allmountain technologies

CIS's 18 Must-Have Cybersecurity Controls

CIS Security Controls were developed by *The Center for Internet Security, Inc.,* a nonprofit community of leading cybersecurity experts.

CIS Security Controls were developed by *The Center for Internet Security, Inc.,* a nonprofit community of leading cybersecurity experts. CIS Controls are globally recognized best practices designed with input from the US government, private-sector, security industry and academia, to help organizations protect themselves against the current range of cybercrime threats.

Recently, the CIS Critical Security Controls were updated to a new list of 18, which will help address and secure every potential risk in an organization's IT environment.

If you're worried you may have overlooked a key aspect of your cybersecurity, then double-check it against these 18 controls solutions.

Need expert assistance? All Mountain Technologies can help you implement these strategies.

Please note that this list represents the first implementation group, which is considered Basic Cyber Hygiene. This is only a starting point—depending on the nature of your company, you may need to roll out additional measures.

What Are The New CIS Critical Security Controls?

Developed by leading cybersecurity experts, the CIS Top 18 Critical Security Controls are a set of best practices designed to help organizations protect themselves against the the current range of cybercrime threats.

1. Inventory And Control Of Enterprise Assets

A key aspect of cybersecurity is knowing what hardware is connected to your network, and what shouldn't be. If you maintain an accurate inventory of authorized and unauthorized devices on your network, you're better prepared to identify when something connects that shouldn't have.

Don't forget to scan your network for Internet Of Things devices. Wearables and "smart" technology are easy to overlook, but they can still access network data, and therefore, still be a risk.

Consider adding a detective control, especially for secondary networks, such as those committed to backup, VoIP or network device management, as they are often popular and easy targets for hackers.

2. Inventory Of Critical Software Assets

This goes hand in hand with control #1. Just as you need to know what type of hardware is connected to your network, you also need to know what software is in use, what permissions it has, and if they come with any identified vulnerabilities.

Don't provide local administrator access to users that don't need it. This one seems like a no-brainer, but it's more common than you'd think. Giving admin privileges to the wrong person can allow them to install unauthorized software.

Also, make sure to keep your software up to date. Patches and updates are key in an effective cybersecurity posture, as they protect you against vulnerabilities that the vendor themselves have identified.

---

3. Data Protection

Data protection begins and ends with the consideration of managerial controls. That is, what type of data you have, how it is classified or categorized, and what can or cannot be done with said data—by anyone in the organization, including its leaders.

This is why you need a data inventory, which will help with understanding the nature of your environment and the systems therein, as well as how to define effective data retention policies.

Work from the top down in the organization to make sure best practices are followed in terms of managerial controls. Enacting such policies can be difficult when it comes to leadership, but these members of the organization need to understand that they are a part of the business' cybersecurity culture.

Implement procedural and technical controls to block unnecessary access to data, such as by USB mass storage devices, as well as webmail and file transfer websites.

---

4. Secure Configurations Of Enterprise Assets & Software

You know you shouldn't trust default security settings, right? Just because a program is generally considered to follow standard security practices, that doesn't mean that it's as secure as it should be "out of the box".

Why aren't default hardware and software security configurations enough?

Because greater security often means less convenience—albeit, in small ways. Regardless, when it comes to most products, the priority is usually to enhance the user experience, rather than to configure the best security settings possible.

Here's an example—when it comes to Wi-Fi connectivity settings, would you prioritize security or convenience? On one hand, it's much more convenient to users if the device in question is configured to automatically connect to open and available Wi-Fi hot spots. But as you should know, that's not a very secure practice.

It's examples like these that show why it's your responsibility to double-check default configurations and make the necessary changes if you actually want to maintain a higher level of security.

Make sure to create and securely store master images *(also known as gold images)* of your configurations that can't be altered.

Remote administrative actions should only take place via secure channels, and ideally, on a separate administrative network. Lastly ,double-check that your images are not being altered without authorization by implementing a file integrity checking tool, or application whitelisting tool.

5. Account Management

The fact is that misuse of privilege is often one of the most common ways for cybercriminals to penetrate a network. Either by tricking a user with administrative privileges to download and run malware, or by elevating privileges on a compromised non-admin account, hackers regularly make use of this highly common unsafe business practice.

Make sure to limit administrative privileges to those who actually require them. The fact is that the common business user should not require administrative privileges to do their job—whether that's for installing software, printing, using common programs, etc.

Once you've limited privileges to only a few members of the organization, make sure their accounts have the right protections in place—complex, long passwords, multi-factor authentication, configure alerts for unsuccessful log-ins, and limit administrative actions to devices that are air-gapped from unnecessary aspects of your network.

Again, this control examines how different parts of your infrastructure are accessible by one another. The fact is that cybercriminals often gain access to sensitive data by first breaking into a much less critical part of the network. If those two parts were properly segmented via a DMZ, firewall, etc., they wouldn't be able to.

Classify your data in a simple manner for easy organization:

Level 1: Data for public consumption. Data that may be freely disclosed.
Level 2: Internal data not for public disclosure.
Level 3: Sensitive internal data that if disclosed, could affect the company.
Level 4: Highly sensitive corporate, employee and customer data.

Maintain an inventory of who has access to which levels of data, and audit why that is necessary for the function of their role in the organization. Also, keep track of "stale data"—that is, data that hasn't been accessed in some time. It should be archived and removed from your systems.

6. Access Control Management

This is one of the more basic controls on the list, but no less important. It can't really be automated or outsourced to any technological aids; it's just about doing the work.

You need to have a carefully implemented process to track the lifecycle of accounts on your network.

Follow a careful system for how accounts are created for new members, how their security is maintained and verified through their life, and how they are removed when no longer needed.

Implement secure configuration settings *(complex passwords, multi-factor authentication, etc.)* for all accounts, as well as controls for login and use, such as lockouts for too many unsuccessful logins, unsuccessful login alerts, and automatic log-off after a period of inactivity

7. Continuous Vulnerability Management

The key to this control is understanding that cybersecurity is never at rest. There is no technology, no training program for staff members, and no set of static best practices that will protect you from now until the end of time.

Day by day, cybercriminals are working to update their methodology, identify new vulnerabilities in the technology you use and the way you use it. That's why it's vital for you to stay up to date on how cybercrime tactics are changing and what you can do to stay secure.

Your devices need to be scanned for vulnerabilities on a regular basis. CIS recommends a weekly scan, but for less mature businesses, that might not be feasible. In this case, the scan should take place at the very least on a monthly schedule.

8. Audit Log Management

One of the most important aspects of cybersecurity management is the careful use of the logging system, which will allow you to record nearly any type of event that occurs so you can keep a detailed account of how your systems are performing, as well as manipulate the logs to retrieve the information that you require for a given task.

Ensuring you can sort and read the logs collected by your system will allow you to gain actionable and understandable intel about any and all security events that occur. Ideally, your SIEM solution will collect logs from the following parts of your network and infrastructure:

- **Network gear**
  - Switches
  - Routers
  - Firewalls
  - Wireless Controllers and their APs
- **Servers**
  - Application servers
  - Database servers
  - Web Servers
  - File Servers
- **3rd Party Security support platforms**
  - Web proxy and filtration
  - Anti-malware solutions
  - Endpoint Security platforms (HBSS, EMET)
  - Identity Management solutions
  - IDS/IPS
- **Workstations**
  - All security log files

9. Email And Web Browser Protections

Email is perhaps the most ubiquitous technology used in the business world today—possibly even more so than the phone. It's instantaneous, can deliver important files, and doesn't require the immediate attention that a phone call does.

However, just as it is popular with consumers around the world, it is just as popular a method for hackers trying to do damage to unsuspecting businesses.

Similarly, your staff uses a web browser to access online applications, perform Google searches, and a range of other tasks every day. It needs a similar level of security as well.

Content Filtering is a key consideration in both your email client and your web browser. Nothing should make it into an employee inbox, and no web page should be accessible to an employee without first passing through a filter that can eliminate any identified threats.

Be sure to also manage a safe sender's list. No matter how new, or costly, or flashy your current spam filter is, it won't keep unwanted spam out of your inbox forever. Whenever you see that a spammer's email has made it past your filter, take a moment to block it so that it won't happen again. Furthermore, make sure to only open emails from confirmed contacts.

Lastly, email encryption measures are easy to use and make sure that the user's communication is secured against unwelcome readers while in transit. Furthermore, mobile device capability will allow users to read and send encrypted messages from the mobile platform without having to store the message locally, or any unnecessary battery or bandwidth usage.

10.Malware Defenses

Malware remains among the top cyber threats that businesses face today. As malware types like ransomware continue to become more prevalent, it's more important than ever for businesses of all sizes to be aware of what threats are out there, and which specific threats they need to be the most concerned about.

Antivirus and antimalware software should be used in conjunction with a firewall, encryption, data backup, and other IT strategies to provide defense against malware, adware, spyware, and ransomware.

Each of these cybercriminal tactics has the potential to do immense damage to your internal processes and your company's reputation. The job of these types of software is to spot, block, and isolate intrusive, malicious applications so they can't do damage to your data and legitimate software.

---

11. Data Recovery Capabilities

Data loss is often the result of poor digital security; without the right defenses, cybercriminals can easily infect an IT system with ransomware or other types of malware and compromise company data.

You may have heard that the right antimalware solution will minimize the chance of data loss, but what about human error?

The fact is that data loss due to user-based exploits and human error—whether it's an overwritten file or an accidentally deleted folder—and more frequent and often just as dangerous as most other forms of cyber-crime, and no matter how effective your antimalware solution is, it won't protect you from yourself.

Key tips:

- ✔ Make sure your data is backed up on a regular basis—at least weekly.
- ✔ Test your backups on a regular basis
- ✔ Run a full data restoration process to make sure you have a contingency in the event of a real crisis.
- ✔ Protect your backups with physical and digital security.
- ✔ Local hard drive backups should be under lock and key, and secured with encryption.

12. Secure Configurations for Network Devices

This control covers devices such as firewalls, routers, and switches. As key aspects of your network *(and the defense of your network)*, these devices need to be configured properly to ensure optimal security.

As explored above, the default configurations of such devices may not be sufficient. It's up to you to make sure they are made secure.

Keep these device configurations in line with secure configurations defined for each type of network device in use by your organization. Make use of automated tools in order to verify standard device configurations, as well as to detect any unauthorized changes that are made.

Also, implement multi-factor authentication and encryption for all network devices. Keep all network devices up to date and patched.

Lastly, segment administrative tasks and elevated access to machines dedicated for that use. As mentioned above, such devices should be air-gapped from unnecessary parts of the network when possible.

---

13. Network Monitoring & Defense

It's critical that you effectively manage all the ports, protocols and services on devices that are connected to your network. If you don't, each and every one of them could be a viable means of access for cybercriminals.

If you have detailed, real-time data on what is running on your network, and are careful to close off any unnecessary means of communication, you can drastically reduce your risk of penetration.

Before installing new software, scan its baseline ports, and then do so again after installation. Compare the results to double-check which ports are actually required. Host-based firewalls on your servers should be used in conjunction with whitelists to only allow communication between aspects of the systems.

Gain a high-level view and complete control of your exposure by scanning the ports of your infrastructure—this is your baseline. At any time after the fact, you can compare it with the results of a test scan to double-check what additional ports are in use. If there is a discrepancy, you can then investigate to find out why, and address any potential risks.

Furthermore, by using firewalls and proxies, you can cut off unnecessary connections between different parts of your network that, if left open, provide easy access from one to another for cybercriminals.

Set up a DMZ *(a demilitarized zone)* between your internal network and the Internet, so that attackers cannot easily pivot between systems. Also, monitor and track any remote access to your network that is required as a part of the work your staff does. Configuration policies for such access should be regularly scanned to double-check that patches are applied and everything is up to date.

14.Implement A Security Awareness and Training Program

Organizations are often at risk based on the weakest links in their cybersecurity—poorly trained employees. That's why continuous training with a variety of different methodologies is necessary in order to have employees be knowledgeable and aware.

Security awareness training helps users to recognize and avoid being victimized by phishing emails and scam websites. They learn how to handle security incidents when they occur. If users are informed about what to watch for, how to block attempts and where they can turn for help, this alone is worth the investment.

Make sure your staff knows how to identify and address suspicious emails, phishing attempts, social engineering tactics, and more. Implement training that shows how to use business technology without exposing data and other assets to external threats by accident.

Test your staff on how to respond when they suspect that an attack is occurring or has occurred.

15.Service Provider Management

Supply chain attacks—targeting weak points in organizations multiple degrees separated from your business—are on the rise.

Are you sure the businesses you work with are upholding their end's cybersecurity? Any third-party organizations that access your data need to properly demonstrate that they;re preventing vulnerabilities from affecting your cybersecurity.

Consider making CIS control compliance a part of your contracts with third-parties.

16.Application Software Security

Depending on how many different programs you use for your operations, and how specialized they are, they could pose a risk to your systems based on unidentified vulnerabilities or lack of support.

As with so many other controls on this list, this is all about making sure that you have a clear, high-level view of what is in use, and the state it is in. Make sure that third-party software is still supported by the vendor, and double-check what its life cycle is. Use a web application firewall to inspect traffic for common vulnerabilities.

Regularly test your internally developed software for errors and vulnerabilities, use a web application scanner to test all software on at least a monthly basis, and segregate production and development environments for internally developed software.

17. Incident Response and Management

An Incident Response Plan provides the plans, procedures, and guidelines for the handling of data breach events at your office*(s)*, or via any of your servers or mobile devices.

The plan encompasses procedures on incident response engagement and how the incident response team will communicate with the rest of the organization, with other organizations, with law enforcement and provides guidance on federal and local reporting notification processes.

This plan is necessary to clarify the roles and responsibilities of your employees so you can quickly mitigate risks, reduce the organization's attack surface, contain and remediate an attack, and minimize overall potential losses.

There are three main components of an incident response plan: technical, legal, and managerial.

As part of your plan, designate specific, skilled people who are best positioned to cover those functions. Make sure you answer the following questions:

- What information does each component need?
- What should you expect from each component?
- What's the chain of command?
- To whom does the team report?
- Who has the authority to make judgment calls as to when the computer networks will be taken down, quarantined, or put back online?

Double-check that your legal, technical, and management experts approve of your incident response plan. And make sure your response team regularly reviews and practices the plan.

---

18. Penetration Tests And Red Team Exercises

The last control on the list is one of the most important. After all, no matter how carefully you follow the prior 17 controls, you'll never know how effective they are if you don't test them.

The penetration test is an authorized attack on your organization's technology and staff and is one of the best ways to accurately evaluate your security controls. In combination with a red team exercise *(in which a full-scope attack simulation is executed to test organizational security)*, you can double-check each and every aspect of your cybersecurity posture.

Running an effective penetration test and red team exercises all come down to goals. Before undertaking one of the test processes, answer the following questions:

- Do you want to test external or internal defenses?
- Do you want to test employee security knowledge and capabilities via red team social engineering simulations?
- Do you want to target a specific section of your network?
- Are there any systems that should not be targeted in the test?

Don't Make Dangerous Assumptions About Your Cybersecurity

The AMT team knows that the only way to effectively develop cybersecurity is through a fully managed approach that builds a culture of best practices, in combination with a range of carefully chosen technologies.

We can provide expert assistance implementing CIS' security controls to address your company's specific needs, and we can do this in a cost-effective manner.

Set a meeting with our team to get started.

allmountain technologies

(970) 748-8880 | allmtntech.com | info@allmtntech.com