WHITE PAPER

Advanced Cybersecurity for Managed Service Providers

Are you ready to take the next step in your cybersecurity?

This white paper is meant to help anyone seeking guidance—or maybe is overwhelmed by—implementing sound, best practice cybersecurity operations, technology, and behavior. Specifically, this paper addresses topics considered more "advanced," but still essential to a robust cybersecurity program. Paired with CompTIA's Fundamental Cybersecurity for Managed Service Providers, a more complete view of the aspects of cybersecurity MSPs serving small-to-medium businesses needs to understand and implement can be seen.

Each topic is expanded with a brief definition of what it is, why it is important to address, and to whom does the topic apply. The following topics are covered by this white paper:

- IT risk management
- Risk assessment
- Change management
- Access control
- Internet of things
- Encrypted configuration backups
- Data encryption and digital certificates
- Business continuity disaster recovery
- Incident response
- Threat hunting
- Security information and event management (SIEM)

All graphics in this paper are from:

CompTIA's 2021 State of Cybersecurity and CompTIA's IoT Industry Trends Analysis.
https://connect.comptia.org/content/research/cybersecurity-trends-research
https://connect.comptia.org/content/research/iot-industry-trends-analysis

IT Risk Management

What is it?

IT risk management is the continual process of managing the risks that come with the ownership, operation, adoption, and use of IT assets as part of your MSP. There are five essential steps of a risk management process:

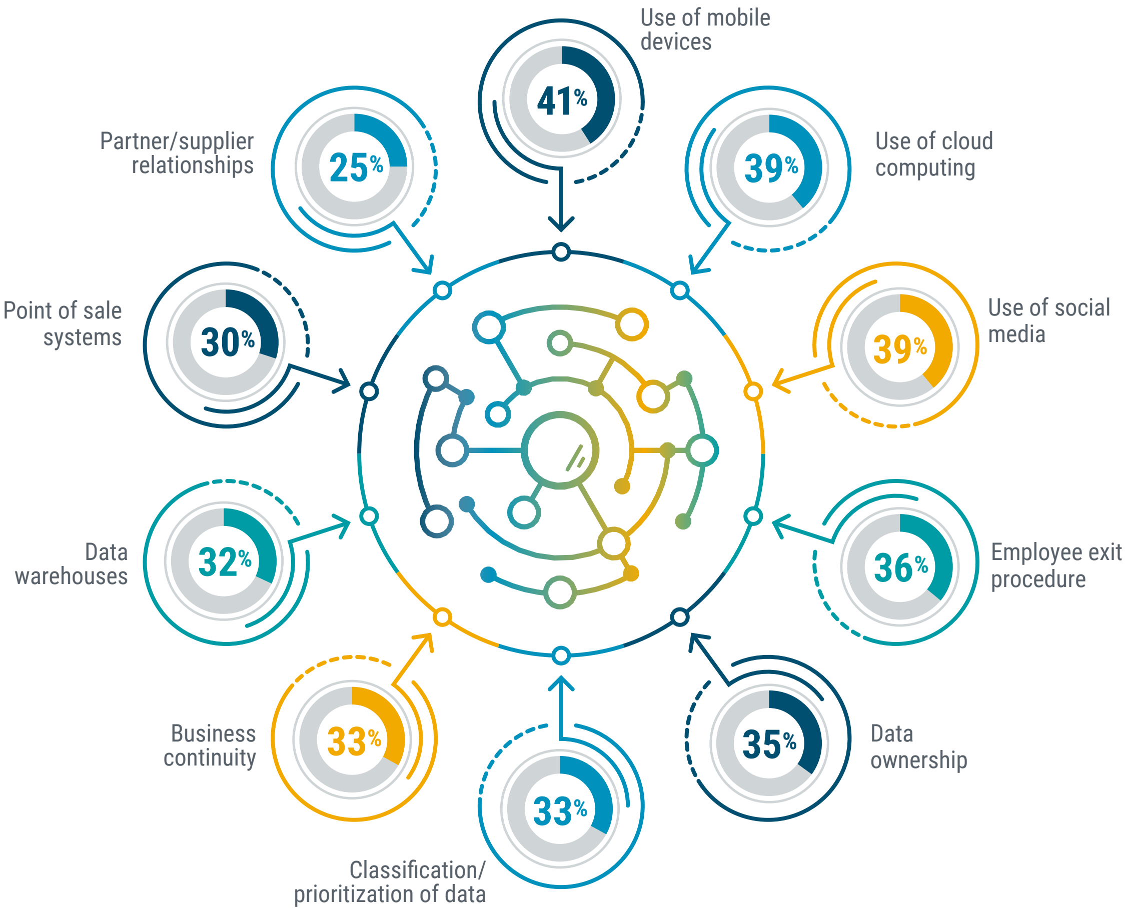
1. Identification
2. Analysis
3. Evaluation and ranking
4. Treatment
5. Monitoring and review

Why is it important?

Managing the risks of your vendors, suppliers, service providers, and contractors is called third-party risk management. As an MSP, it is a very important part of your overall risk management process. Each tool that you use, every piece of software that is installed on your computers, every vendor you use must go through the risk management process.

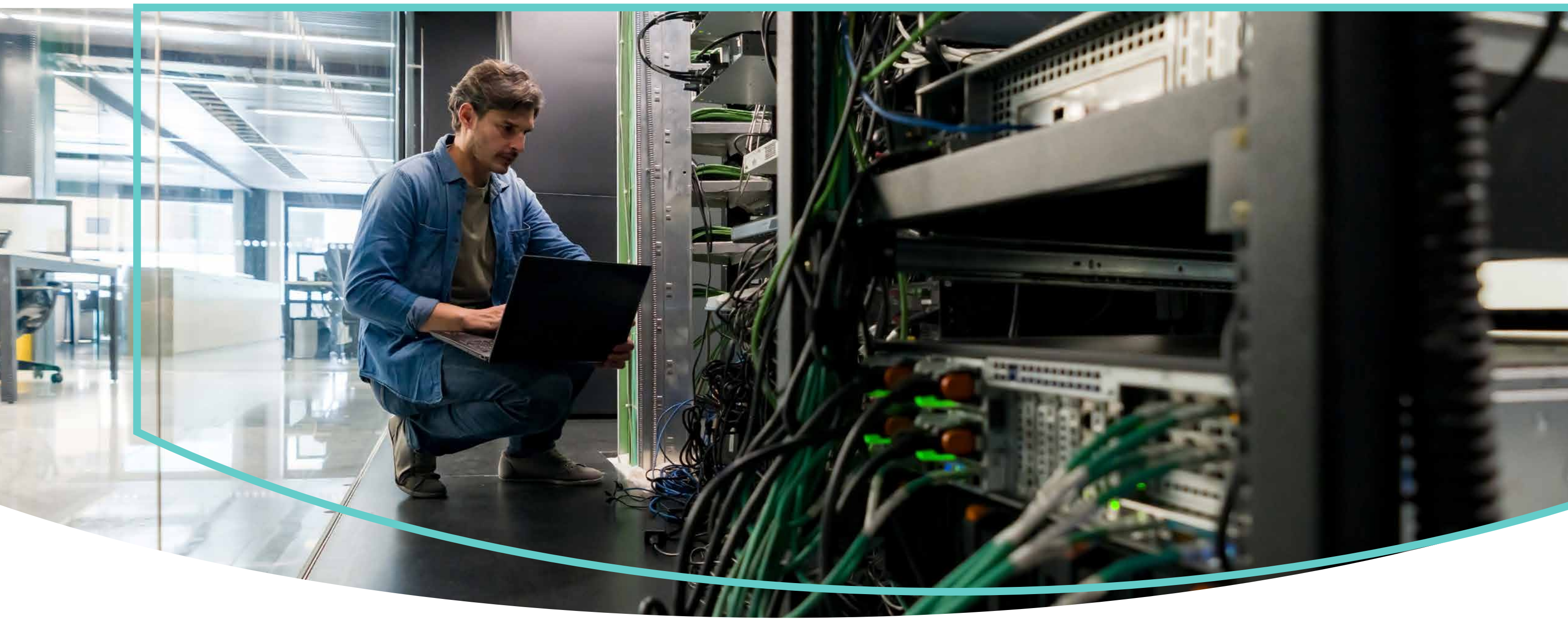
Each company has a different level of risk tolerance and a different set of company objectives. The main goal of risk management is not to eliminate all risk, but to get that risk down to a tolerable level for your MSP based on your goals and budget. Risk management is an ongoing process of evaluating and re-evaluating the risks.

Components of Risk Management



Who is involved?

There are many resources and frameworks available online for risk management. The National Institute of Standards and Technology (NIST) has issued the cybersecurity framework and special publications on third-party risk management and supply chain risk management. There are also companies and consultants that will work with you on your risk management program.



Risk Assessment

What is it?

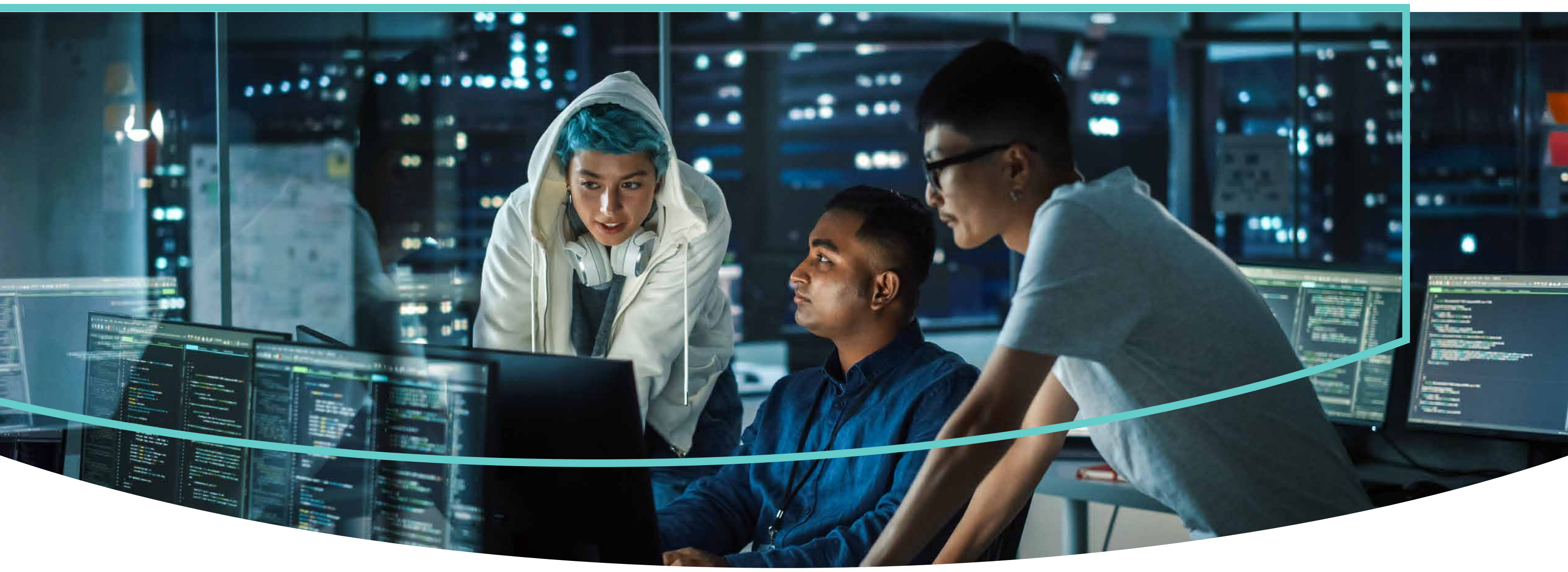
A cybersecurity risk assessment identifies the various information assets that could be affected by a cyberattack (such as hardware, networks, systems, computers, customer data, company data, and intellectual property), and then identifies the various risks that could affect those assets.

Why is it important?

A cybersecurity risk assessment is crucial in your risk management process by revealing vulnerabilities. This process ensures that your security measures are adapted to current and future potential risks, preventing adverse events like data loss and data breaches.

Who is involved?

The assessment should cover all systems and devices regardless of their physical location. Consider all computers, laptops, local and cloud networks, data storage, transmission, and processing systems, and other potential points of vulnerability to gain a more robust understanding of cybersecurity risk.



Change Management

What is it?

Change management is the process used by an organization to outline and document what procedure(s) should be adhered to in a given scenario or problem. These details help provide the guardrails for addressing changes of all magnitudes in the organization.

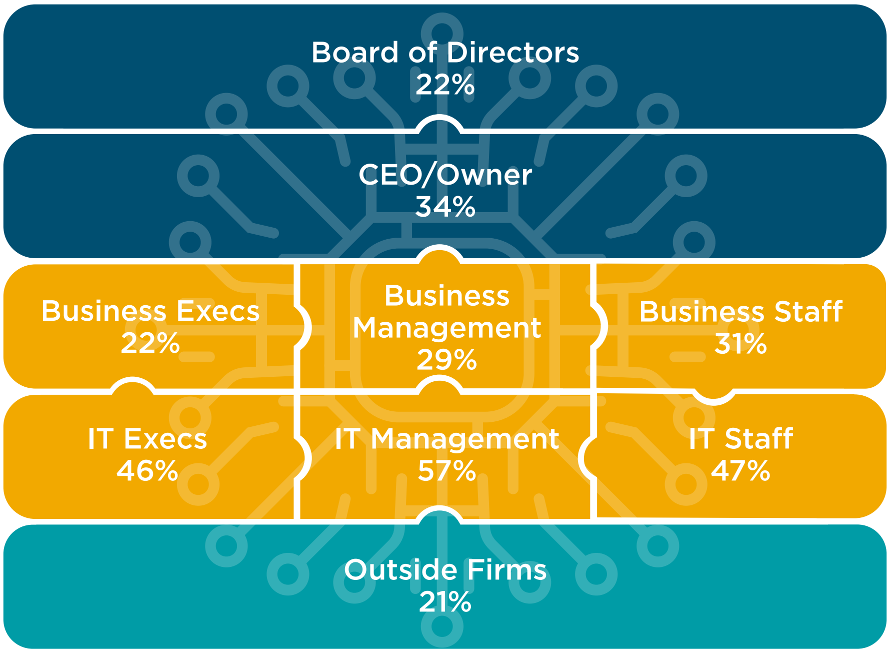
Why is it important?

Implementing a good change management process improves the company workflow, which as a by-product enhances efficiency and output. Having a process or standard operating procedure (SOP) allows for a seamless transition among employees with reference to resolving an issue. Also, as a documented process, it is easier to modify if it is determined that an update is needed.

Who is involved?

Since change management is a global initiative, all stakeholders are impacted because these procedures outline how various processes in the business should be handled. A failure to follow these guidelines could result in effort duplication and financial losses, for example. The more robust a plan you have developed, the less individuals involved will have to deviate from the norm, which will aid in the tracking process.

Groups Involved in Cybersecurity Chain



Access Control

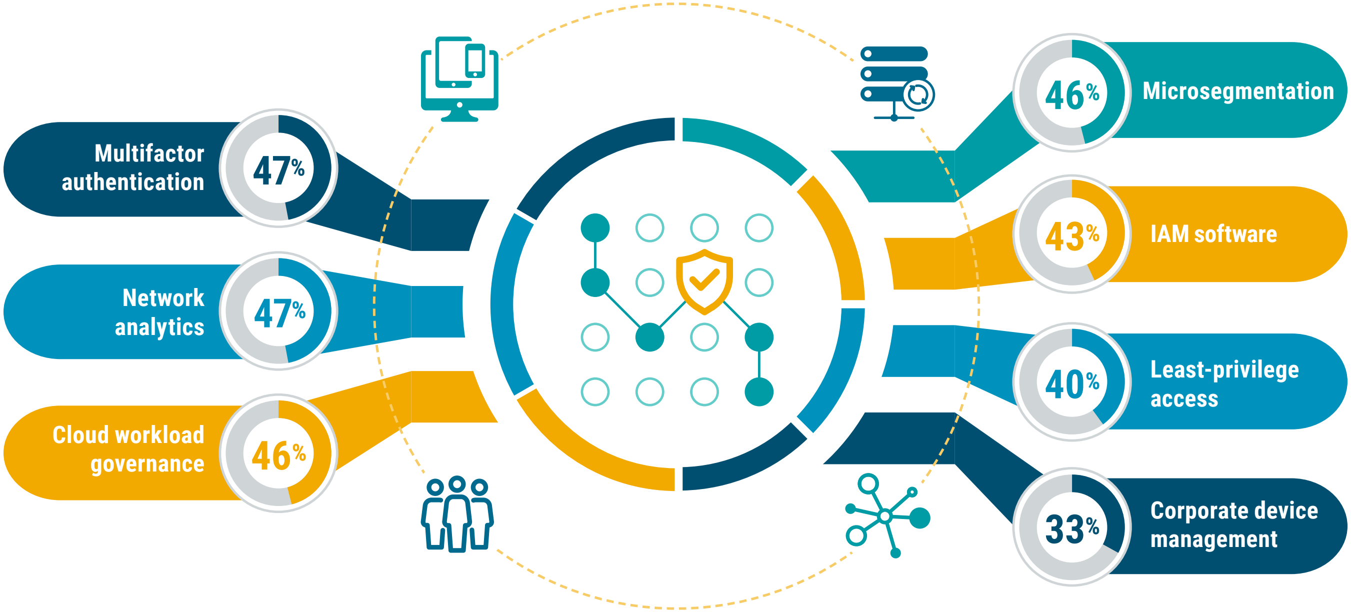
What is it?

Access control is a security practice that determines who or what can view or utilize data or resources in a business. The two main components of access control are physical and logical systems. These two systems are crucial to maintaining security and compliance programs to protect confidential information, such as customer data, intellectual property, financial information, etc.

Access control for the logical environment consists of things like login or security restrictions, limiting what user accounts can view or see to the things necessary to complete their jobs. Access control for the physical environment consists of access cards, badges, biometric scanning, etc., to limit the physical access someone has to a building, office, room or other space.

Zero trust, the methodology of having the least access required for your role or job, is a crucial example of access control. Zero trust includes ring-fencing applications, employees only having access to data or physical environments necessary to complete their role, and having no administrator access to computers, systems or servers unless necessary. Those elevated privileges should be tracked and set to expire the moment a task or job is complete.

Components of Zero Trust Framework



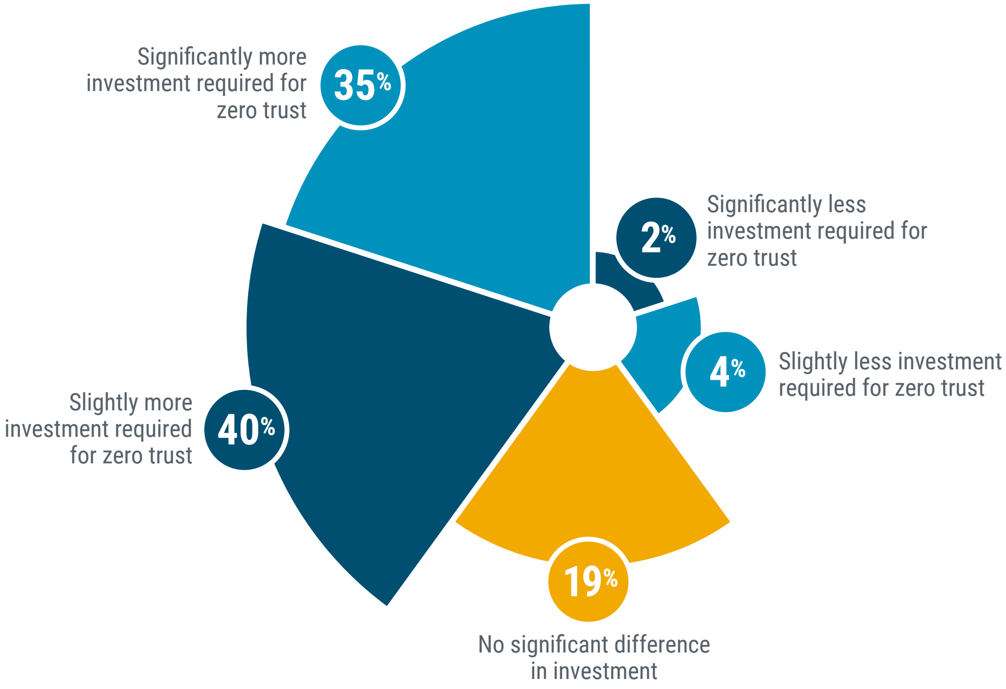
Why is it important?

Access control must be in place for the security and protection of a business. Access control will minimize the security risk of unauthorized services or people accessing physical and virtual aspects of your data or business. Access control documentation and logging are essential for forensic audits or disaster recovery situations so you can pinpoint weaknesses or factors in a breach.

Who is involved?

MSPs should work with their clients and their own internal networks to determine the risk and what levels of zero trust may be necessary.

Investment Required for Zero Trust Framework



Internet of Things

What is it?

Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that have unique identifiers (UIDs) and have the ability to transfer data over a network without human involvement. An estimated 35.82 billion devices were installed at the end of 2021 worldwide and by 2025, it is estimated that there will be 75.44 billion devices, according to Statista.

Why is it important?

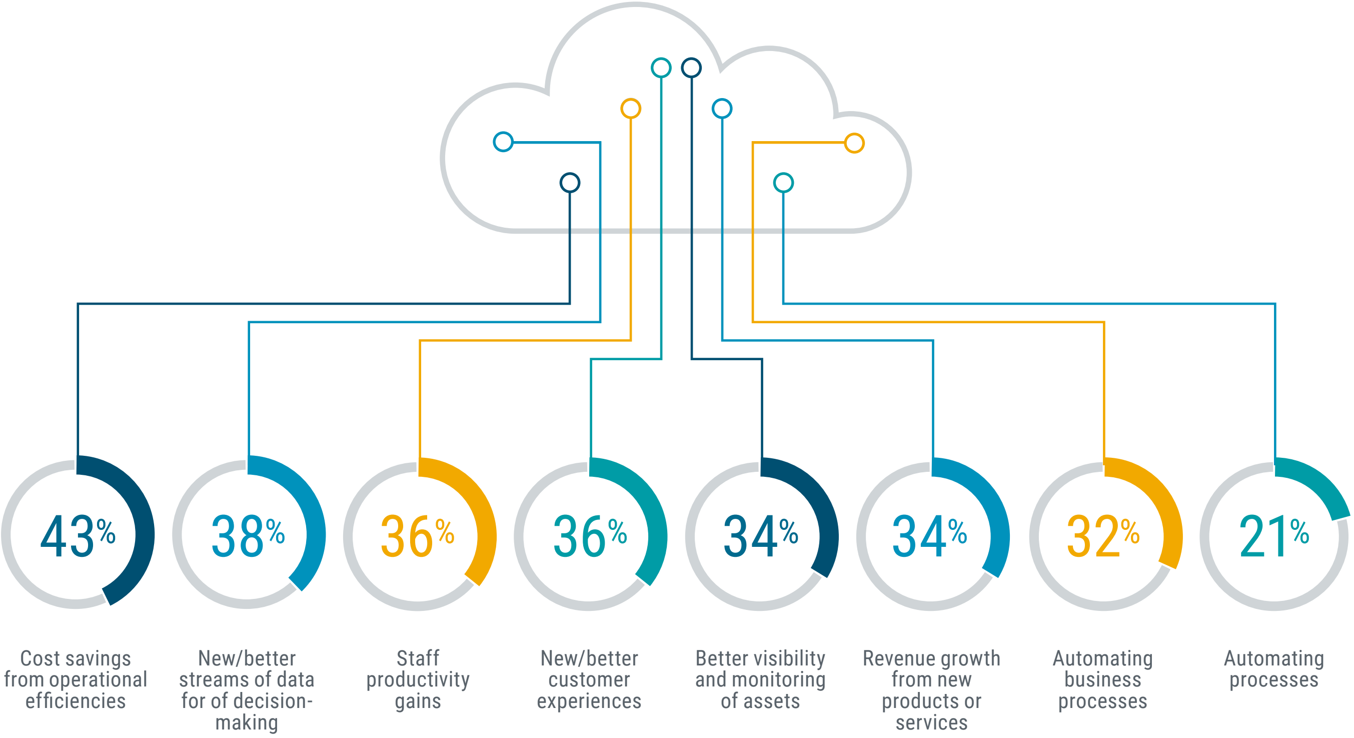
IoT is here, for better or worse. It can cut down on waste and improve service delivery, making it less expensive to manufacture and deliver goods and services. On the downside, as the number of IoT devices increases so does the importance of securing these devices. One of the most important things a home or business can do with these devices is segment their networks to protect private information and place IoT devices on separate networks.

Who is involved?

IoT devices are in almost everything we use in our day-to-day lives. Used in automobiles, home appliances, medical, agriculture, physical security, mobile devices, home entertainment and more, they have grown rapidly over the last 10 years.

Network segmentation for IoT devices is recommended to run on parallel networks. Network administrators should work with C-level executives to determine the best segmentation in order to not disrupt operations. For more information about implementing IoT solutions, check out CompTIA's 6 Layers of an IoT Solution.

Potential Benefits of IoT



Encrypted Configuration Backups

What is it?

Today's networks are expanding at a rapid pace and becoming increasingly complex. Large networks add and subtract hosts, servers, routers, switches, appliances, miscellaneous hardware, etc., continuously. Network administrators need tools to streamline network configurations and backing up those configurations is a must. Automated detection and backup of new or unprotected assets should be standard. Like all other backups, a best practice is to encrypt these backups at the source (i.e., AES-256 bit) and stream to an off-site repository. By encrypting configuration backups, organizations make it impossible for cybercriminals to access the sensitive information contained in them without depriving themselves of the ability to quickly integrate new assets and recover from configuration problems, regardless of cause. Restorations involve backed-up files and configurations delivered back and decrypted at the source.

Why is it important?

To operate correctly and efficiently, entire networks and device configuration settings must be optimized, which often takes time. For production networks, costs for an outage add up fast. Immediate restoration of an entire production network (or segment) is critical. Having network configurations protected, off-site and quickly restorable may make the difference in an enterprise surviving an outage.

Who can help?

An MSP must manage critical assets via encryption to minimize risk of losing that information. Numerous providers of this service are available across the market. Compare products and vendors to find the best fit for your tech needs.

Data Encryption and Digital Certificates

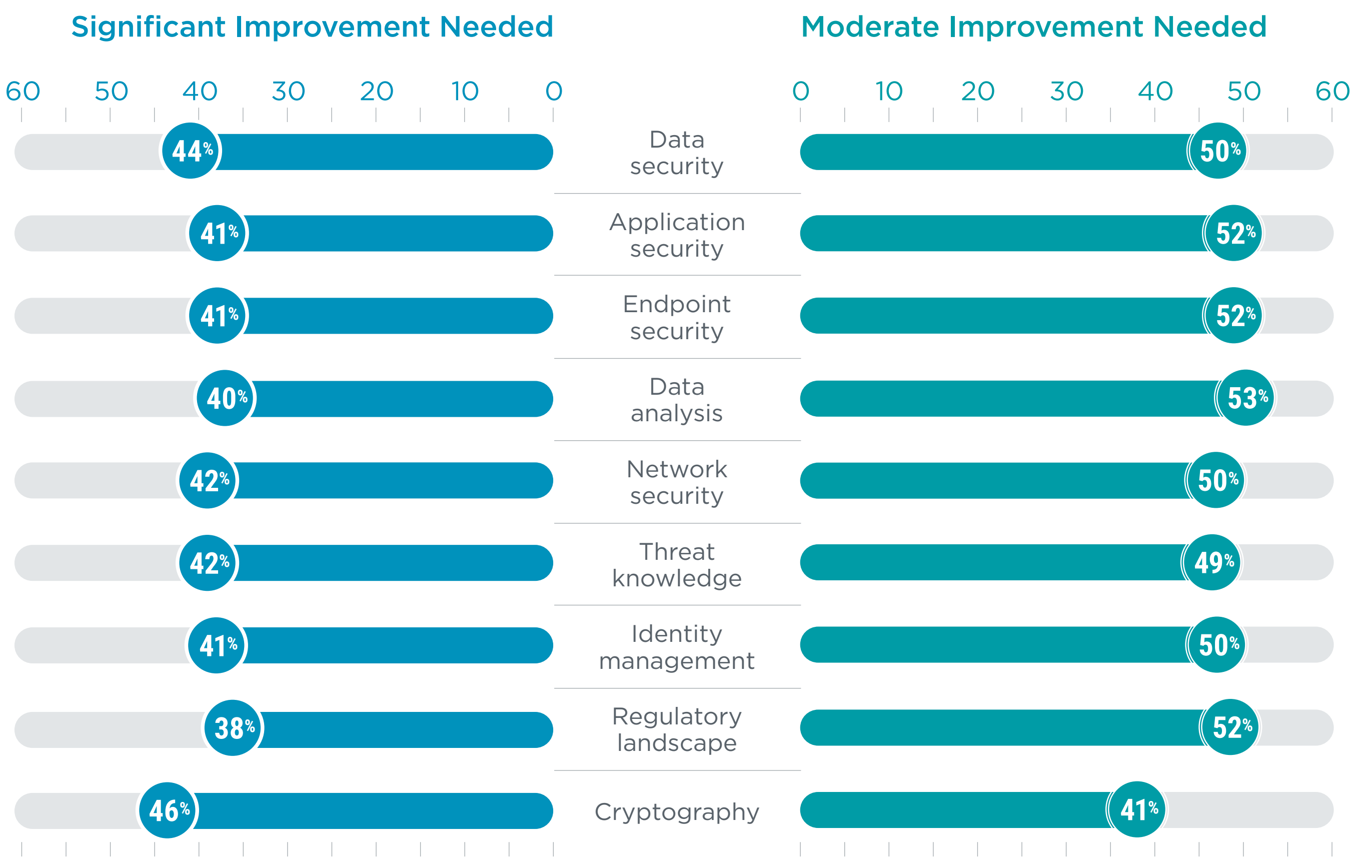
What is it?

Data encryption is a security operation where data is put through a process that makes it unreadable unless a specific key to decrypt it is known. It is the underpinning of the “s” in https and generally allows our world to communicate in a more secure manner.

Encryption is seen primarily in two ways: data at rest and data in transit. Data at rest is data on a storage device (hard drive, flash drive, tape, etc.), while data in transit is data moving from device to device (https, SSH, SFTP, etc.).

In the MSP world, certificates are used in encryption and decryption. They take two primary forms: symmetric and asymmetric. A typical symmetric key can be used to encrypt and decrypt. Asymmetric keys are either public or private; with a private key typically used to encrypt, and a public key to decrypt. There are benefits and drawbacks to each type of key and they can even be paired together—for example, transferring a symmetric key to another party using an asymmetric encryption—so be sure to weigh the exposure risks when encrypting.

Need to Improve Cybersecurity Skills



Why is it important?

Understanding encryption and certificates is very important to understanding how communication inside and outside of a network functions—from websites to copiers to server message block (SMB) file shares. These items are seen as industry standards, almost every vendor in the technical space uses and understands these concepts in the practice and products.

Who is involved?

Network administrators and IT decision makers need to identify critical assets and make sure encryption is in place. Note that cryptographic skills were the area where the most significant improvement was needed in the chart on page 11.

Business Continuity Disaster Recovery (BCDR)

What is it?

A holistic business continuity disaster recovery (BCDR) approach requires thorough planning and preparation. BCDR professionals can help an organization create a strategy for achieving resiliency. Developing such a strategy is a complex process that involves conducting a business impact analysis and risk analysis and developing BCDR plans, tests, exercises, and training.

Planning documents, the cornerstone of an effective BCDR strategy, also help with resource management, providing employee contact lists, emergency contact lists, vendor lists, instructions for performing tests, equipment lists, and technical diagrams of systems and networks.

Why is it important?

The role of BCDR is to minimize the effects of outages and disruptions on business operations. BCDR practices enable an organization to get back on its feet after problems occur, reduce the risk of data loss and reputational harm, and improve processes while decreasing the chance of emergencies.

However, BCDR is broader than IT, encompassing a range of considerations—including crisis management, employee safety, and alternative work locations.

Business continuity and disaster recovery are closely related practices that support an organization's ability to remain operational after an adverse event. The goal is to limit risk and get an organization running as close to typical as possible after an unexpected interruption.

Who is involved?

Developing a BCDR plan typically starts by gathering BCDR team members and performing a risk analysis and business impact analysis. The organization identifies the most critical aspects of the business and how quickly and to what extent they must be running after an incident. After the organization writes the step-by-step procedures, the documents should be consistently tested, reviewed, and updated.

Although certain aspects of the process involve select members of the organization, it's vital that everyone understands the plan and is included at some point. The program should also encompass third parties and the services they provide. For example, a business might rely on parts that a third party supplies, so the relationship should be documented in the BCDR plan. Such outside entities must be kept in the loop to understand how the plan will work.

Incident Response

What is it?

Incident response is an organized approach to addressing and managing the aftermath of a security cyberattack, also known as an IT incident, computer incident, or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

Why is it important?

It is essential to have an incident response plan. Similar to a BCDR plan, incident response should be planned and tested. Testing should start with tabletop exercises, and organizations should work toward full-blown incident response tests to fully mature their process. Organizations that plan and test their incident response plan with stakeholders are far more likely to survive an incident than organizations that do not.

Who is involved?

Incident response activities are conducted by an organization's computer security incident response team (CSIRT)—a group comprised of the MSP, internal information security and IT staff, and C-level members. A CSIRT may also include representatives from the legal, human resources, public relations departments, or outside vendors. The CSIRT follows the organization's incident response plan, a set of written instructions that outline the organization's response to network events, security incidents, and confirmed breaches.

For assistance in getting started with an incident response plan, check out CompTIA's Data Breach Response Planning Guide or any number of templates and guidelines available.

Threat Hunting

What is it?

Threat hunting is the practice of proactively searching for cyber threats that are undetected in a network. Cyber threat hunting digs deep to find malicious actors in environments that have slipped past initial endpoint security defenses. These threats are often the most difficult to find and therefore the most damaging.

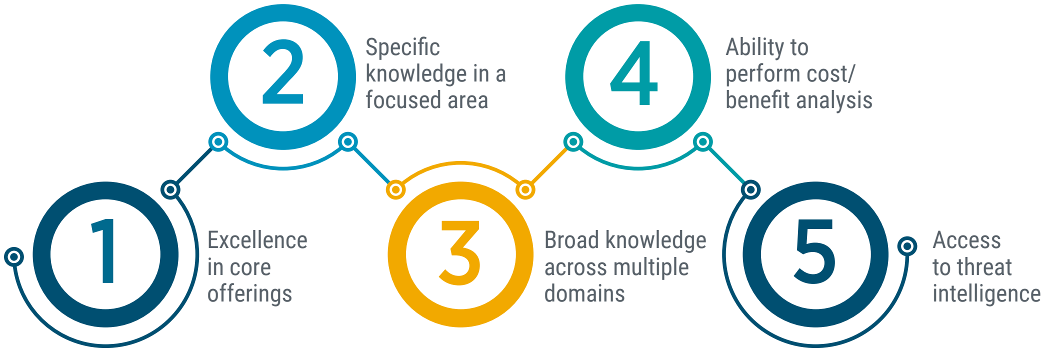
Why is it important?

Threat hunting can be engaged for many reasons. A new vulnerability or attack that is identified could lead to threat hunters looking to see if anything is found in the environment. An indicator of compromise (IOC) could be detected, and systems and networks need to be investigated to find if there is a bigger issue.

Who is involved?

MSPs may not have the necessary skills in-house to conduct threat hunting. It is recommended for MSPs to look at partnering for these services.

Important Criteria for Third-Party Cybersecurity Firms


1 Excellence in core offerings

2 Specific knowledge in a focused area

3 Broad knowledge across multiple domains

4 Ability to perform cost/benefit analysis

5 Access to threat intelligence

Security Incident & Event Monitoring (SIEM)

What is it?

Security incident and event management (SIEM) provides real-time analysis, monitoring and alerting on security logs generated by applications, hosts and network devices. SIEM also aggregates and correlates data from these logs and provides alerting so action can be taken if it is a security threat. SIEM solutions can be purchased as software, appliance or managed service solution.

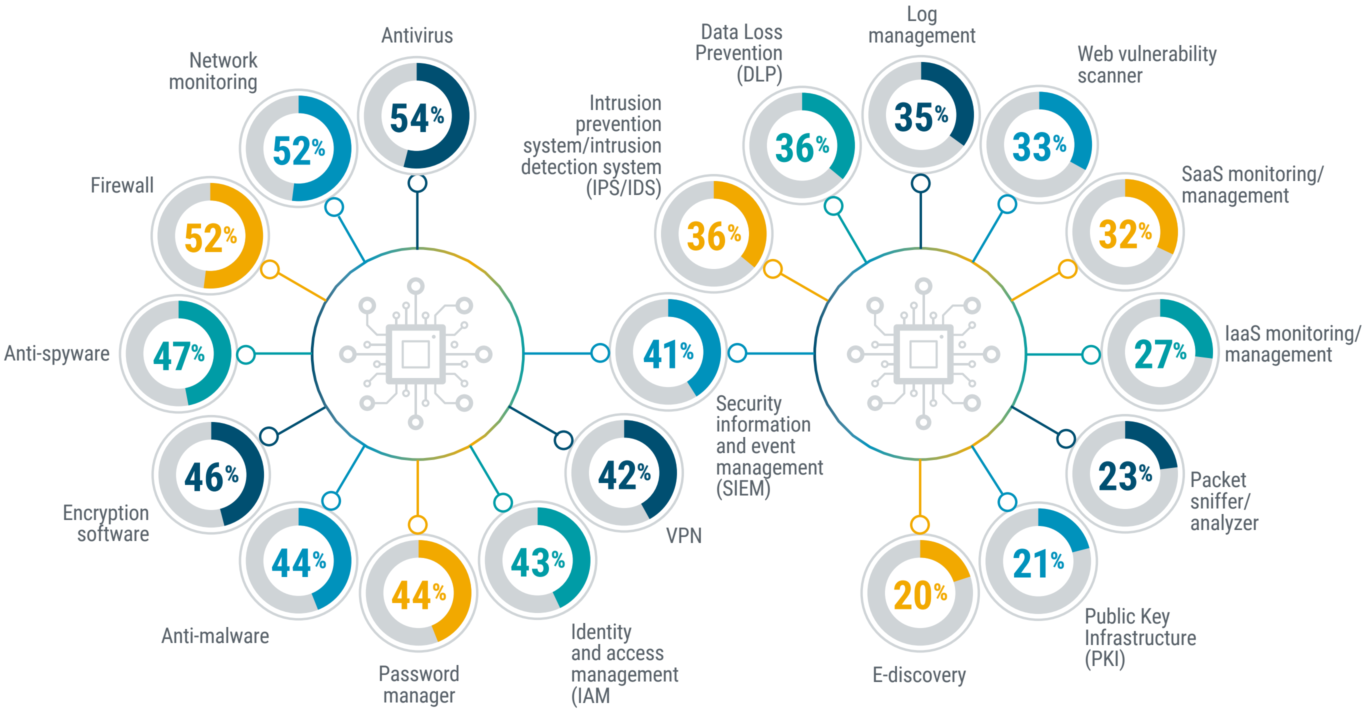
Why is it important?

When proper incident management measures are in place, damage can be contained, and risk reduced. SIEM also helps organizations quickly identify security threats.

Who is involved?

Some industries such as defense contractors, medical or other highly regulated industries are obligated to report on log activity, security event logs and other information as part of showing compliance to HIPAA, CMMC or other laws. MSPs may not have the necessary skills in-house for SIEM. It is recommended for MSPs to look at partnering for these services.

Cybersecurity Products in Use



Additional Resources

The CompTIA Information Sharing and Analysis Organization (ISAO) can help you stay abreast of the latest threats, market trends, and connect with like-minded cyber-first professionals and is included in CompTIA membership.

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

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

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

CompTIA®

Connect.CompTIA.org

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.