
CYBERSECURITY
ESSENTIALS
FOR
HEALTHCARE
BlueGuysIT.com
TECHNOLOGY SOLUTIONS
OWN IT. SECURE IT. PROTECT IT.


BlueGuysIT.com
TECHNOLOGY SOLUTIONS

Contents

OWN IT.
SECURE IT.
PROTECT IT.

Introduction

Cybercrime and cyber attacks are becoming more prevalent with each passing day. Over half of small and medium businesses (SMB) have reported being the victims of cybercrimes. Every day, there are new headlines about data breaches, hackings, cyber attacks, and various forms of crimes against businesses. In a survey, over two-thirds of the participating businesses had suffered at least one cyber attack, while one-third had experienced the same in the last 12-months.

66% of small business are very concerned about cyber security risk.

Cybercrime is a significant threat to businesses. It can lead to disruption of operations, breach of business and customer data, unauthorized access to networks, and more. The average cost of a data breach for a small-to-medium business is a staggering $149,000. On top of that, 80% SMBs worry about becoming the target of cybercrime in the next six months.

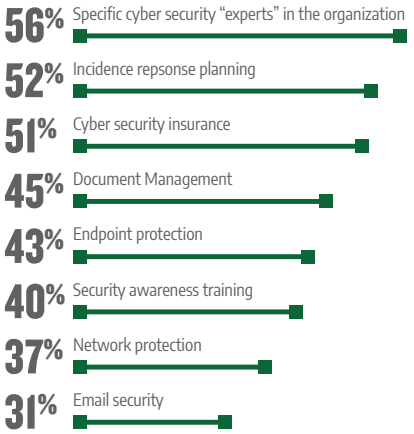
Additionally, cyber-attacks remain a worry whether we are talking about the cloud or through emails.

Many governments have moved to the cloud but are looking for better ways to protect their data. A part of that is to increase collaboration between intelligence and law enforcement agencies worldwide to tackle crime.

The popularity of smartphones and the increased use of apps also pose a significant risk to mobile security. Consumers use apps to input sensitive information like personal, financial and banking information. These apps will need to evolve with new technologies to continually find new ways to resist attacks and data leaks.

Additionally, as more and more applications are moving to the cloud, malicious actors are getting better at evading detection by standard security measures and protocols. The act of distributing ransomware and holding sensitive data is on the increase as organizational data is going beyond the control of the company.

Percentage of Organizations who **DO NOT HAVE** these critical Cyber Security Solutions in place.



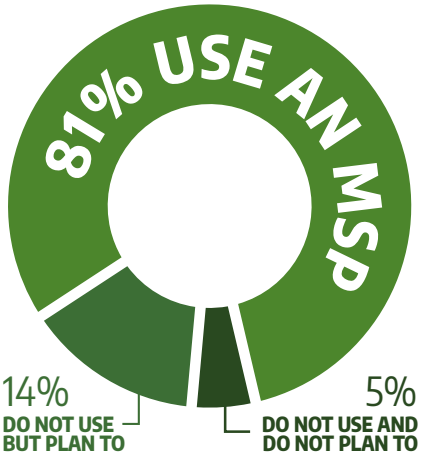
51% of small businesses say they are not allocating any budget to cyber security.

Evolving from simple malware, ransomware has become more sophisticated and efficient. Cybercriminals are now targeting the local backups, which foil the efforts of the security staff to restore encrypted data.

This threat is no longer limited to local networks, ransomeware attacks remain a problem in cloud environments.

Email remains the most favored method of cybercriminals. Over 91% of attacks are initiated by email. Traditional antivirus programs cannot identify the

Organizations' use of an MSP



phishing attacks employed by hackers.

Malware can be delivered and initiated on a system without the user's knowledge, possibly for a long time. One example of such an attack was the one dealing with the US Democratic National Party, where cybercriminals took control of their system.

There is a need to increase the pace of development for holistic solutions to cybercrime. 75% of businesses in the survey above feel they need to put more emphasis on cybercrime prevention.

However, there is a large gap between reality and expectation. Most businesses are under educated when it comes to the nuances of cybercrime. This creates an adverse situation as the organizations are not able to protect themselves from cybercriminals. Without a plan, organizations don't know how to react and what steps to take when their network and systems are compromised.

Here the role of managed IT service providers (MSPs) becomes crucial. MSPs can guide SMBs on the right path and help them stay protected from the increased incidents of cybercrime. MSPs can educate clients about the need for a holistic security solution and the evolving cybercrime landscape. MSPs should also provide SMBs with a complete collection of security solutions so that they can stay protected and minimize risk.

MSPs can help bridge the gap between the current level of protection and the optimum level desired by businesses. Enterprises are recognizing this fact and joining hands with MSPs to eliminate and prevent cyber-attacks and threats.

Eight out of ten surveyed SMBs are working with an MSP, and four of them want to keep working with their current security partners. Three companies out of ten plan to switch to a different MSP in the coming months. 12% SMBs that don't work with an MSP plan to partner up with one within the next twelve months.

9 in 10 employees say their organization would consider switching to a new MSP if they offered a solution that met their needs.

When asked what benefit they expected to see from using an MSP, fifty percent of SMBs said increased security, even if they had outsourced their Cyber Security.

MSPs can be the ideal partner of SMBs to fight cybercrime, as 62% of companies don't have the required in-house skills. The managed IT teams can develop and implement security measures and even layout a recovery plan for probable attacks. The MSP helps the organization stay on top of cybersecurity trends, and enables it to counter evolving cyber threats with full confidence.

An MSP can be your partner in safety and protect you from threats or attacks.

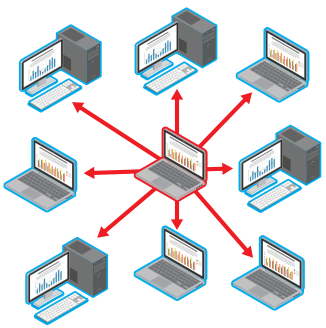
PHISHING & SPEAR FISHING

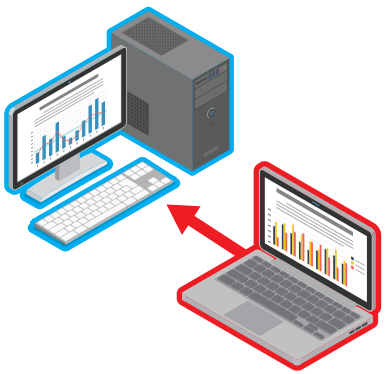
Spear phishing or phishing involves sending emails with malicious attachments designed to steal personal information. The phishing attack can also lead the victim to an illegitimate website that steals passwords, credit card details, business information, and other sensitive data. A phishing attack uses technical trickery and social engineering to achieve its goals. Attackers employing phishing choose their targets carefully and take on the guise of a trusted source that victims are less likely to question. The attackers also use personalized messages that make the emails look relevant and trustworthy. As a result, SMBs might find it challenging to protect themselves from spear phishing attacks.

Phishing is one of the most common forms of cyber threats.

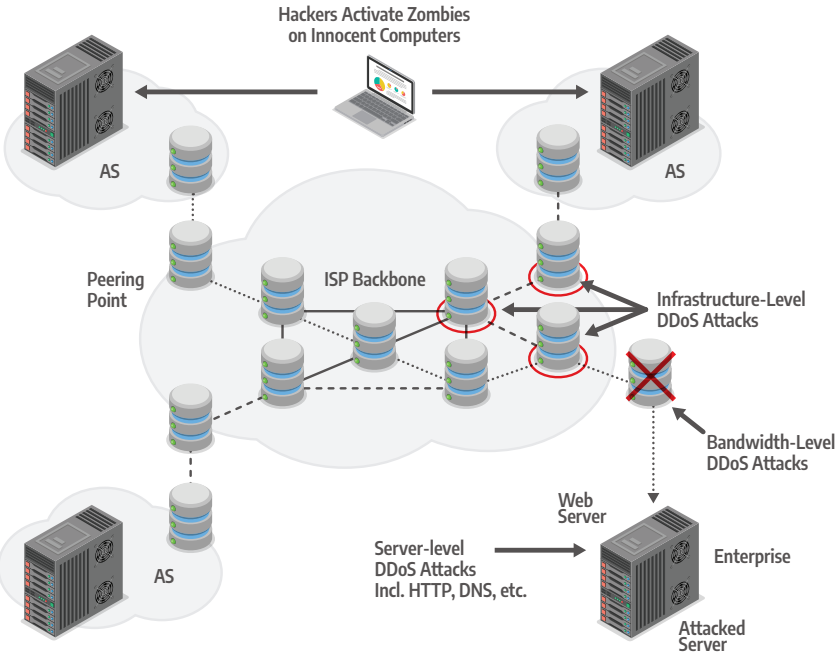
In 2020, phishing was responsible for more than 80% of reported security incidents.

	PHISHING	SPEAR PHISHING
APPROACH	Spray & Pray	Targeted Attack
TARGETING	Broad & Automated	Specific employee and/or company
HACKING LEVEL	Not Very Sophisticated	Requires Advanced Techniques
THE ATTACK	Usually Obvious	Harder to Detect
WHAT THEY'RE AFTER	Usernames, Passwords, Credit Card Details, etc.	Confidential Information, Business Secrets, etc.





AVERAGE COST OF A DDOS ATTACK $20-40K



DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

Distributed Denial-of-service (DDoS) is an attack that targets the resources of a server, network, website, or computer to take it down or disrupt services. DDoS attacks generally have a host system that infects other computers or servers connected to the network. DDoS attacks overload a system with constant flooding of connection requests, notifications, traffic. As a result, the system denies service requests by legitimate users. DDoS attacks don't benefit the attacker directly as they don't steal any information. It just compromises the systems so that they can't function properly. Nonetheless, DDoS attacks can be damaging for businesses as it can halt operations and result in damages worth thousands of dollars.

Between January 2020 and March 2021, **DDoS attacks increased by 55%**

MAN-IN-THE-MIDDLE (MITM) ATTACK

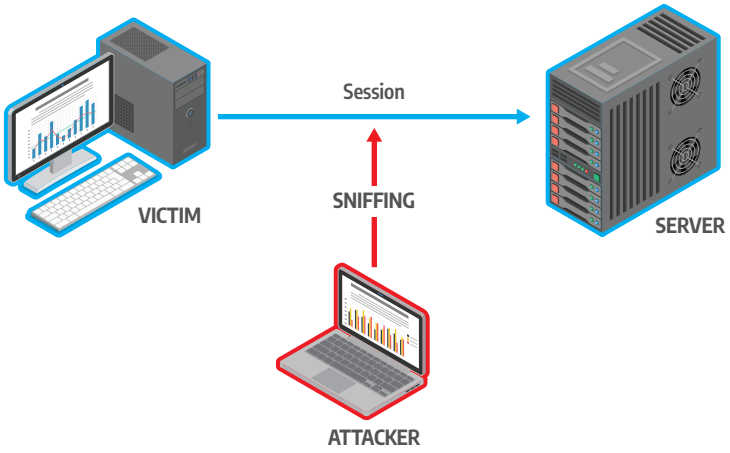
A MitM attack occurs when a hacker inserts themselves between the communications of a client and a server. Here are some common types of man-in-the-middle attacks:

Session Hijacking

Cybercriminals use session hijacking to gain control of the victim's sessions and get access to resources or data. The most common method is IP spoofing, where the hijacker uses the IP of the trusted client to avail unauthorized services from a server or application.

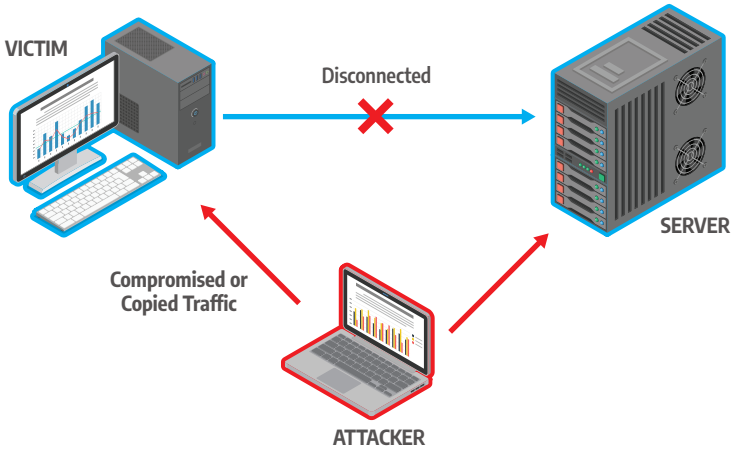
More than one in four small businesses have no security plan at all.

STEP 1: Hijacking the Session



95 PERCENT OF HTTP SERVERS ARE **VULUNERABLE** TO **MitM** ATTACKS

STEP 2: Assuming the Victim's IP Address



Macro viruses

Macro viruses target the initialization sequence of an application to compromise programs such as Microsoft Excel or Word.

Trojans

Trojans are non-replicating viruses that gain unauthorized access to a system. Trojans often camouflage themselves in the form of legitimate software.

System or boot-record infectors

These infectors attach to executable codes residing in parts of a disc. Boot-record infectors can connect to a hard disk's Master Boot Records and even boot sectors of USB flash drives. The infectors are initialized when someone boots using the compromised disk or drive.

Polymorphic viruses

Polymorphic viruses replicate endlessly to sabotage systems. They use dynamic encryption keys every time to avoid detection.

Stealth viruses

Stealth viruses hide under the guise of system functions. They also infect your computer's defenses to stay undetected.

File infectors

File infectors find their way in your system through executable codes like .exe extensions. The infector becomes active when you access the .exe file or the executable code.

Logic bombs

Logic bombs are pieces of malicious codes that get initialized when predefined conditions are met. Attackers can program logic bombs to serve a range of purposes.

Worms

Worms don't need a host file to propagate themselves on a network or system. They are self- contained forms of viruses.

Droppers

Droppers help viruses find their way into your networks and systems. Most often, your antivirus will not detect droppers as they don't contain the malicious code- they just lead to it!

Ransomware

Ransomware can take the form of any virus that holds a victim's data hostage for ransom. Ransomware attacks often encrypt data or files and demand money in exchange for decryption keys.

66 days

The number of days to discover a cyberattack

MALWARE ATTACK

Malware or malicious software is designed for compromising a system for a purpose. A user can unknowingly download malware that infects a system and replicates itself. Malware can be designed to act in many ways, just like software. Some popular types of malware include:

1. Macro viruses
2. Trojans
3. System or boot-record infectors
4. Polymorphic viruses
5. Stealth viruses
6. File infectors
7. Logic bombs
8. Worms
9. Droppers
10. Ransomware

600%

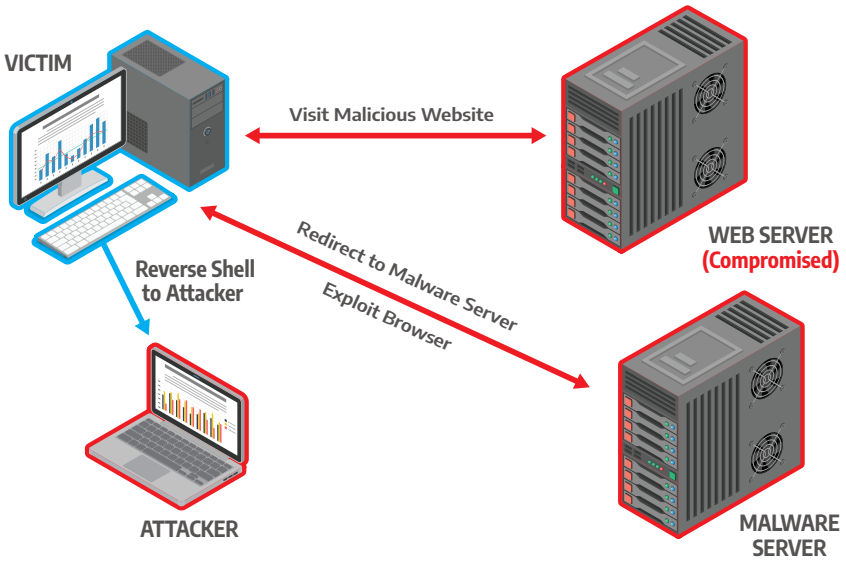
Increase in Cyber Crime DueTo COVID-19 Pandemic

DRIVE-BY ATTACK

Drive-by attacks use various online resources to compromise a user's system. The malicious code can be inserted in internet ads, HTTP or PHP codes on websites, or even applications. Contrary to other forms of cyber attacks, a user doesn't have to do anything to initialize the malicious software or virus. A single click on a pop-up window or website link can do the job!

Drive-by attacks are increasingly used to spread viruses and malware. The attacks take advantage of security vulnerabilities in apps or websites to exploit victim systems. These include not updating the app, flaws in security patches, bugs, and more.

The attacks also run in the background and are not visible to the user. As a result, you can't take any concrete steps to identify incorrect codes. Only being proactive can help businesses protect themselves from drive-by attacks.



92 PERCENT
of Malware is Delivered by Email.

ONE HALF
of all Cyber Attacks Specifically Target Small Businesses.

IN 2018 HACKERS STOLE **160 000 000** PERSONAL RECORDS.

73 PERCENT
of Passwords are Duplicates.

PASSWORD ATTACK

Password attacks enable cybercriminals to gain unauthorized access to user accounts and networks. Someone in your office can just guess or look around your desk to steal your password. That's why it's always recommended not to write down your passwords. Attackers may also spy on your network, use decryption tools, and use brute force to break your passwords.

A range of precautions can help save you from password attacks. You can program your system to lock accounts after a few wrong passwords. Using two-step authentication is also an excellent way to keep your accounts safe from prying eyes.

98 PERCENT
of Cyber Attacks rely on Social Engineering.

5 Crucial Elements of an Effective Cyber Security Program:

1. Offence Informs Defense
Learning and acquiring knowledge from actual attacks that compromised your system can lead to effective and practical defenses.

Your defense should be built only on controls that have proven successful in preventing real-world attacks for the best results.

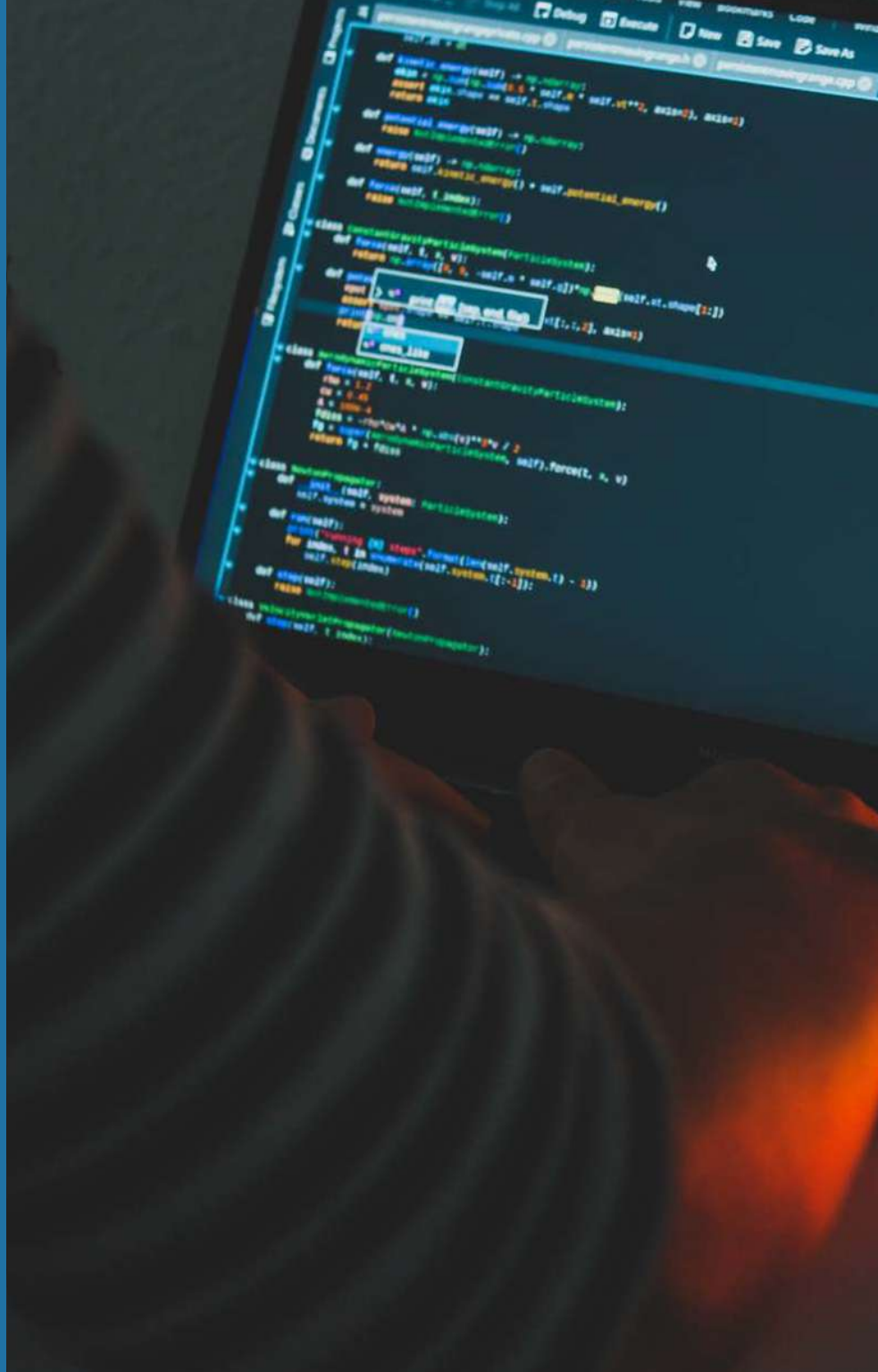
2. Prioritization
Businesses should only focus on controls that can reduce risk most effectively and protect the organization from dangerous cyber threats. Also, the control should be feasible enough to be implemented in your computing environment.

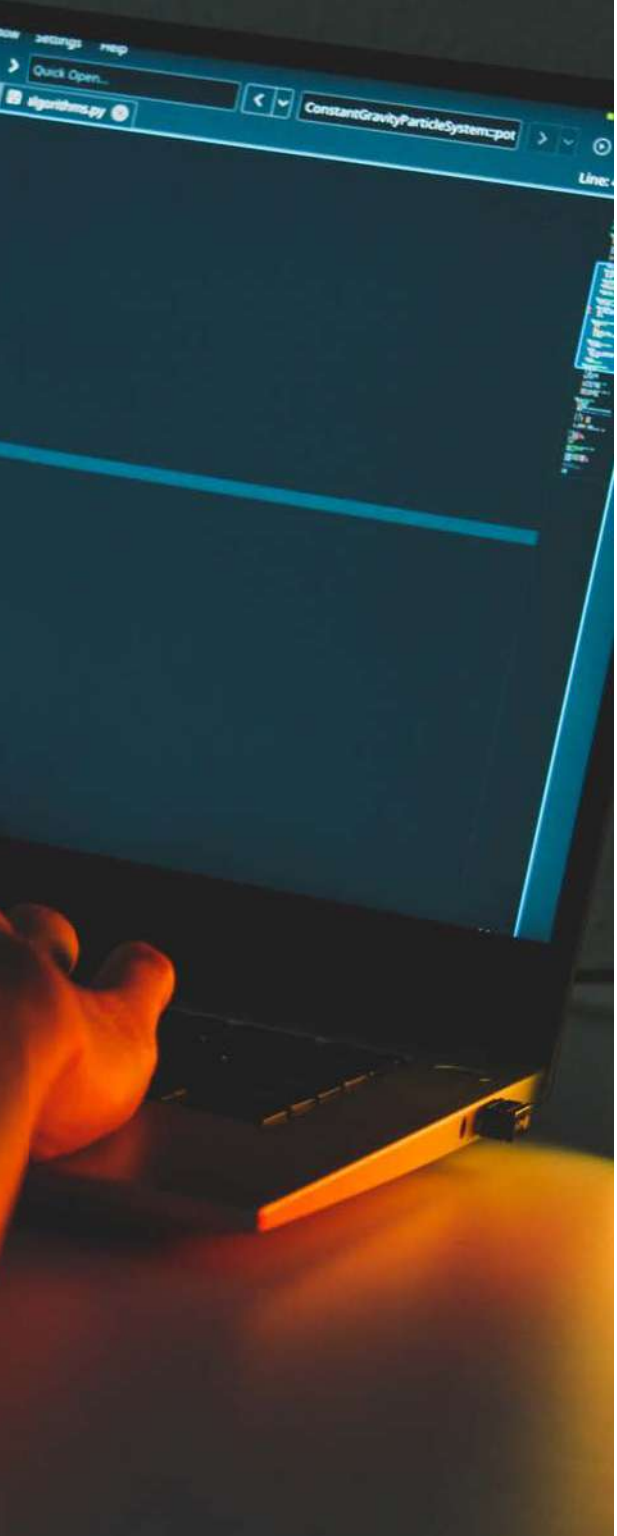
You can identify Sub-Controls to implement by visiting the CIS Implementation Groups.

3. Measurements and Metrics
You should have standard metrics or KPIs in place so that all stakeholders like IT, executives, officers, and auditors can stay on the same page. Metrics are also necessary to monitor the effectiveness of your security measures and make improvements.

4. Continuous Diagnostics and Mitigation
You should always be proactive and monitor your security measures' effectiveness. Any issues should be resolved as soon as possible to ensure the integrity of the following actions.

5. Automation
Automation helps businesses ensure compliance with controls and gain a scalable and reliable way to fight off cyber threats. Automation also increases efficiencies and saves both time and labour.





The CIS Controls™ is a set of **security best practices** that help businesses mitigate and protect themselves against the **most common** Cyber Attacks and Threats out there.

There were developed and are maintained by IT and Security Experts at the **Center for Internet Security (CIS)** and are recognized by Businesses and Governments globally.

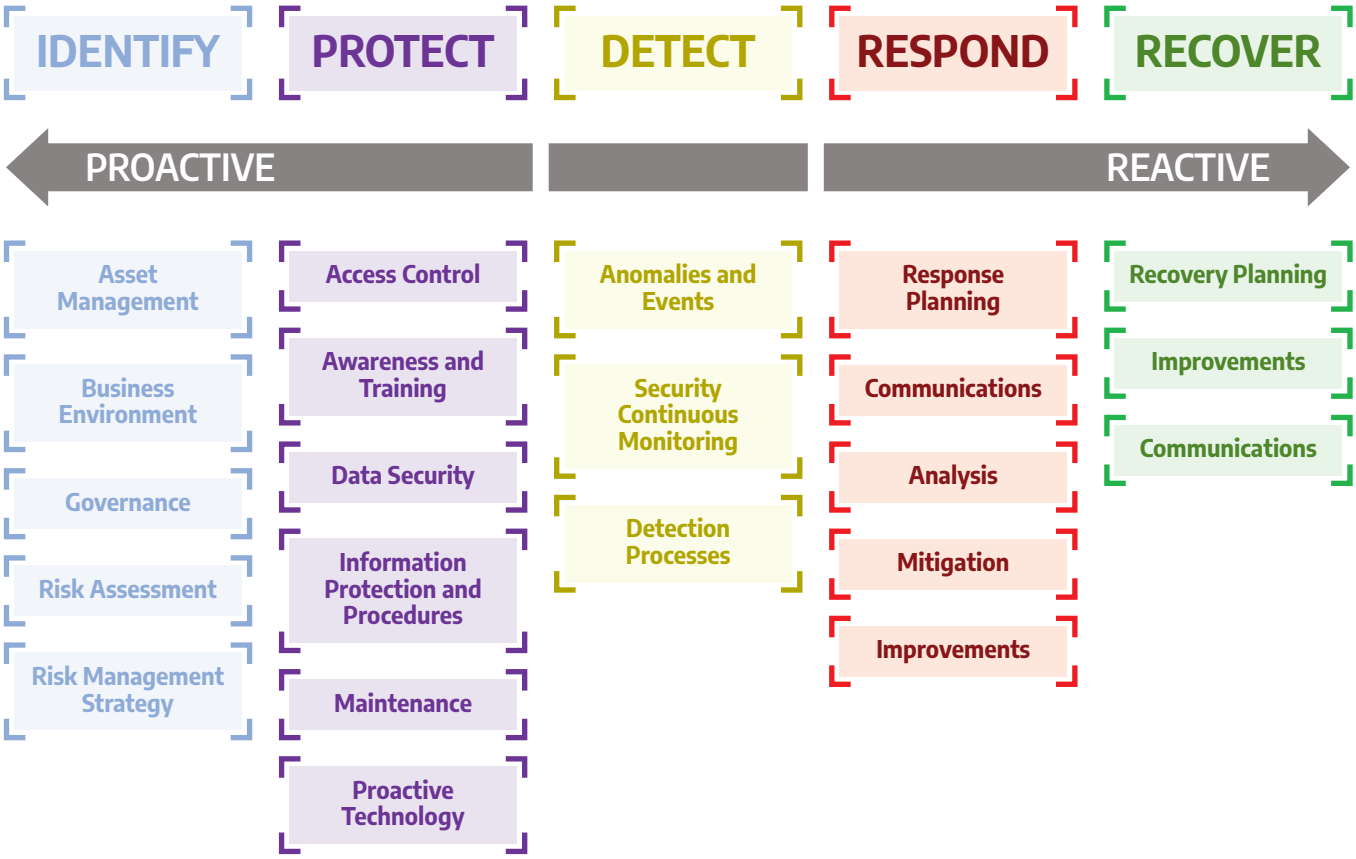
The List of Controls P18

NIST Cybersecurity Framework

The NIST Cybersecurity Framework enables businesses and enterprises to evaluate the risks they encounter. The framework consists of three parts.

The Framework Core presents a range of references, outcomes, and activities associated with aspects and approaches to cyber defense. The Framework Implementation Tiers help organizations establish their approach to cybersecurity and clarify their stance to all stakeholders. The tier also portrays the degree of sophistication of the management approach. The Framework Profile contains a collection of outcomes the enterprise picked from the categories and subcategories based on its risk evaluation and requirements.

Organizations can create a "Current Profile" based on the framework that includes the cybersecurity activities and goals the company aims for. Then it can develop a "Target Profile" or go for a baseline profile that meets the organization's specific industry needs. Ultimately, the organization can craft actionable steps to achieve the target profile.



CIS Controls™

The CIS Controls™ is a set of 18 actions that make up the best practices to tackle major attacks against systems and networks. The best practices are developed by a bunch of IT experts with years of experience in Cybersecurity. They come from a range of industries, including government, defense, healthcare, education, retail, manufacturing, and others. The CIS Controls are considered to be an international-level collection of best security practices.

Over the years, various forms of cyber attacks have targeted businesses. They include data breaches, stealing of credit card information, theft of identity and intellectual property, denials of service, privacy breaches, and much more. Experts have developed a range of security protocols to address these cyber threats, which is termed as Cyber Defense.

The IT Industry uses a plethora of resources and tools to counter Cyber Threats. We also have different technologies, security controls, vulnerability databases, certifications, training material, and security checklists too. We have access to studies and reports, tools, notification services, and more to keep us protected from any form of Cyber Threat. The IT Industry also depends on a number of regulations, risk assessment frameworks, and security requirements to keep themselves safe from cybercrime.

However, this overload of information and technology often leads to confusion. The competing security measures and options can paralyze an organization from taking the required step to counter Cybercrime. In the present day, the business process has grown more complex along with the proliferation of mobile devices and expanding dependencies. The advance in technology has led to the distribution of data across several channels, even outside the organization. As a result, security has transformed from a standalone problem to a multi-faceted threat in this interconnected world.

> The average cost of a ransomware attack on businesses was $133,000.

The situation brings up the need to act as a community and come up with solutions and support for different industries, sectors, and partnerships. We need to use our knowledge and advancing technology to create solutions that address the crucial aspects of an organization's risk management approach. Such an approach will be a step in the right direction and help enterprises take the proper steps to resolve security issues. The best way to do this is to follow a roadmap of fundamentals that help organizations develop their Cyber Defense and security protocols.

The CIS Controls™ were developed based on the above principles to help organizations take a holistic approach towards Cybersecurity. They were originally created as a grass-roots program to help cut down the confusion and focus on fundamental actions that enable a business to overcome cyber threats. The controls are intrinsically valuable and provide the data and knowledge to organizations for staying alert, responding, and preventing Cyber Attacks.

The CIS Controls™ are led by CIS®, a global community that offers the following:

- Shared insight into Cybercrimes, Cyber Attacks, and threats to get to the root cause of problems and come up with appropriate measures.
- Documentation of all required approvals and distribution of critical tools.
- Tracking of the nuances of a threat, including growth, severity, and intrusiveness.
- Highlighting of the importance of CIS Controls™ to help make them compliant with regulatory frameworks.
- Sharing of knowledge, tools, working aids, translations, and more.
- Tackling the common threats before they become serious and implement roadmaps to solve them as a community.

The CIS Controls are made up of a highly-actionable collection of actions that organizations can implement, use, and scale. The controls also comply with most applicable laws and security safeguards and are backed by the IT Community.

We help our Clients align with the CIS Controls™ to help Safeguard their business.

Doctrines of Effective Cyber Defense

As we already discussed, there are five tenets to a reliable Cybersecurity program:

Offence informs defense: Build more effective security measures learning from past attacks and threats. Only controls proven to be effective should be considered.

Prioritization: Prioritize the controls that have been effective in the real-world against threats. The ease of implementation should also be a consideration.

Measurements and metrics: Measurements and metrics are essential to assess the effectiveness of your security measures. They also enable all stakeholders in your security team to speak the same language.

Continuous diagnostics and mitigation: Test and assess your security protocols regularly to help implement the next steps.

Automation: Automate your cybersecurity activities to ensure compliance and gain a reliable and scalable cyber defense.

The CIS Controls best practices help enterprises to counter and prevent cyber attacks and threats. The controls are divided into three categories- basic, foundational, and organizational controls.

THE IMPLEMENTATION GROUPS

The CIS understands that not every Business or Organization will have the means, budget or requirement to properly implement all the Safeguards that they recommend.

To combat this, all of the **Safeguards** underneath each **Control** are categorized into **Implementation Groups.**

Each **Implementation Group** builds on the one before it, so **IG2** includes all the **Safeguards** from **IG1** and **IG3** includes all the **Safeguards** from both **IG1** and **IG2.**

A good goal for an organization or business of any size is to start with implementing everything that as a part of **Implementation Group 1 (IG1).**

Once they have implemented all **IG1** Safeguards Depending on requirements and budget, , they can then start to implement **Safeguards** from **Implementation Group 2 (IG2).**

Finally, again depending on requirements and budget, they can then start to implement **Safeguards** from **Implementation Group 3 (IG3).**

Each of the 18 CIS Controls has a number of **Safeguards** that form a part of it. There are 153 in total. These 153 **Safeguards** are categorized into three (3) groups: **Implementation Group 1 (IG1)** has 56, **Implementation Group 2 (IG2)** has 74 & **Implementation Group 3 (IG3)** has an additional 23 Safeguards.

Implementation Group 1 (IG1) - Basic Cyber Hygiene

In most cases, an **IG1** enterprise is typically small to medium-sized with limited IT and Cybersecurity expertise to dedicate towards protecting IT assets and personnel. A common concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime.

Implementation Group 2 (IG2)

An **IG2** enterprise usually employes individuals or an external party such as a Managed Service Provider (MSP) to help manage and protect IT Infrastructure. These enterprises typically have multiple departments with different risk profiles based on job function and mission.

Implementation Group 3 (IG3)

An IG3 Enterprise typicaly employs dedicated security experts that specialize in the different facets of Cybersecurity. The Assets and Data of an IG3 Enterprise typically contain sensitive information and they are often subject to regulatory and compliance oversight.

CONTROL 01

01 - Inventory and Control of Enterprise Assets

Safeguards Total 5 | IG1 2/5 | IG2 4/5 | IG3 5/5

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Why Is This CIS Control Critical?

Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.

External attackers are continuously scanning the internet address space of target enterprises, premise-based or in the cloud, identifying possibly unprotected assets attached to an enterprise's network. Attackers can take advantage of new assets that are installed, yet not securely configured and patched. Internally, unidentified assets can also have weak security configurations that can make them vulnerable to web- or email-based malware; and, adversaries can leverage weak security configurations for traversing the network, once they are inside.

Did You Know?

Nearly 66% of IT Managers have an incomplete record of their IT assets. Knowing what IT Equipment you have and where is a critical function. We can help with an initial Asset Audit and ongoing Asset List Management.

THE SAFEGUARDS

1.1 Establish and Maintain Detailed Enterprise Asset Inventory
Devices | Identify | ● ● ●

1.2 Address Unauthorized Assets
Devices | Respond | ● ● ●

1.3 Utilize an Active Discovery Tool
Devices | Detect | ○ ● ●

1.4 Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory
Devices | Identify | ○ ● ●

1.5 Use a Passive Asset Discovery Tool
Devices | Detect | ○ ○ ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

02 - Inventory and Control of Software Assets

Safeguards Total 7 | IG1 3/7 | IG2 6/7 | IG3 7/7

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

THE SAFEGUARDS

2.1 Establish and Maintain a Software Inventory
Applications | Identify | ● ● ●

2.2 Ensure Authorized Software is Currently Supported
Applications | Identify | ● ● ●

2.3 Address Unauthorized Software
Applications | Respond | ● ● ●

2.4 Utilize Automated Software Inventory Tools
Applications | Detect | ○ ● ●

2.5 Allowlist Authorized Software
Applications | Protect | ○ ● ●

2.6 Allowlist Authorized Libraries
Applications | Protect | ○ ● ●

2.7 Allowlist Authorized Scripts
Applications | Protect | ○ ○ ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

Why Is This CIS Control Critical?

A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. For example, if a user opens a malicious website or attachment with a vulnerable browser, an attacker can often install backdoor programs and bots that give the attacker long-term control of the system. Attackers can also use this access to move laterally through the network. One of the key defenses against these attacks is updating and patching software. However, without a complete inventory of software assets, an enterprise cannot determine if they have vulnerable software, or if there are potential licensing violations.

Even if a patch is not yet available, a complete software inventory list allows an enterprise to guard against known attacks until the patch is released.

Some sophisticated attackers use "zero-day exploits," which take advantage of previously unknown vulnerabilities that have yet to have a patch released from the software vendor. Depending on the severity of the exploit, an enterprise can implement temporary mitigation measures to guard against attacks until the patch is released.

Management of software assets is also important to identify unnecessary security risks. An enterprise should review its software inventory to identify any enterprise assets running software that is not needed for business purposes. For example, an enterprise asset may come installed with default software that creates a potential security risk and provides no benefit to the enterprise. It is critical to inventory, understand, assess, and manage all software connected to an enterprise's infrastructure.

Did You Know?

56% verify asset location only once a year, while 10-15% verify only every five years. Regular asset & inventory maintenance is crucial to keeping accurate records. We can help you with your Software Inventory and Control Management.

CONTROL 03

03 - Data Protection

Safeguards Total 14 | IG1 6/14 | IG2 12/14 | IG3 14/14

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Why Is This CIS Control Critical?

Data is no longer only contained within an enterprise's border; it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services that might have it anywhere in the world. In addition to sensitive data an enterprise holds related to finances, intellectual property, and customer data, there also might be numerous international regulations for protection of personal data. Data privacy has become increasingly important, and enterprises are learning that privacy is about the appropriate use and management of data, not just encryption. Data must be appropriately managed through its entire life cycle. These privacy rules can be complicated for multi-national enterprises of any size; however, there are fundamentals that can apply to all.

Once attackers have penetrated an enterprise's infrastructure, one of their first tasks is to find and exfiltrate data. Enterprises might not be aware that sensitive data is leaving their environment because they are not monitoring data outflows.

Did You Know?

78 Percent of Small Businesses that store valuable or sensitive data do not encrypt their data making it easy for hackers to gain access. There are tools and systems available now that can cost-effectively manage data protection and encryption across organizations.

THE SAFEGUARDS

3.1 Establish and Maintain a Data Management Process
Data | Identify | ● ● ●

3.2 Establish and Maintain a Data Inventory
Data | Identify | ● ● ●

3.3 Configure Data Access Control Lists
Data | Protect | ● ● ●

3.4 Enforce Data Retention
Data | Protect | ● ● ●

3.5 Securely Dispose of Data
Data | Protect | ● ● ●

3.6 Encrypt Data on End-User Devices
Data | Protect | ● ● ●

3.7 Establish and Maintain a Data Classification Scheme
Data | Identify | ○ ● ●

3.8 Document Data Flows
Data | Identify | ○ ● ●

3.9 Encrypt Data on Removable Media
Data | Protect | ○ ● ●

3.10 Encrypt Sensitive Data in Transit
Data | Protect | ○ ● ●

3.11 Encrypt Sensitive Data at Rest
Data | Protect | ○ ● ●

3.12 Segment Data Processing and Storage Based on Sensitivity
Data | Protect | ○ ● ●

3.13 Deploy a Data Loss Prevention Solution
Data | Protect | ○ ○ ●

3.14 Log Sensitive Data Access
Data | Detect | ○ ○ ●

THE SAFEGUARDS

4.1 Establish and Maintain a Secure Configuration Process
Applications | Protect | IG1 IG2 IG3

4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure
Network | Protect | IG1 IG2 IG3

4.3 Configure Automatic Session Locking on Enterprise Assets
Users | Protect | IG1 IG2 IG3

4.4 Implement and Manage a Firewall on Servers
Devices | Protect | IG1 IG2 IG3

4.5 Implement and Manage a Firewall on End-User Devices
Devices | Protect | IG1 IG2 IG3

4.6 Securely Manage Enterprise Assets and Software
Network | Protect | IG1 IG2 IG3

4.7 Manage Default Accounts on Enterprise Assets and Software
Users | Protect | IG1 IG2 IG3

4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
Devices | Protect | IG2 IG3

4.9 Configure Trusted DNS Servers on Enterprise Assets
Devices | Protect | IG2 IG3

4.10 Enforce Automatic Device Lockout on Portable End-User Devices
Devices | Respond | IG2 IG3

4.11 Enforce Remote Wipe Capability on Portable End-User Devices
Devices | Protect | IG2 IG3

4.12 Separate Enterprise Workspaces on Mobile End-User Devices
Devices | Protect | IG3

04 - Secure Configuration of Enterprise Assets and Software

Safeguards Total 12 | IG1 7/12 | IG2 11/12 | IG3 12/12

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Why Is This CIS Control Critical?

As delivered from manufacturers and resellers, the default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older (vulnerable) protocols, and pre-installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the life cycle of enterprise assets and software. Configuration updates need to be tracked and approved through configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and to support audits. This CIS Control is important to on-premises devices, as well as remote devices, network devices, and cloud environments.

Service providers play a key role in modern infrastructures, especially for smaller enterprises. They often are not set up by default in the most secure configuration to provide flexibility for their customers to apply their own security policies. Therefore, the presence of default accounts or passwords, excessive access, or unnecessary services are common in default configurations.

Did You Know?

Only 14% of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective. Setting up and managing appropriate security and configuration policies and procedures doesn't have to take a lot of effort if you work with a professional.

05 - Account Management

Safeguards Total 6 | IG1 4/6 | IG2 6/6 | IG3 6/6

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Why Is This CIS Control Critical?

It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through "hacking" the environment. There are many ways to covertly obtain access to user accounts, including: weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an online account that has been compromised (in a public password dump), social engineering a user to give their password, or using malware to capture passwords or tokens in memory or over the network.

Administrative, or highly privileged, accounts are a particular target, because they allow attackers to add other accounts, or make changes to assets that could make them more vulnerable to other attacks. Service accounts are also sensitive, as they are often shared among teams, internal and external to the enterprise, and sometimes not known about, only to be revealed in standard account management audits.

Finally, account logging and monitoring is a critical component of security operations.

Did You Know?

98% of Microsoft Windows critical vulnerabilities could be mitigated by removing administrative rights from end-user systems. There's amazing Zero Trust tools available to help make ongoing management of this much easier.

THE SAFEGUARDS

5.1 Establish and Maintain an Inventory of Accounts
Users | Identify | ● ● ●

5.2 Use Unique Passwords
Users | Protect | ● ● ●

5.3 Disable Dormant Accounts
Users | Respond | ● ● ●

5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts
Users | Protect | ● ● ●

5.5 Establish and Maintain an Inventory of Service Accounts
Users | Identify | ○ ● ●

5.6 Centralize Account Management
Users | Protect | ○ ● ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

THE SAFEGUARDS

6.1 Establish an Access Granting Process
Users | Protect | ● ● ●

6.2 Establish an Access Revoking Process
Users | Protect | ● ● ●

6.3 Require MFA for Externally-Exposed Applications
Users | Protect | ● ● ●

6.4 Require MFA for Remote Network Access
Users | Protect | ● ● ●

6.5 Require MFA for Administrative Access
Users | Protect | ● ● ●

6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems
Users | Identify | ● ●

6.7 Centralize Access Control
Users | Protect | ● ●

6.8 Define and Maintain Role-Based Access Control
Data | Protect | ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

06 - Access Control Management

Safeguards Total 8 | IG1 5/8 | IG2 7/8 | IG3 8/8

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Why Is This CIS Control Critical?

Where CIS Control 5 deals specifically with account management, CIS Control 6 focuses on managing what access these accounts have, ensuring users only have access to the data or enterprise assets appropriate for their role, and ensuring that there is strong authentication for critical or sensitive enterprise data or functions. Accounts should only have the minimal authorization needed for the role.

Developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralizing this function is ideal.

Did You Know?

In early November 2020, Microsoft urged users to stop using phone-based MFA and instead recommend using app-based authenticators and security keys. We can assist you to implement an organization wide Enterprise Multi-Factor and Identity Management system.

CONTROL 07

07 - Continuous Vulnerability Management

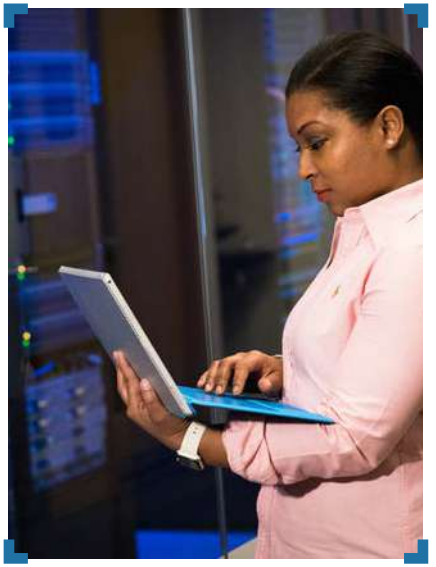
Safeguards Total	7	IG1	4/7	IG2	7/7	IG3	7/7

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Why Is This CIS Control Critical?

Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Attackers have access to the same information and can often take advantage of vulnerabilities more quickly than an enterprise can remediate.



Did You Know?

One of the main points of entry used by threat actors is to exploit unpatched vulnerabilities within systems. According to one survey from the Ponemon Institute, 60% of breaches in 2019 involved unpatched vulnerabilities.

THE SAFEGUARDS

7.1 Establish and Maintain a Vulnerability Management Process
Applications | Protect | ● ● ●

7.2 Establish and Maintain a Remediation Process
Applications | Respond | ● ● ●

7.3 Perform Automated Operating System Patch Management
Applications | Protect | ● ● ●

7.4 Perform Automated Application Patch Management
Applications | Protect | ● ● ●

7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets
Applications | Identify | ○ ● ●

7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
Applications | Identify | ○ ● ●

7.7 Remediate Detected Vulnerabilities
Applications | Respond | ○ ● ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

THE SAFEGUARDS

8.1 Establish and Maintain an Audit Log Management Process
Network | Protect

8.2 Collect Audit Logs
Network | Detect

8.3 Ensure Adequate Audit Log Storage
Network | Protect

8.4 Standardize Time Synchronization
Network | Protect

8.5 Collect Detailed Audit Logs
Network | Detect

8.6 Collect DNS Query Audit Logs
Network | Detect

8.7 Collect URL Request Audit Logs
Network | Detect

8.8 Collect Command-Line Audit Logs
Devices | Detect

8.9 Centralize Audit Logs
Network | Detect

8.10 Retain Audit Logs
Network | Protect

8.11 Conduct Audit Log Reviews
Network | Detect

8.12 Collect Service Provider Logs
Data | Detect

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

08 - Audit Log Management

Safeguards Total 12 | IG1 3/12 | IG2 11/12 | IG3 12/12

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Why Is This CIS Control Critical?

Log collection and analysis is critical for an enterprise's ability to detect malicious activity quickly. Sometimes audit records are the only evidence of a successful attack. Attackers know that many enterprises keep audit logs for compliance purposes, but rarely analyze them. Attackers use this knowledge to hide their location, malicious software, and activities on victim machines. Due to poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target enterprise knowing.

There are two types of logs that are generally treated and often configured independently: system logs and audit logs. System logs typically provide system-level events that show various system process start/end times, crashes, etc. These are native to systems, and take less configuration to turn on. Audit logs typically include user-level events—when a user logged in, accessed a file, etc.—and take more planning and effort to set up.

Logging records are also critical for incident response. After an attack has been detected, log analysis can help enterprises understand the extent of an attack. Complete logging records can show, for example, when and how the attack occurred, what information was accessed, and if data was exfiltrated. Retention of logs is also critical in case a follow-up investigation is required or if an attack remained undetected for a long period of time.

Did You Know?

Most businesses are legally obligated to have a data audit trail. Multiple government-mandated standards and regulations, including ISO 27001, PCI-DSS, HIPAA, PNR Directive, and more, require some form of audit trail. Talk to us today to help configure your Auditing.

09 - Email and Web Browser Protections

Safeguards Total 7 | IG1 2/7 | IG2 6/7 | IG3 7/7

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Why Is This CIS Control Critical?

Web browsers and email clients are very common points of entry for attackers because of their direct interaction with users inside an enterprise. Content can be crafted to entice or spoof users into disclosing credentials, providing sensitive data, or providing an open channel to allow attackers to gain access, thus increasing risk to the enterprise. Since email and web are the main means that users interact with external and untrusted users and environments, these are prime targets for both malicious code and social engineering.

Did You Know?

The top malicious email attachment types are Office documents which make up 38%, the next highest is Archive (.zip etc.) at 37%. A multi-layered approach to web and email protection is vital.

THE SAFEGUARDS

9.1 Ensure Use of Only Fully Supported Browsers and Email Clients
Applications Protect

9.2 Use DNS Filtering Services
Network Protect

9.3 Maintain and Enforce Network-Based URL Filters
Network Protect

9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions
Applications Protect

9.5 Implement DMARC
Network Protect

9.6 Block Unnecessary File Types
Network Protect

9.7 Deploy and Maintain Email Server Anti-Malware Protections
Network Protect

1 2 3 4 5
Asset Type | Security Function

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

10 - MalwareDefenses

Safeguards Total 7 | IG1 3/7 | IG2 7/7 | IG3 7/7

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Why Is This CIS Control Critical?

Malicious software (sometimes categorized as viruses or Trojans) is an integral and dangerous aspect of internet threats. They can have many purposes, from capturing credentials, stealing data, identifying other targets within the network, and encrypting or destroying data. Malware is ever-evolving and adaptive, as modern variants leverage machine learning techniques.

Malware enters an enterprise through vulnerabilities within the enterprise on end-user devices, email attachments, webpages, cloud services, mobile devices, and removable media. Malware often relies on insecure end-user behavior, such as clicking links, opening attachments, installing software or profiles, or inserting Universal Serial Bus (USB) flash drives. Modern malware is designed to avoid, deceive, or disable defenses.

THE SAFEGUARDS

10.1 Deploy and Maintain Anti-Malware Software
Devices | Protect | ● ● ●

10.2 Configure Automatic Anti-Malware Signature Updates
Devices | Protect | ● ● ●

10.3 Disable Autorun and Autoplay for Removable Media
Devices | Protect | ● ● ●

10.4 Configure Automatic Anti-Malware Scanning of Removable Media
Devices | Detect | ○ ● ●

10.5 Enable Anti-Exploitation Features
Devices | Protect | ○ ● ●

10.6 Centrally Manage Anti-Malware Software
Devices | Protect | ○ ● ●

10.7 Use Behavior-Based Anti-Malware Software
Devices | Detect | ○ ● ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

Did You Know?

Cyber attacks and threats are constantly evolving, with 350,000 new malware signatures detected every day. We can help you implenent advanced enterprise level threat protection and detection tools that use technologies such as A.I. and Machine Learning to help protect.

11 - Data Recovery

Safeguards Total 5 | IG1 4/5 | IG2 5/5 | IG3 5/5

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Why Is This CIS Control Critical?

In the cybersecurity triad—Confidentiality, Integrity, and Availability (CIA)—the availability of data is, in some cases, more critical than its confidentiality. Enterprises need many types of data to make business decisions, and when that data is not available or is untrusted, then it could impact the enterprise. An easy example is weather information to a transportation enterprise.

When attackers compromise assets, they make changes to configurations, add accounts, and often add software or scripts. These changes are not always easy to identify, as attackers might have corrupted or replaced trusted applications with malicious versions, or the changes might appear to be standard-looking account names. Configuration changes can include adding or changing registry entries, opening ports, turning off security services, deleting logs, or other malicious actions that make a system insecure. These actions do not have to be malicious; human error can cause each of these as well. Therefore, it is important to have an ability to have recent backups or mirrors to recover enterprise assets and data back to a known trusted state.

Did You Know?

75% of small business owners don't have a Disaster Recovery plan in place. A basic Disaster Recovery plan can start off small and grow over time. Something is better than nothing. We can help you build a Disaster Recovery plan so you are ready for when something happens.

THE SAFEGUARDS

11.1 Establish and Maintain a Data Recovery Process
Data | Recover | ● ● ●

11.2 Perform Automated Backups
Data | Recover | ● ● ●

11.3 Protect Recovery Data
Data | Protect | ● ● ●

11.4 Establish and Maintain an Isolated Instance of Recovery Data
Data | Recover | ● ● ●

11.5 Test Data Recovery
Data | Recover | ○ ● ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

THE SAFEGUARDS

12.1 Ensure Network Infrastructure is Up-to-Date
Network | Protect

12.2 Establish and Maintain a Secure Network Architecture
Network | Protect

12.3 Securely Manage Network Infrastructure
Network | Protect

12.4 Establish and Maintain Architecture Diagram(s)
Network | Identify

12.5 Centralize Network Authentication, Authorization, and Auditing (AAA)
Network | Protect

12.6 Use of Secure Network Management and Communication Protocols
Network | Protect

12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure
Devices | Protect

12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work
Devices | Protect

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

12 - Network Infrastructure Management

Safeguards Total 8 | IG1 1/8 | IG2 7/8 | IG3 8/8

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Why Is This CIS Control Critical?

Secure network infrastructure is an essential defense against attacks. This includes an appropriate security architecture, addressing vulnerabilities that are, often times, introduced with default settings, monitoring for changes, and reassessment of current configurations. Network infrastructure includes devices such as physical and virtualized gateways, firewalls, wireless access points, routers, and switches.

Default configurations for network devices are geared for ease-of-deployment and ease-of-use—not security. Potential default vulnerabilities include open services and ports, default accounts and passwords (including service accounts), support for older vulnerable protocols, and pre-installation of unneeded software. Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defenses.

They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept data while in transmission.

Network security is a constantly changing environment that necessitates regular re-evaluation of architecture diagrams, configurations, access controls, and allowed traffic flows. Attackers take advantage of network device configurations becoming less secure over time as users demand exceptions for specific business needs.

Did You Know?

Research from Gartner suggests that, through 2022, 99% of firewall breaches will be caused by simple firewall misconfigurations. Regular and ongoing Network Configuration Monitoring and Audits can help pick up any weak points. We can work with you to develop a plan.

CONTROL 13

13 - Network Monitoring and Defense

Safeguards Total 11 | IG1 0/11 | IG2 6/11 | IG3 11/11

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Why Is This CIS Control Critical?

We cannot rely on network defenses to be perfect. Adversaries continue to evolve and mature, as they share, or sell, information among their community on exploits and bypasses to security controls. Even if security tools work "as advertised," it takes an understanding of the enterprise risk posture to configure, tune, and log them to be effective. Often, misconfigurations due to human error or lack of knowledge of tool capabilities give enterprises a false sense of security.

Security tools can only be effective if they are supporting a process of continuous monitoring that allows staff the ability to be alerted and respond to security incidents quickly. Enterprises that adopt a purely technology-driven approach will also experience more false positives, due to their over-reliance on alerts from tools. Identifying and responding to these threats requires visibility into all threat vectors of the infrastructure and leveraging humans in the process of detection, analysis, and response. It is critical for large or heavily targeted enterprises to have a security operations capability to prevent, detect, and quickly respond to cyber threats before they can impact the enterprise.

Did You Know?

In the first half of 2019, 4.1 billion data records were compromised from 3,800 publicly disclosed data breaches. The reputational damage from a data leak can often be the most costly part of all, greatly increasing the risk of a business shutting down after a breach.

THE SAFEGUARDS

13.1 Centralize Security Event Alerting
Network | Detect | ● ●

13.2 Deploy a Host-Based Intrusion Detection Solution
Devices | Detect | ● ●

13.3 Deploy a Network Intrusion Detection Solution
Network | Detect | ● ●

13.4 Perform Traffic Filtering Between Network Segments
Network | Protect | ● ●

13.5 Manage Access Control for Remote Assets
Devices | Protect | ● ●

13.6 Collect Network Traffic Flow Logs
Network | Detect | ● ●

13.7 Deploy a Host-Based Intrusion Prevention Solution
Devices | Protect | ●

13.8 Deploy a Network Intrusion Prevention Solution
Network | Protect | ●

13.9 Deploy Port-Level Access Control
Devices | Protect | ●

13.10 Perform Application Layer Filtering
Network | Protect | ●

13.11 Tune Security Event Alerting Thresholds
Network | Detect | ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

14 - Security Awareness and Skills Training

Safeguards Total	9	IG1	8/9	IG2	9/9	IG3	9/9

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Why Is This CIS Control Critical?

The actions of people play a critical part in the success or failure of an enterprise's security program. It is easier for an attacker to entice a user to click a link or open an email attachment to install malware in order to get into an enterprise, than to find a network exploit to do it directly.

Users themselves, both intentionally and unintentionally, can cause incidents as a result of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password they use on public sites.

No security program can effectively address cyber risk without a means to address this fundamental human vulnerability. Users at every level of the enterprise have different risks. For example: executives manage more sensitive data; system administrators have the ability to control access to systems and applications; and users in finance, human resources, and contracts all have access to different types of sensitive data that can make them targets.

The training should be updated regularly.

THE SAFEGUARDS

14.1 Establish and Maintain a Security Awareness Program
N/A | Protect | ● ● ●

14.2 Train Workforce Members to Recognize Social Engineering Attacks
N/A | Protect | ● ● ●

14.3 Train Workforce Members on Authentication Best Practices
N/A | Protect | ● ● ●

14.4 Train Workforce on Data Handling Best Practices
N/A | Protect | ● ● ●

14.5 Train Workforce Members on Causes of Unintentional Data Exposure
N/A | Protect | ● ● ●

14.6 Train Workforce Members on Recognizing and Reporting Security Incidents
N/A | Protect | ● ● ●

14.7 Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
N/A | Protect | ● ● ●

14.8 Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
N/A | Protect | ● ● ●

14.9 Conduct Role-Specific Security Awareness and Skills Training
N/A | Protect | ○ ● ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

Did You Know?

90% of U.S. organizations required or requested most of their users to work from home in 2020, however only 29% train their employees about best practices for working remotely. We can get your team access to some of the best End-User Cybersecurity training available.

15 - Service Provider Management

Safeguards Total 7 | IG1 1/7 | IG2 4/7 | IG3 7/7

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Why Is This CIS Control Critical?

In our modern, connected world, enterprises rely on vendors and partners to help manage their data or rely on third-party infrastructure for core applications or functions.

There have been numerous examples where third-party breaches have significantly impacted an enterprise; for example, as early as the late 2000s, payment cards were compromised after attackers infiltrated smaller third-party vendors in the retail industry. More recent examples include ransomware attacks that impact an enterprise indirectly, due to one of their service providers being locked down, causing disruption to business. Or worse, if directly connected, a ransomware attack could encrypt data on the main enterprise.

Did You Know?

Many Cyber Attacks originate through 3rd-party Vendors and Software so it's important to make sure you do Due Diligence whenever you pick a new vendor to work with. We can help you through the vetting process when selecting new Vendors so you know what security questions to ask.

THE SAFEGUARDS

15.1 Establish and Maintain an Inventory of Service Providers
N/A | Identify | ● ○ ○

15.2 Establish and Maintain a Service Provider Management Policy
N/A | Identify | ○ ○ ○

15.3 Classify Service Providers
N/A | Identify | ○ ○ ○

15.4 Ensure Service Provider Contracts Include Security Requirements
N/A | Protect | ○ ○ ○

15.5 Assess Service Providers
N/A | Identify | ○ ○ ○

15.6 Monitor Service Providers
Data | Detect | ○ ○ ○

15.7 Securely Decommission Service Providers
Data | Protect | ○ ○ ○

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

THE SAFEGUARDS

16.1 Establish and Maintain a Secure Application Development Process
Applications Protect

16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities
Applications Protect

16.3 Perform Root Cause Analysis on Security Vulnerabilities
Applications Protect

16.4 Establish and Manage an Inventory of Third-Party Software Components
Applications Protect

16.5 Use Up-to-Date and Trusted Third-Party Software Components
Applications Protect

16.6 Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities
Applications Protect

16.7 Use Standard Hardening Configuration Templates for Application Infrastructure
Applications Protect

16.8 Separate Production and Non-Production Systems
Applications Protect

16.9 Train Developers in Application Security Concepts and Secure Coding
Applications Protect

16.10 Apply Secure Design Principles in Application Architectures
Applications Protect

16.11 Leverage Vetted Modules or Services for Application Security Components
Applications Protect

16.12 Implement Code-Level Security Checks
Applications Protect

16.13 Conduct Application Penetration Testing
Applications Protect

16.14 Conduct Threat Modeling
Applications Protect

16 - Application Software Security

Safeguards Total 14 | IG1 0/14 | IG2 11/14 | IG3 14/14

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Why Is This CIS Control Critical?

Applications provide a human-friendly interface to allow users to access and manage data in a way that is aligned to business functions. They also minimize the need for users to deal directly with complex (and potentially error-prone) system functions, like logging into a database to insert or modify files. Enterprises use applications to manage their most sensitive data and control access to system resources. Therefore, an attacker can use the application itself to compromise the data, instead of an elaborate network and system hacking sequence that attempts to bypass network security controls and sensors. This is why protecting user credentials (specifically application credentials) defined in CIS Control 6 is so important.

Did You Know?

Small businesses are not investing enough in cyber security, 62% don't regularly upgrade or update their software solutions. We can work with you to develop an IT Budget and Plan that fits your business and requirements so there are no hidden surprises.

17 - Incident Response Management

Safeguards Total 9 | IG1 3/9 | IG2 8/9 | IG3 9/9

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Why Is This CIS Control Critical?

A comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. Often, the final two get overlooked in immature enterprises, or the response technique to compromised systems is just to re-image them to original state, and move on. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern.

We cannot expect our protections to be effective 100% of the time. When an incident occurs, if an enterprise does not have a documented plan—even with good people—it is almost impossible to know the right investigative procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover.

Did You Know?

65% of small businesses have failed to act following a cyber security incident. 23% of small businesses have a leadership role dedicated to Cyber, whereas 46% have no defined role at all. We have a Security Incident Response process in place to assist you if ever needed.

THE SAFEGUARDS

17.1 Designate Personnel to Manage Incident Handling
N/A | Respond | ● ● ●

17.2 Establish and Maintain Contact Information for Reporting Security Incidents
N/A | Respond | ● ● ●

17.3 Establish and Maintain an Enterprise Process for Reporting Incidents
N/A | Respond | ● ● ●

17.4 Establish and Maintain an Incident Response Process
N/A | Respond | ○ ● ●

17.5 Assign Key Roles and Responsibilities
N/A | Respond | ○ ● ●

17.6 Define Mechanisms for Communicating During Incident Response
N/A | Respond | ○ ● ●

17.7 Conduct Routine Incident Response Exercises
N/A | Recover | ○ ● ●

17.8 Conduct Post-Incident Reviews
N/A | Recover | ○ ● ●

17.9 Establish and Maintain Security Incident Thresholds
N/A | Recover | ○ ○ ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

18 - Penetration Testing

Safeguards Total 5 | IG1 0/5 | IG2 3/5 | IG3 5/5

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Why Is This CIS Control Critical?

A successful defensive posture requires a comprehensive program of effective policies and governance, strong technical defenses, combined with appropriate action from people. However, it is rarely perfect. In a complex environment where technology is constantly evolving and new attacker tradecraft appears regularly, enterprises should periodically test their controls to identify gaps and to assess their resiliency. This test may be from external network, internal network, application, system, or device perspective. It may include social engineering of users, or physical access control bypasses.

Often, penetration tests are performed for specific purposes:

- As a "dramatic" demonstration of an attack, usually to convince decision-makers of their enterprise's weaknesses
- As a means to test the correct operation of enterprise defenses ("verification")
- To test that the enterprise has built the right defenses in the first place ("validation")

Did You Know?

As sophisticated as security devices are today, almost 90% of Cyber Attacks are Caused by Human Error or Behavior. Penetration Testing can help improve the overall security posture of an organization. We can simulate common attacks to help you find potential weak points.

THE SAFEGUARDS

18.1 Establish and Maintain a Penetration Testing Program
N/A | Identify | ● ●

18.2 Perform Periodic External Penetration Tests
Network | Identify | ● ●

18.3 Remediate Penetration Test Findings
Network | Protect | ● ●

18.4 Validate Security Measures
Network | Protect | ●

18.5 Perform Periodic Internal Penetration Tests
N/A | Identify | ●

1 2 3 4 5
Asset Type | Security Function | ● ● ●

1= Asset Type
2= Security Function
3= Implentation Group 1
4= Implentation Group 2
5= Implentation Group 3

FROM YOUR FRIENDS AT:

BlueGuysIT.com
TECHNOLOGY SOLUTIONS

(870) 425-2583 | blueguysit.com