A PRACTICAL GUIDE FOR IT PROS: DO YOU HAVE THESE 8 CORE CYBERSECURITY CAPABILITIES?

October 2023

Derek E. Brink, CISSP
Vice President and Research Fellow, Cybersecurity and IT GRC

ABERDEEN
STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.

Executive Summary

You're already working with your strategic solution providers to leverage the cybersecurity capabilities of their products and services — but you'd also like some practical guidance on how to think more broadly about the cybersecurity needs throughout your environment. Or perhaps you're a value-added reseller, thinking about what additional cybersecurity capabilities should be incorporated into your offerings to current and potential buyers.

In that spirit, Aberdeen offers a practical guide for IT and cybersecurity professionals — in the form of **eight core cybersecurity capabilities** that can help you work through these questions and establish a reasonable sequence of next steps.

It's not practical to address all cybersecurity concerns — so which controls and safeguards matter most?

The so-called "critical security controls" movement has evolved and matured over the last 15 years, but the underlying concept has remained the same: Use the power of the technology professional community to identify a small number of security controls that have shown to have a high payoff in terms of preventing known cybersecurity attacks. The enduring idea has been to help IT and cybersecurity practitioners navigate more quickly through the rich, complex, and ever-changing array of security technologies that are currently available, by distinguishing the *vital few* from the *useful many*.

Along these lines, the latest CIS Critical Security Controls (version 8) describes **18 technical controls** — which then expand into **153 specific actions** to be implemented (the Center for Internet Security refers to these actions as **Safeguards**). CIS also provides a mapping from the Critical Security Controls to the more generalized (and more complex) *NIST Cybersecurity Framework*, for those who need it.

In Aberdeen's view, organizations should be thinking about a particular mix of technical controls and safeguards not as the end in itself, but as the means to establishing a higher-level set of core cybersecurity capabilities — because the landscape of security-related threats, vulnerabilities, exploits, and technologies will continue to evolve over time, but performing well at this handful of foundational capabilities will serve the organization again and again over the long term.

In that spirit, Aberdeen has identified **eight core cybersecurity capabilities** that are enabled by the 18 CIS Critical Security Controls and the 153 associated CIS Safeguards (they are also summarized in Table 1):

Founded in 2000, the Center for Internet Security (CIS) mission is "to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats."

1. **We understand what systems, applications, and service providers are in our environment.**
    - CIS 01: Inventory and Control of Enterprise Assets *(e.g., devices, servers)*
    - CIS 02: Inventory and Control of Software Assets *(e.g., operating systems, applications)*
    - CIS 15: Service Provider Management
2. **We keep our systems and applications securely configured.**
    - CIS 04: Secure Configurations of Enterprise Assets and Software
3. **We keep our networks, systems, and applications patched and up to date.**
    - CIS 07: Continuous Vulnerability Management
    - CIS 10: Malware Defenses
    - CIS 16: Application Software Security
4. **We protect and backup our important data.**
    - CIS 03: Data Protection
    - CIS 11: Data Recovery
5. **We protect our network.**
    - CIS 12: Network Infrastructure Management
    - CIS 13: Network Monitoring and Defense
6. **We manage our users, their accounts, their access to resources — and their behaviors.**
    - CIS 05: Account Management
    - CIS 06: Access Control Management
    - CIS 09: Email and Web Browser Protections
    - CIS 14: Security Awareness and Skills Training
7. **We maintain visibility into what's happening in our environment.**

- CIS 08: Audit Log Management
- CIS 15: Service Provider Management
- CIS 18: Penetration Testing

8. **We are in a position to respond and recover when something goes wrong.**
    - CIS 17: Incident Response Management
    - CIS 11: Data Recovery

Table 1: A practical guide for IT Pros — 8 core cybersecurity capabilities

Aberdeen Strategy & Research		Center for Internet Security (CIS)		
Capability #	**Core Cybersecurity Capabilities**	**Control #**	**Cristical Security Controls**	**# of Safeguards**
1	**We understand what systems, applications, and service providers are in our environment.**	01	Inventory and Control of Enterprise Assets (devices, servers)	5
		02	Inventory and Control of Software Assets (operating systems, applications)	7
		15	Service Provider Management	7
2	**We keep our systems and applications securely configured.**	04	Secure Configurations of Enterprise Assets and Software	12
3	**We keep our networks, systems, and applications patched and up to date.**	07	Continuous Vulnerability Management	7
		10	Malware Defenses	7
		16	Application Software Security	14
4	**We protect and backup our important data.**	03	Data Protection	14
		11	Data Recovery	5
5	**We protect our network.**	12	Network Infrastructure Management	8
		13	Network Monitoring and Defense	11
6	**We manage our users, their accounts, their access to resources — and their behaviors.**	05	Account Management	6
		06	Access Control Management	8
		09	Email and Web Browser Protections	7
		14	Security Awareness and Skills Training	9
7	**We maintain visibility into what's happening in our environment.**	08	Audit Log Management	12
		15	Service Provider Management	7
		18	Penetration Testing	5
8	**We are in a position to respond and recover when something goes wrong.**	17	Incident Response Management	9
		11	Data Recovery	5
8 Capabilities		18 Controls		153 Safeguards

Source: Adapted from *CIS Critical Security Controls* (version 8), Aberdeen, October 2023

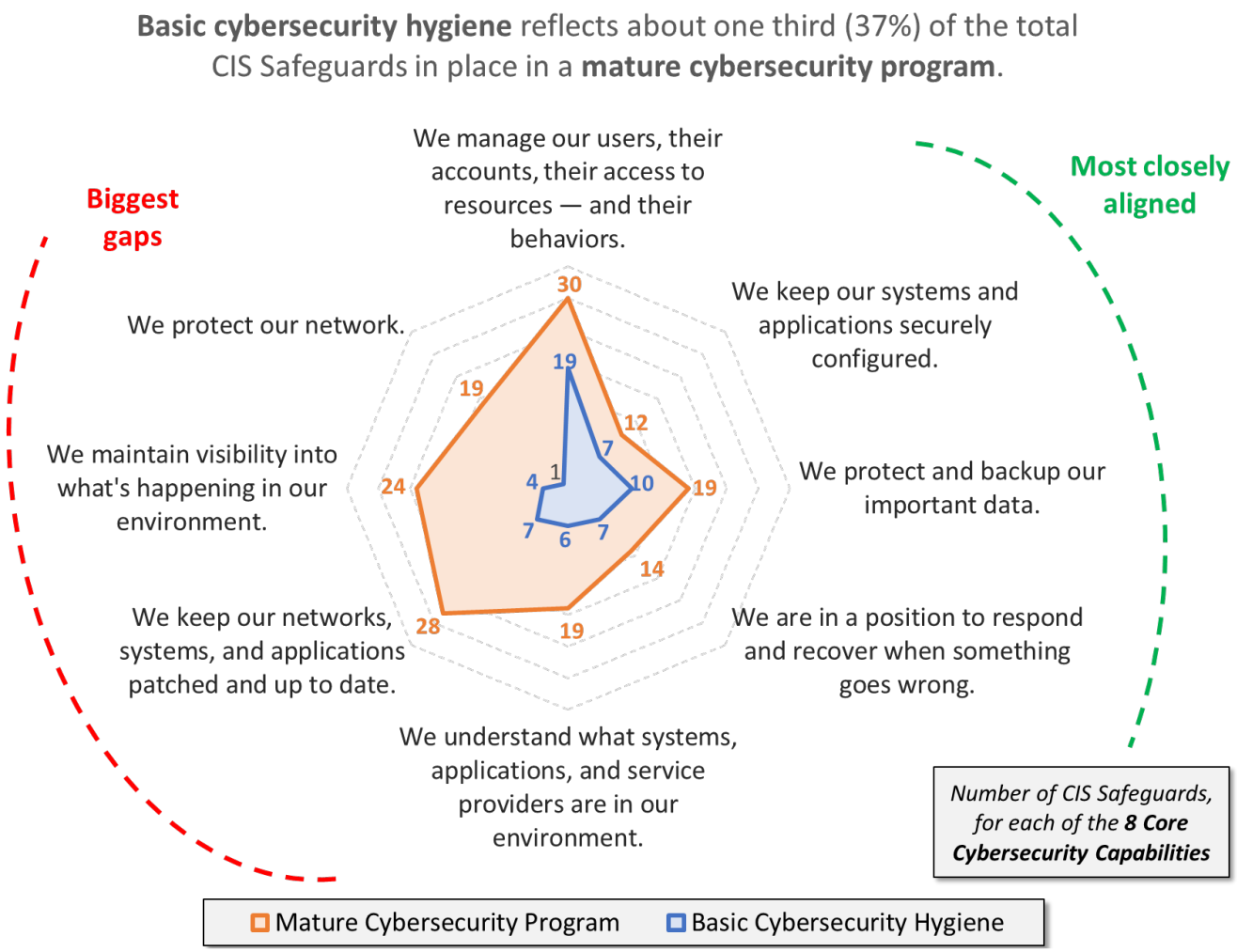
We can't implement every safeguard, everywhere, all at once — so which ones should be first?

Recognizing that no organization can simply flip a switch and implement all of the 153 CIS Safeguards in support of the 18 CIS Critical Security Controls at

once, the Center for Internet Security describes three distinct “Implementation Groups” — ranging from **basic cybersecurity hygiene** (IG1) to a **mature cybersecurity program** (IG3).

Figure 1 shows the differences between these two groups, based on the total number of CIS Safeguards that align with Aberdeen’s eight Core Cybersecurity Capabilities. Altogether, IG1 represents about one third (37%) of the total number of CIS Safeguards associated with IG3.

Figure 1: Comparing the CIS Safeguards for basic security hygiene (CIS IG1) versus those in a mature security program (CIS IG3)



Source: Adapted from *CIS Critical Security Controls* (version 8), Aberdeen, October 2023

The Core Cybersecurity Capabilities where *basic security hygiene* and *mature cybersecurity programs* are most closely aligned generally reflect what many would refer to as basic blocking-and-tackling:

- We manage our users, their accounts, their access to resources — and their behaviors.
- We keep our systems and applications securely configured.
- We protect and backup our important data.
- We are in a position to respond and recover when something goes wrong.

In contrast, the Core Cybersecurity Capabilities where the two implementation groups have the biggest gaps are much more pronounced in dimensions of organization-wide visibility and monitoring — such as would be found in a *Network Operations Center (NOC)* and / or *Security Operations Center (SOC)*:

- We understand what systems, applications, and service providers are in our environment.
- We keep our networks, systems, and applications patched and up to date.
- We maintain visibility into what's happening in our environment.
- We protect our network.

Aberdeen's traditional benchmark data provides some corroboration for many of the cybersecurity technologies that are commonly used for Safeguards that are in the basic cybersecurity hygiene group — for example, among Small and Mid-Sized Businesses (<1,000 employees) in Aberdeen's study:

- 93% continue to use *traditional passwords* — but 65% have also deployed *multi-factor authentication*
- 79% have capabilities for ensuring *compliance* (e.g., with signature updates, software version levels, and corporate policies) for enterprise endpoints
- *Data encryption* is widely deployed, both on endpoints (73%) and on servers (69%)
- 73% have implemented *data backup and recovery* capabilities

Another simple way to think about prioritizing the capabilities, controls, and safeguards needed for basic cybersecurity hygiene is to sort by the total number of CSI-identified safeguards. These too can be seen in Figure 1, and the sorting that results is summarized in Table 2 below. This logically reflects having the greatest number of controls and safeguards applied to your *users*,

It's worth noting that comparing and ranking based on the number of CIS Safeguards is not necessarily the same as ranking by the *total annual cost of implementing and managing* those Safeguards, or the *total annualized reduction in risk* from implementing and managing those Safeguards. For the purposes of this Knowledge Brief, Aberdeen makes this comparison as a rough proxy.

In addition, the CIS development process is based on discussions and negotiated consensus between smart people, based on their own experiences — which is not the same as *quantifying* how specific controls and safeguards actually affect the frequency and impact of cybersecurity-related incidents. To that end, Aberdeen looks forward to ongoing developments from more recent initiatives such as the FAIR Controls Analytics Model.

As an illustrative example of core security capabilities for enterprise servers, see the Aberdeen infographic *Building Your Organization's Trusted Supply Chain Starts from the Silicon Up*.

your *data*, the configurations and patching of your *systems*, and your ability to *respond and recover* when necessary.

Table 2: Basic cybersecurity hygiene prioritizes users, data, configurations and patching, and response and recovery

CSI IG1	
Rank (by # of CIS Safeguards)	**Core Cybersecurity Capabilities**
1	We manage our users, their accounts, their access to resources — and their behaviors
2	We protect and backup our important data
3	We keep our systems and applications securely configured
3	We keep our networks, systems, and applications patched and up to date
3	We are in a position to respond and recover when something goes wrong
6	We understand what systems, applications, and service providers are in our environment
7	We maintain visibility into what's happening in our environment
8	We protect our network
56	**Total number of Safeguards**

Source: Adapted from *CIS Critical Security Controls* (version 8), Aberdeen, October 2023

Summary and Key Takeaways

- **Simplify your strategic thinking, by leveraging the structure described in this Knowledge Brief.** To help you think more broadly about your organization's cybersecurity needs, consider using Aberdeen's *8 Core Cybersecurity Capabilities* in the form of questions — e.g., in what ways are you currently managing your users, their accounts, their access to resources, and their behaviors? In what ways are you currently protecting and backing up your important data? And so on.
- **Do a gap analysis.** The result of responding to these questions will be an organized inventory of your organization's current cybersecurity capabilities, controls, and safeguards — which you can then compare with community-based recommendations such as the CIS Critical Security Controls.

- **Evaluate and prioritize your next steps.** Based on the gap analysis, you can then evaluate the costs (i.e., build vs buy, products vs services) and benefits (i.e., reduction in risk) of implementing selected incremental controls and safeguards, and prioritize which ones to pursue.

About Aberdeen Strategy & Research

Aberdeen Strategy & Research (a division of Spiceworks Ziff Davis), with over three decades of experience in independent, credible market research, helps **illuminate** market realities and inform business strategies. Our fact-based, unbiased, and outcome-centric research approach provides insights on technology, customer management, and business operations, to **inspire** critical thinking and **ignite** data-driven business actions.

18640