The Critical Security Controls *(V6)*
Executive Summary

Background

Credit card breaches, identity theft, ransomware, theft of intellectual property, loss of privacy, denial of service – these 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 have been prevented by action, technology, and policies that are already known to exist in the marketplace. We're not being attacked by wizards wielding unstoppable magic, we're being overwhelmed by massive numbers of relatively mundane parlor tricks.

It's not that organizations aren't aware, or that their defenders 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 more unclear or daunting recommendations than anyone can manage. Even for the rare Enterprise that has the information, expertise, resources, and time to figure this out, it's rarely true for all of their key business partners, suppliers, and clients.

The Philosophy

These are the kinds of issues that led to and now drive the CIS Critical Security Controls ("the CIS Controls"). The CIS Controls are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber attacks aimed at IT users worldwide. The Controls are developed, refined, and validated by a community of leading global experts. They started as a grass-roots activity to cut through the fog to sharpen focus on the most fundamental and valuable actions every enterprise should take. They align with and map to all of the major compliance frameworks such as NIST Cybersecurity Framework, NIST guidelines, and the ISO 27000 series or regulations such as PCI DSS, HIPAA, NERC CIP, FISMA. Their **value** is determined by knowledge and data – the ability to prevent, alert, and respond to the attacks that are plaguing enterprises today. Strong evidence reveals that the vast majority of threats out in the wild affect all organizations, directly or indirectly, and whether or not they know it.

The history of cyber defense has been driven by very well-intentioned experts defining or demonstrating all of the things that Bad Guys ***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 take a Pareto Principle, "80/20 Rule" approach to this problem by focusing on what the Bad Guys ***are doing now***. What are the core, foundational, steps I can take to get most of my security value and stop these attacks?

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

How are they created?

Led by the Center for Internet Security (CIS), the CIS Controls have 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;
- share tools, working aids, and translations;
- review leading breach reports that reveal the defenses that could have prevented most of the reported breaches
- identify common barriers (like initial assessment and implementation roadmaps) and solve them as a community instead of alone; and
- make the output of this work available at no cost to any organization trying to improve their cyberdefenses.

Who are the expert volunteers?

The volunteers who develop the CIS Controls 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, users, policy-makers, auditors, etc.); and within many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT). These are professionals most companies can't afford to hire, bringing knowledge you don't have, creating content that you could not build on your own.

Their extensive experience ensures 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 support network to make them implementable, usable, scalable, and compliant with all industry or 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 idea.

The Corporate View

While the Controls document contains a lot of specialized technical jargon, keep in mind that any effective cybersecurity improvement program should be able to bridge the gap from detailed technical security requirements up into 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 risk by tracking 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 maps directly into one of more of the CIS Controls.

Getting Started

Your journey of cybersecurity improvement starts at www.cisecurity.org. In exchange for an email registration, you can download the CIS Critical Security 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.

The Center for Internet Security (CIS) is a 501(c)(3) organization dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. Utilizing its strong industry and government partnerships, CIS combats evolving cybersecurity challenges on a global scale and helps organizations adopt key best practices to achieve immediate and effective defenses against cyber attacks. CIS is home to the Multi-State Information Sharing & Analysis Center (MS-ISAC®), CIS Security Benchmarks, and CIS Critical Security Controls. To learn more, visit CISecurity.org and follow us on Twitter @CISecurity.

The Critical Security Controls

CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 2: Inventory of Authorized and Unauthorized Software
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 5: Controlled Use of Administrative Privileges
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capability
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12: Boundary Defense
CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 15: Wireless Access Control
CSC 16: Account Monitoring and Control
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18: Application Software Security
CSC 19: Incident Response and Management
CSC 20: Penetration Tests and Red Team Exercises