WHITE PAPER

CompTIA

Fundamental Cybersecurity for Managed Services Providers

Do you know what you need to operate securely as an MSP?

This whitepaper provides the fundamental aspects of cybersecurity a managed technology solutions business serving small-to-medium businesses needs to understand and implement. It is meant to help anyone seeking guidance—or is maybe overwhelmed by—implementing sound, best practice cybersecurity operations, technology, and behavior.

Each topic is expanded with a brief definition of what it is, why it is important to address, and who are some resources that could help. The following topics are covered by this white paper:

- Acceptable use policy
- Password policy
- Next generation firewalls
- Advanced endpoint defense
- Protective filtering
- Patch approval & management
- Data backup
- User awareness training
- Two-factor authentication
- Network assessment
- Domain Name System (DNS) security
- Dark web monitoring

a follow up to this paper will include more advanced cybersecurity topics, including:

- Threat hunting/threat intelligence
- Internet of things
- Access control
- Security information and event management (SIEM) system
- Change management
- Vulnerability management
- Data encryption
- Digital certificates
- Encrypted configured backups
- Business continuity/disaster recovery
- Risk assessment
- Third-party vendor risk management
- Incident response
- Risk management

All graphics in this paper are from:

CompTIA's 2021 State of Cybersecurity and CompTIA's Ahead of the Curve: MSP Trends in Cybersecurity.
https://my.comptia.org/resource-library/content/state-of-cybersecurity-2021
https://my.comptia.org/resource-library/content/2021-msp-trends-in-cybersecurity

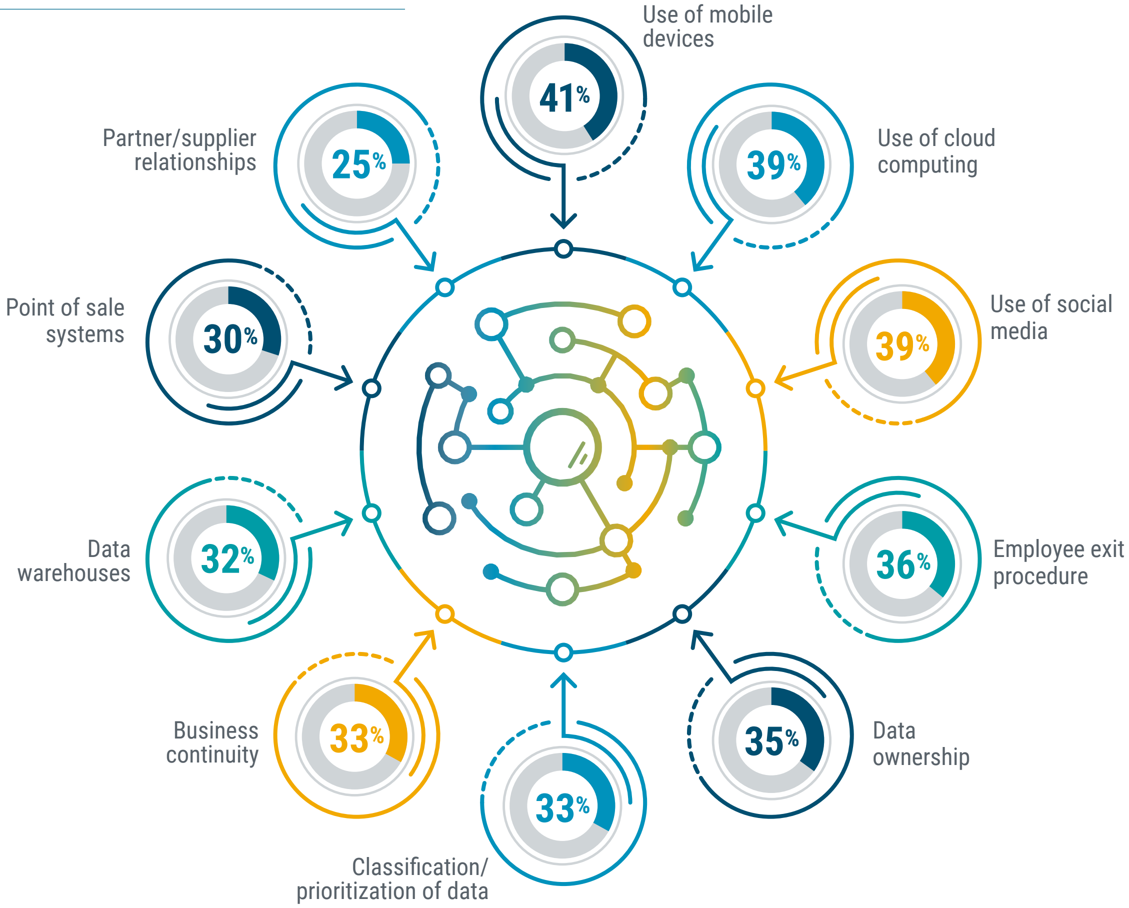
Introduction to a Risk-based Approach to Cybersecurity:

Oftentimes, technologists seek a technical solution to solve a problem. This approach is equated to throwing a dart at the board, and hoping for a bullseye. Unfortunately, this approach is also very expensive, often resulting in the wrong tool and creating a drain on an organization's financial and personnel resources. So, how can we be more efficient and effective with identifying the problems, aligning the business objectives, and finding solutions to solve for gaps in the existing pillars of cybersecurity (people, process and technology)? We recommend a risk-based approach.

What is it?

Cybersecurity risk is simply defined as an effect of uncertainty on or within an information and technology environment. We see this materialize in the loss of confidentiality, availability and integrity for our systems, devices, data, people and processes. As we become more aware and increase our level of understanding related to cybersecurity and what it means, we start to ask questions around the risk to our business and the risk to others. The awareness starts with identifying the risk across the three pillars of cybersecurity, understanding the threats which impact those three pillars, and creating a gap analysis to solve for the limitations in your environment.

Components of Risk Management



Why is it important?

Once you have clearly identified the risk, you can prioritize the list and solve for the greatest likelihood and impact to the organization. Instead of haphazardly throwing a dart at a board, you can be more precise in hitting the target. Spend money and time on the items of importance to keep the business running, even in the event of a security incident. Risk is not the same for every business or business owner. Be careful making an assumption that one size fits all, as that is not the case.

In the items which follow, evaluate each of these areas from the risk lens for your business first. Once you have everything implemented to meet your business objectives, then evaluate each of these areas for your customers in the same manner. You will have asked yourself many of the same questions your customers are going to ask you, "Why is this important?" You will have the answers at your fingertip since you already went through it.

Contact CompTIA membership or post in the CompTIA ISAO Cyber Forum if you have questions.

Acceptable Use Policy

What is it?

A comprehensive acceptable use policy is one of the cornerstones of an effective cybersecurity program. It is a document that defines the do's and don'ts while using corporate resources, i.e., information technology. This can take on myriad forms, but it is paramount to spell things out as succinctly as possible to minimize misinterpretation and lapses in your security posture.

Why is it important?

An acceptable use policy aids in protecting from internal and external threats or mishaps. This is done by outline or providing guidelines as to how technology, the network, and data are handled and interacted with on a continuous basis. It also helps to define reporting and accountability measures to aid in addressing issues as they arise, so the organization can take a very proactive approach to mitigation. The creation and acceptance of this document can serve as the framework for aiding the company in its compliance efforts related to insurance and government regulations as well.

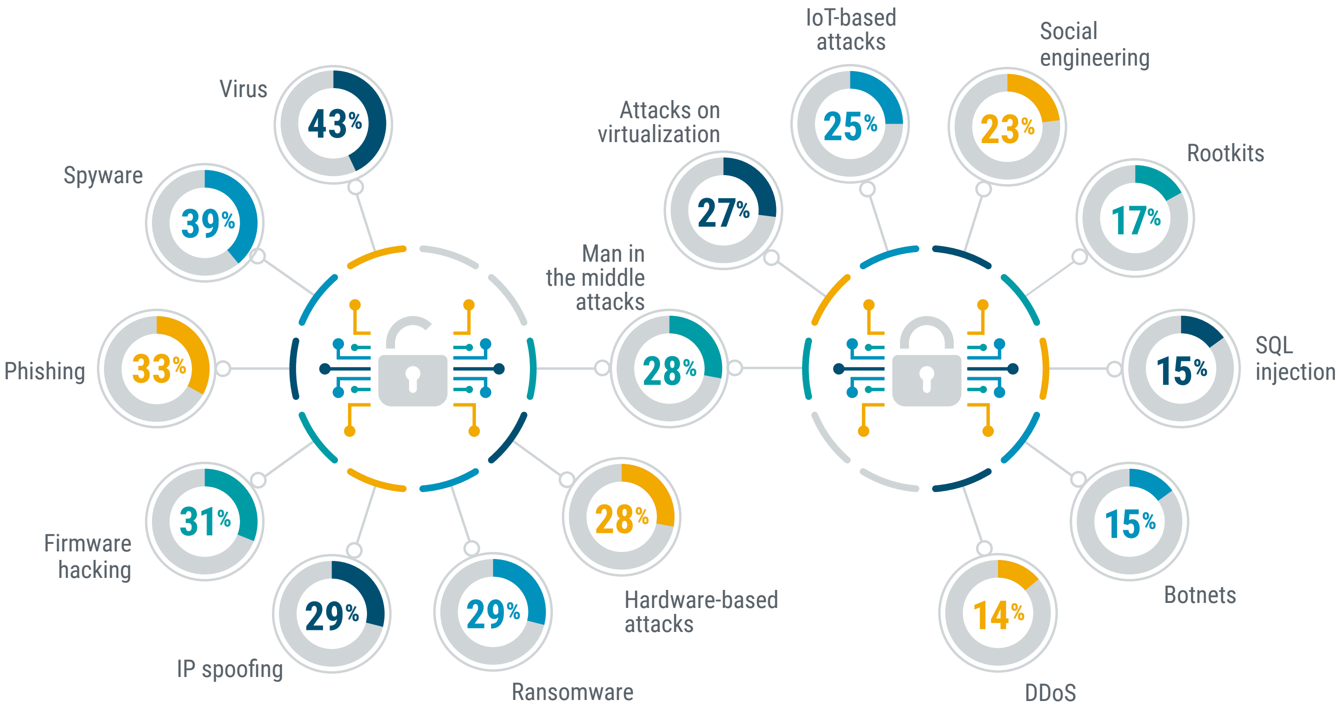
Where can I find more help?

The SANS Institute is focused on cybersecurity skills and leadership and have curated a wealth of template policies to assist. www.sans.org/information-security-policy/

Who does this policy cover?

All employees, visitors and contractors should adhere to some level of acceptable use policy while using company resources, i.e., technology, network, etc. These stakeholders should be required to acknowledge and accept the policies in place by the organization prior to being granted access to resources.

Need to Improve Threat Understanding



Password Policy

What is it?

This is a written policy within the organization that defines the requirements for passwords used with the organization. This can be enforced through technical setups using a directory service (such as Active Directory), but the written policy is designed to enforce these rules beyond what is used just for these directory services.

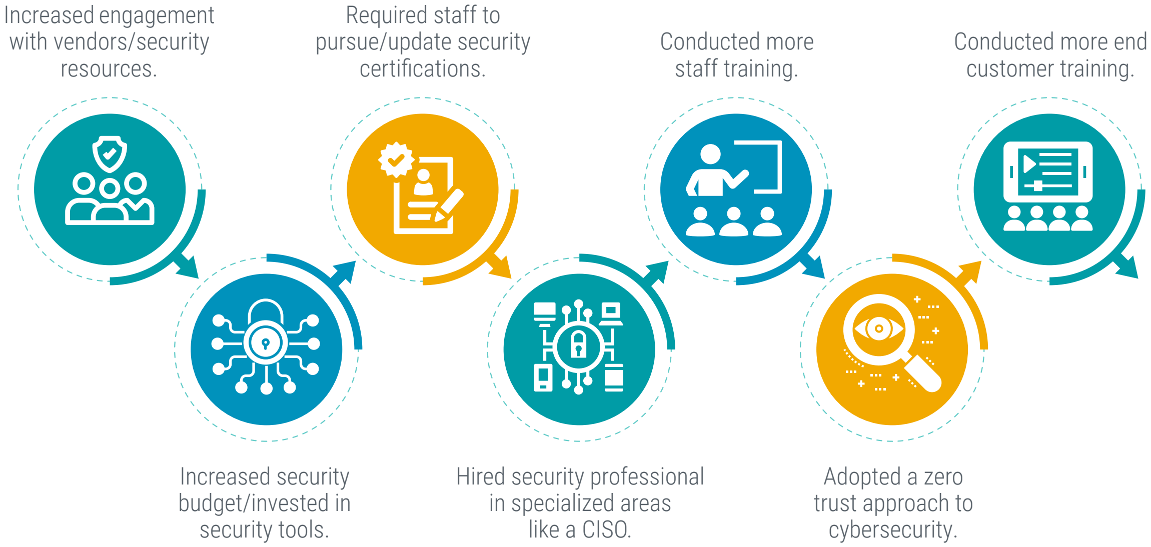
Why is it important?

Not all logins are controlled by the directory service logins and when new vendors are brought in, they need to be able to follow this written policy. Follow best practices for passwords, pass phrases, etc., for guidelines.

Where can I find help?

This is typically written by leadership, trained with assistance of HR and is an ongoing item reinforced by the generated organizational awareness. NIST provides password recommendations as well.

Steps MSPs are Taking to Mitigate Cybersecurity Risks



Increased engagement with vendors/security resources.
Increased security budget/invested in security tools.
Required staff to pursue/update security certifications.
Hired security professional in specialized areas like a CISO.
Conducted more staff training.
Adopted a zero trust approach to cybersecurity.
Conducted more end customer training.

Next-Generation Firewalls

What is it?

Next-generation firewalls are more advanced versions of a traditional firewall. They still have some of the old protection capabilities, but they add additional layers of protection to help keep your network secure. For example, next-generation firewalls add the ability to filter packets based on applications. They have integrated intrusion prevention, deep packet inspection, and cloud-delivered threat intelligence.

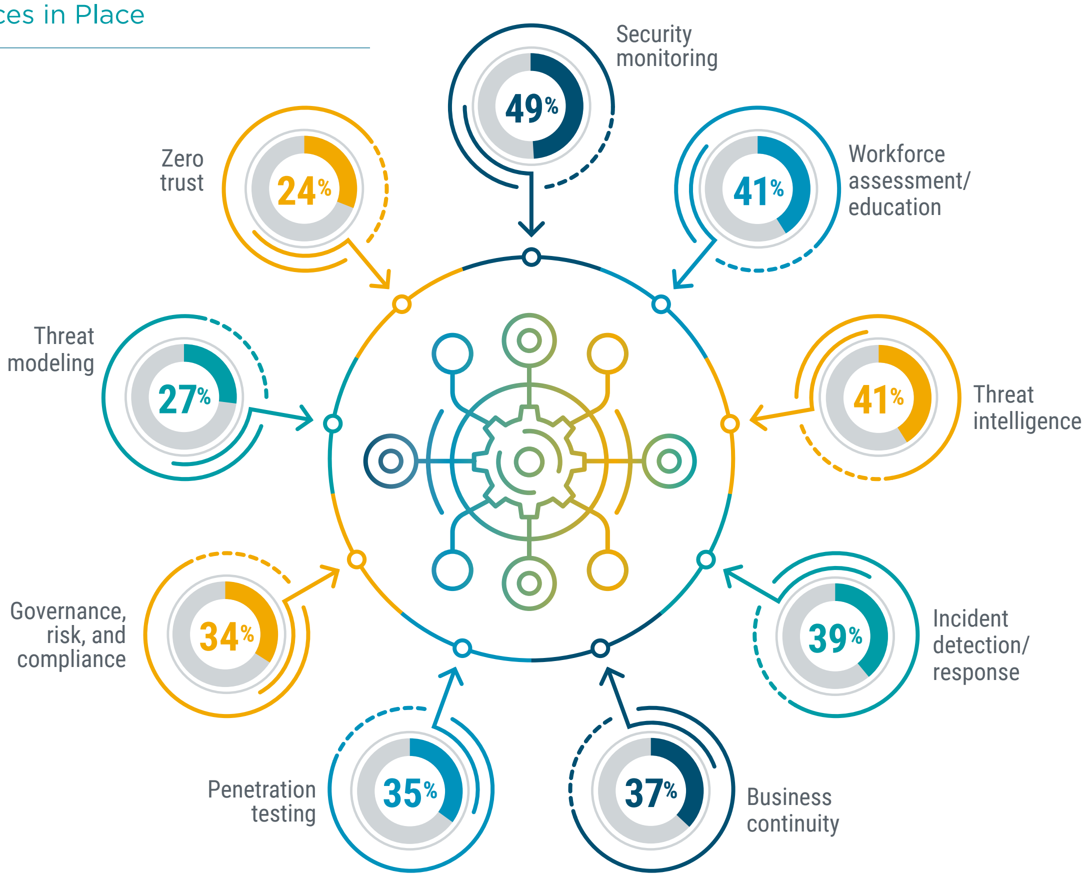
Why is it important?

Next-generation firewalls help prevent attacks before they get inside your network. Next-gen firewalls block malware from entering your network, which is something that traditional firewalls would never be able to do. They monitor traffic from layer 2 through layer 7 of the Open Systems Interconnection (OSI) model and determine what is being sent. If it meets the policy restrictions, it is forwarded. They can detect the presence of a breach faster with IDS which will help you eliminate the threat.

Where can I find help?

There are numerous providers of next generation firewalls. Talk to peers or post in the CompTIA ISAO Cyber Forum to ask for next-generation firewall recommendations.

Cybersecurity Practices in Place



Advanced Endpoint Defense

What is it?

This security product lives on workstations, servers, and likely mobile phones and IoT devices where applicable. It is often described anti-virus 2.0 as it incorporates anti-virus principles but extends into assisting with investigation, enabling rollback or response to a threat as well as assisting with data leak protection. These tools are often paired with a security operations center (SOC) to ensure response times can meet today's threats. Some higher-end tools assist with threat hunting through this SOC as well as perform vulnerability management. You will often hear the terms endpoint detection and response (EDR), managed detection and response (MDR), or extended detection and response (XDR) as references.

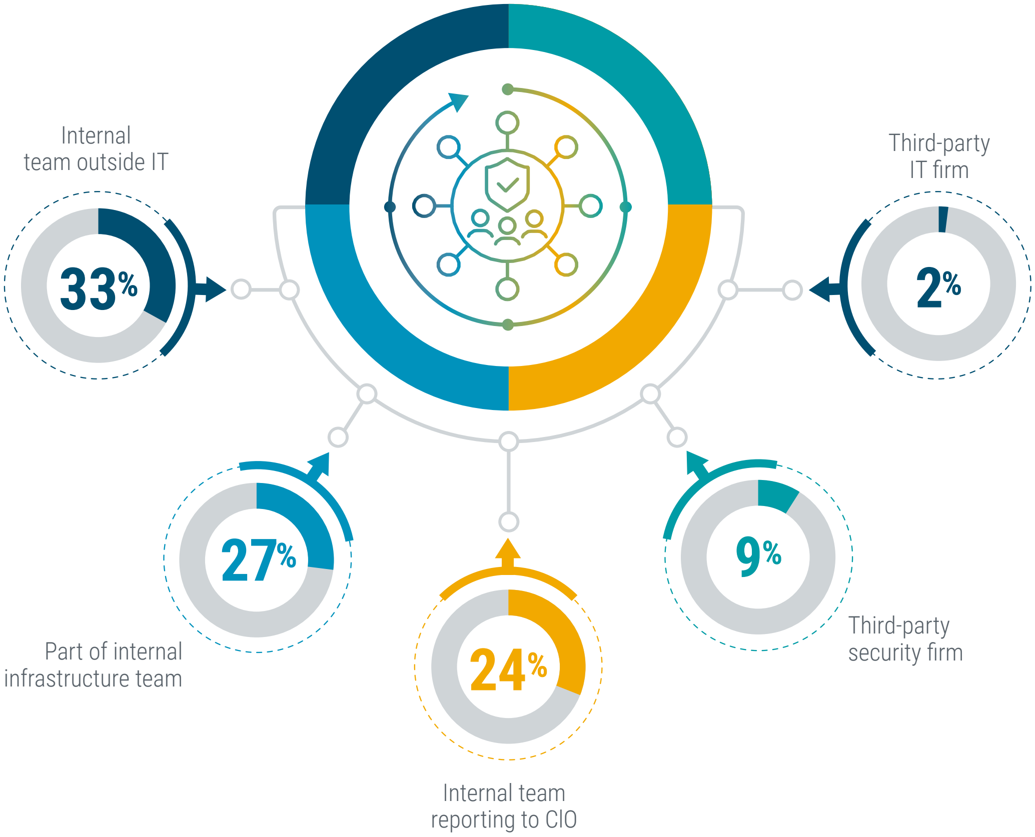
Why is it important?

Today's threats cannot be ignored and need investigation to ensure a persistent threat doesn't exist on systems. These tools also assist in helping prevent issues occurring through tighter controls on items such as network connections and USB devices.

Where can I find help?

There are numerous providers of advanced endpoint defense. Conduct some market research to find a provider that aligns with your business needs and client outcomes.

Location of Security Operations Center



Protective Filtering

What is it?

Protective filtering uses computers, machine learning, and artificial intelligence to automate the protection of environments by auditing the traffic or content being sent over the filter. If the traffic meets a certain threshold, the traffic is then automatically handled by an action set by the administrator. This can be a complete block of the traffic, quarantine or sandboxing, or simply logging and alerting the administrator that no automatic action was taken.

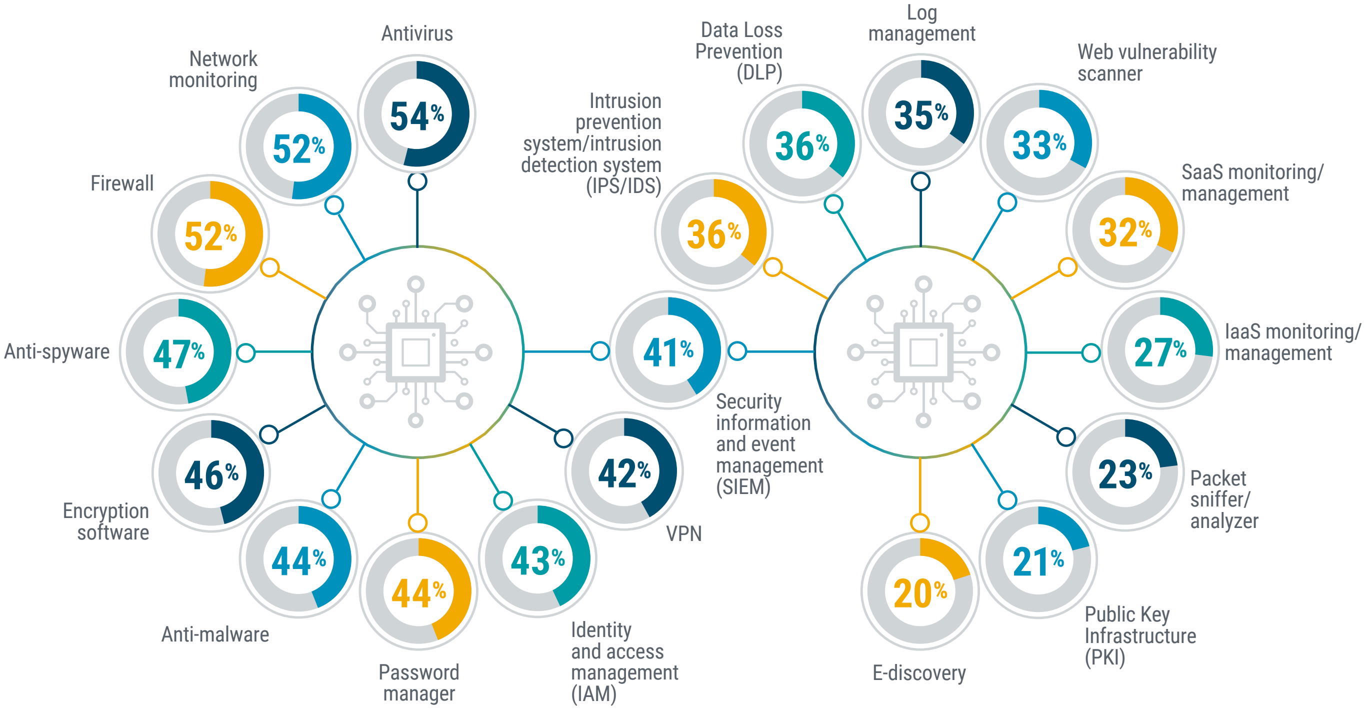
Why is it important?

The current threat landscape is based on humans being tricked into doing what an attacker wants. Sometimes these tactics can be difficult for the average user to discern from a legitimate transaction. Protective filtering allows IT admins to block, quarantine, or log specific activity known to be harmful or lead to sites or servers controlled by threat actors. Protective filtering should be used along with a security and awareness training program.

Where can I find help?

Numerous email and web content filtering options are available. It is important to consider the integration, features, and your needs when selecting a product.

Cybersecurity Products in Use



Patch Approval & Management

What is it?

Patch management is the process of distributing and applying updates to software. These patches are often necessary to correct errors (vulnerabilities or "bugs") in the software. Common areas that will need patches include operating systems, applications, and embedded systems such as network equipment, switches and firewalls. When a vulnerability is found after the release of a piece of software, a patch can be used to fix it. Doing so helps ensure that assets in your environment are not susceptible to exploitation.

Why is it important?

Patch management is important for the following key reasons:

Security: Patch management fixes vulnerabilities on your software and applications that are susceptible to cyber-attacks, helping your organization reduce its security risk.

System uptime: Patch management ensures your software and applications are kept up-to-date and run smoothly, supporting system uptime.

Compliance: With the continued rise in cyber-attacks, organizations are often required by regulatory bodies to maintain a certain level of compliance. Patch management is a necessary piece of adhering to compliance standards.

Feature changes: Patch management can go beyond software bug fixes to also include feature/functionality updates. Patches can be critical to ensuring that you have the latest and greatest that a product has to offer.

Where can I find help?

While you can manually patch systems on a small scale, it isn't feasible or efficient to do this without a remote monitoring management (RMM), tool. An RMM platform is crucial for professionally maintaining a healthy network, allowing you to patch your systems and allow technicians to securely connect to PCs and servers at the click of a button. There are many RMM tools than can handle patch management. Be sure to check the capabilities of your existing tool set.

Cybersecurity Threat Statistics

$4.24 million

Average cost of a data breach[1]

287

Average number of days to identify and contain a data breach[2]

350K

Number of new malware programs found per day[3]

18K

Number of Solarwinds customers affected by supply chain breach[4]

$1.85 million

Average cost of remediating ransomware attack[5]

74%

U.S. companies experiencing successful phishing attack in 2020[6]

Sources

[1] IBM/Ponemon Cost of a Data Breach Report 2021

[2] IBM/Ponemon Cost of a Data Breach Report 2021

[3] AV-TEST Institute

[4] U.S. SEC filing, 12/14/20

[5] Sophos State of Ransomware 2021 report

[6] Proofpoint 2021 State of the Phish Report

Data Backup

What is it?

Quite simply, backups are copies of your critical data, files and systems, physically and logically separated from your production data, files and systems. In the event of a disruption, loss or encryption, backups are your failsafe to restore to normal operations. Backup strategy is critical—different systems, files and data sets have different levels of importance and value. Critical systems and data take priority in the race to restoration. A commonly accepted practice is the 3-2-1-1 rule—3 copies of data, 2 different media to store backups, 1 offsite location to store backups online, and 1 offsite location to store backups offline. Equally important is testing. Regularly recurring test restores are a must. Know that you can restore your systems and data.

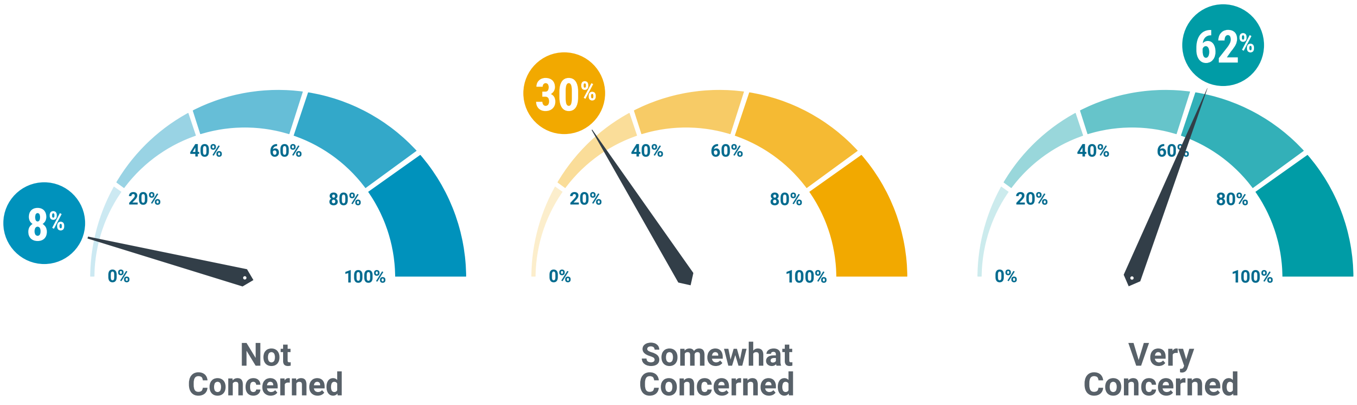
Why is it important?

Hope is not a contingency plan. Systems crash, physical disasters happen, and threat actors are constantly attacking. A high percentage (up to 93%) of businesses fail within months of a major data loss. if they couldn't restore to normal operations quickly. Offline copies are a must as a final layer of defense against encryption/ransomware attacks, as threat actors are known to compromise online backups long before they make their presence known to their victims. In these cases, an offline (aka: "air-gapped") backup is the only recourse in restoring your systems, files and data.

Where can I find help?

Numerous organizations provide backup solutions. Regular market research will help you stay abreast of the best solution for you.

Concern Level Over Hackers Targeting MSP Networks



User Awareness Training

What is it?

No matter how hardened your IT infrastructure and cloud-based app security are, the weakest link is your people. Training them to recognize threats is critical. User awareness training (aka: security awareness training) is a systematic, recurring process that flexes as threats advance and change.

Why is it important?

For your team members to do their jobs, they must have access to your assets. Once their credentials are compromised, threat actors have the same access. They are being baited constantly. On a macro level, threat actors use social engineering tactics to get your team members to slip up. On a micro level, threat actors are researching them specifically. They need to be aware of this and recognize it.

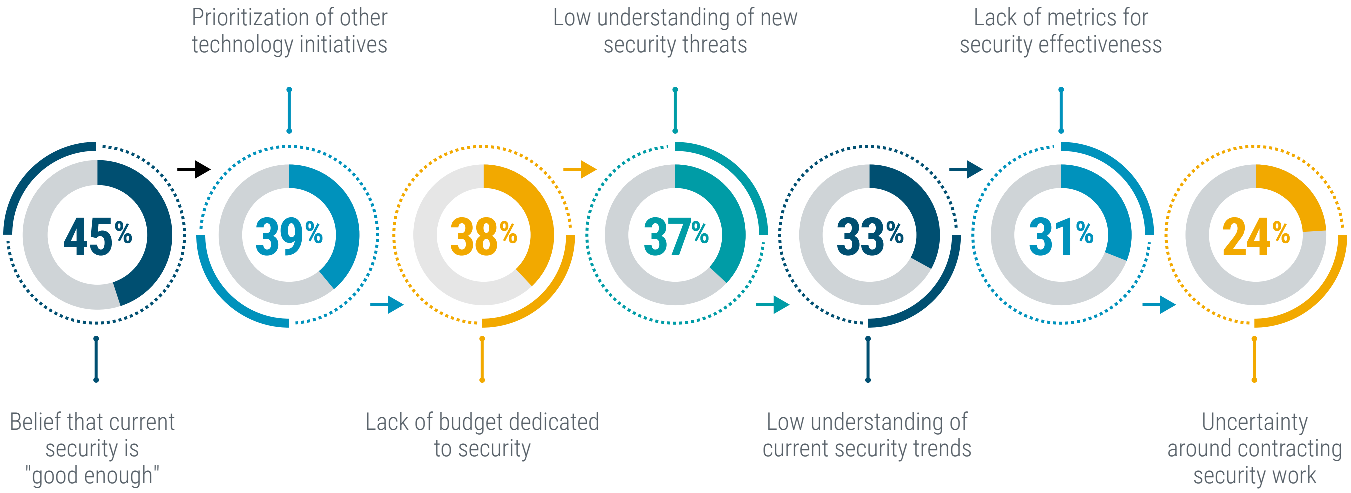
Where can I find help?

Security and user awareness education programs come in many forms. Some examples of providers include: KnowB4, Proofpoint, InfoSecInstitute, SANS.

Who is covered by this training?

Providing this training for every team member in your organization is very important. Consider vendors and contractors who have access to your facilities, communications systems, networks and apps. In your supply chain, every upstream and downstream contractor should have training in place. Make this mandatory. If they get compromised and have access to your assets, you're now compromised.

Hurdles for Changing Approach to Cybersecurity



Two-Factor Authentication

What is it?

Two-factor authentication, or 2FA, is a security process in which users provide two different authentication factors to verify themselves. Two-factor authentication methods usually rely on a user providing a password as the first factor and a second different factor, usually a security token or biometric such as a fingerprint or facial scan.

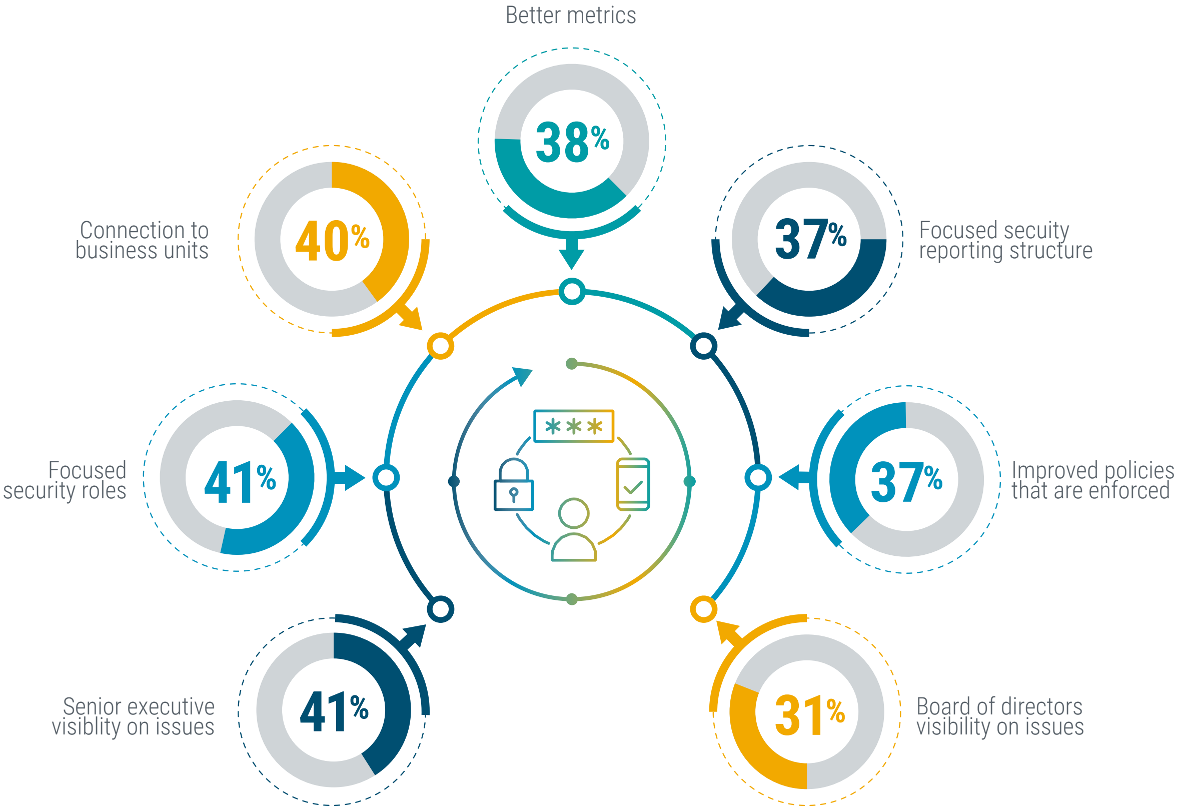
Why is it important?

Two-factor authentication provides an additional layer of security to the authentication process to gain access to devices or online accounts. If a user password is hacked, a password is not enough to gain access. Online service providers are beginning to enforce two-factor authentication to protect their users' credentials from being used by hackers who stole a password or used phishing campaigns to obtain user passwords. Insurance companies are starting to require two-factor authentication for everything or will not honor claims by parties not implementing two factor authentication. Furthermore, according to Microsoft, two-factor authentication can prevent 99.9% of attacks on your accounts.

Where can I find help?

Common 2FA examples include mobile device apps and SMS texts that generate a mobile device app such as Google Authenticator or Microsoft Authenticator or using SMS text that generates a code that is sent to the user. The use of mobile apps is generally considered a more secure method compared to SMS texts.

Actions to Improve Effectiveness of Security Resources



Network Assessment

What is it?

This is a process of reviewing local area networks (LANs) and wide area networks (WANs) to inspect assets to help identify all resources on the network and assist in following best practices and industry standards. Reports from network assessments are used to understand risk and to support improvements to the network and associated devices.

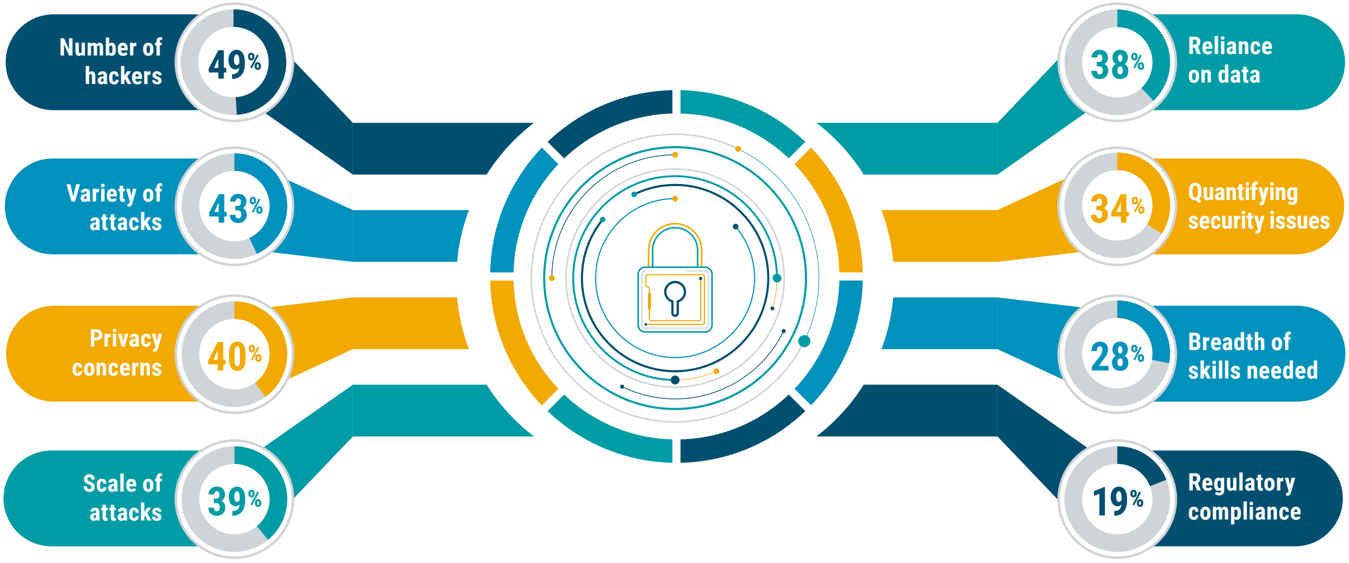
Why is it important?

In order to improve from a security perspective, it is valuable to know what needs to be needs to be improved. A network assessment is a key component of understanding what has to be managed. Regular network assessments help demonstrate due diligence and a focus on continual improvement.

Where can I find help?

Network assessment tools are plentiful in the market. Compare products to find the best option for your business.

Main Issues Driving Cybersecurity



DNS Security

What is it?

Domain Name System (DNS) security provides an additional layer of protection between an employee and the internet by blacklisting dangerous sites and filtering out unwanted content.

Why is it important?

With remote and distributed workforces and digital business transformation driving consolidation of networking and security functions to the cloud, DNS security is more important than ever. By using secure DNS servers both at home and at work, employees can avoid unnecessary risks and the potential for malicious attacks. DNS servers can also be another vector of attack because an attacker could identify a vulnerability and take over or redirect the domain name to somewhere else or spoof it completely.

Where can I find help?

There are numerous products available to perform DNS protection. Check with your peers, your security needs, and the capabilities of the products to select the best option for you.

Dark Web Monitoring

What is it?

Dark web monitoring is the act of monitoring the part of the internet that is accessed through a Tor browser. The dark web provides a layer of anonymity that attracts criminals who feel they can operate undetected. There are 2 million active users who connect to the dark web through the Tor browser every day. An estimated 2% to 5% of the global GDP is laundered on the dark web annually.

Why is it important?

Dark web monitoring is essential for the following key reasons: 1) The price for access to corporate networks increased by 61% in Q1 2020. 2 over Q1 2019) Cybercrime yields over $1.5 trillion in revenue per year. 3) Information on 267 million Facebook users sold in Q1 2020 for just $540. 4) In Q1 2020 alone, over 73.2 million new user records hit the dark web. 5) About 164 million user records from a dozen major companies were exposed in a single Q1 2020 dump. 6) 53% of organizations have had a data breach caused by third-party information theft.

While you can manually monitor the dark web by downloading a Tor browser and locating and joining various dark web forums, it isn't feasible or efficient to do this for several reasons. First, many dark web sites are hidden or unpublished to the public, and the search engine within the dark web does not function like the one on the surface web, like Google. Second, many cybercriminals are very careful who they interact with, so establishing yourself as a trusted entity on the dark web can prove challenging. MSPs should seek dark web monitoring tools to aid in these efforts, along with their own. These services dive deep into the corners of the dark web to look for potential risks to an organization. They'll monitor for new dark web threats to your systems and data 24/7/365 and quickly alert you to possible trouble, enabling you to stop cyberattacks before they start.

Where can I find help?

Dark web monitoring services are available from many vendors. As always, verify your requirements, business outcomes, and how it will integrate with your solution stack before selecting one.

Thank you to these contributing members of the CompTIA ISAO Cyber Fundamentals SME Workgroup for helping to make it happen.

- Bryan Hornung, Xact IT Solutions, Inc.
- Bob Paradise, Attain Technology, Inc.
- Sandy McGrath, Final Frontiers
- Matthew Lang, IND Corporation
- Helder Machado, Machado Consulting
- Frank Hannaford, CoreTech
- William Palisano, Lincoln Archives, Inc./LACyber
- Rich Szymanski, CMIT Solutions of Appleton
- Rick Monnig, TechSolutions, Inc.
- Ernest Dean, ERoboServices

And a VERY BIG thank you to the BLOKWORX team for their generous support and use of their intellectual property in the development of this paper.

CompTIA.org

Copyright © 2022 CompTIA, Inc.. All Rights Reserved.

CompTIA is responsible for all content and analysis. Any questions regarding the report should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.