SENTINEL
INTRUSION PREVENTION SYSTEMS™

CIS CONTROLS 101

THE ESSENTIAL INTRODUCTION TO CIS 20 IMPLEMENTATION

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

WHAT IS THIS?

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

Cyber threats will continue to appear in worldwide headlines for the foreseeable future. If you're reading this, you're likely looking to keep your organization from co-starring in them. We offer good news, however. Even organizations with tight budgets and limited resources can take proven steps to dramatically improve security, and they can begin today.

BEST PRACTICES MAKE PERFECT

The Center for Internet Security® (CIS) is a non-profit that crowdsources various experts within the global IT community to safeguard organizations against cyber threats. Among other outputs, their list of CIS Controls™ (the “CIS 20”) is compiled and vetted by both public agency experts (think NSA) and private experts and is considered to be the gold standard for improving an organization’s basic cyber hygiene.

These basic guidelines are free to download, and the best part is that they are organized step-by-step to make it approachable for actual, living, breathing humans. State and local governments can even use the powerful scanning tool for free as well.

WHY SOONER IS BETTER THAN LATER

Security threats to organizations of all types and sizes are now constant, pervasive, and dangerous to varying degrees. Even if infrastructure is not damaged or held hostage, one needs only to recall the great 2017 Equifax debacle (and the resulting $425 million settlement[1]) to find an illustration of how a failure to implement even a few basic CIS Controls can derail an organization's mission.

Sentinel has many municipal and public institution clients and has warned clients of an increase of state and local government ransomware attacks. Even since the summer of 2019, there have been too many incidents to count, from the coordinated attacks in Texas to the two Florida cities that paid more than $1 million combined to free their systems[2].

THE SHORT STORY IS THAT SERIOUS THREATS ARE ONLY INCREASING IN FREQUENCY AND SOPHISTICATION, YET MANY CAN BE AVOIDED WITH A SIMPLE ADHERENCE TO THE MOST BASIC CIS CONTROL IMPLEMENTATIONS.

THE MAIN GOAL OF CIS CONTROLS AND WHO BENEFITS MOST

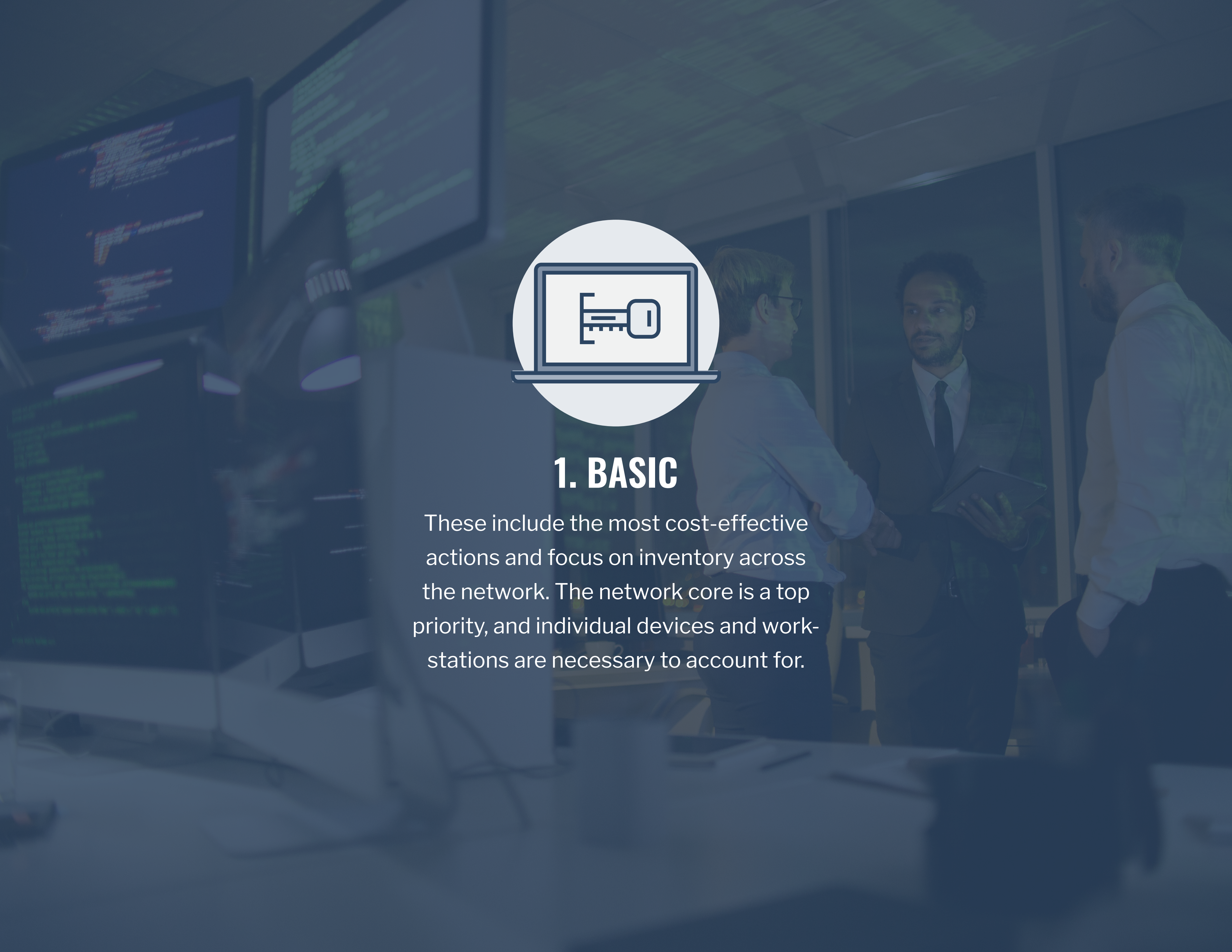
The essential purpose of implementing CIS Controls is to increase the internal visibility of the organization's digital operations, from physical infrastructure to the software it runs. Incidentally, Sentinel specializes in making entire networks "invisible" to threatening actors in the first place, 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 implementing CIS Controls, but naturally those with fewer physical and human resources and smaller budgets will realize the greatest benefits of even basic protective measures. 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 7.1 was released in April 2019 and takes simplicity a step further. As the first version to include ‘Implementation Groups,” this offers an easier way to help organizations to classify themselves and focus resources on what matters most to their missions. Previous versions did not include this self-selecting sub-grouping of the CIS Control hierarchy.

The beauty of the CIS Controls is in its simplicity. You may laugh at that when you first glance at the number of sub-controls and the whole task feels Herculean. But the entire list is organized to be a linear guide, not a Choose Your Own Adventure. Just follow the recommendations in order and it will take you through the following phases:

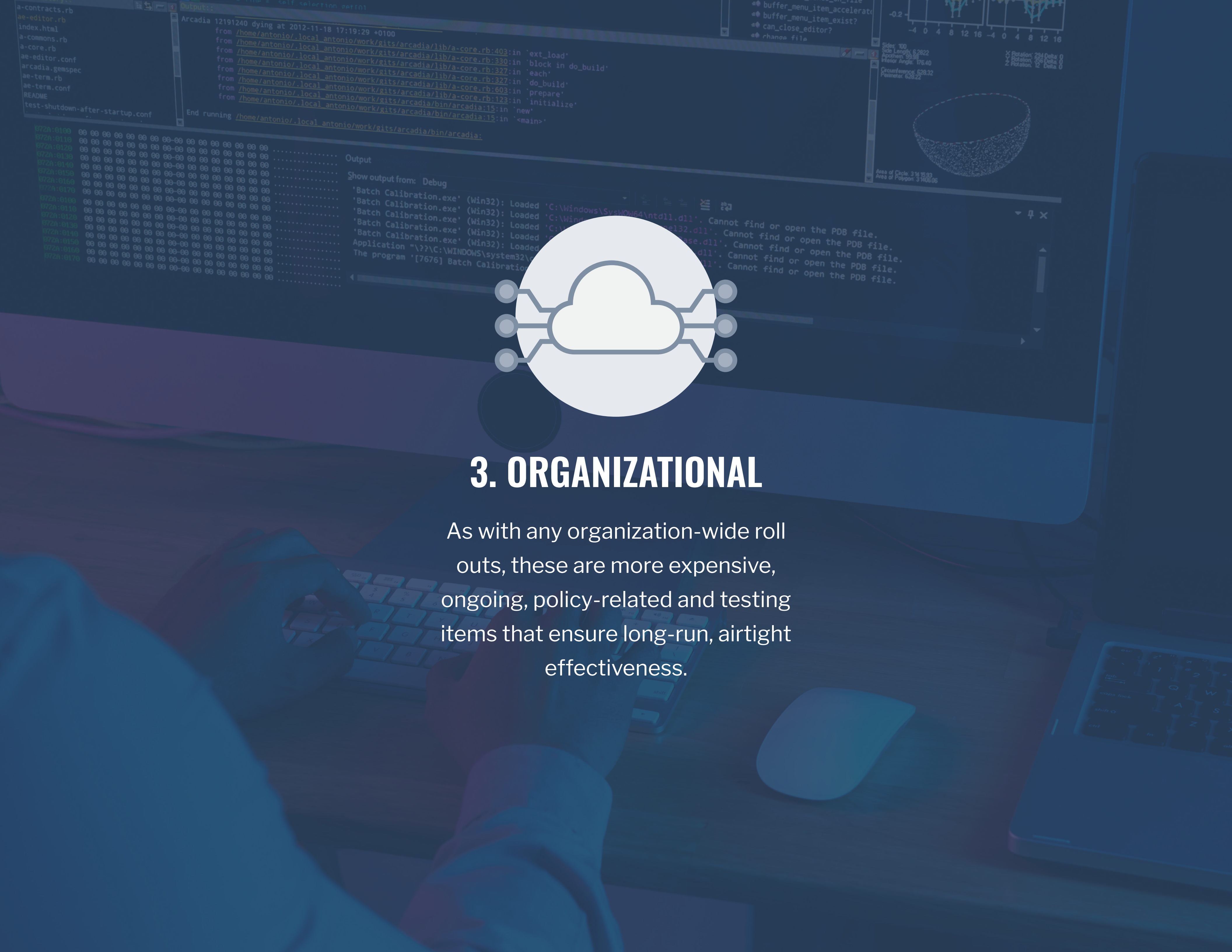


1. BASIC

These include the most cost-effective actions and focus on inventory across the network. The network core is a top priority, and individual devices and workstations are necessary to account for.

2. FOUNDATIONAL

These are spread across a number of special organizational operations, and sometimes require more time, effort and cost to implement properly. Expertise is often required to determine what are the right items for your organization to focus on.



3. ORGANIZATIONAL

As with any organization-wide roll outs, these are more expensive, ongoing, policy-related and testing items that ensure long-run, airtight effectiveness.

A DIFFERING OPINION...

IF SENTINEL WROTE THE CONTROLS

The CIS Controls are written by a vast network of the smartest network security experts available as a logical, linear guide, to be consumed item-by-item, but the Sentinel team of experts have one qualm about the stated priorities as they currently exist: If you have the opportunity, elevate the security threat awareness training of employees to the first group of CIS Controls that you tackle. An organization's people are the most dangerous element of a network full of moving parts. In the end, they should be conscripted as allies in the fight against threats by educating them on common issues early and often.

REALISTIC TIMING EXPECTATIONS

Timelines for each CIS Control, sub-control, and phase of implementation 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've prioritized getting through the six "basics," or the first items in the CIS Controls guidelines. We approached the process with a mixed mindset of patience and urgency. It has taken time to implement but is worth doing to mitigate a large amount of risk.

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.

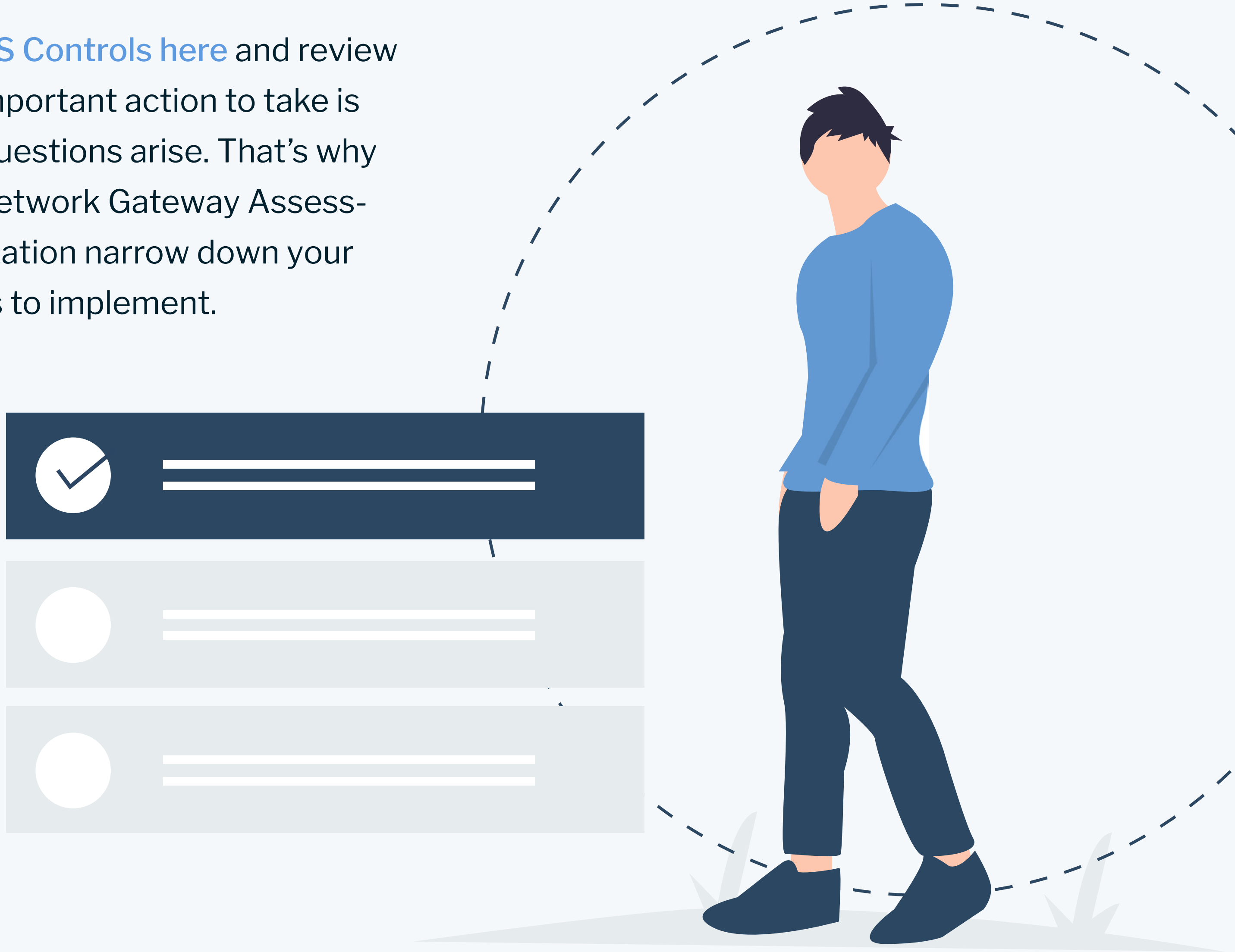
OVERCOMING ORGANIZATIONAL BARRIERS

Resistance to change is a rule in any organization, 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 follow a few simple rules of thumb:

- ✓ 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, which can help your organization narrow down your own list of prioritized CIS Controls to implement.



SENTINEL
INTRUSION PREVENTION SYSTEMS™

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.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement

[2] https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/

SENTINEL

INTRUSION PREVENTION SYSTEMS™