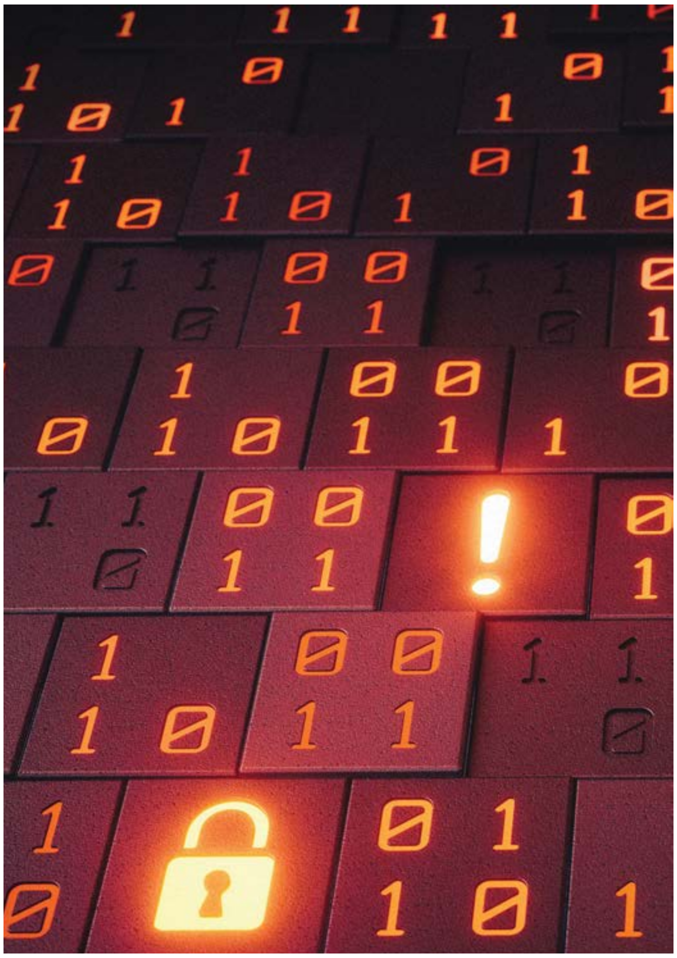
Nation-states are not only condoning but also actively promoting cyber crime. How twisted is that?! Cyber crime doesn't hit the books as a source of income—but the "take" can be significant. Who would some of the nation-states be?

North Korea, Iran, Venezuela, and other cash-strapped nations come readily to mind.
Oh, and don't forget Russia.

On top of that, there are many "companies" who have no nation-state affiliation but whose annual income rivals that of many major (legitimate) corporations.

Here are a few of the more prominent ones: **Dark Side, REvil, FIN7, Cobalt, Clop, Lazarus, MageCart, and GozNym Gang,** to name a few. They're making billions by attacking businesses and individuals.

I don't know about you, but even though I know a lot about computers, I know that when it comes to cybersecurity, I'm no match against organized crime perpetrated by nation-states and well-oiled criminal syndicates. Neither is your "IT guy" or most IT teams, for that matter. So, if you're trusting your personal security or the security of your business to anything but a professionally trained security team—you're a statistic waiting to happen.



CASE STUDY

“We’re tightening things up”

Berge Auto Group Protects Cyber Assets with the Help of One Step Secure IT

Who is Berge Auto Group?

It was 1972, and Brent Berge opened the doors of his first car dealership, Berge Mazda. Their business kept growing over the years, and he opened several more locations in the Phoenix metro area. Berge Auto Group operates seven dealership locations with over 100 computers or servers at each location—plenty of devices for cyber criminals to target, and Berge Auto Group’s Chief Financial Officer, Duane Wilkes, knows it.

> *“That’s one of the reasons I am here—to protect the company’s assets—that includes cyber assets. Data is one of the major assets of the company. It might not be on the balance sheet, but if you don't have that data—you can’t put anything on the balance sheet.”*
>
> DUANE WILKES

Proactive, not reactive

Wilkes has worked with Berge Auto Group for over 20 years. As technology in the industry has developed and changed, he saw the need to implement a cybersecurity strategy. To determine if Berge Auto Group’s cybersecurity strategy was vulnerable, Wilkes decided it would be beneficial to run a third-party scan. He knew their systems were not in ship-shape, but others in the company found the results shocking.

A third-party looking in

One Step Secure IT runs two types of scans for Berge Auto Group to make sure their cybersecurity strategy is keeping the company protected.

- A **Network/Security Scan** that checks for vulnerabilities and gaps within Berge Auto Group’s systems that cyber criminals can exploit.
- A **Payment Card Industry (PCI) Compliance Scan** is part of an overall PCI Compliance Assessment. This scan helps Berge Auto Group meet the PCI compliance requirements.

One Step then creates a full report at the conclusion of the scans, including scan results, areas of concerns, and plan of action to address the security gaps. One Step cyber-security and IT experts over-see the projects to address and fix all issues uncovered by the scans. Communication is key, and One Step creates a timeline for strengthening Berge Auto Group's cybersecurity strategy.

"We felt it was very important to not only understand our systems from the view of a third-party looking in but also to be able to create a roadmap to address what we need to work on." DUANE WILKES

An eye on security

Cyber criminals could be in your system silently watching and gathering information for a cyber attack on a business that doesn't monitor its systems or run regular scans.

287 days **is the average time it takes a business to detect and contain a cyber attack.**

IBM's Cost of Data Breach Report

Wilkes has witnessed other dealerships get hit by ransomware and face other cybersecurity issues. He knew he needed to protect Berge Auto Group's data, and One Step Secure IT could help him.

"I wouldn't want to negotiate with ransom-ware people, but if I was in that situation, One Step could help me. They live in the data world day-to-day. My focus is totally different, but I've got to keep at least one eye on our security." DUANE WILKES

The transformation

"We're tightening things up... I can tell we've made a lot of improvement." DUANE WILKES

As a result of working with One Step, Wilkes better understands Berge Auto Group's systems. As One Step monitors their systems, they notice if there are, for example, 2,000 failed login attempts on one computer or if someone is poking around their system at 3 a.m. Those red flags don't go unnoticed.

When working with Berge Auto Group, One Step uncovered the following:

End-of-life Windows 7 Computers
This was a major problem because their computers weren't being patched or protected from new vulnerabilities.

Poor Password Management
Employees were not required to change their passwords every 90 days, which increased their exposure.

The average business owner may not recognize these things as issues, but they pose significant security risks.

The FTC is cracking down

The auto industry is heavily regulated to protect consumers. Business owners must take extra steps to ensure they comply with the law. Among the many standards they must meet and adhere to is the Gramm-Leach-Bliley Act.

Under the GLBA, any company that offers credit, financial advice, financing, or leasing must have a comprehensive security program in place to protect customer information. Dealers must act immediately to meet GLBA requirements; otherwise, they will face stiff penalties of up to $43,792 per violation.

Customers expect auto dealerships to safe-guard their information, and if they don't trust the dealership to do so, they will take their business elsewhere.

One Step has been able to help Berge Auto Group as an independent third-party IT and cybersecurity expert, uncovering vulnerabilities and helping them prioritize projects to fix major security risks.

"One Step is a well-oiled company that knows what they're doing...If we ever have a problem, we know we can count on them to help work through it."

DUANE WILKES

WORD SEARCH
Cybersecurity Best Practices

D	M	T	C	G	M	T	S	N	W	U	P	P	I	K	D	K	E	2	V	P	W	D	I
A	F	N	A	G	O	Y	F	L	E	R	R	F	I	U	L	P	O	C	A	S	V	I	X
R	B	I	V	K	I	X	C	T	I	S	R	U	L	R	R	C	K	S	I	U	A	G	N
K	X	N	Y	F	G	M	A	E	P	V	O	D	O	E	E	T	S	Y	W	L	E	S	D
W	C	C	C	I	Y	X	C	C	T	A	L	N	X	2	K	W	E	X	Y	D	X	M	G
E	M	I	I	N	C	S	E	X	O	N	E	R	E	O	O	G	W	Y	W	W	D	O	B
B	N	D	L	Y	T	I	U	N	I	T	N	O	C	R	A	B	M	F	A	D	W	M	G
M	M	E	O	C	C	B	M	L	U	U	C	C	D	D	L	E	G	A	R	E	V	O	C
O	T	N	P	B	2	L	W	B	T	Y	T	V	G	F	2	U	L	X	F	V	S	M	E
N	F	T	Y	S	W	P	C	P	K	Y	A	E	C	L	O	K	R	X	R	K	R	M	S
I	R	R	T	P	P	O	K	G	I	U	O	S	N	O	K	2	I	M	2	M	P	L	F
T	C	E	I	X	A	U	C	T	L	A	P	G	V	R	M	C	S	Y	N	L	P	O	V
O	P	S	R	K	W	R	K	T	2	R	O	P	Y	K	I	P	M	S	O	O	L	N	P
R	K	P	U	N	2	Y	A	C	K	O	K	W	F	T	C	2	L	Y	A	D	O	L	W
I	M	O	C	G	C	E	B	O	A	Y	C	B	E	A	Y	G	E	I	O	A	S	T	L
N	Y	N	E	W	R	P	A	T	F	B	A	X	X	W	2	E	F	I	A	N	R	U	V
G	A	S	S	Y	F	C	R	A	V	2	P	2	S	A	T	O	N	V	K	N	O	L	M
W	R	E	R	Y	D	W	U	T	K	E	O	M	V	R	T	T	C	P	L	E	C	X	S
B	I	P	E	C	Y	M	S	R	R	A	T	U	A	E	E	L	2	K	W	Y	Y	E	E
S	2	L	B	V	O	E	U	T	U	I	F	I	S	N	K	U	W	X	N	D	E	K	T
F	N	A	Y	U	T	R	S	X	U	S	N	O	F	E	K	X	D	N	A	2	L	P	A
M	M	N	C	N	2	N	U	L	V	I	F	R	X	S	Y	O	N	2	O	I	T	2	D
S	Y	D	E	V	Y	E	N	A	N	P	R	E	O	S	N	F	M	F	O	V	Y	P	P
D	W	P	N	O	U	G	G	G	M	A	F	A	O	M	C	P	R	A	C	U	K	R	U

IT Experts
Pen Test
Awareness
Backups
Compliance
Updates
Cybersecurity Policy

Darkweb Monitoring
Password Vault
Coverage
2FA
Incident Response Plan
Employee Training
Continuity

SCAN CODE FOR
ANSWER KEY

One Step Secure IT
22520 North 18th Drive
Phoenix, AZ 85027

CONNECT WITH US
@onestepsecureit

www.OneStepSecureIT.com
(623) 227-1997