



# The Latest Byte

**ROADMAP TO 2023**

**Vol. 1 | 2023**

# ROADMAP TO 2023

**Join us in welcoming the new year!** This fresh start gives us a chance to reflect on the past year and implement changes to make us stronger in the future.

Here at One Step Secure IT, we are going into 2023 with a clear perspective on what improvements are going to be made. It's wise to start a journey with a roadmap to make sure all key milestones are met.

Since helping businesses secure themselves with cybersecurity best practices is what we're best at, we hope this newsletter gives you insightful tips and useful advice from our resident cyber experts to help you improve your cybersecurity strategy in the new year.

For further guidance in creating your cybersecurity roadmap, One Step Secure IT is always here to offer direction.

**Happy New Year,  
friends.**

**Since our  
start in 1985,**



One Step has helped businesses nationwide ensure their technology delivers a competitive advantage so they can focus on business growth and increasing revenue.

We specialize in Cybersecurity, Managed/Co-Managed IT, Information Security, and Compliance Services.

We understand that as the customer journey continues to evolve so do the threats to your business. Our team works with you to develop an IT strategy, identify vulnerabilities, and close gaps to strengthen your IT environment.

One Step corporate headquarters is in Phoenix, AZ and we serve businesses nationwide. For more information about our services, visit [www.OneStepSecureIT.com](http://www.OneStepSecureIT.com)

Cybersecurity Experts Share Insight into

# How to Protect Yourself & Your Business in



# 2023

## What do you think is one of the biggest challenges businesses will face in 2023 regarding cybersecurity?

As the trend of working from home continues, businesses will face a more significant threat landscape. **Employees are already the number one vulnerability** in a secure office environment but when they are home it becomes **exponentially more difficult to secure**. Although there is no foolproof strategy, there are several of things that can be done to reduce the likelihood of an event, and we can help people with that.

**Scott Kreisberg**, *Founder and CEO*



An area to keep an eye on will be corporations continuing to **move more services into the cloud**. “Software as a Service” and “Security as a Service” is being used more and more. Threat actors will try to get into systems that will provide a **better platform for launching attacks against businesses**.

**The number one vulnerability in any environment remains the user**. Email phishing remains the most used attack against organizations and it will continue as long as threat actors can use it as a vector to get into organizations' infrastructure to add malicious software and ransomware.

**Tim Derrickson**, *Virtual Chief Security Officer (vCSO)*



From what I have seen the challenges for cybersecurity are twofold. The first obstacle will be getting a company to get the correct packages for the clients. **Some people think IT and Compliance are enough for security** but being compliant doesn't necessarily mean you are secure. Compliance is the positioning for a regulator or governing body. IT is what keeps your systems running. **While both have a portion of security, they are not security**.

The second is the fact that **most businesses need to be protected for the future**. They are protected for the now and the yesterday. **Each time the threat of cyber warfare is stopped, the bad actors make changes**. So not only do you need a company that can handle the threat and help remediate today, you also need a company that **continues to evaluate its tools and grow with the threats**. This will help you take a proactive role in your security instead of complacency.

**Roman Stanton**, *Virtual Chief Information Officer (vCIO)*

## What can businesses do to start 2023 off on the right foot regarding IT and cybersecurity?

At a minimum I can think of two things, and they are **1) make sure you have cyber liability insurance** and **2) conduct and remediate via regular threat assessment.**

By following the requirements to qualify for a cyber liability policy you are **better off than the majority of businesses** without a policy. Conducting a **third-party threat assessment each year** and fixing anything that shows up puts you **significantly in a safer position.**

**Scott Kreisberg**, *Founder and CEO*



One of the biggest challenges businesses are going to face is protecting identities. **Identity management is becoming one of the best ways to protect an environment.** Using least privilege and **Zero Trust** with application whitelisting and auditing will help to strengthen organizations and give visibility to blue teams of what is happening in environments being defended.

**Also, one of the strongest tools in our cybersecurity arsenal is an end user properly trained in general cybersecurity.** It is important that end users understand the different types of common attacks against the organization and the importance of alerting IT and IS to odd behavior of systems and applications.

**Tim Derrickson**, *Virtual Chief Security Officer (vCSO)*



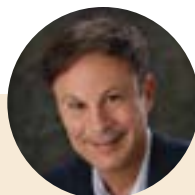
**In 2023, it will be imperative that companies take an active role in technology.** This means they need to **create a technology committee.** This can be a group or a couple that meet with the C-level to discuss the role technology plays in their business.

The person involved in the IT department then needs to **align the devices in their network to each other creating a baseline of technology.** When your devices are misaligned, it is easier for the **bad actors to get in and make lateral movements.** The ultimate goal for a bad actor is not to disrupt the business, but to gather as much detail and information as possible, **leading to financial gain for them and loss for you.**

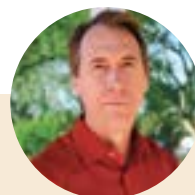
In 2023, we all need to take this seriously and work methodically to help **prevent loss of data, productivity, and money.**

**Roman Stanton**, *Virtual Chief Information Officer (vCIO)*

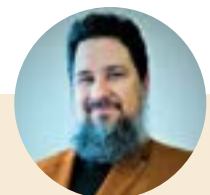
## Our Cybersecurity Experts



Scott Kreisberg



Tim Derrickson



Roman Stanton

All In, All the Time: Robyn Longmire, James Tullai, & Rosa Stocks



Culture Warrior!!!  
Jesse Looper

## End-of-the-Year 2022 CORE VALUE AWARD WINNERS

Our team honored those who exemplified One Step's core values.

The winners were nominated by their peers who admired each nominee for their positive contributions to the One Step team.



Imagine the Possibilities  
Joshua Kreisberg



Imagine the Possibilities  
Joshua Fisher



Imagine the Possibilities  
Kerrin Siegler



Humbly Exceptional: Michelle Major, Timothy Derrickson, & Andrew Gallagher



# Cheryl Blasnek

Spotlight on Secure IT's VP

**When did you first take an interest in technology?** I remember in the 80's learning to write Excel formulas so I could take the company I worked for to digital instead of paper. When I finished that project and saw the profound effect it had on our company in terms of streamlining, productivity, efficiency, etc., I was hooked on technology.

**Where did you go to school?** Hawaii! I graduated from BYU-Hawaii but also learned to become a pretty good beach bum in those 4 years!

**What's your role at One Step?** I am the Vice President of One Step Secure IT which is the IT/IS arm of the company. We work with businesses with 2 goals in mind: keep them as technologically secure as possible and help their employees be as productive as possible.

**How long have you worked at One Step?** I have worked at One Step since 2012. I started doing projects as an independent contractor before becoming a full-time employee.

**What do you enjoy about your work?** I enjoy the fact that One Step is always transitioning...a totally smart thing to do to adjust to the changing world around us. This means as an employee, there's always something new to do, to learn.

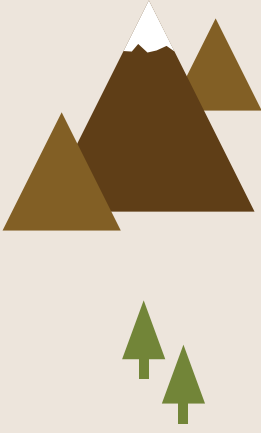
**What do you like to do outside of the IT world?** I love Yellowstone. It has a different beauty in every season and I have had the opportunity to be up-close and personal with the animals. I have been nose-to-nose with a bison, surrounded by elk, inspected by wolves! Very exciting!

## CHERYL'S ROADMAP TO IT & CYBERSECURITY IN 2023 STARTS HERE...

### What is a cybersecurity threat you expect to rise in 2023?

The biggest threat I often see is companies who look at cybersecurity as an expense instead of as an investment. Laws, regulatory agencies and insurance organizations are pushing businesses to make the investment in their environment because getting hacked is so expensive and disruptive to a company's ability to do business. More and more, business owners are responding to the threats and the need for security consultation and guidance.

# 2023



**If you could magically have all businesses in the U.S. adopt this one cybersecurity practice in 2023, what would it be and why?** Hire One Step to address their IT needs through our MSP services and hire One Step to address their cybersecurity needs through our vCSO services. We work very hard to provide technology solutions that are relevant to a company and their business goals.



## What is an aspect of cybersecurity you have noticed many businesses overlook?

Layers of security.

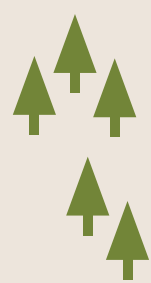
Security is not a “one and done” kind of affair. For instance, one 30-minute training session on email security is not enough. Employees need constant reminders, simulated phishing emails and feedback. Apply that same philosophy to passwords, backups, and checking what goes out of a network as well as what comes in, etc. It is a big ask that requires professionals to craft a program that works for each individual company.



Implement email education for all employees. The majority of breaches come because of employees clicking on something they shouldn't. Constant education helps raise awareness and keeps email security top-of-mind for employees.



**3** Prioritize remote employee security. Since the pandemic, businesses have become aware that they do not need all employees working in an office environment. However, an employee working from home introduces different security vulnerabilities that should be addressed.



**1** Schedule a security consultation with a vCSO who will help a company with the necessary details and roadmaps to make cybersecurity attainable.

**If you had to create a “roadmap” for a business that wants to make sure its data is secure, what are three steps you would recommend they take?**





## Case Study

# Christ's Church of the Valley found 'Peace of Mind' with Co-Managed IT

**Christ's Church of the Valley (CCV)** is one of the largest churches in the nation with a weekly attendance of over 35,000 across fourteen campuses.

Over the past decade, CCV has grown rapidly across the Phoenix Metro Area. That growth leads to more computers, servers, and, unfortunately, more vulnerabilities to cyber attacks.

As CCV's IT Director for 11 years, Chris Holub has played an important role in the company's growth. CCV operates with a small IT team that takes care of day-to-day technology issues leaving little time for server maintenance and technology upkeep.

After CCV suffered a ransomware attack about five years ago, cybersecurity became a priority, but CCV's team wasn't large enough to cover all the bases.

Ransomware is a type of malware growing in popularity with cyber criminals. The ransomware encrypts data until the demanded ransom is paid. If you're lucky, cyber criminals give you the encryption key after they are paid. Some people aren't so fortunate and lose everything anyway.

“

We lovingly refer to it as Hacks-giving because it happened around Thanksgiving,” Holub said. “I got woken up by my phone constantly buzzing—it was my systems administrator frantically texting everybody because he couldn't get into anything and all of our servers had some sort of message demanding payment... it was bad.”

Once the cyber criminals gained access to one remote desktop computer, they had access to all of them. With the CCV server under the control of the hackers, church leaders found themselves



worried about sensitive data loss, extended downtime, and wondering if they would ever recover critical information.

After weighing their limited options, CCV decided to pay the ransom in Bitcoin and considered themselves lucky after receiving the encryption keys.

“They could’ve just taken the money and ran,” Holub said.

Even with the encryption keys, gaining access to their data again was difficult. They had to run the 12 encryption keys on over 30 different servers.

“It was extremely inconvenient and embarrassing at the same time—tough conversations with my boss and other people. It’s just one of those things—after you’ve learned your lesson, it’s always in the forefront of your mind,” Holub said.



## CCV Today

Pivoting to co-managed IT allowed their current IT staff to focus on resolving day-to-day tech issues quickly and providing their staff with better support.


After talking with One Step, Holub saw the advantages of having One Step’s IT experts manage and monitor their systems 24/7. They no longer have to worry about issues arising while someone on their internal team is out sick or on vacation.

“There’s just not going to be gaps,” Holub said.

The ransomware attack demonstrated the importance of having a strong cybersecurity strategy in place. Holub wanted to make sure his IT partner had a focus and understanding of cybersecurity—One Step Secure IT was the right fit.

“IT is just so broad. So it’s great being able to work with people who have the upper-level expertise that you can count on,” he said.

One Step Secure IT’s cybersecurity and IT experts make sure all CCV systems are up-to-date, along with other services, including:

 **Network and Security Scanning**

 **24/7 Defense**

 **Employee Security and Awareness Education**

With One Step’s help, Christ’s Church of the Valley has server maintenance and day-to-day tech issues taken care of while cybersecurity is at the forefront of all they do.

“

Hackers are always evolving in the ways they can get into your systems. You’ve gotta be just as resilient.”



# end of the year

## CELEBRATION

One Step team members met up at our Phoenix headquarters, welcoming remote employees who flew in from all over the country, to celebrate the end of a successful year!

Having everyone together in-person for the annual One Step Holiday Party is always fun. We played games, enjoyed dinner and dessert, and recognized several team members for their dedication to upholding One Step's core values.

One Step Secure IT Founder and CEO Scott Kreisberg reflected on the year by celebrating the year's successes.

The holiday party is always a great way to cap off a year of hard work.



# Let's Be Social & Follow One Step!

Staying on top of your cybersecurity is an ongoing process, and we are here to simplify it.

Stay in the loop and find us on LinkedIn, Facebook, or Twitter

**@OneStepSecureIT**

where we share the latest cybersecurity news, blogs, events, and real stories that you can relate to. Leave us a comment on one of our recent posts to say hello!

**See you there!**



## Cybersecurity Scorecard

Did you know **66% of businesses** were hit with ransomware last year?  
Don't wait until it's too late.



Get your free comprehensive scorecard to assess your cybersecurity hygiene and identify potential risks to your business.

Get the added value of a quick consultation with a security professional to help you understand your score and how you can improve your cybersecurity posture.

**Schedule Your Assessment Today!**

[www.OneStepSecureIT.com/cybersecurity-scorecard](http://www.OneStepSecureIT.com/cybersecurity-scorecard) or scan



**Don't lose money on your technology investments**

Every business has unique needs. Our Cybersecurity Scorecard Assessment helps you better understand which areas in your IT environment need the most attention, so you can make informed decisions.

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

**CONNECT WITH US**  
**@onestepsecureit**



**[www.OneStepSecureIT.com](http://www.OneStepSecureIT.com)**  
**(623) 227-1997**