SENTINEL

CIS CONTROLS 101

THE ESSENTIAL GUIDE TO A SUCCESSFUL IMPLEMENTATION

Coauthored by Ted Gruenloh, Sentinel COO and
Scott Smith, CISO City of Bryan, Texas.

SENTINEL

WHAT IS THIS?

EVERYTHING YOU NEED TO KNOW ABOUT CIS CONTROLS, INCLUDING WHERE TO START.

Cyber threats will continue to appear in headlines globally for the foreseeable future. If you're reading this, you're probably looking to keep your organization from co-starring in them. We come bearing good news: even if you have a tight budget and limited resources, you can take proven steps to dramatically improve your security. Best of all, you can begin today.

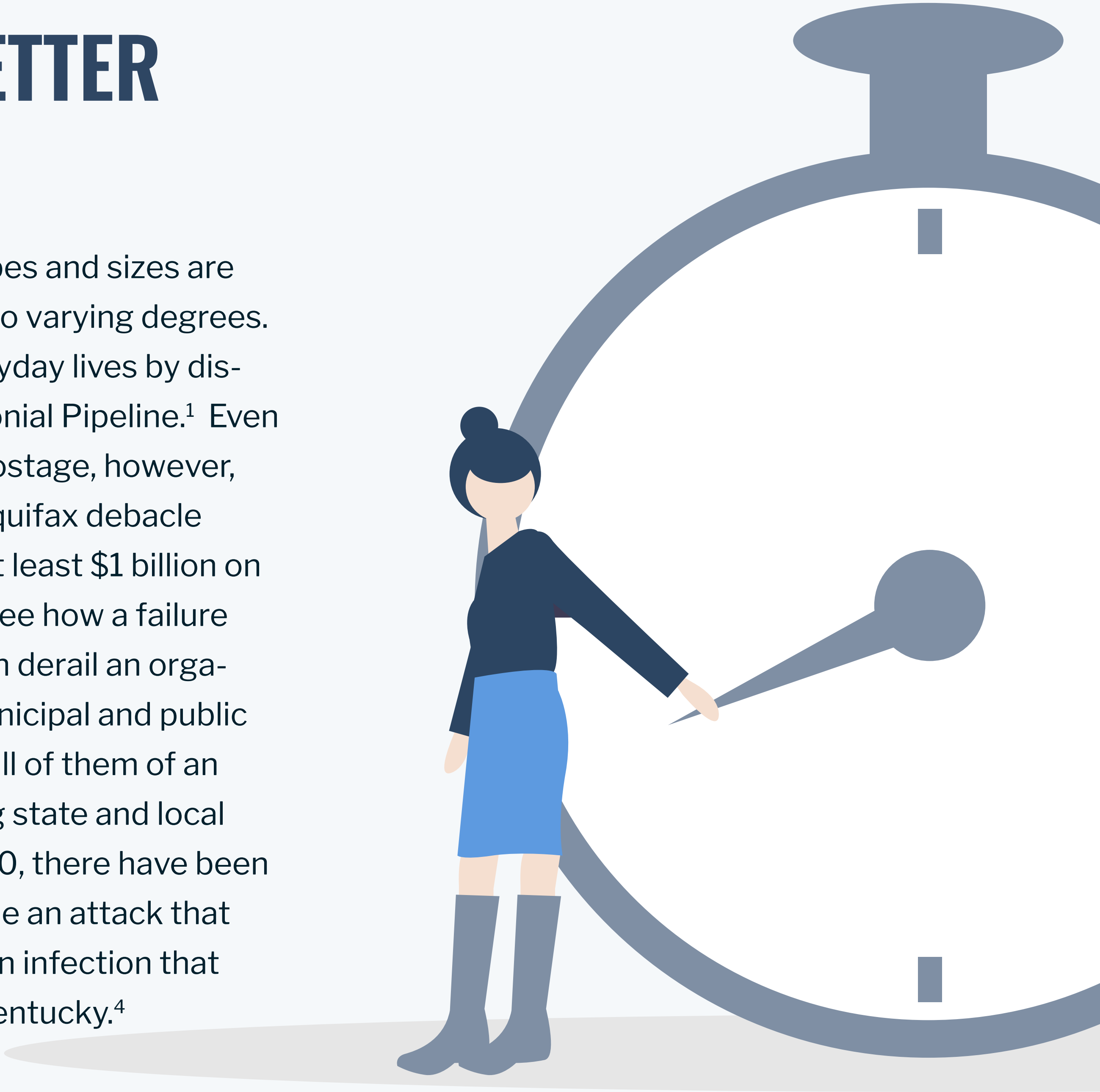
BEST PRACTICES MAKE PERFECT

The Center for Internet Security® (CIS) is a nonprofit that crowdsources various experts within the global IT community to safeguard organizations against cyber threats. Among other outputs, its list of CIS Controls™ is perhaps the most famous. Compiled and vetted by both public agency experts (think NSA) and private experts, the CIS Controls are designed to help an organization improve its security posture.

These basic guidelines are free to download, and they're organized in a prioritized way that's approachable for actual living and breathing human beings.

WHY SOONER IS BETTER THAN LATER

Security threats to organizations of all types and sizes are now constant, pervasive, and dangerous to varying degrees. Sometimes, these attacks touch our everyday lives by disrupting critical infrastructure like the Colonial Pipeline.[1] Even if infrastructure is not damaged or held hostage, however, one needs only to recall the great 2017 Equifax debacle (and its resulting commitment to spend at least $1 billion on data security and related technology) to see how a failure to implement a few basic CIS Controls can derail an organization's mission.[2] Sentinel has many municipal and public institution customers, and it has warned all of them of an increase of ransomware attacks targeting state and local governments. Since the beginning of 2020, there have been too many incidents to count. These include an attack that struck St. Clair County in Michigan[3] and an infection that affected a planning agency in Northern Kentucky.[4]



THE SHORT STORY? SERIOUS THREATS ARE ONLY INCREASING IN FREQUENCY AND SOPHISTICATION, YET MANY OF THEM CAN BE AVOIDED BY IMPLEMENTING JUST SOME OF THE CIS CONTROLS.

THE MAIN GOAL OF CIS CONTROLS AND WHO BENEFITS MOST

The essential purpose of implementing CIS Controls is to increase the internal visibility of the organization's digital operations, from physical infrastructure to the software it runs. Incidentally, Sentinel specializes in making entire networks "invisible" to threatening actors in the first place. But again, you must have a thorough understanding of all entry points in order to fully cloak complex infrastructure.

Any organization of any size will benefit from even partially implementing the CIS Controls, but those with fewer physical and human resources as well as smaller budgets could end up realizing some of the greatest benefits. For CISOs and CTOs entering a new organization or role, CIS guidelines are an excellent roadmap for creating a sound, organization-wide digital foundation.

GETTING STARTED

Note: CIS Controls Version 8.0 was released in May 2021. Like the version that came before it, it includes Implementation Groups (IGs) to help organizations classify themselves and focus resources on what matters most to their missions. Some earlier versions did not include this self-selecting sub-grouping of the CIS Control hierarchy.

The beauty of the CIS Controls is in its simplicity. That might make you laugh when you first realize just how many Safeguards there are. The whole task might feel Herculean. But the entire list is organized according to how things are actually managed in your organizations. Just follow the IGs in order. They will take you through the following phases:

IG1 – BASIC CYBER HYGIENE

These measures include the most cost-effective actions that organizations can take to improve their overall security posture. They include a focus on building an inventory of individual devices and workstations across the network.

IG2 – FOUNDATIONAL SECURITY

This IG includes all the Safeguards listed in IG1. It also covers other security measures that might be spread across special organizational operations and thus require more time, effort, and/or budget to implement properly.

IG3 – COMPREHENSIVE PROTECTION

IG3 consists of all the Safeguards listed in the CIS Controls. As such, it contains everything recommended by IG1 and IG2 along with more expensive, ongoing, policy-related, and testing items that can help to ensure comprehensive protection in the long run.

REALISTIC TIMING EXPECTATIONS

Timelines for each CIS Control, Safeguard, and IG vary widely according to specific organizational needs, available resources, and risk appetite. Clearly, a mid-sized municipality will have different priorities than a banking institution, and timing is affected by priority.

At the City of Bryan, we prioritized getting through the first five CIS Controls listed in previous versions. (Those security measures were helpful in minimizing 85% of vulnerabilities confronting many organizations.)[5] We approached the process with a mixed mindset of patience and urgency. It took time to implement, but it was worth doing.

While it is of utmost importance to begin (and begin soon), it may take years to implement the CIS Controls that make sense for your organization. You want to do it right, so make sure your stakeholders know what that commitment takes.

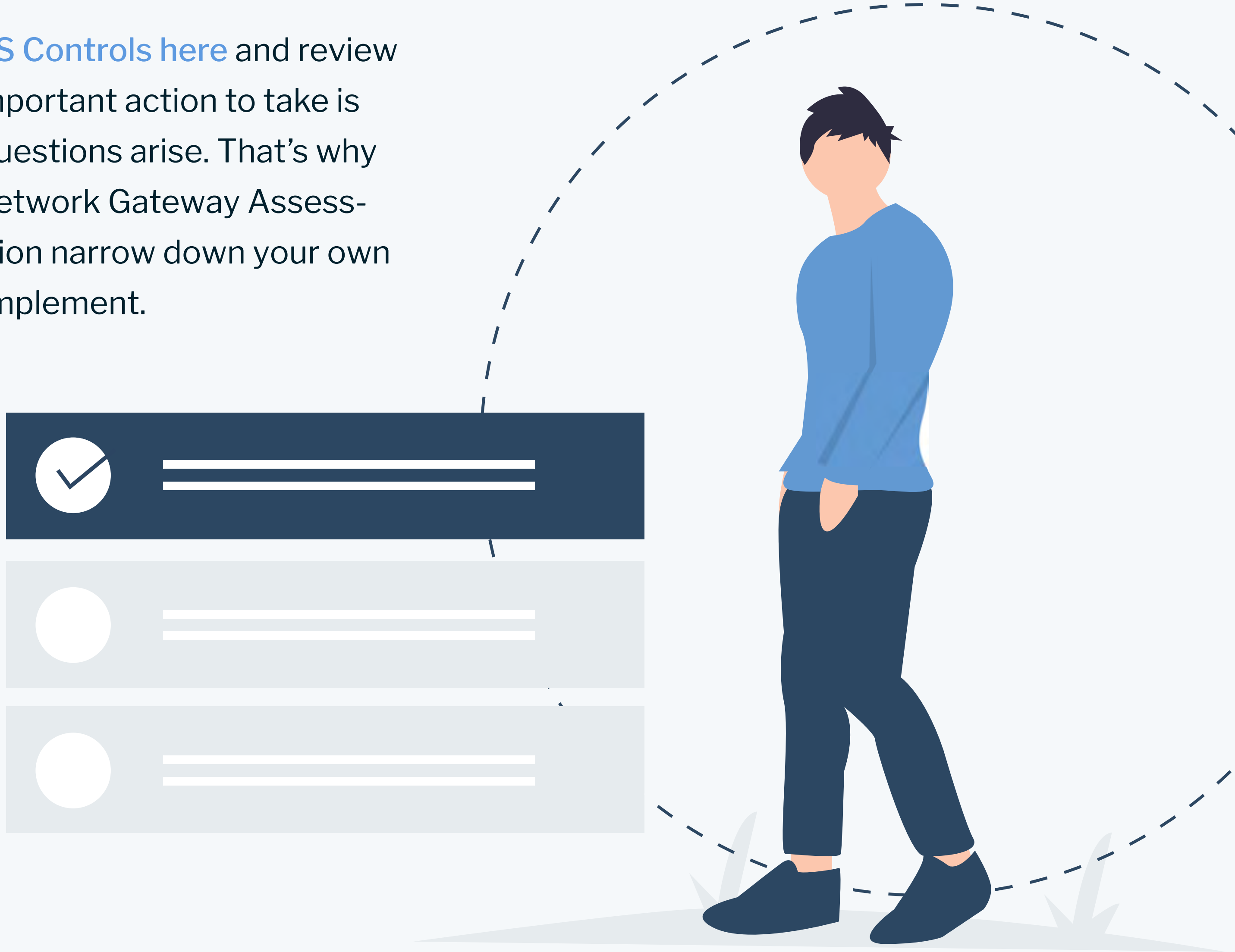
OVERCOMING ORGANIZATIONAL BARRIERS

Resistance to change is commonplace in many organizations, and when policy is shifted or information is demanded across multiple departments, it is natural to expect pushback. The most successful leaders of network security overhauls thus follow a few simple rules of thumb to make things go a little more smoothly:

- ✓ Communicate motivations transparently. There has never been a more important "same-team" effort.
- ✓ Educate yourself on each department's business practices and goals to approach their concerns from an angle of support.
- ✓ Educate departmental stakeholders on their value as security advocates, encouraging early internal notification of possible threats.

TAKING THE FIRST STEP

Download the latest version of CIS Controls here and review them with your team. The most important action to take is to simply take action. Invariably, questions arise. That's why Sentinel is here. We offer a free Network Gateway Assessment that can help your organization narrow down your own list of prioritized CIS Controls to implement.



SENTINEL

SENTINEL IS HERE TO HELP

Our mission is to provide expertise, focus, and firepower for organizations that may not have the resources of giant global players. CIS and the CIS Controls are built for people exactly like our customers, and we want them to be aware of every tool that is available. If you or anyone in your organization has questions about the implementation of CIS Controls or how we can help, please feel free to contact us.

SEE AN INSTANT DEMO

[1] https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

[2] https://www.securityweek.com/court-approves-equifax-data-breach-settlement

[3] https://www.bnd.com/news/local/article251871213.html

[4] https://www.cincinnati.com/restricted/?return=https%3A%2F%2Fwww.cincinnati.com%2Fstory%2Fnews%2F2021%2F06%2F22%2Fransomware-hackers-encrypt-northern-kentucky-government-planning-agency-files-kenton-county%2F7602200002%2F

[5] https://www.darkreading.com/perimeter/why-you-need-a-global-view-of-it-assets/a/d-id/133510

SENTINEL