SourceOne
TECHNOLOGY

‹THE SOURCE›

Hints, tips, tools and resources from real IT geeks.

CYBER SELF-DEFENSE TIPS

Flex your security muscles and keep your network, data and users safe online.

IN PARTNERSHIP WITH

FORTINET®

Your trusted IT Partner, located in Brookfield, WI

Welcome!

As businesses have grown increasingly dependent on interconnected technology, there's been a corresponding growth in technology-based crime.

In this special edition of our free IT hints and tips magazine, we look at keeping your organization safe online with useful security tools, actionable processes and a dose of common sense.

I hope you find the magazine useful and if you have any questions check out our blog, connect with us online or give us a call.

Sincerely, Jesse.

CONTENTS

Jesse Rink

PRESIDENT
SOURCE ONE TECHNOLOGY

An experienced network engineer, Jesse has been sharing his expertise and experience with organizations across Wisconsin for over 20 years.

Source One Technology provides IT security services to organizations of all sizes across Wisconsin.

Just The Facts, Ma'am

The findings in Fortinet's 2023 Cybersecurity Skills Gap Report show that organizations are fighting an uphill battle against cyberthreat.

More organizations were breached last year than in 2021. 84% of respondents indicate their organization experienced one or more breaches in the past 12 months, up from 80% the year before.

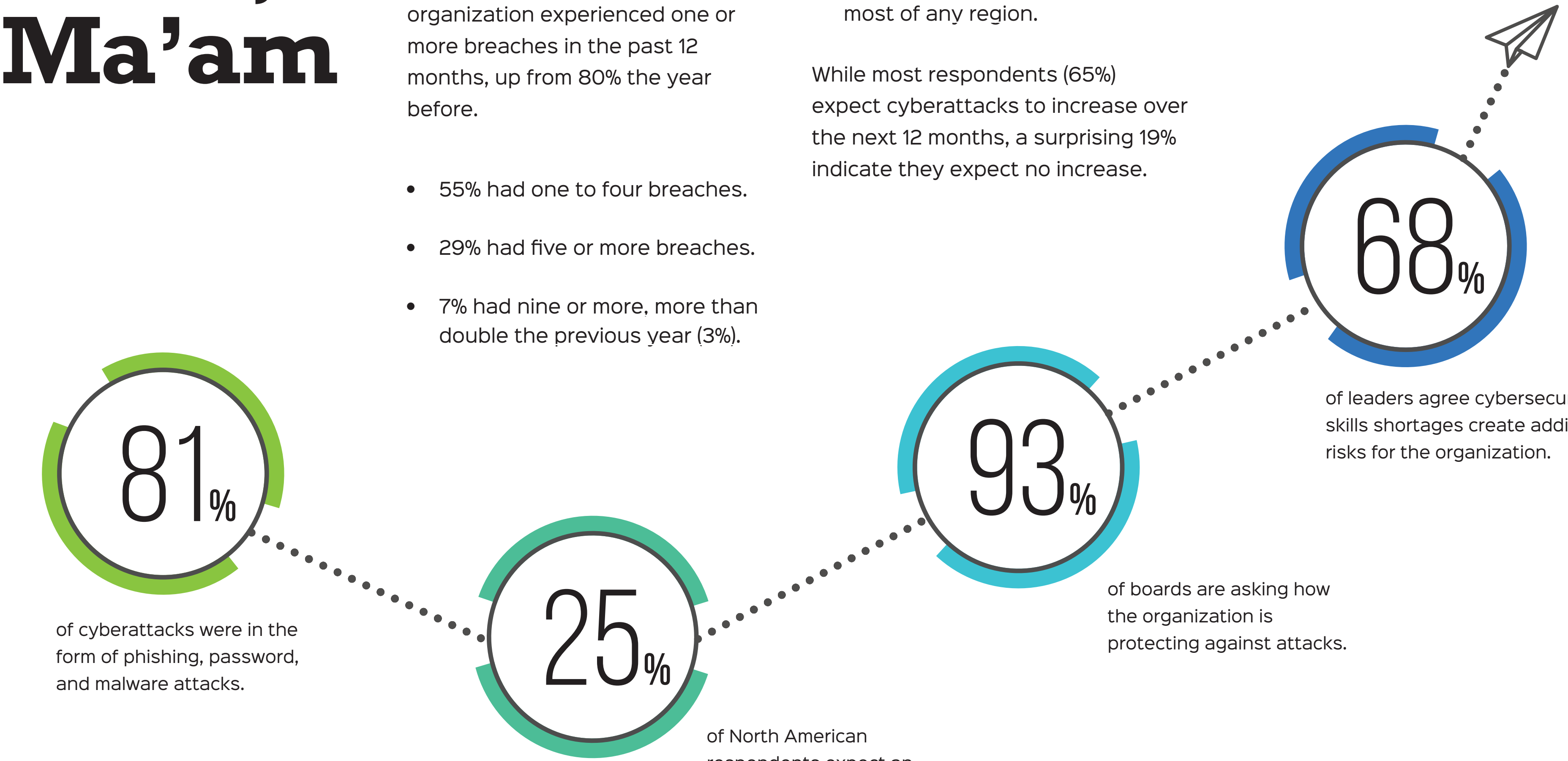
- 55% had one to four breaches.
- 29% had five or more breaches.
- 7% had nine or more, more than double the previous year (3%).

Nearly half (48%) of organizations that suffered at least one breach in the past 12 months indicate that it cost more than $1 million to remediate, up from 38% in 2021.

- 64% of North American organizations report a total cost of breaches above $1 million, the most of any region.

While most respondents (65%) expect cyberattacks to increase over the next 12 months, a surprising 19% indicate they expect no increase.

Given analyst predictions to the contrary, these organizations could be vulnerable, as they likely won't prioritize security preparation for their networks, IT recruitment, or cyber-skills development for staff.



81%

of cyberattacks were in the form of phishing, password, and malware attacks.

25%

of North American respondents expect an increase in attacks next year.

93%

of boards are asking how the organization is protecting against attacks.

68%

of leaders agree cybersecurity skills shortages create additional risks for the organization.

Basic email hygiene

When it comes to basic email hygiene, prevention goes a long way. In fact, an old adage, which has become conventional wisdom over the years, states, 'a closed relay keeps the spammers at bay'. OK, while that might be conventional wisdom, it's never been an old adage.

Whether you've inherited new infrastructure or have managed the same one for years, it's a good idea to periodically check your environment—specifically your mail server and firewall configurations as well as your email authentication mechanisms—to ensure your organization doesn't unexpectedly wind up on any email or spam blacklists or being used to send unauthorized emails.

"Look, Mom - no vulnerabilities!"

First, make sure you have outbound firewall rules in place which restrict ports 25, 465, and 587. The only system which should need this is your mail server, not your entire network. Anyone could start sending anonymous emails from your network whether they intend to - or not.

Second, ensure your mail server isn't configured as an open relay. Spammers constantly scan the Internet for open relays to route their email through, damaging your organization's email reputation in the process.

Then, check to ensure attackers cannot pretend to be from your organization by spoofing your email addresses.

There are three free mechanisms for verifying an email was not spoofed/ sent from an outsider that, when combined, are highly effective at protecting everyone, including those outside your organization, from attackers pretending to be you.

The first of these mechanisms is an SPF DNS record identifying where your organizational emails may legitimately come from and guiding organizations on what to do if they come from somewhere else (such as a hacked cloud server).

The second mechanism is a DKIM DNS record which proves that the message is authentic - that it was not intercepted or modified in transit and could only be sent by your organization. You will get your DKIM record details from your mail provider.

Finally, a DMARC DNS record tells everyone's email servers what to do if the SPF and/or DKIM records are not matched - you can tell those email servers to reject unmatched messages, mark them as spam, or deliver them. You can even instruct them using DNS to send you a report about the email that server received. This way, you can protect your parents/customers/clients and get reports about spoofing attempts that never even made it to your organization.

Combining effective firewall blocking of email traffic with mechanisms that protect your users from spoofing attempts will minimize the chances that mail is interrupted or that users are being tricked into clicking links from attackers.

Check out our blog for more great tips, tricks, and guidance on managing your organization's email.

When you're done there, check out MxToolbox for a great selection of additional tools and resources to check and test various aspects of your email environment. You can even create a free account and have them monitor a few things for you!

→ MXTOOLBOX.COM/EMAILHEALTH

Password managers

Fingerprint readers. Voice recognition. Iris scanners. The start of a new 007 movie, or how you access your bank accounts?

Recently, there has been widespread adoption and acceptance of multi-factor authentication. In addition to providing your username and password, you might have to provide something you have (such as a token) and prove who you really are (fingerprint or voice).

Maybe with the exception of iris scanners, other biometric identification technologies have been quickly commercialized and scaled to consumer laptops, tablets, and smartphones, which can offer extra security and sometimes convenience. But think briefly about how you access most of your accounts—a list of usernames and passwords might come to mind.

It's challenging to balance security and convenience and almost impossible to have both. You probably know you should use unique, complex passwords for each account. But how do you remember them all? Do you write them on Post-It notes? Save them in Office documents? Do you store those documents on a flash drive, your network, or the cloud? What if any of those locations or devices were compromised?

Enter encrypted password managers. While no silver bullet (nothing in Information Security is), you can store and secure everything in a single program. You can choose between online/cloud-based password managers and offline password managers. Many are cross-platform and keep your information synchronized across multiple devices.

Most password managers seamlessly integrate into your browser, and some even have mobile app capabilities or can integrate into select applications. If you're signing up for a new service, just about every password manager can even generate and store unique complex passwords for you.

Some password managers are free, and others aren't. You'll need to decide which one has the required features and capabilities.

To get started, try the ones below. You can always start with a free version and migrate to a paid version if you want more.

- **KeePass** - Free and open-source and light-weight password manager primarily for Windows.
- **Bitwarden** – Freemium open-source password management that stores credentials in an encrypted vault.
- **Keeper** – Protects your organization's passwords with an ultra-secure and easy-to-use vault.
- **Hudu** – Passwords are a vital part of IT documentation and Hudu's built-in interface is tailored towards them.
- **IT Glue** – Next-level password management with access control, host-proof hosting, at-risk password report and audit trail.

Tip #1 – Password-protected encryption that is included with Excel/Word documents is noted to be historically weak and can be cracked on today's hardware. Don't rely on this method to secure your data!

Tip #2 – Be careful of sharing too much personal information on Social Media. Hackers can use that information about your favorite teacher, the name of your pet, where you went to school, etc. as a means to correctly answer the security questions that might be presented during a password reset process.

Enabling UTM and NGFW security services

Are you blocking access to known botnets? Are you preventing people from simply bypassing policies by using proxies? Are you preventing someone from submitting 10,000 logon requests to your Domain Controller in a lockout attack?

By default, network security appliances performing Unified Threat Management (UTM) or Next Generation Firewall (NGFW) functions are not performing any inspection except for blocking traffic that hasn't been explicitly allowed.

→ FORTINET.COM

If you have valid subscriptions and are not currently experiencing performance problems you should ensure you slowly enable and apply the following features to most of your traffic, **in descending order,** monitoring performance as each feature is enabled.

01

Intrusion Prevention (vulnerabilities and attacks)

Set to block Medium and above threat to any traffic to/from any.

02

SSL/TLS Decryption

Over 70% of web traffic is now encrypted, and many of the following security services simply cannot work without full deep packet inspection. Apply, minimally, to any traffic to WAN.

03

Anti-malware/Gateway Anti-virus and Anti-spyware

Set to scan all available protocols and inspect all traffic.

04

Botnet/C&C and Geo-IP

Apply to any traffic to/from WAN, blocking inbound countries for nearly all countries and outbound for all countries for which no known use case exists.

05

Content Filtering/URL Filtering and Application Control

Set to block proxies, malware, peer-to-peer, and, if feasible, unrated sites, for any traffic to/from WAN.

06

Sandboxing

Configure executables and archives for sandbox analysis.

> We brought Source One Technology in to assist us with improving the overall security posture on our IT systems. The initial security assessment and recommendations they provided, along with continued on-going server and firewall updates, ensure that our entire network remains secure. I would highly recommend Source One Technology to any organization!

Ryan Jonas
DIRECTOR OF TECHNOLOGY
VILLAGE OF GREENDALE

The Source One Technology Difference

01 10 Senior Network and Systems Engineers with individual experience ranging between 10 and 25+ years.

02 Highly capable team with numerous industry and vendor certifications (including Fortinet NSE 1-5, 7).

03 Subject Matter Experts with high-level IT engineering, consulting and management backgrounds.

04 Engineers have extensive experience across various industries, including highly-regulated environments.

05 Tried-and-true cybersecurity experts and enthusiasts who have been there, done that and still love doing it.

06 People persons that join, lead and educate -- no non-communicative nonsense that disappears in a datacenter.

Time to say goodbye to VPNs

The recent rise in remote working has highlighted the limitations of virtual private networks (VPNs). A mainstay for decades, organizations are now looking for alternatives to VPNs that better meet their objectives. With better security, more granular control, and a better user experience, zero-trust network access (ZTNA) can be a smarter choice for securely connecting a remote workforce.

Three Key Drawbacks of VPNs

VPNs have been the de facto method of accessing corporate networks, but they have some serious issues, particularly regarding security. Here are three key drawbacks of relying on a traditional VPN:

- A VPN takes a perimeter-based approach to security.
- VPNs have no insight into the content they are delivering.
- Networks are now highly distributed.

ZTNA Offers a Better Option

Because so many people are now accessing critical resources and applications from outside the network perimeter, security experts have been promoting the need to shift away from the paradigm of an open network built around inherent trust to a zero-trust model.

Unlike a traditional VPN-based approach, which assumes that anyone or anything that passes network perimeter controls can be trusted, the zero-trust model takes the opposite approach: No user or device can be trusted to access anything until proven otherwise.

Five Advantages of ZTNA

- Organizations can extend the zero-trust model beyond the network.
- ZTNA works transparently in the background, which improves the user experience.
- Each user and device is verified and validated before being given access to an app or resource.
- Because ZTNA focuses on application access, it doesn't matter what network the user is on.
- ZTNA reduces the attack surface by hiding business-critical applications from the internet.

Improve Remote Access

ZTNA is proving to be a better solution, easier to use, with the added benefit of adding application security to a remote access solution. Organizations should be careful to select ZTNA solutions that integrate with their existing infrastructure.

Building a zero-trust network access solution requires a variety of components, which may include a client, a proxy, authentication, and security that can be used to apply ZTNA to remote users, no matter where they're located.

Want to see a quick video overview of one ZTNA solution? **Search "Fortinet ZTNA Overview" in YouTube.**

WORK FROM ANYWHERE

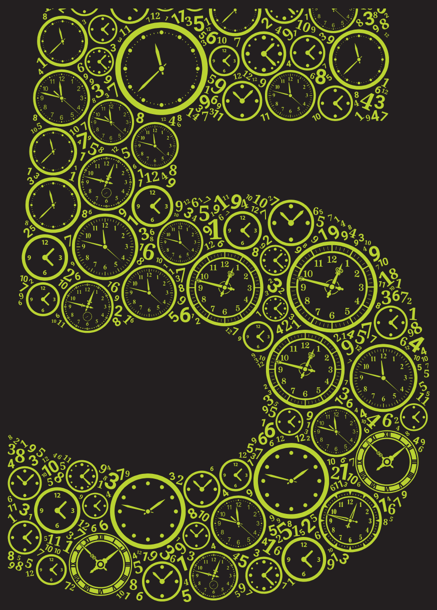
Over the past decade or so, technology has been steadily evolving to give workers more flexibility in the devices they use, the locations they can work from, and the resources they can access. Bring your own device (BYOD) and cloud application access were the first steps toward enabling flexible work.

Although organizations were on track to embrace a true work-from-anywhere (WFA) strategy sometime in the next few years, the COVID-19 pandemic accelerated the need. And now, more workers are demanding that employers provide a WFA option. The challenge is delivering a hybrid work experience that keeps workers both productive and secure.

When the pandemic hit, few organizations were prepared to support remote work. Workers were suddenly dialing into the office from poorly secured home networks. Access controls were inadequate, and endpoint devices were vulnerable. To support work from anywhere, organizations need to think about security and deploy solutions capable of following, enabling, and protecting users no matter where they are located. They need security on the endpoint (EDR/MDR), preferably combined with zero-trust access (ZTA) and zero-trust network access (ZTNA). They also need secure software-defined wide-area networking (SD-WAN) and secure access service edge (SASE) for secure connectivity. Access policy engines must provide appropriate access based on user and device identity, location, device type, and posture to establish secure access.

To support WFA, organizations should identify a cybersecurity mesh platform (for example, Fortinet) with solutions designed to work as an integrated system with actionable threat intelligence to keep the security products informed and prepared with threat identification and protection information across all of the types of locations. This type of platform approach means zero trust, endpoint, and network security can all be unified by a common set of application programming interfaces (APIs) and integration points to ensure users can seamlessly shift from one location to another with a consistent and secure experience. And on the IT side, the cybersecurity mesh simplifies policy creation and enforcement, ensures uniform configurations, centralizes management, and makes it possible to monitor and control users, devices, data, applications, and workflows.

Work from anywhere has become more important due to the recent pandemic, but the pandemic has only accelerated a trend that was in progress. The hybrid work environment is here to stay, and organizations must ensure they are ready to safely use that model.



minute firewall check

Out of the box, most default firewall policies allow any internal host on your network to access any external host over any port or service.

Instead, strongly consider implementing egress / outbound access rules to allow specific internal hosts, or range of devices, to access specific external hosts using only your specified services/ports. By whitelisting outbound traffic at the network level, you're gaining more control over your network and further reducing the surface area for potential threats.

In addition, today's next-gen UTM firewalls are far more advanced than firewalls of old. To supplement standard network-level whitelisting, consider enabling other security services such as Intrusion detection/ prevention and application whitelisting, as well.

Combining network and application-level filtering will further bolster your network against more recent and advanced threat types. In many environments, especially schools, this combination can also prevent the more inquisitive users on your network from circumventing other controls, such as web filtering!

Are you curious about what your firewall allows out of your network? Load up your favorite port/security scanner, such as nmap, and target allports.exposed. You may be surprised by what you find!

Also, consider occasionally monitoring the utilization of all inbound/outbound firewall rules. This will allow you to locate and disable any legacy firewall rules that are no longer necessary and further help to reduce attack surfaces. Finally, always be sure to keep your firewall's firmware revision level up to date and current to protect your device against potential vulnerabilities.

back it up

Good backups are a critical piece of any IT infrastructure. Without an effective backup solution and regular validation of those backups, your information could be at high risk and prone to unexpected data loss during a recovery process. Here are a few important key points to remember when evaluating your backup solution to help protect your organization's data and information:

Follow industry guidelines and recommendations by utilizing a 3-2-1 backup solution:

3 Different copies of data at a minimum - preferably a lot more!

2 Different types of media - disk, tape, in the cloud, etc.

1 Copy of that data stored offsite - different physical location, in the cloud, etc.

Furthermore, a solid backup plan should also consider including the following recommendations:

1 Or more copy of that data marked as immutable - air-gapped, offline, immutable, Public AWS S3, etc.

0 Backup errors/failures and data backup verification - be sure it's recoverable!

Keep in mind that when designing a backup strategy, make sure it adheres to your company's defined policies for both:

- RTO – the recovery time objective (RTO) is the maximum amount of time permitted after event-failure to restore normal operation and services, for example, 24 hours.
- RPO – the recovery point objective (RPO) is the maximum amount of data permitted from an event-failure that your organization can tolerate losing or incurring data loss (for example, 4 hours)

Following these guidelines will help ensure your organization has an effective backup solution against data loss, hardware failure, ransomware, and bad actors.

Holey Software Batm...

Third-party patching programs

Hackers are using unpatched third-party applications like Adobe Flash and Firefox to gain access to company networks. While many of these applications update themselves, it's in your company's best interests to make sure they're updated. Here are a few programs you can use to keep your third-party applications up to date.

Ninite Pro is a cloud-managed, agent-based program that can keep the most popular third-party applications updated on your Windows computers. Ninite Pro is managed via a live web-based interface where you can control the deployment of updates and view the status in real-time.

➔ NINITE.COM

PDQ Deploy is an on-premise application deployment software with over 200 prebuilt third-party applications. Paring PDQ Deploy with its counterpart, PDQ Inventory, will allow you to automate the process of locating and updating multiple third-party applications in your environment.

➔ PDQ.COM

Don't want to deal with any of this third-party updating? Then utilizing a Managed Service Desktop solution, like the ones Source One Technology can provide, may be the solution for you. For a monthly per desktop fee, this service performs OS and third-party application updating saving you time for other essential tasks.

SECURITY AWARENESS TRAINING

IT security controls, such as UTM, NGAV, NGFW, SIEM, IDS/IPS, Patch/Vulnerability Management, and 3-2-1 Backups, can help protect your technology infrastructure and company assets. However, they may not prevent Bob in the Dispatch department from purchasing $5,000 worth of iTunes gift cards or prevent a bad actor from hijacking an unencrypted and unsigned email conversation and redirecting a customer's banking wire payment, either.

The fact is employees continue to be high-value targets for threat actors. They may be targeted through a variety of means, including a phishing email attempt, tricked into a drive-by download online, or unknowingly letting a bad actor into a facility. An untrained workforce can introduce serious risk.

Fortinet offers a SaaS-based Security Awareness Training service that delivers timely and current awareness training on today's cybersecurity threats. This service helps IT, security, and compliance leaders build a cyber-aware culture where employees recognize and avoid falling victim to cyberattacks. It also helps satisfy regulatory or industry compliance training requirements.

The service offered by Fortinet provides the following benefits:

- Training employees to recognize and report on potential security threats, whether in email, online, or a physical setting.
- Satisfy requirements for security and awareness training across major frameworks.
- Prevent the impact of breaches caused by employee errors and poor judgment.
- Ensure employees are aware of data privacy and security and are motivated to protect personally identifiable information.
- Reduce the costs and strain on your IT department directly by minimizing the risk of cyber attacks.

Even better, this Security Awareness Training service from Fortinet is **ABSOLUTELY FREE** for organizations with less than 25 users or if your organization is a K-12 School District!

Despite ever-increasing budgets and overall strengthening of cyber-resilience, without modern Security Awareness Training, one of the greatest but most at-risk resources — your people — remain vulnerable.

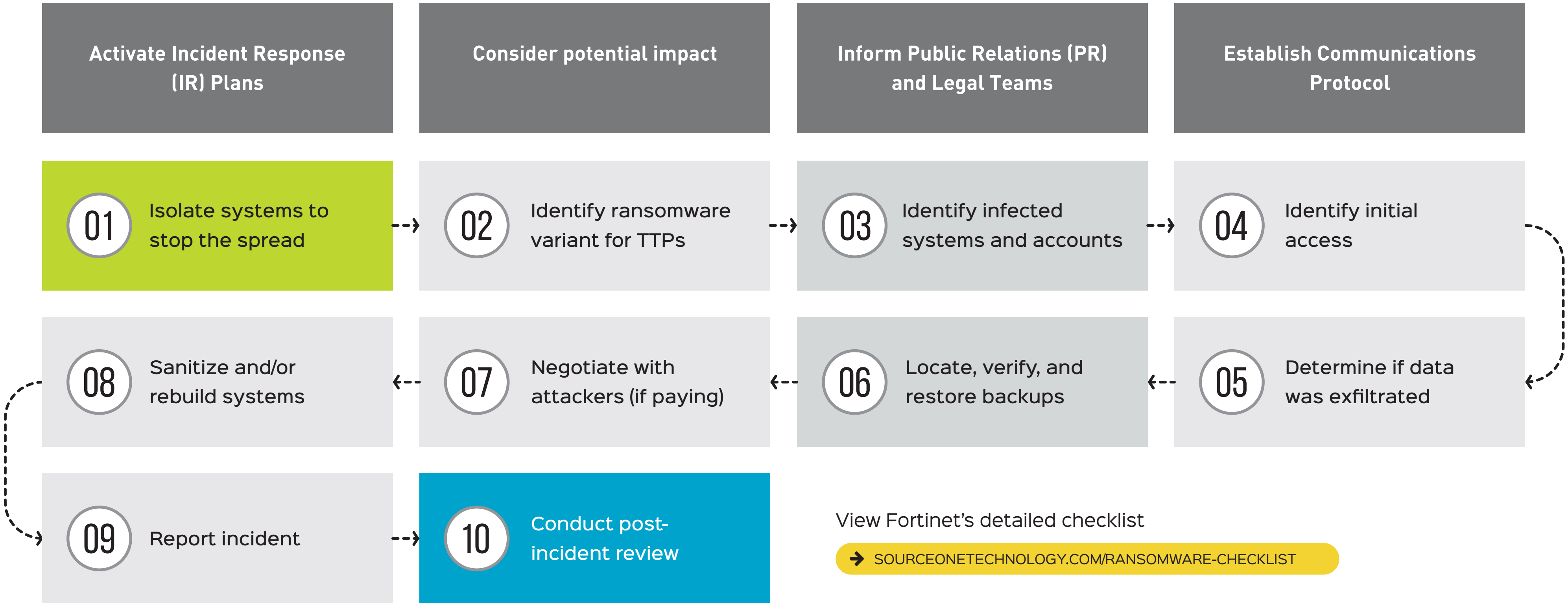
Call us at (262) 432-9000 or email sales@sourceonetechnology.com to discuss further.

DON'T PANIC!

Steps to take during a ransomware attack

There were over 493.33 million ransomware attacks in 2022*. If you've not yet been a victim of a ransomware attack, the odds are that it's just a matter of time. And if you've already been breached, you're not immune.

When that day comes, it's essential that you know what to do to minimize the impact to you, your team, and your business. Here is a quick overview of the steps your organization will need to take to deal with an active ransomware attack:



Activate Incident Response (IR) Plans

Consider potential impact

Inform Public Relations (PR) and Legal Teams

Establish Communications Protocol

01 Isolate systems to stop the spread

02 Identify ransomware variant for TTPs

03 Identify infected systems and accounts

04 Identify initial access

05 Determine if data was exfiltrated

06 Locate, verify, and restore backups

07 Negotiate with attackers (if paying)

08 Sanitize and/or rebuild systems

09 Report incident

10 Conduct post-incident review

View Fortinet's detailed checklist

➔ SOURCEONETECHNOLOGY.COM/RANSOMWARE-CHECKLIST

Need an IT Partner to help you with Incident Response or Disaster Recovery? Get in touch with us by phone at (262) 432-9000.

* Statista.com

FREE cybersecurity scan

Limited to the first 20 organizations to apply

Keep your network, data, and users safe.

We will scan your public-facing assets for vulnerabilities and send you a report of any areas you need to address. The scan includes:

- Your website
- Your firewalls
- Your VPNs
- Any servers you are hosting

Claim your scan at:

➔ SOURCEONETECHNOLOGY.COM/FREESCAN

Who we are

Locally owned and operated in Brookfield, WI since 2006, we employ a highly experienced team of senior level Engineers, each with 10-25 years of advanced technical experience, to help you troubleshoot, design, and implement solutions that drive down costs and simplify your IT management.

No sales people

98% retention

16+ years experience

No long-term contracts

and what we do

Business management

Business accounting software – Quickbooks, Peachtree.

Virtual CIO – Helping you create and implement the right IT strategy for your organization.

Communication and collaboration

Business email – Office 365 and Google Workspace solutions.

Cybersecurity and business continuity

Data backup – Local, offsite and hybrid business continuity and disaster recovery solutions for servers and SaaS.

Disaster recovery planning – Helping you take back control in the event of a disruptive event with a clear, actionable plan.

Endpoint security – Installing, configuring, and maintaining endpoint protection.

Incident response – Addressing and managing the aftermath of a security breach or cyberattack.

IT assessments – Offering vulnerability management, penetration testing, risk assessment, security awareness training and compliance consulting services.

Security awareness training - Protecting your staff and organization from malicious behavior using reputable programs from KnowBe4 and Proofpoint.

Desktop support services

Apple support – Installing, configuring, and optimizing macOS and iOS devices, and MacPractice software.

PC and printer support – Managing the entire desktop lifecycle from procurement, deployment and support through to disposal.

Digital transformation and cloud migration

Migrate services to Azure and AWS – Microsoft Azure and Amazon AWS public/hybrid cloud solutions.

Remote access/work from anywhere – Site-to-Site VPNs, IPSec VPNs, SSL VPNs, Remote Desktop Services.

IT infrastructure services

Firewall and network security – Protecting your organization from risks and vulnerabilities.

IT performance monitoring – Making sure your environment is healthy and performing as expected.

Networking support – Providing the switching and routing backbone and highway for your devices.

Server administration – Windows 2012, 2016, 2019, 2022, Linux and Mac.

Storage and SANs – Design, build and manage your infrastructure across different vendor platforms.

Virtualization – VMware vSphere, Microsoft Hyper-V virtualization solutions.

Call us at (262) 432 9000 or visit www.sourceonetechnology.com

WHAT NOW?

To find out more about cybersecurity and what you can do to protect your organization, get in touch!

Read the latest from our engineers or ask us a question whenever you need advice.

sourceonetechnology.com/blog

@sourceone_wi

linkedin.com/company/source-one-technology-inc

> With the increase of cyber incidents in K-12 schools, we knew we needed to ensure a safe online learning environment for our school community, and Source One Technology's Cybersecurity Assessment and follow-up went above and beyond our expectations. Throughout the process, they checked in, asked questions, researched, and provided insight for us. We highly recommend Source One Technology for your Cybersecurity Assessment.
>
> Valerie Verhunce
> DIRECTOR OF TECHNOLOGY
> HARTFORD UNION HIGH SCHOOL

Source One TECHNOLOGY

Call us on (262) 432 9000 or visit www.sourceonetechnology.com
333 Bishops Way, Suite 120, Brookfield, WI 53005