# CIS Controls

## Auditing, Assessing, Analyzing:
## A Prioritized Approach using the Pareto Principle

By Tony Sager, Senior Vice President and Chief Evangelist and Shannon McClain, GISF

# Auditing, Assessing, Analyzing:
## A Prioritized Approach using the Pareto Principle

### Contents



### Introduction

Credit card breaches, identity theft, ransomware, theft of intellectual property, loss of privacy, denial of service – cybersecurity threats have become everyday news. For most of us, it's a head-spinning mix of dense technical jargon, conflicting expert opinions, doomsday predictions, and market hyperbole.

And here's the really concerning part: **the vast majority of cybersecurity problems that plague us today could be prevented by action, technology, and policies that are already known or exist in the marketplace.** Malicious cyber actors are not magicians wielding unstoppable powers; in truth, most organizations are being overwhelmed by massive numbers of relatively mundane parlor tricks.

It's not that companies aren't aware of these threats or that their technical teams aren't skilled enough. Instead, most are just overwhelmed by what we call the "Fog of More"[1] – more work, problems, regulatory and compliance requirements, conflicting opinions, marketplace noise, and unclear or daunting recommendations than anyone can manage. Conducting a cybersecurity audit can help organizations understand their technical maturity and preparedness – but where to begin improving? In this white paper, we'll

[1] https://www.youtube.com/watch?v=OZLO-xekp3o

explain how CIS (the Center for Internet Security) applies the Pareto Principle to cybersecurity in order to develop the CIS Controls; a prioritized list of actions which effectively increase cybersecurity posture. The CIS Controls are a free-to-use cybersecurity document which has been downloaded over 100,000 times.

## The Fog of More

As technologies grow more sophisticated and interconnected, developing an organizational approach to cybersecurity seems more complicated than ever. DDoSing, phishing, ransomware, data leaks, IT security breaches – how can organizations protect themselves in a perpetually-advancing threat landscape? Many organizations start with a cybersecurity audit to help them understand their current posture. Sometimes these audits are required by regulatory organizations. However, companies that are conducting a cybersecurity audit – whether to meet compliance, protect digital assets such as intellectual property and trade secrets, or safeguard client/employee information – often run into what CIS calls "the fog of more." This fog surrounds the multitude of problems and solutions facing businesses when it comes to cybersecurity, obfuscating the task ahead. Most cyber attacks are not the sophisticated, complex activity shown on television and in movies – in fact, attacks often rely on simply misconfigured or outdated systems.

Typically, cyber defense has been driven by very clever experts dreaming up or demonstrating *all of the things* that cybercriminals *might do*, and *all of the things* that *might go wrong*. And then they tell you all about the things that you *could do* to defend yourself. The CIS Controls focus on what the cybercriminals *are doing now*, in order to ask "Out of all *that I could do*, what are the core, foundational, steps I can take to get most of my security value and stop these attacks?"

These are the kinds of issues that gave birth to and continue to drive the CIS Controls. The development of the CIS Controls started as a grass-roots activity to cut through the fog and focus on the most fundamental and valuable actions that every enterprise should take. Their **value** is determined by knowledge and data – the ability to prevent, alert, and respond to the attacks that are plaguing organizations and businesses today. Regardless of industry requirements, it's important to evaluate your organization's cybersecurity posture. There is clear evidence that the vast majority of threats out in the wild affect all enterprises, directly or indirectly, whether or not they know it. This means that it is essential for every organization – regardless of industry, size, or function – to take a proactive approach to cybersecurity.

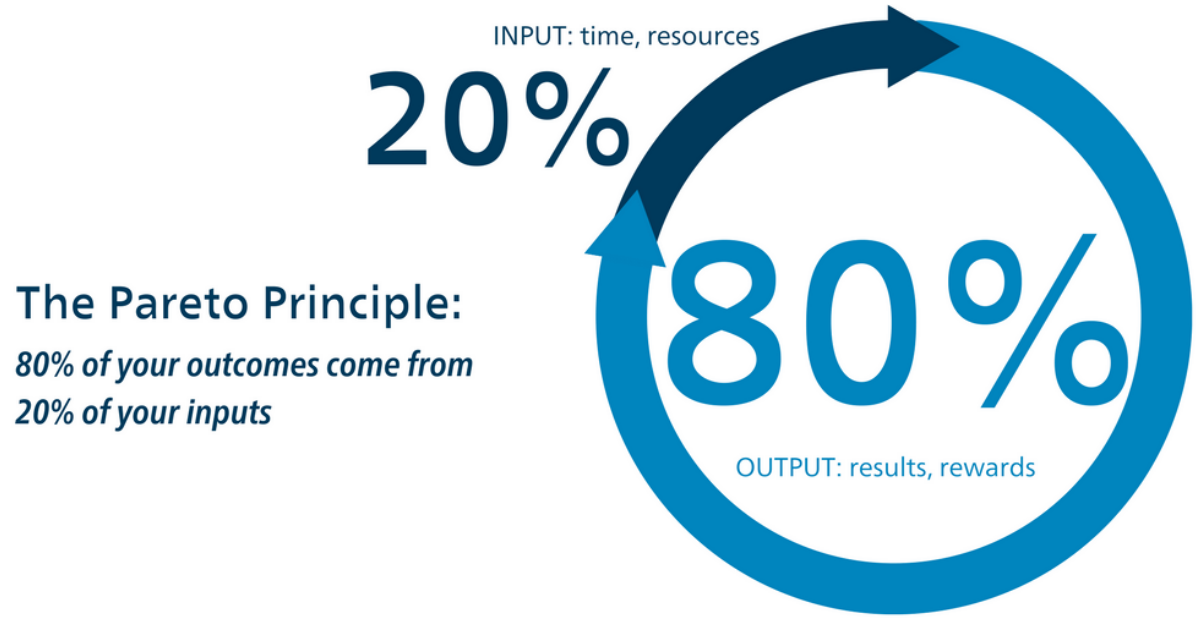
## Applying the Pareto Principle

Once you've conducted an initial cybersecurity assessment, it's time to start making improvements. You've likely discovered more than a few flaws in your network; unauthorized applications, gaps in incident response plans, or a need for more employee training. Where should you start improving?

In an ever-growing mix of hundreds of potential cybersecurity concerns and even more proposed solutions, CIS applies the Pareto Principle – the concept that for many activities, roughly 80% of the effects come from 20% of the causes[2] – to help prioritize cybersecurity actions. For example: in 2002, Microsoft found that roughly 20% of all bugs were causing 80% of reported errors,[3] allowing them to focus their resources on the most needed fixes.

[2] http://www.nytimes.com/2008/03/03/business/03juran.html

[3] http://www.crn.com/news/security/18821726/microsofts-ceo-80-20-rule-applies-to-bugs-not-just-features.htm




*Focus your efforts on the 20% that will make a difference, instead of wasting time, resources, and effort on the 80% that doesn't matter much.*[4]

By applying the Pareto Principle to cyber defense actions, CIS has developed the CIS Controls: a set of 20 prioritized actions intended to help any organization improve its cyber defenses. How does CIS narrow down all the possible cybersecurity actions that an organization can take?

## A Community Approach

Deciding which tasks make the cut isn't a job for just one person or one organization. The CIS Controls are developed by a community of cybersecurity experts around the globe, bringing their knowledge and experience with multiple technologies to the table.

Who are these expert volunteers? They come from every part of the cyber ecosystem (companies, governments, individuals); representing every role (threat responders and analysts, technologists, vulnerability-finders, tool makers, solution providers, defenders,

[4] http://athinala.com/the-pareto-principle-8020-rule/

users, policy-makers, auditors, etc.); and within many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT). These are people you can't afford to hire, bringing knowledge you don't have, creating content you could not build on your own.

Led by CIS, this community has matured into an international movement of individuals and institutions that:

- Share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action;
- Document stories of adoption and share tools to solve problems;
- Track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions;
- Map the CIS Controls to regulatory and compliance frameworks and bring collective priority and focus to them;
- Identify common barriers (like initial assessment and implementation roadmaps) and solve them as a community instead of alone; and
- Make the result of this work available at no cost to any organization trying to improve its cyber defenses.

Their activities ensure that the CIS Controls are not just another list of "good things to do", but a *prioritized, focused set of actions* driven by a community network to make them implementable, usable, scalable, and compliant with all industry and government security requirements. Over the decades, many great ideas in cybersecurity have been abandoned, forgotten, and reinvented because no one planned for the long-term support of the ideas. The CIS Controls community brings form, structure, and prioritization to the cybersecurity auditing and remediation process.

## Managing Corporate Risk

While the CIS Controls document contains some specialized technical jargon, keep in mind that any effective cybersecurity improvement program should be able to bridge the gap from detailed technical security requirements through basic questions of corporate risk management, like:

- Do we know what is connected to our systems and networks?
- Do we know what software is running (or trying to run) on our systems and networks?
- Are we continuously managing our systems using "known good" configurations?
- Are we continuously looking for and managing "known bad" software?

- Do we minimize and track the people who can bypass, change, or over-ride our security defenses?
- Are our people aware of the most common threats to our business or mission, and what they can do about them?

These questions aren't rocket science, and most are similar to the kinds of questions that corporate leaders already ask about physical inventory, safety, finances, and numerous other areas of corporate risk management. Each of these questions map directly into one or more of the CIS Controls.

In addition, the CIS Controls map to other popular cybersecurity regulatory and compliance frameworks, including NIST CSF and PCI DSS. As you implement the CIS Controls, you'll be able to track and demonstrate improvements to auditors, vendors, business partners, and other cybersecurity professionals.

## First 5 CIS Controls

By using the Pareto Principle working together to prioritize and organize important cybersecurity actions, the CIS Controls community has effectively cut through the "Fog of More" to distill the most essential and foundational steps an organization can take to improve their cyber defense. Below, we'll briefly examine how each of the first 5 CIS Controls can help every organization bolster its cyber defenses and prepare for cybersecurity audits.

### CIS Control 1 | Inventory of Authorized and Unauthorized Devices

This CIS Control helps organizations define a baseline of what must be defended. After all, how can you protect a device unless you're aware of its presence? The inventory process should be as comprehensive as possible, and scanners (both active and passive) that can detect devices are the place to start.

In addition to scanning your network for devices, be sure to implement a clear organizational policy to help track and manage devices as they move around the enterprise. Be sure to include company-affiliated cell phones, printers, and other network devices.

### CIS Control 2 | Inventory of Authorized and Unauthorized Software

While not a silver bullet for defense, this CIS Control is often considered one of the most effective at preventing and detecting cyberattacks. The purpose of this CIS Control is to ensure that only authorized software is allowed to run on an organization's systems. While developing an inventory of software is important, application whitelisting is a

crucial part of this process, as it limits the ability to run applications to only those which are explicitly approved.

Implementing CIS Control 2 might mean revisiting company policies and culture—no longer will employees be able to install software whenever and wherever they like. But this CIS Control, already successfully implemented by numerous organizations, will likely provide immediate returns to an organization attempting to prevent and detect cyber attacks.

**CIS Control 3 | Secure Configurations for Hardware and Software**
By default, most systems are configured for ease-of-use and not necessarily security. In order to meet CIS Control 3, organizations need to reconfigure systems to a secure standard. Many organizations already have the technology necessary to securely configure systems at scale, such as Microsoft® Active Directory Group Policy Objects and Unix Puppet or Chef.

By utilizing configuration standards such as the CIS Benchmarks, most organizations can successfully implement this CIS Control. The consensus-driven CIS Benchmarks are free to download in PDF format for over 150 technologies, including operating systems, middleware and software applications, and network devices.

**CIS Control 4 | Continuous Vulnerability Assessment and Remediation**
The goal of this CIS Control is to understand and remove technical weaknesses that exist in an organization's information systems. One solution: implement patch management systems that cover both operating system and third-party application vulnerabilities. This allows for the automatic, ongoing, and proactive installation of updates to address software vulnerabilities.

In addition to patch management systems, organizations should implement a commercial vulnerability management system to give themselves the ability to detect and remediate exploitable software weaknesses.

**CIS Control 5 | Controlled Use of Administrative Privileges**
This CIS Control ensures that workforce members have only the system rights, privileges, and permissions that they need in order to do their job—no more and no less. Unfortunately, for the sake of speed and convenience, many organizations allow staff to have local system or even domain administrator rights which are too generous and open the door for abuse, accidental or otherwise. The simple answer for CIS Control 5 is to remove unnecessary system rights or permissions.

## Taking the Next Steps

Tackling an organization's cybersecurity can often feel intimidating, confusing, and just plain daunting; but you'll be amazed at what you can achieve by starting with an audit and implementing the most effective strategies first. By working with subject matter experts from around the world and applying a *Pareto Principle*-informed approach, CIS has helped to bring priority to the world of cyber defense.

Your journey of cybersecurity improvement starts at www.cisecurity.org, where you can download the CIS Controls document and have access to numerous working aids, use cases, resources, and a growing user community of volunteers to help you succeed. You'll still have lots of hard work ahead, but the journey becomes manageable with a plan, and with trusted help along the way.

**Contact Information:**
CIS (Center for Internet Security)
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org