TECHNOLOGY BRIEF

A Quick Look into the Center for Internet Security (CIS) Controls Cybersecurity Framework

Prepared by

RAVENTEK

Background

It's shouldn't come as a surprise that the exhaustive list of cybersecurity breaches over the last decade is quite extensive. CSO.com recently reported that 3.5 billion personal records were exposed from just the top two breaches in recent history. [1] The diversified totality of industries hit is evidence that threat actors are target agnostic.

With economists now placing the value of data above that of oil - are enterprises getting any better at protecting their most valuable asset from cyber-attacks? [2] The consensus between industry experts is a resounding "no." The reality is when breaches happen, enterprises loose money. While the age of cloud computing has lead to advances in IoT devices, Software-as-a-Service (SaaS) and the ability to work remotely from anywhere, these advancements come paired with a larger attack surface for threat actors across the enterprise. Organizations are not where they need to be when it comes to protecting their online ecosystems against attacks and the reality of the situation is troubling.

But there is good news - it is possible to significantly reduce your risk of cyber-attack.

RavenTek has looked to the Center for Internet Security (CIS) Controls [3] as a framework to help build, strengthen and maintain a strong cybersecurity posture for our customers. The CIS provides a framework for organizations to improve their security posture while also creating a culture of compliance. At the end of the day, no single tool will a substitute for action. The controls are only as good as the people and resources implementing them and the Culture of the Organization trying to implement them.

The following summary of the CIS framework was prepared to help information technology (IT) leaders and security teams gain visibility throughout their enterprise technology stack. Our methodology allows for a more sophisticated and refined understanding of what IT leaders are "looking for" versus what they are "looking at" which leads to a more conscientious approach in their decision-making process.

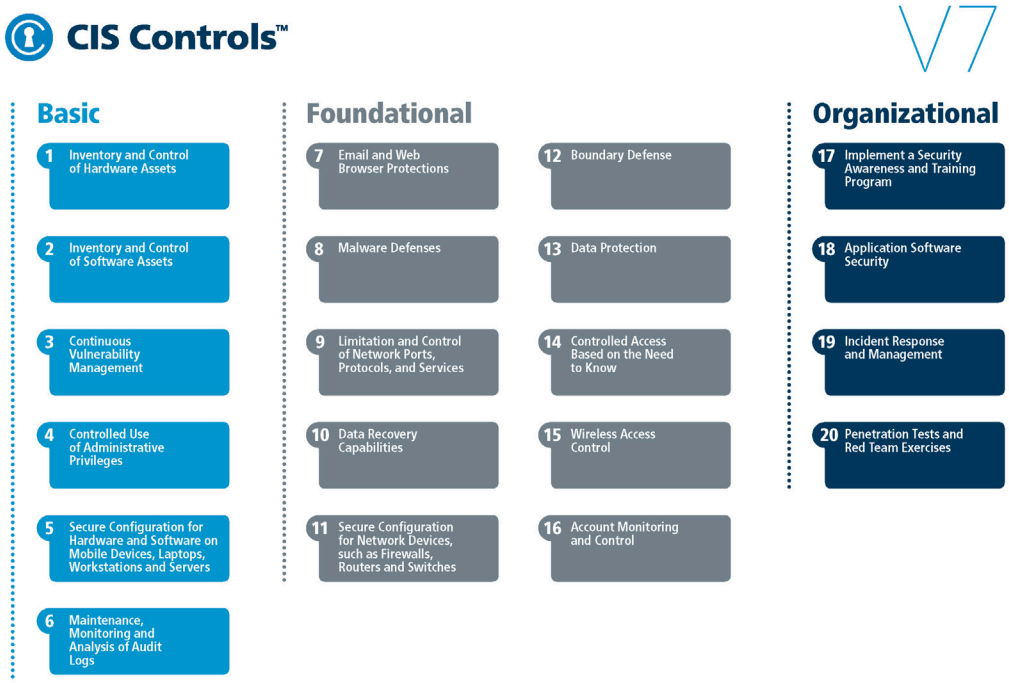
There is an adage that there are two types of organizations: Those who have been hacked and know it and those who have been hacked and don't know it. Understanding the CIS Top 20 can help IT leaders with the groundwork to identify which of the two camps their enterprises fall into. With this in mind, RavenTek's approach provides for a continuous beat of the drum to focus on what matters most. It will require the tenacity to fight message fatigue to ensure that your organization remains vigilant.

The Red Cross First Aid Handbook says it best… "Apply constant and appropriate pressure to stop the bleeding". [4] RavenTek is prepared to help you do just that.

1 Swinhoe, D. (2020, April 17). The 15 biggest data breaches of the 21st century. Retrieved from www.csoonline.com
2 The Economist. (2017, May 7). The world's most valuable resource is no longer oil, but data. Retrieved from www.economist.com
3 The Center for Internet Security (CIS). The 20 CIS Controls & Resources. Retrieved from www.cisecurity.org
4 American Red Cross. First Aid for Severe Bleeding Online Course. Retrieved from www.redcross.org

The Center for Internet Security (CIS)

outlines the top 20 controls into three categories:



The Center for Internet Security (CIS). CIS Controls Version 7 – What's Old, What's New. Retrieved from www.cisecurity.org

1 Basic: Controls 1-6

The Basic Controls are intended to be the baseline for protecting your organization from cybersecurity risk. ***It includes actively managing technology assets through inventory control, tracking and correction***. By implementing the first six controls you will be able to prevent 90-95% of all threats and attacks.

2 Foundational: Controls 7-16

The Foundational Controls are technical best practices that provide clear security benefits and are a smart move for any organization to implement.

3 Organizational: Controls 17-20

The first steps in your cybersecurity approach require developing and implementing technical tools to fend off attackers and protect your organizational assets. However, those technical defenses will have limited impact if they are not combined with a robust, strategic approach to cybersecurity processes, training, and attack response across the organization. The Organizational Controls help you solidify your strategy.

Each control is wide in scope but aligns with solid principles: making sure the right users have access to the right assets, and that all systems are kept up-to-date and as hardened as possible.

Basic CIS Controls

CIS Control 1: Inventory and Control of Hardware Assets
Actively manage all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

CIS Control 2: Inventory and Control of Software Assets
Actively manage all software 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.

CIS Control 3: Continuous Vulnerability Management
Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

CIS Control 4: Controlled Use of Administrative Privileges
The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CIS Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
Establish, implement, and actively manage the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs
Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Foundational CIS Controls

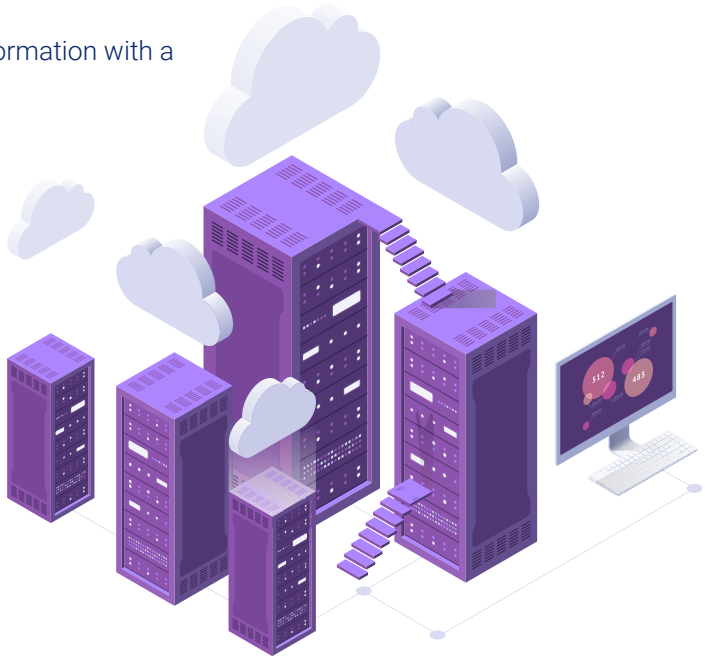
CIS Control 7: Email and Web Browser Protections
Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

CIS Control 8: Malware Defenses
Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Foundational CIS Controls

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services
Actively manage the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

CIS Control 10: Data Recovery Capabilities
The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.



CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
Establish, implement, and actively manage the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CIS Control 12: Boundary Defense
Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

CIS Control 13: Data Protection
The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

CIS Control 14: Controlled Access Based on the Need to Know
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources and systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

CIS Control 15: Wireless Access Control
The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.

CIS Control 16: Account Monitoring and Control
Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

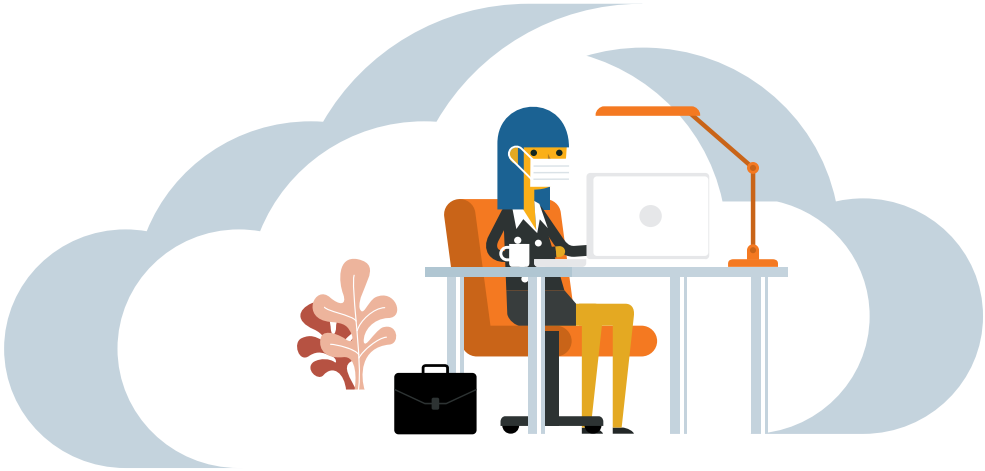
Organizational CIS Controls

CIS Control 17: Implement a Security Awareness and Training Program

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

CIS Control 18: Application Software Security

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.



CIS Control 19: Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications and management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

CIS Control 20: Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defense (the technology, the processes and personnel) by simulating the objectives and actions of an attacker.

Let's Get Started

RavenTek believes that cybersecurity is not simply an investment in tools or technology - it requires a "Culture of Compliance" to ensure the human element makes your employees the first line of defense which needs to be continuously strengthened.

Formulated around the CIS Top 20 Controls, RavenTek's cybersecurity roadmap has helped our customers think critically about their security practices and provide comprehensive coverage for any organization to dramatically improve their readiness for cyber-attacks. Our approach has proven to dramatically improve the security posture of your organization and limits the attack surface that attackers can access your most critical infrastructure and data.

RavenTek's goal is to introduce what is possible and how to build a strategic Culture of Compliance at your organization. Contact your RavenTek Enterprise Account Executive to get started.

About RavenTek

RavenTek recognizes that in today's challenging fiscal environment, enterprises and federal agencies alike need the right partner who can help them actualize their digital transformation goals. We are committed to quality solutions which are delivered through our innovative engineering and network of technology partners. Contact us with your requirements, or to learn more about our complete network of products and solutions.

Learn more at **www.raventek.com**.

RAVENTEK 13900 Lincoln Park Dr, Suite 150 | Herndon, VA 20171 | (833) 728-3601