Towerwall
Protecting Data Integrity

Michelle Drolet
CEO, Towerwall

20 CRITICAL SECURITY CONTROLS AS PROPOSED BY THE CENTER FOR INTERNET SECURITY

Introduction

Cyberattacks are costing businesses between $400 billion and $500 billion per year, depending on which analysts you listen to. Cybersecurity has never been a hotter topic. The market is expected to grow from $106 billion this year to more than $170 billion by 2020, according to ***Markets and Markets***. The average cost of a data breach, by the time you factor in remediation, non-compliance fines, and brand damage, is tough to accurately calculate, but it's high, and it's rising.

The Heartbleed vulnerability was 2014's catastrophic security bug, and it had a wide-reaching impact. But even as companies pour more money into security services and platforms, the exploit still remains on many servers. As the Internet of Things (IoT) threatens new avenues of risk, the response in the enterprise is mixed, and good practices in some areas are being severely undermined by a casual approach in others.

We hear plenty about the growth in software vulnerabilities, the rise of malware and ransomware, and the risk of ignoring threats, but what should you be doing?

A great place to start creating your InfoSec framework is with the ***CIS*** (Center for Internet Security) Critical Security Controls. This is a recommended set of best practices, put together by government and law enforcement agencies, that focuses on actionable ways to bolster your cyber defenses.

Michelle Drolet, CEO, Towerwall

This eBook strives to make the 20 security controls as described in detail by the *SANS institute* more accessible to everyday business people.

Taking any one of these 20 actions on the list will have a positive impact on your security status, but the smart move is to work towards fulfilling all 20 of these recommendations. These are simple common-sense rules, but you'd be amazed at how often they're overlooked.

In this eBook we're going to break them down and explain each one in turn, looking at why they're important and how you can fulfill them.

Implement all 20 and you'll be well on your way to a solid InfoSec framework that will dramatically diminish your risk of suffering a successful cyberattack.

Information security practices require a lot of expertise best left to InfoSec professionals. Your organization's welfare is at stake. Let us be your partner on this path to securing your networks.

Contents

Use CSC to help build your InfoSec framework

Critical Security Controls is a set of best practices devised by the Center for Internet Security, anonprofit dedicated to improving cybersecurity in the public and private sectors.

Cyberattacks are costing businesses between $400 billion and $500 billion per year, depending on which analysts you listen to. Cybersecurity has never been a hotter topic. The market is expected to grow from $106 billion this year, up to more than $170 billion by 2020, according to ***Markets and Markets***. The average cost of a data breach, by the time you factor in remediation, non-compliance fines, and brand damage, is tough to accurately calculate, but it's high, and it's rising.

The ***Heartbleed vulnerability*** was 2014's catastrophic security bug, and it had a wide-reaching impact. But, even as companies pour more money into security services and platforms, the exploit still remains on many servers. As the IoT threatens new avenues of risk, the response in the enterprise is mixed, and good practices in some areas are being severely undermined by a casual approach in others.

Critical Control 1 - Inventory of Authorized and Unauthorized Devices

Building a good security foundation is about asking the right questions and identifying gaps in your knowledge. This first control is absolutely fundamental to security, but many organizations will struggle to answer questions like:

- *How many servers do you have in total?*
- *How many devices are connected to your network?*
- *How secure are your firewalls, switches and routers?*
- *Can you control what joins your network?*

There's no way you can have a complete map, or flag potential vulnerabilities, without knowing exactly what hardware you have. An up to date, comprehensive hardware inventory is essential.

Critical Control 2 - Inventory of Authorized and Unauthorized Software

You should take this together with the first control, and devise a list of authorized software that covers every system and device you're using. You'll need to monitor your software in real-time to validate versions and ensure that unapproved apps are blocked or, at least, flagged.

To ensure vulnerabilities and exploits are dealt with in a timely fashion, you also need to know what operating systems and versions of software are in use, and have a system to flag necessary updates based on new threats as they emerge.

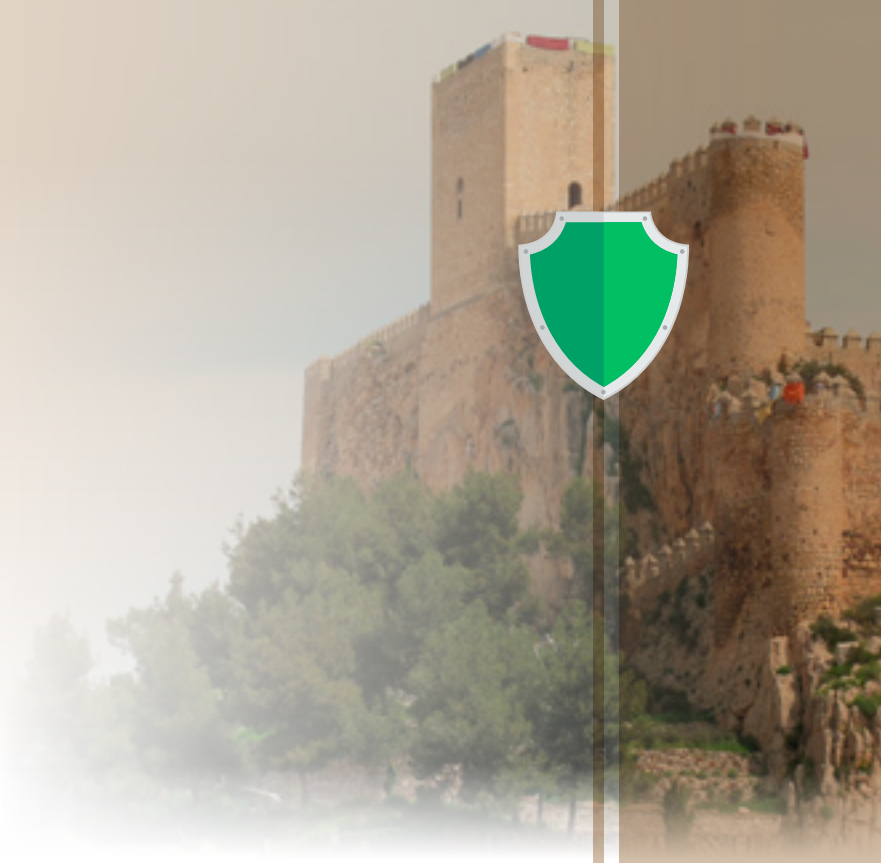
Critical Control 3 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

The laptops, computers, and other hardware in your office are not secure out of the box. The default configurations for new devices in terms of the operating systems and pre-installed applications are designed for an easy setup, NOT for security. Common vulnerabilities are well known and this makes hardware and software in its default state ripe for exploitation.

You should develop a security baseline for every software system and create standardized images that are securely stored and deployed through secure channels. It's also important to validate these configurations and update them on a regular basis to manage any new vulnerabilities that are discovered.

IT TAKES TIME

As you can see, simply creating an accurate inventory of your hardware and software can be a big undertaking. What's important is to formulate a plan that takes a holistic view. Start working through the steps outlined in this eBook and your defenses will be strengthened.



Stay vigilant and act quickly if you want to stay secure

Keep checking for vulnerabilities, control privileges, and monitor your logs

In the previous chapter, we looked at how Critical Security Controls (CSC) can help you build your InfoSec framework starting with getting a handle on your software and your hardware inventories. This chapter will discuss the importance of continually assessing and remediating vulnerabilities, keeping a tight control of administrative privileges, and monitoring your audit logs. These concepts are encapsulated in CSCs 4, 5, and 6.

You should develop stringent policies, consider devoting resources to properly circulating them and educating employees, and continually measure their effectiveness, making changes wherever necessary.

Critical Control 4 - Continuous Vulnerability Assessment and Remediation

New ***vulnerabilities emerge every day***. If you aren't continually scanning for them, then cybercriminals have an advantage they can exploit. The idea that you can put security in place and then rest on your laurels is dangerous. Identifying vulnerabilities is not enough, you also have to take action.

If you don't find and deal with vulnerabilities, then you're a sitting duck, when you really want to be a moving target.

It takes organizations 176 days on average to remediate a vulnerability, but it only takes a cybercriminal an average of 7 days to exploit it, according to NopSec's 2015 State of Vulnerability Risk Management report. It's vital to root out vulnerabilities and be proactive about addressing them or you will be compromised.

Think about the following:

- *Automated real-time vulnerability scanning with intelligence updates*
- *Automated patch management for all software*
- *Compare results to confirm vulnerabilities have been patched*

You will also need to consider patch evaluation in a test environment to ensure business functions aren't going to be adversely impacted. In some cases, alternative countermeasures to deal with a vulnerability might be necessary. It can also be a good idea to phase your patch rollouts to minimize disruption and prioritize patches for the riskiest vulnerabilities.

Critical Control 5 - Controlled Use of Administrative Privileges

The weakest link in your defenses is very often your employees. Verizon's 2015 Data Breach Investigations Report revealed that more than two-thirds of cyber-espionage incidents are a result of phishing scams. It's much easier for cybercriminals to get around your defenses by hacking passwords or tricking employees with administrative privileges into unwittingly downloading malware. You can ***stop insider attacks with the right tools***, but it pays to tighten your policy in general.

- *Minimize administrative privileges*
- *Validate accounts and make sure privileges have been authorized*
- *Enforce usage of complex passwords and make sure they're encrypted*
- *Flag new accounts and login attempts*

Keeping tight control over administrative privileges can drastically reduce the risk of a data breach.

Critical Control 6 - Maintenance, Monitoring, and Analysis of Audit Logs

If you don't maintain a system of audit logs, you may not even be able to determine when you've been attacked. According to the ***2015 Trustwave Global Security Report*** only 19% of data breaches in 2014 were detected by the victim organization. It's not unusual for companies to collect logs, but never check them, leaving breaches

undetected for months. Many companies keep records in order to tick a compliance box, but if you don't monitor and analyze them thoroughly, then they aren't doing their job.

- *You need at least two synchronized time sources for consistent timestamps*
- *Audit logs should be validated and recorded in a standardized format*
- *Make sure you have storage space and retain logs for a decent length of time*
- *Consider using separate logging servers to prevent attackers manipulating logs*
- *Collect, aggregate, and analyze logs regularly*

Proper analysis will help you to detect, understand, and recover from an attack.

MEASURE YOUR EFFECTIVENESS

When you're trying to monitor vulnerabilities, privileges, and logs in real-time, you'll often rely upon automated software systems to gather the data you need and flag any potential issues. Make sure that you test their effectiveness regularly. Dummy attacks [or staged attacks] can help you to identify weaknesses and flaws in your defenses.

Time is of the essence. The faster you remediate vulnerabilities, identify suspicious behavior, and uncover attacks, the better. You should set benchmarks for performance and put metrics in place, so that you can ensure your security performance is actually meeting expectations. Keep working to improve that performance and you can make life untenably difficult for would-be attackers.

Build malware defenses and control your email, web browsers, and ports

Our last chapter looked at applying Critical Security Controls 4, 5, and 6 to your organization, covering vulnerability assessment, administrative privileges, and audit logs. Now, it's time to move on to CSCs 7, 8, and 9.

Email programs and web browsers are still the most common points of entry for attackers. Too many companies have woefully inadequate malware defenses, and a failure to control ports and limit services is like leaving a window open for cybercriminals.

Critical Control 7 - Email and Web Browser Protections

Human behavior is still the path of least resistance for cybercriminals and they often employ social engineering techniques to gain access to systems. Despite the rising profile of phishing, 23% of recipients open phishing messages, and 11% click on attachments, according to Verizon's ***2015 Data Breach Investigations Report*** (DBIR).

Dodgy attachments, spoof websites, and vulnerable plug-ins can all be used by attackers to gain a foothold.

It's vital to ensure that web browsers and email programs are kept fully up to date. Don't allow employees to use unsupported browsers or email programs, and prevent them from installing unnecessary plug-ins or add-ons. All URL requests should be logged, and you should have a filter in place that blocks access to unauthorized websites. All email attachments should be scanned and blocked if they are unnecessary for business.

Keeping tight control over web browsers and email like this doesn't just reduce the risk of phishing, it also reduces spam, and helps prevent wasted time.

Critical Control 8 - Malware Defenses

There are five malware events every second, according to Verizon's 2015 DBIR report, and malware can come into your system from all sorts of sources including email, cloud services, web pages, smartphones, or even USB thumb drives.

It may not always be possible to detect it at the point of entry, but you can ensure that it's detected and stopped before it can do too much damage by putting the right defenses in place.

Employing automated tools for real-time monitoring and threat assessment should be mandatory. You need malware defenses deployed throughout your system. Sadly, a ***Ponemon Institute report*** found that only 41% of respondents had automated tools to capture intelligence and evaluate the true threat of malware, even though organizations with automated tools reported that they can handle 60% of malware containment without human intervention, saving a huge amount of time and resources.

It makes sense to limit the use of external devices, use network-based anti-malware tools that can pick malicious content out of the traffic flow, and ensure that updates for your defenses are automated.

The expense of investigating malware incidents is high and inaccurate intelligence is common. Spend money on improving your intelligence and automated containment, and you won't have to spend as much on security staff investigations.

Critical Control 9 - Limitation and Control of Network Ports, Protocols, and Services

Configuration errors, remote access, and default services in newly installed software can leave a window open for would-be attackers. All of the ports, protocols, and services on all of your networked devices need to be properly managed. That means tracking them, controlling, and correcting them where necessary.

Your IT staff needs to have a clear picture of what is and isn't needed. A clear configuration plan at the outset can save a lot of time spent fixing problems further down the line.

Scan ports, review services, and shut down anything that isn't necessary for business operations. Make sure that you verify servers, and put firewalls in place to validate traffic. These are simple vulnerabilities for attackers to exploit, but they're also easy loopholes to close, so close them!

DON'T DELAY

Educate your employees on these issues and put the right systems in place to ensure they aren't a weak spot for your organization. Remember to measure the effectiveness of your automated systems, and make sure you learn from mistakes and failures.

The most effective defense against phishing, malware, and vulnerability exploitations is a multi-pronged strategy that includes security expertise, educated staff, automated real-time systems, and clear, concise policies that are validated.

Create a data recovery plan and secure your network

We discussed building malware defenses, now we're going to focus on Critical Security Controls 10, 11, and 12, covering data recovery, secure network configuration, and boundary defense.

It's unrealistic to think that you can completely avoid cyberattacks and data breaches, so it's vital to have a proper data recovery plan in place. You can also tighten your defenses significantly by ensuring all of your network devices are properly configured, and by putting some thought into all of your potential network borders.

Critical Control 10 - Data Recovery Capability

Do you have a proper backup plan in place? Have you ever tested it to see that it works? Disaster recovery is absolutely vital, but an alarming number of companies do not have an adequate system in place.

A survey of 400 IT executives by ***IDG Research*** revealed that 40% rate their organizations' ability to recover their operations in the event of disaster or disruption as "fair or poor". Three out of four companies fail from a disaster recovery standpoint, according to the ***Disaster Recovery Preparedness Benchmark***.

A successful malware attack can lead to altered data on all compromised machines and the full effects are often very difficult to determine. The option to roll back to a backup that predates the infection is vital. Backed up data must be encrypted and physically protected. It's also important that a test team routinely checks a random sampling of system backups by restoring them and verifying data integrity.

Critical Control 11 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

The default configurations for network devices like firewalls, routers, and switches are all about ease of use and deployment. They aren't designed with security in mind and they can be exploited by determined attackers. There's also a risk that companies will create exceptions for business reasons and then fail to properly analyze the potential impact.

The 2015 Information Security Breaches Survey found that failure to keep technical configuration up to date was a factor in 19% of incidents. Attackers are skilled at seeking out vulnerable default settings and exploiting them. Organizations should have standardized secure configuration guidelines applied across devices. Security updates must be applied in a timely fashion.

You need to employ two-factor authentication and encrypted sessions when managing network devices, and engineers should use an isolated, dedicated machine without Internet access. It's also important to use automated tools to monitor the network and track device configurations. Changes should be flagged and rule sets analyzed to ensure consistency.

Critical Control 12 - Boundary Defense

When the French built the Maginot Line in WW2, a series of impregnable fortifications that extended along the border with Germany and beyond, it failed to protect them because the Germans invaded around the North end through neutral Belgium. There's an important lesson there for security professionals. Attackers will often find weaknesses in perimeter systems and then pivot to get deeper into your territory.

They may gain access through a trusted partner, or possibly an extranet, while your defensive eye is focused on the Internet. Effective defenses are multi-layered systems of firewalls, proxies, and DMZ perimeter networks. You need to filter inbound and outbound traffic and take caution not to blur the boundaries between internal and external networks. Consider network-based IDS sensors and IPS devices to detect attacks and block bad traffic.

Segment your network and protect each sector with a proxy and firewall to limit access as far as possible. If you don't have internal network protection, then an intruder can successfully breach the outer defenses.

THE REAL COST

A lot of businesses argue that they can't afford a comprehensive disaster recovery plan, but they should really consider whether they can afford to lose all their data or be uncertain about its integrity. They may lack the expertise to ensure that network devices are securely configured, but attackers don't lack the skills to exploit that. It's understandably common to focus on the outer boundary of your network and forget about threats that come from unexpected directions or multiply internally, but it could prove costly indeed.

Compared to the cost of a data breach, all of these things are cheap and easy to set up.

Protect your data and control access

We delved into disaster recovery and network security, now it's time to take a look at Critical Security Controls 13, 14, and 15, which cover data protection and access control.

A company's data is its crown jewels and because it's valuable there will always be people looking to get their hands on it. Threats include corporate espionage, cybercriminals, disgruntled employees, and plain old human error, but it's relatively easy to reduce your potential exposure. You need to protect your data, use encryption and authentication, and carefully restrict access.

Critical Control 13 - Data Protection

Do you know where your data is? A ***Voltage Security survey*** of nearly 300 IT professionals found that 48% didn't even know which countries their data resided in once uploaded. Using cloud services and offering mobile device access is the norm now, and it delivers many business benefits, but we must take care to limit and audit data flow.

The most obvious first step is to encrypt your data at all times – in transit and at rest. Use popular cryptographic algorithms and evaluate on an annual basis to ensure your protection is still strong. You can refer to the ***National Institute of Standards and Technology*** (NIST) for recommendations and further information. If properly encrypted, even compromised data will be inaccessible to attackers.

Identify sensitive data and take steps to ensure it's always encrypted. Use monitoring tools to expose suspicious activity and unauthorized attempts to access data and flag them. Do regular scans to ensure that no plain text data is on your systems. Prevent write access, block file transfer websites, and be vigilant for rogue connections.

Critical Control 14 - Controlled Access Based on the Need to Know

Far too many companies don't distinguish between sensitive data and publicly accessible information. If attackers gain entry through a weak link, then they essentially have access to the entire network. Of 2,260 confirmed breaches, 63% leveraged weak, default, or stolen passwords according to Verizon's ***2016 Data Breach Investigations Report***. If you don't restrict access to data based on who actually needs it, then you are presenting a much larger potential attack surface.

Divide your data into categories and make sure that sensitive data is protected and can only be accessed by authorized employees with a legitimate reason to access it. If sensitive data must be sent across less-trusted networks, then make sure it's encrypted. Use authentication to verify the person accessing the data and create audit logs that can be scanned for suspicious behavior. Restricting data access strictly to what's required for each job role is essential if you want to prevent a sensitive data breach.

Critical Control 15 - Wireless Access Control

Wireless access is ubiquitous now, but the added convenience comes at a cost in terms of security. Attackers can potentially gain access without even having to gain entry to your building. It's also alarmingly common for wireless attacks on traveling employees to result in data loss and sometimes infection which is then carried back into the office. The BYOD trend has drastically increased the number of devices that could be usefully compromised from an attacker's perspective.

You can clamp down on this threat by ensuring that every wireless device connected to your network has an authorized configuration and security profile. If you don't know what the device is or who owns it, then it doesn't get access. The network should be scanned constantly to identify rogue access points or unauthorized devices and to expose attempted attacks.

In some cases, business hardware can be configured to block wireless access or to restrict it to authorized wireless networks only. Consider blocking the use of wireless peripherals, such as Bluetooth headsets, which can be very insecure. Always use encryption and authentication. Create separate virtual local area networks for untrusted devices and make sure all that traffic is filtered and audited.

TIGHTEN UP

It will take some time to classify your data and create a hierarchy of access based on job roles, but it’s a necessary foundation for data security. It’s not enough to have a system to protect your data and restrict access, you must also continue to monitor and audit to identify weak spots and then act immediately to strengthen them.

Don’t make it easy for attackers.

Cybersecurity is only as strong as the weakest link

Stay on top of account management and assess staff security skills with CIS Controls 16 and 17.

In our last chapter we explored ways to protect data and control access to it. Today, we're going to focus on your biggest asset and a potential weak link in your armor – your staff. We're going to look at Critical Security Controls 16 and 17, covering account management, security skills assessment, and training.

You can have the most secure system in the world, but hackers will always seek out the path of least resistance. When your defenses are good, the weak link is often your employees. Data breaches are most likely to be the result of employee error or an inside job, according to the ***ACC Foundation: State of Cybersecurity Report***.

It's good to focus on firewalls, malware defenses, and data protection, but too often employees are an afterthought.

Critical Control 16 - Account Monitoring and Control

Inactive user accounts are ripe for exploitation by attackers. By using legitimate, but inactive accounts, they can easily impersonate legitimate users and mask their nefarious activity.

There's also serious potential risk involved when accounts associated with former employees or temporary contractors are not deleted when employment ends. They may be left with unauthorized access to sensitive data, which is especially dangerous if the split wasn't amicable. Some unscrupulous former employees may see an opportunity to profit.

There are a few simple rules you can put in place to ensure inactive accounts aren't a potential route in for attackers or a potential route **out** for sensitive data.

- *Account access should be revoked immediately when an employee or contractor is terminated or leaves for any reason. You may prefer to disable access, rather than delete accounts.*
- *Accounts should be monitored and flagged if they don't have an associated business process and owner.*
- *Automatically log off users after a period of inactivity and use screen locks to guard against access via unattended computers.*
- *Be vigilant for failed log-ins and attempts to access deactivated accounts.*
- *Profile user behavior so that log-ins at odd times of the day or night, or log-ins from new devices, are flagged.*

You'll also want to enforce multi-factor authentication wherever possible, ensure that passwords and usernames are fully encrypted, and configure and authenticate centrally.

Careful account monitoring is especially important at large organizations where breaches are more than twice as likely, according to that same ACC Foundation report.

Critical Control 17 - Security Skills Assessment and Appropriate Training to Fill Gaps

It's easy to focus in on the technology that you need to employ to bolster your cybersecurity defenses and forget that people can neatly sidestep all your efforts by taking the wrong action. Perhaps your IT staff aren't quick enough to patch or review logs, maybe your security policies are not enforced in any meaningful way, or your employees don't know better than to click on a malicious link in a phishing email.

Attackers will go to great lengths to exploit any weaknesses or gaps here, and in many cases they can persuade people to effectively lower the defenses and let them in.

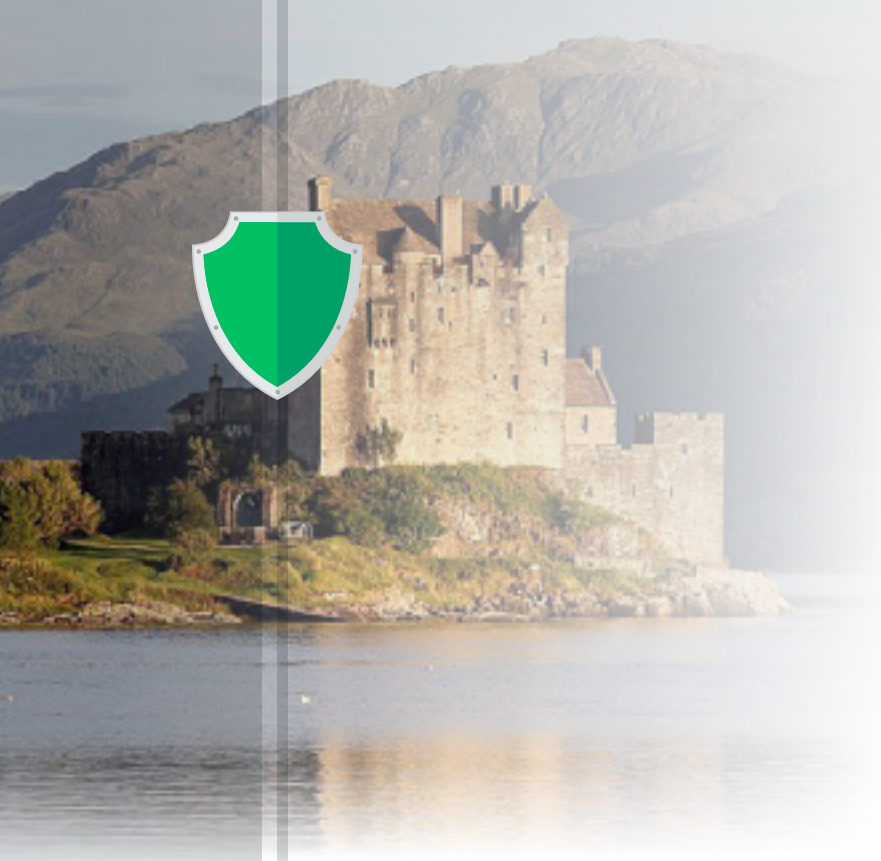
The first thing to do here is to perform gap analysis and find where employees lack the skills required to implement your cybersecurity plans and policies. You have to know where they are going wrong before you can hope to fix it.

Provide relevant training via senior staff with the right skills, outside experts, or even conferences and online courses. Make learning modules bite-sized and easy to understand. They must be updated to reflect the latest

threats and employees should complete them every few months. No one should be immune from this. Senior management may be resistant, but they actually pose the greatest risk if a phishing attack is successful, so they should complete the same training.

JPMorgan boosted its cybersecurity spending after a data theft, but when it tested staff with a fake phishing email a few weeks later, ***20% of them clicked on it***. Had it been real, that action would have downloaded a malicious payload onto the bank's network.

If you don't take some time out to spend resources on awareness for employees and specific training where necessary, then you can undo all your good efforts to improve your cybersecurity.



Always be prepared: monitor, analyze and test your security

Stay vigilant, plan your response and test your defenses with CIS Controls 18, 19 and 20

This is the final chapter in our series on the 20 Critical Security Controls devised by the Center for Internet Security (CIS) as best practices to help the public and private sectors tighten their cybersecurity. We started down the path of building a solid security foundation by taking inventory of hardware and software, we looked at vulnerability assessment and administrative privileges, and we discussed how to build malware defenses. We've also explored how to create a data recovery plan, how to protect your data, and the importance of monitoring and training employees.

We've reached the last three Critical Security Controls. This chapter will round off our eBook with a look at the importance of monitoring software, establishing a response protocol, and conducting pen tests and red team exercises.

Critical Control 18 - Application Software Security

Vulnerabilities in software offer a potential route into your organization for attackers. Vulnerabilities can be caused by a wide variety of different errors, so you have to take steps to prevent them, detect them, and correct them. When a vulnerability is present in open source software, it's more likely to become common knowledge and be exploited by attackers. Consider that 93% of organizations use open source software and 78% run part or all of their operations on it, according to ***The Tenth Annual Future of Open Source Survey***.

It's vital to ensure that all the software you use is fully updated to the latest version and patched for the latest security fixes. Web application firewalls should be deployed to inspect traffic and identify common attacks. In-house and third-party software must be stringently tested to identify security weaknesses. Avoid exposing error messages to end users and don't allow developers unmonitored access to production environments. Your developers should ideally have some training in Secure Development Life Cycle (SDLC). A great resource to learn more about web application security is ***OWASP***.

Critical Control 19 - Incident Response and Management

Assuming that you can completely block all attacks is not realistic, no matter how many resources you devote to security. Incidents will occur from time to time, so you must have a framework in place to discover them, contain the damage, purge the attacker and restore your systems. Far too many companies find vulnerabilities or suspicious activity, but fail to take action swiftly enough to limit the damage.

You need a clear incident response plan with procedures to follow and a hierarchy of roles assigned, so that everyone understands their responsibilities. Make sure that the key players are empowered to take the necessary actions to deal with an incident. You should also establish standards to ensure that incidents are reported in detail in a timely manner and meet all legal and regulatory requirements. All employees should be aware about who in the organization needs to know about an incident for it to be resolved. When you have a plan in place, test it with a mock scenario [tabletop exercise] to ensure that it works as expected.

Critical Control 20 - Penetration Tests and Red Team Exercises

The only way to ensure that your defenses actually work is to simulate real world situations and emulate a cyber-attack. Hire someone or a group, to play the part of an attacker ["the red team"] and have them try to gain access to your systems and data. An experienced security professional can view your organization as an attacker might and find the weak spots to exploit. This will help you to find gaps that need to be plugged.

Internal and external penetration testing should reveal vulnerabilities that attackers might use to breach your systems. With a clear demonstration of where a problem lies, you can plan mitigation. Red team exercises take a holistic view of your defenses, including your policies and processes, to identify where improvements might be made. Both penetration tests and red team exercises should be conducted regularly and the results should show a steady improvement over time.

Your security has to evolve over time, because attackers are constantly developing new methods and finding new ways in. Your security standards and your response plan depend upon monitoring, analysis and testing to be truly effective.

We hope this CIS Critical Security Controls eBook has been useful for you as an introduction to security standards. Follow these best practices and you can dramatically reduce your potential attack surface and make life much harder for any would-be attackers.

About Towerwall

Founded in 1993 and based in Framingham, Massachusetts, Towerwall provides organizations such as AMG, Middlesex Savings Bank, Becker College, CannaCare, Allegro MicroSystems and Smith & Wesson, with IT security technology services required for secure business-class networks. Strategic partnerships with Sophos, Varonis, AlienVault, Websense, Snoopwall, Qualys, and many other nationally-recognized security vendors allows Towerwall to offer its customers an integrated approach to solving their security needs by coupling best-of-breed technology with top-notch integration services. For more information please call (774) 204-0700 or email us at ***info@towerwall.com***.