tripwire CONFIDENCE: SECURED

THE EXECUTIVE'S GUIDE TO THE TOP 20 CRITICAL SECURITY CONTROLS

KEY TAKEAWAYS AND IMPROVEMENT OPPORTUNITIES

About the Top 20 Critical Security Controls

The "Top 20" Critical Security Controls (20 CSC—also known as the Consensus Audit Guidelines (CAG) and formerly referred to as the SANS 20 Critical Security Controls) have emerged as the "de facto yardstick by which corporate security programs can be measured," according to the Cybersecurity Law Institute. The 20 CSC are now governed by the Council on CyberSecurity, an independent, expert, not-for-profit organization with a global scope.

The development of this set of standards was first undertaken in 2008 by the National Security Agency at the behest of the US Secretary of Defense in an effort to efficiently direct resources towards combating the most common network vulnerabilities which resulted in the greatest number of attack vectors.

This publication was designed to assist executives by providing guidance for implementing broad baseline technical controls that are required to ensure a robust network security posture. The content was developed by a former Tripwire Security and Compliance Architect, now employed at a non-profit information security organization.

PREV PAGE

NEXT PAGE

Welcome to this Executive Guide

The genesis of this e-book is a series of entries from Tripwire's *The State of Security* blog (tripwire.com/state-of-security). The author, a security and compliance architect, examined each of the Controls and has distilled key takeaways and areas of improvement. This is collection of those posts. At the end of each section, you'll find a link to the complete text of the Control, fully annotated by the author.

On your way, you'll see two types of callouts:

Key Takeaways

The analysis of the Control boiled down to the most important three to five concepts.

Improvement Opportunities

Where areas of improvement with respect to the Control are identified, the most important are provided.

PREV PAGE

NEXT PAGE

The 20 Critical Security Controls	Page	NSA Rank
CSC1: Inventory H/W Assets, Criticality & Location	4	Very High
CSC2: Inventory S/W Assets, Criticality & Location	7	Very High
CSC3: Secure Configuration Servers	10	Very High
CSC4: Vulnerability Assessment & Remediation	13	Very High
CSC5: Malware Protection	16	High/Medium
CSC6: Application Security	19	High
CSC7: Wireless Device Control	22	High
CSC8: Data Recovery	25	Medium
CSC9: Security Skills Assessment	28	Medium
CSC10: Secure Config-Network	31	High/Medium
CSC11: Limit and Control Network Ports, Protocols & Services	34	High/Medium
CSC12: Control Admin Privileges	37	High/Medium
CSC13: Boundary Defense	40	High/Medium
CSC14: Maintain, Monitor, and Analyze Audit Logs	43	Medium
CSC15: "Need-to-Know" Access	46	Medium
CSC16: Account Monitoring & Control	49	Medium
CSC17: Data Loss Prevention	52	Medium/Low
CSC18: Incident Response	55	Medium
CSC19: Secure Network Engineering (secure coding)	58	Low
CSC20: Penetration Testing & Red Team Exercises	61	Low

Click on any Critical Security Control above to jump to its page.

CONTROL 1: Inventory of Authorized and Unauthorized Devices

Critical Security Control Description Reduce the ability of attackers to find and exploit unauthorized and unprotected systems: Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.

The Upshot:

Key Takeaways

- Don't do it all at once
- Take these requirements to your vendors
- Look for standard data formats to be supported in tools
- Start small and basic

Improvement Opportunities

- Use consistent terminology consistently
- Level of abstraction
- Explain why
- Dependencies

PREV PAGE

NEXT PAGE

CONTROL 1: Inventory of Authorized and Unauthorized Devices

Key Takeaways	Explanation
Don't do it all at once	Having an accurate inventory is undoubtedly important, but meeting the full spirit of this control is more than just standing up a process. It involves orchestration of several business processes, and the intricacy of this orchestration is likely to increase with the size of the organization.
Take these requirements to your vendors	If your tool vendors aren't aware of these requirements, the data integration between business processes, which likely rely upon disparate tools, will be your burden.
Look for standard data formats to be supported in tools	The tools you have today should support standard data formats. The tools you acquire in the future, should support data formats listed here. In particular, the Asset Identification specification, or one that is well-aligned with the model it puts forward, should be high on your list.
Start small and basic	This Control is process heavy and will benefit from automation, but if you move too big too fast, you're likely to end up in the integration ring of hell. If I had to do this, I would not start with NAC or bothering with any automation in terms of access. Instead, I would start by getting the discovery and inventory maintenance down pat and integrating that with my incident detection and response system (in the sense that a system is people, process, and technology).

PREV PAGE

NEXT PAGE

CONTROL 1: Inventory of Authorized and Unauthorized Devices

Improvement Opportunities	Explanation
Use consistent terminology consistently	I found myself asking rather pedantic, but important, questions about the intended meaning of words. The term "system" is a great example. Sometimes it's used when it really means a tool or technological component, such as an Intrusion Detection System like, Snort. Other times, it's used in a more comprehensive sense to encompass people, process, and technology.
Level of abstraction	There's one case that really stood out to me, and perhaps I'm picking a nit, but this Control really assumes an IP-based network. Yes, an IP-based network is important to consider and likely covers 80 percent (at least) of the problem space, but some of the more critical problem domains may not use IP-based networks exclusively. SCADA systems (about which I admittedly know little), may use different protocols and have different requirements. It would be nice to see some level of abstraction to cover these edge cases, even if the details stick to IP networking.
Explain why	In a couple of instances recommendations are made without any real explanation as to why. The better example is in mapping information to assets. This will help identify "critical" assets, but why? Presumably, it is because a priority approach can be taken to address ensuring you have inventory accuracy for the assets that store, process, and/or transmit the most critical information to your organization.
Dependencies	Throughout this Control (and I don't expect this to be any different to others we'll explore) there are allusions to processes that must exist for the Control to be successful. Using the information mapping example again, consider that some information classification scheme has to be determined and applied before the criticality can be understood, which is what makes mapping information to assets worth the effort. I do not recall seeing this particular dependency mentioned, nor do I believe it's covered elsewhere in the 20 CSCs.

PREV PAGE

NEXT PAGE

CONTROL 2: Inventory of Authorized and Unauthorized Software

Critical Security Control Description Identify vulnerable or malicious software to mitigate or root out attacks: Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.

The Upshot:

Key Takeaways

- Don't do it all at once
- Start small and basic
- Take Control 1 and Control 2 together
- Take these requirements to your vendors

Improvement Opportunities

- Combine Control 1 and Control 2
- Dependencies
- Rethink today's organizational needs

PREV PAGE

NEXT PAGE

CONTROL 2: Inventory of Authorized and Unauthorized Software

Key Takeaways	Explanation
Don't do it all at once	Asset inventory is hard, and the software piece of that is no exception.
Start small and basic	Another repeat from Control 1. There's too much that can go wrong if you try to go big too soon. Start with the understanding that there are some pretty obvious edge cases that you'll need to eventually cover.
Take Control 1 and Control 2 together	There are too many similarities between Control 1 and Control 2 to not treat them as one control. The reality is that computing devices and software are, from a business perspective, assets. Tracking them both with a reasonable degree of accuracy is important, so why make the distinction from a process perspective?
Take these requirements to your vendors	This is another one that is likely to turn into a trend. This Control is littered with requirements you can take to your security tool vendors. The requirements that are especially important are related to interoperability feature/functionality.

PREV PAGE

NEXT PAGE

CONTROL 2: Inventory of Authorized and Unauthorized Software

Improvement Opportunities	Explanation
Combine Control 1 and Control 2	If we look at the world from the perspective of what an "asset" is, then it's pretty easy to see that computing devices are the same as software—they all have some value to an organization. When you read the tenth requirement below, you'll get the idea. As I suspected, there are allusions to a plethora of processes and/or procedures throughout this Control. It makes some sense, but having a distinct list of these dependencies could be helpful for those less experienced with interpreting control frameworks.
Dependencies	There are always exceptions and there's no possible way a single written control framework can address everything for all organizations. I recognize this as a fact. Still, I think some of the requirements are stuck somewhere in the last decade. What organization is going to subject a R&D organization, for example, to a change management process for installing software? Perhaps in the most rigorous of environments this is tolerated, but I would wager that the supermajority of R&D shops give developers administrative rights expressly because they need them to develop and install software on their machines. This presents an interesting dilemma from an information security perspective, but it's reality.
Rethink today's organizational needs	In a couple of instances recommendations are made without any real explanation as to why. The better example is in mapping information to assets. This will help identify "critical" assets, but why? Presumably, it is because a priority approach can be taken to address ensuring you have inventory accuracy for the assets that store, process, and/or transmit the most critical information to your organization.

PREV PAGE

NEXT PAGE

CONTROL 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Critical Security Control Description Prevent attackers from exploiting services and settings that allow easy access through networks and browsers: Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.

The Upshot:

Key Takeaways

- If you do one thing do this
- Prepare for incidents
- Take these requirements to your vendors
- Take these requirements to your developers

Improvement Opportunities

- Use Consistent Terminology
- Dependencies
- Leverage Data Exchange Formats

PREV PAGE

NEXT PAGE

CONTROL 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Key Takeaways	Explanation
If you do one thing do this	The truth is that you're going to have to implement some of Controls 1 and 2 to get this Control under way. So, if you're going to do "just one thing," you ought to start with Security Configuration Management (which is really what this Control is all about). Do some homework and look at the past years breach reports from any of a variety of sources, and you'll likely find that misconfigurations (also known as configuration vulnerabilities) are common breach enablers.
Prepare for incidents	This Control has a links to the Incident Detection and Response processes your organization has in place, whatever level of maturity they may be. If you need SCM resources to be on stand-by for your Incident Response program, then prepare for it here.
Take these requirements to your vendors	There are several requirements here that you need to take to your tool vendors. This is a responsibility that you have as a security professional, especially if you'd like to see frameworks such as the 20 CSC succeed in the long run.
Take these requirements to your developers	If you're developing software in-house, then this Control is a source of requirements for your internal developers the same way it's a source of requirements for your vendors. Have your developers read through this Control. Especially those requiring interoperability between tools and/or alerting to administrative personnel. It would also benefit your organization to consider internal Common Configuration Enumeration identifiers for your in-house application configuration settings.

PREV PAGE

NEXT PAGE

CONTROL 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Improvement Opportunities	Explanation
Use Consistent Terminology	Again I found that some of the terms used in this Control are ill-defined or ambiguous.
Dependencies	I find it annoying that we have such intricate dependencies in our Control Frameworks, and this Framework is, unfortunately, no exception. The first Key Take Away says to do this Control first, but also indicates that pieces of Controls 1 and 2 are also needed. That's a plain example. Consider that there are unmentioned, but alluded to, business processes this Control will affect. It seems that there should be a better way.
Leverage Data Exchange Formats	This particular Control and others in this Control Framework are begging for automation. You're never going to get far without it, in fact, and having tools that work together without complicated, one-off integrations works to your advantage. If you're developing in-house, leverage data exchange formats such as those described in the Security Content Automation Protocol. Ask for SCAP by name from your vendors.

PREV PAGE

NEXT PAGE

CONTROL 4: Continuous Vulnerability Assessment and Remediation

Critical Security Control Description Proactively identify and repair software vulnerabilities reported by security researchers or vendors: Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.

The Upshot:

Key Takeaways

- Operational Maturity
- Interoperability
- Coverage

Improvement Opportunities

- Provide more explanation
- Categorize requirements more appropriately
- General housekeeping

PREV PAGE

NEXT PAGE

CONTROL 4: Continuous Vulnerability Assessment and Remediation

Key Takeaways	Explanation
Operational maturity	Perhaps it is because the vulnerability/patch cycle has been around for so long, but I found this Control to be somewhat different than the others I have so far examined. It's different in that it seems more focused on the time it takes to accomplish specific tasks more than it is on the quantity of the specific results. For example, this Control wants you to measure how quickly you're applying available patches, and does not care how many you've applied. Another example, this Control wants you to prioritize application of patches based on vulnerability criticality without concern for how many there might be. This Control, in other words, is all about the process of continuous vulnerability management. I see other controls leaning in this direction in the very near future—the efficiency of security processes are what's most important, and they can always be improved over time with increasingly demanding standards/benchmarks.
Interoperability	This Control is no different from any of the others in that it really is part of the overall framework's intricate web. The three most obvious points of integration are with the asset management, alerting, and ticketing systems. Somewhat less obvious, but no less important, are integration opportunities with LDAP for user roles and the relationship of vulnerability management with configuration management. These points of interoperability are not always explicitly mentioned, but are critically important to the security automation story we would like to tell in the future.
Coverage	One of the concepts covered well by this Control is that it leans quite heavily on ensuring that you've covered your enterprise. At more than one point, the requirements explicitly state that integration with the asset inventory system is important. As you're looking for scanning tools, be sure to have a list of all software asset classes covered straight out of your asset inventory system. This will help you in your evaluation to ensure that you have adequate coverage of your enterprise.

PREV PAGE

NEXT PAGE

CONTROL 4: Continuous Vulnerability Assessment and Remediation

Improvement Opportunities	Explanation
Provide more explanation	At times, the requirements are not obvious—even to security professionals. Consider what it must be like from the organizational, non-security perspective to read some of these requirements. You want to track or trend a particular metric because it provides some insight to you, but you don't really know what that insight is. This Control, as with others in the framework, would bode well to provide further explanation in such cases. If the reason for doing work is not clearly articulated, that work will not be supported by the organization.
Categorize requirements more appropriately	This might be somewhat of a nit, but I found a couple of requirements describing metrics that were not in the "metrics" section of the framework. This may simply be an oversight, but it's still something that could be corrected. If I'm moving quickly or if I'm only interested in the prescribed metrics for a given control, I would miss those that are inappropriately categorized.
General housekeeping	There are a few things that I would change, but nothing critical. Some of the requirements should probably be reworded (one in particular talks about patches when I think it would be far better to talk about vulnerabilities), and others can be safely omitted.

PREV PAGE

NEXT PAGE

CONTROL 5: Malware Defenses

Critical Security Control Description Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading: Use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.

The Upshot:

Key Takeaways

- Automation is your friend
- Don't be that guy
- Start with the most common vectors

Improvement Opportunities

- Consider different perspectives
- General clean-up
- Add some personnel warnings

PREV PAGE

NEXT PAGE

CONTROL 5: Malware Defenses

Key Takeaways	Explanation
Automation is your friend	I don't think this is a secret when it comes to anti-malware, but automation is the only way to play the game. Be sure that the tools you use can be configured to automatically update signatures, to automatically "learn" behavioral analysis, and to automatically interoperate with other tools in the system (see the next take away). Of course, because we've covered Control 3 (Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers), ensure that your anti-malware systems are covered by your Configuration Assessment tools as well.
Don't be that guy	Many of the recommendations made in this Control, if implemented, would cause an uproar in many organizations. Consider blocking personal e-mail, instant messaging, and social networks in your environment not from the perspective of a security manager, but from the perspective of your average user. Let's face it, most people don't love their jobs and need some outlet during the day to break up the monotony. If you cut off their connection to the outside world without justification—that is, without supporting data—you're going to be "that security guy" who is nothing more than a blocker. Don't be that guy.
Start with the most common vectors	If I were starting from scratch, then I would start with the most common attack vector, which I consider to be e-mail and Web traffic. You most certainly won't catch everything—anti-malware, like most other security tools, is not perfect. Once e-mail and Web traffic is covered, I'd start looking at detachable media, but be careful when it comes to relying on configuration settings in your Operating System. Windows, for example, is not as straightforward as it might seem, so ensure that you've got someone who knows what they're doing (or use Tripwire's Cybercrime Controls)

PREV PAGE

NEXT PAGE

CONTROL 5: Malware Defenses

Improvement Opportunities	Explanation
Consider different perspectives	This is in direct relation to the second Key Take Away. Most Control Frameworks, and this one is no exception, consider only the "security perspective." I think security managers would be better served by Frameworks if they looked at the world a bit more pragmatically. Do I know how this would be done? Not really. But, I do have the strong sense that most Frameworks are concerned with only one thing—security. They pay no attention to the real-world goals, aspirations, and problems that security managers face today. Such a perspective may be passable in certain environments (the Government, Finance, and Energy verticals come to mind), but not in most.
General clean-up	There are a few requirements I would prefer to see rewritten, so that they are clearer to the reader. There are some undefined and/or uncommon terms used in the requirements, which can make the "letter of the law" difficult to understand (the spirit is there, but try telling your auditor about the spirit vs. the letter).
Add some personnel warnings	That may not be the best way to phrase this, but the truth is that many of the processes and tools mentioned or alluded to in this Control require very specific, skilled expertise. I would not rely on certifications alone when hiring personnel for these positions—there is plenty of uncertified, but brilliant, talent out there. When it comes to understanding IP flow, detecting and reverse engineering malware, and things of that nature, you'll be better served to hire well, which will take longer. If you don't feel comfortable hiring on your own, you can probably find some very qualified people to help you—not your typical "headhunter" outfit. If anyone has advice for other readers out there, talk about it in the comments or contact me directly and I'll take and share some notes.

PREV PAGE

NEXT PAGE

CONTROL 6: Application Software Security

Critical Security Control Description **Neutralize vulnerabilities in web-based and other application software:** Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).

The Upshot:

Key Takeaways

- **Implement a Software Development Lifecycle (SDLC)**
- **Add security attributes to your SDLC**
- **Enlist QA to test for basic application security holes**

Improvement Opportunities

- **Split and refocus**
- **Yet again, define terms**
- **Provide examples on using standards or pointers to examples**

PREV PAGE

NEXT PAGE

CONTROL 6: Application Software Security

Key Takeaways	Explanation
Implement a Software Development Lifecycle (SDLC)	This might be better posed as a Software Procurement Lifecycle, because the Control pertains to operating application-level software as well as acquiring (i.e. buying or building) application-level software.
Add security attributes to your SDLC	It's not enough to have an SDLC. You need to ensure that your SDLC is 1) performing the right activities with, 2) qualified personnel. You can do static code analysis as part of your automated build/release process, but that's not a substitute for eyes-on code reviews. Further, eyes-on code reviews by unknowledgeable personnel won't catch what you want it to.
Enlist QA to test for basic application security holes	How many of you organizations out there have QA personnel who have been trained to attack application-level software? How many can analyze your SSL implementation? Your app-specific PKI deployment? Your input sanitization? Train up your QA personnel to handle the "basics" of security testing your applications and, if the organization is so inclined, get a team of security assessors to do the heavy lifting. I suspect most organizations don't need heavy lifting, but do need trained personnel to handle the basics.

PREV PAGE

NEXT PAGE

CONTROL 6: Application Software Security

Improvement Opportunities	Explanation
Split and refocus	There are two facets to this Control, and I think they would be better called out separately. The first facet is the operational perspective that applies to all application-level software, not just the software you may have developed in-house. The second facet pertains to how you develop in-house software. If you create a Software Procurement Lifecycle, you can use that against your in-house development and then have a Software Development Lifecycle to support in-house development.
Yet again, define terms	After reading through the control requirements a couple of times and really thinking about what it means, I still don't: third-party-procured. If anyone has a clue, I'm all ears.
Provide examples on using standards or pointers to examples	Both CWE and CAPEC were referenced in the requirements as being beneficial for development and test-tracking. The CWE use case is straightforward—we have a good taxonomy in the CWE dictionary at MITRE and more shops should use it. Using CAPEC to for test-tracking probably isn't as straightforward to most who will be held to this Control. Thus, an example would be useful. Additionally, and perhaps most important, is that if CAPEC is good to use for test-tracking, is there a tool that leverages CAPEC? Development shops aren't likely to track things in raw XML.

PREV PAGE

NEXT PAGE

CONTROL 7: Wireless Device Control

Critical Security Control Description **Protect the security perimeter against unauthorized wireless access:** Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.

The Upshot:

Key Takeaways

- **Wireless is (not) special**
- **Marry wireline and wireless requirements**
- **Be careful with BYOD**

Improvement Opportunities

- **Wireless is not special**
- **Consolidate**

PREV PAGE

NEXT PAGE

CONTROL 7: Wireless Device Control

Key Takeaways	Explanation
Wireless is (not) special	Be practical in your treatment of wireless devices and use common sense. You can take this for what it's worth in your organization, but the 20 Critical Controls really view wireless as special—as do many other Control Frameworks. I think we're still holding on to a lingering "newness" to wireless and still not really able to recognize that wireless is just another thing we need to secure. I found many of the requirements to be better suited for Controls 1, 3, or 10.
Marry wireline and wireless requirements	Don't treat the requirements for device authentication and access control as separate for wired and wireless networks—you'll operate less efficiently if you use different technologies. Does wireless have requirements that differ from wired networks in some cases? Of course, they use a different physical medium, for example. Nevertheless, most of your technical security requirements should be the same. You want to authenticate devices, you want to kick unauthorized devices off the network, you want to alert appropriate administrators when something goes awry, you want to configure your devices according to organizational standards, and so on.
Be careful with BYOD	If you were to follow the more advanced guidance in this Control, you'd be spending resources to register BYOD devices and scan them to conned to the corporate network. Given privacy and civil liberty concerns that employees will undoubtedly have when it comes to BYOD, you're probably better off having a solid policy in place for VPN access and standing up a segregated "guest" network the BYOD'ers can use at the office.

PREV PAGE

NEXT PAGE

CONTROL 7: Wireless Device Control

Improvement Opportunities	Explanation
Wireless is not special	Please don't treat wireless as a special set of requirements. The Control Framework should be concerned with devices and ensuring that specific security properties have been considered for a variety of contexts. I have no problem with specific technology recommendations to meet authentication or confidentiality or integrity, for example (802.1x, AES, SHA-2, and so on). What I really don't like to see is a type of device treated as "special." As I said in the key takeaways, a wireless device is just another device and we have a need to ensure operating the device is done so with specific security properties intact. Specific mechanisms may differ, but I don't see a reason to treat wireless devices as separate from other devices.
Consolidate	There were several requirements that seemed to be repeats or possessing nuanced differences. I would prefer to see these requirements cleaned up. Here, I had to look between them and determine for myself what the differences were. Why not just be crystal clear right up front? This is really a problem with prose Control Frameworks (is there another kind?) in general.

PREV PAGE

NEXT PAGE

CONTROL 8: Data Recovery Capability

Critical Security Control Description **Minimize the damage from an attack:** Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.

The Upshot:

Key Takeaways

Be aware of process dependency

Encrypt wisely

Oh, right... backup your data

Improvement Opportunities

Make allusions explicit

Be prescriptive only when necessary

Acknowledge the extreme importance of good key management

Add a Metrics section

PREV PAGE

NEXT PAGE

CONTROL 8: Data Recovery Capability

Key Takeaways	Explanation
Be aware of process dependency	The case in point is in requirement 6, which implies that your incident response team ought to be trained in backup and recovery. It makes some sense, but this is an example of a character flaw I see across most frameworks: They merely allude to some of the most important relationships between your controls and your business.
Encrypt wisely	This Control recommends encryption of backup data in transit and when stored off-site. The devil in these details is key management, which is something that might be mentioned by some Control Frameworks, but is a subject about which most steer clear. If you're doing encryption on your backups, be sure you're generating keys for the right purpose—long-lived confidentiality and integrity. NIST has some documentation (PDF) you can read through on cryptographic key management—it's good stuff. The basic thing to remember is that keys are generated for different purposes and not all key generation methods are suitable for all purposes. It's complicated.
Oh, right... backup your data	This Control can't be understated. If you don't like it when Word crashes and hasn't saved your work for the past hour, imagine how much you'll dislike losing your organization's systems that run the business.

PREV PAGE

NEXT PAGE

CONTROL 8: Data Recovery Capability

Improvement Opportunities	Explanation
Make allusions explicit	Don't make it more difficult than it already is for us in the profession. The more complicated and ambiguous a control framework is, the less likely it is that we're going to get it right. Not only are we likely more vulnerable, we are also wasting valuable resources.
Be prescriptive only when necessary	There's a requirement (the first one, in fact) that says you need to ensure that each system is backed up on at least a weekly basis. That may not be true, as per my notes on the matter. In my opinion, a prescription should be provided only when it can be generalized well, and I don't believe this requirement carries that property. Instead, I would have characterized the requirement in a manner that ensures backups happen when significant or materiel change occurs. Of course, this would assume that you're forwarding daily information (i.e. audit logs) to a central place (see what I mean about process dependency?).
Acknowledge the extreme importance of good key management	I'm picking on this subject primarily because I called it out as part of the second Key Take Away, but it's an area of improvement for this Control Framework (and others) overall. Key management is hard and takes resources. A lot depends on key management, not just encrypted backups. Consider SSH, HTTPS, POP-S, and the countless other protocols relying on public or private key systems. We have keys everywhere, and mostly in places we don't know and almost certainly under no real management. This could be an area of Control in its own right, and would be one I'd argue belongs in any Top 20.
Add a Metrics section	So far, all the Controls being examined have a Metrics section. Why not this one? At least cite measurements that would substantiate a claim that 1) you're doing backups appropriately, 2) they're secured appropriately, and 3) you're validating restoration capability appropriately.

PREV PAGE

NEXT PAGE

CONTROL 9: Security Skills Assessment and Appropriate Training to Fill Gaps

Critical Security Control Description **Find knowledge gaps, and fill them with exercises and training:** Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.

The Upshot:

Key Takeaways

Outsource

Do the boring work

Improvement Opportunities

Take a stand with metrics

PREV PAGE

NEXT PAGE

CONTROL 9: Security Skills Assessment and Appropriate Training to Fill Gaps

Key Takeaways	Explanation
Outsource	I strongly recommend looking into a security awareness provider in place of standing up your own awareness program. We're all suffering from scarce human resources in this field, so why should you spend their valuable time teaching and increasing awareness? Unless you have a credibility problem in your organization, don't spend this valuable resource teaching something that may not be as effective as we had once hoped.
Do the boring work	This can be very boring work, maintaining links between policy and implementation—especially the security awareness piece. Still, this is some of the most important work you can perform. Why? Consider what might happen when "that day" comes and your organization suffers a materiel breach. The organization is subsequently sued. You land in court and are asked: Did you train your people appropriately—as others in your industry have? Would you be able to answer that well?

PREV PAGE

NEXT PAGE

CONTROL 9: Security Skills Assessment and Appropriate Training to Fill Gaps

Improvement Opportunities	Explanation
Take a stand with metrics	One of the shortcomings I've seen across frameworks is a lack of metrics specification (some frameworks identify metrics, but leave off there). We all have day jobs. Metrics are not as straightforward as they sometimes seem ("just measure it" doesn't always work). There are a variety of useful resources for metrics, and there should be no reason to omit a set of prescriptive metrics at the Control Framework level. I recommend looking up Security Metrics: Replacing Fear, Uncertainty and Doubt, Security Metrics, A Beginner's Guide, or Security Metrics: A Practical Framework for Measuring Security & Protecting Data to get a start. Finally, join the discussion at SecurityMetrics.org.

PREV PAGE

NEXT PAGE

CONTROL 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Critical Security Control Description Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments: Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.

The Upshot:

Key Takeaways

- Focus on network boundaries
- Align with your business
- Keep good records

Improvement Opportunities

- Do Configuration Management once
- Clean up terminology
- Correct the level of abstraction

PREV PAGE

NEXT PAGE

CONTROL 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Key Takeaways	Explanation
Focus on network boundaries	This Control repeatedly references boundaries. A network boundary can be internal or external. Where it's external, pay particular attention to your configuration details and be restrictive. Where it's internal and the boundary distinguishes between two enclaves with different security level requirements, also pay particular attention to configuration details and be restrictive.
Align with your business	There are several mentions of "necessary ports" or "necessary services." How do you know whether something is necessary unless it's part of a service that is required for getting business done? One implication of this Control is that you need to have a very good handle on what services have to be provided to support the needs of getting things done within the organization. This tie can go missing in many IT shops, often to their detriment. Remember that the business may require more to be opened up just as much as you may realize that they don't need as much as they sometimes think. That's an odd way of saying, be fair to the organization and approach them with a "How can we help?" attitude.
Keep good records	If you're not documenting what you're doing, then how do you have any control? This Control asks for documented configuration standards and deviations to those standards. "Documenting" need not be heavyweight, either, it can be lightweight, or something that you're able to simply report out of the tools you use. If I were doing this, I'd want to enumerate exactly the questions I want to answer and be able to retrieve the answers inside of 15 minutes.

PREV PAGE

NEXT PAGE

CONTROL 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Improvement Opportunities	Explanation
Do Configuration Management once	I really don't understand why Controls 3 and 10 are segregated. Back in Control 3 I recommended that you "do this one thing" and you're on your way (because it implies doing at least a little of some other Controls). The same goes for this Control. But, what I find really odd is that the Key Takeaways I have for Control 3 aren't really what I found for Control 10. That means that there's something I'm missing, or there's something wrong—I don't feel that I'm missing anything. For example, I didn't see anything in this Control that alluded to incident response, but it seems to me that any detected, unauthorized change should be handled as an incident (it might exit the incident handling process quickly, but it should be recorded).
Clean up terminology	I'm probably starting to sound like a broken record here, but if you're starting out from a position of ill-defined terminology, no one is going to capture the same meaning by reading the same document. To look at an extreme, consider the field of abstract algebra. Look up the definitions for concepts in that field like "groups" and "rings." They're very precise definitions. When someone then says they're calculating a field over Group x, then there is precise meaning behind it and everyone can make progress. This industry is riddled with terminology having either no or multiple definitions, so getting the glossary cleaned up and using the terms consistently is critically important.
Correct the level of abstraction	On a couple of occasions, I found the requirements in this Control to be too prescriptive or too specific. A Control Framework should be relatively long-lived—it should certainly outlive certain technology life cycles. Where that can be the case, it makes more sense to leave specific technologies and/or capabilities to the organizational standards—neatly separated from the framework itself. There's nothing that would prevent a framework from offering suggestions, but do that in an appendix or companion publication.

PREV PAGE
NEXT PAGE

CONTROL 11: Limitation and Control of Network Ports, Protocols, and Services

Critical Security Control Description **Allow remote access only to legitimate users and services:** Apply host-based firewalls and port-filtering and -scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.

The Upshot:

Key Takeaways

Interoperability is required

Automation is your friend

Improvement Opportunities

Language clean up

Requirement placement

Keep it focused

PREV PAGE

NEXT PAGE

CONTROL 11: Limitation and Control of Network Ports, Protocols, and Services

Key Takeaways	Explanation
Interoperability is required	You need to have a deep understanding of your asset inventory before you're going to make very much progress on this Control. And, your asset management system is going to need to be up to par. It's great if you have an asset management system that knows about everything you have, but if it is unable to characterize each asset down to the port level, then interoperability hasn't been realized.
Automation is your friend	If you've not automated the scans required by this control, you're in for a lot of work—especially if you're larger. Automate as much as you possibly can, then validate the automation from time to time. You'll save time and money this way.

PREV PAGE

NEXT PAGE

CONTROL 11: Limitation and Control of Network Ports, Protocols, and Services

Improvement Opportunities	Explanation
Language clean up	There were only a couple of them in this Control, but some word choices didn't sit well with me. For example, the fourth requirement uses the word "change" when I would prefer to see "deviation." It's semantic, but I think important.
Requirement placement	I really think that some of the requirements found herein should be in a different Control. The Control that kept coming up was Control 19 (Secure Network Engineering).
Keep it focused	At least one of these requirements was written in an operational form rather than a security requirement form. The Controls would be best suited if they stuck to a single perspective (security requirements on operational processes) rather than try to be a chameleon.

PREV PAGE

NEXT PAGE

CONTROL 12: Controlled Use of Administrative Privileges

Critical Security Control Description Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open a malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.

The Upshot:

Key Takeaways

- Automation is your friend
- Be an enforcer
- Think seriously about two-factor authentication

Improvement Opportunities

- Stay focused
- Get rid of reversible instruction
- Address operational concerns over technical concerns

PREV PAGE

NEXT PAGE

CONTROL 12: Controlled Use of Administrative Privileges

Key Takeaways	Explanation
Automation is your friend	The plain truth is that you're not going to manually enumerate and double-check your user base every day or even once a week. Automate as much as you can. If your base toolset doesn't help you, then break out that shell programming book and get ready to get your hands dirty. But don't just report—report with trending and changes—which means you're going to need to save your output for the next run.
Be an enforcer	Not the kind you find on the ice. The kind that doesn't bend the rules for anyone. If your users are having a hard time remembering il#VMNnAY/j, then spring for 1Password or teach them how to use Password Safe; there are probably others.
Think seriously about two-factor authentication	There's a recommendation in this Control that Administrative access should always use two-factor authentication. That's a good strategy. But why not apply that for all of your users? Not just when accessing the VPN, but all the time? I'm sure it's a cost/resource issue, but we're pretty well overdue for this.

PREV PAGE

NEXT PAGE

CONTROL 12: Controlled Use of Administrative Privileges

Improvement Opportunities	Explanation
Stay focused	There weren't many (one is enough), but some of these requirements should be found elsewhere. For example, any of the password-related requirements could easily be left to Control 16 (Account Monitoring and Control). When similar requirements exist in more than one place, you're asking for document maintenance headaches at best and user confusion at worst.
Get rid of reversible instruction	If any password guidance is kept in this Control, then at least remove any allowance for reversible encryption.
Address operational concerns over technical concerns	I feel that many of these requirements simply don't address what really needs addressing—the operational process of granting, maintaining, and removing administrative privileges. Instead, this Control seems a lot like Control 16, but slightly tailored for Administrators. The reality is that most everything for account and credential management is the same, so this Control should just concentrate on what's different.

PREV PAGE

NEXT PAGE

CONTROL 13: Boundary Defense

Critical Security Control Description Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines: Establish multi-layered boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks ("extranets").

The Upshot:

Key Takeaways

Use proxies and monitor

Improvement Opportunities

Focus

Key management requirements

PREV PAGE

NEXT PAGE

CONTROL 13: Boundary Defense

Key Takeaways	Explanation
Use proxies and monitor	This Control isn't bad (though see Improvement Area number one) and it provides what I think is some really great advice. Use proxies when you can, and when you do use proxies detect any traffic bypassing that proxy. The idea is to allow traffic through known locations and monitor based on those "choke points." Some of those who won't want to be monitored will try to get around the choke point, which would then, presumably, be detected by appropriate monitoring. Some of those who won't want to be monitored will simply tunnel out—but you should be able to monitor for that as well.

PREV PAGE

NEXT PAGE

CONTROL 13: Boundary Defense

Improvement Opportunities	Explanation
Focus	To me, this Control could easily be merged with Control 19 (Secure Network Engineering) and it should be—appropriate boundary defense is part of engineering a secure network. If what this control is really seeking to convey is how to secure the services you provide through your boundary (i.e. VPN, SMTP, and so on), then the control could be renamed.
Key management requirements	Don't forget that when you recommend that things can be encrypted or signed that you're also recommending the key management that comes with it. Key management is not easy, and you won't be able to rely on your users to do it well—we can't rely on users to manage their passwords well, right?

PREV PAGE

NEXT PAGE

CONTROL 14: Maintenance, Monitoring, and Analysis of Audit Logs

Critical Security Control Description Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines: Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run biweekly reports to identify and document anomalies.

The Upshot:

Key Takeaways

- Enable (centralized) logging
- Review logs regularly
- Take the time

Improvement Opportunities

- Just some minor cleanup
- Oh, and metrics clarification

PREV PAGE

NEXT PAGE

CONTROL 14: Maintenance, Monitoring, and Analysis of Audit Logs

Key Takeaways	Explanation
Enable (centralized) logging	QED.
Review logs regularly	And, not just "look" at them. Use a tool to help you make sense of it all—this isn't the realm for manual processes. Find vendors that offer content out-of-the-box or that can be easily customized for your specific needs. Remember this: Tools should be force multipliers for you. That means that they should help your security analyst get the work of several done in the same time period.
Take the time	Getting this right is important, but if you take the time to get some of the other Controls in place (i.e. Controls 1, 2, 3, and 10) and you're using "gold" images/ configuration files, then you're actually in a really good place. Just make sure the "gold" information is appropriately configured, and that part of your asset deployment process includes validating centralized logging is taking place.

PREV PAGE

NEXT PAGE

CONTROL 14: Maintenance, Monitoring, and Analysis of Audit Logs

Improvement Opportunities	Explanation
Just some minor cleanup	All things considered, I feel that this is a decently written control. It doesn't seem to stray too far from what I expected it's target subject matter to be, and it is, for the most part, clear (there are a few areas that could use some crystallization).
Oh, and metrics clarification	I'd like to see some clearer metrics. I'll be the first to admit that I am not a statistician or a "metrics guy" by trade or training. But I have been learning. The metrics given throughout these Controls are probably intended to suggest that the controls are, in effect, working—that they're doing some good. But, specific measures and the sample size from which the measures are taken matters very much to the ability to generalize to the entire enterprise. We have resource constraints, that's true, but if the sample size is too small, your conclusions will be wrong at best.

PREV PAGE

NEXT PAGE

CONTROL 15: Controlled Access Based on the Need to Know

Critical Security Control Description **Prevent attackers from gaining access to highly sensitive data:** Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to non-public data and files.

The Upshot:

Key Takeaways

- Start with the obvious
- Leverage standards

Improvement Opportunities

- Focus
- Tighten notification demands
- Key management

PREV PAGE

NEXT PAGE

CONTROL 15: Controlled Access Based on the Need to Know

Key Takeaways	Explanation
Start with the obvious	At full tilt, this requirement is going to murder your processes, so start off slow and with the obvious. Where are the "crown jewels?" Cordon them off, ensure they're transmitted only over secure channels, tag them with appropriate classification identifiers, and audit everything that happens to them or near them (as should be described in Control 14 on audit logging).
Leverage standards	FIPS 199 is a standard that some must adhere to, but it's useful (and available) to everyone. Try it out as a mechanism to help you categorize your information and information systems. See if you can get your Asset Management System to "speak" FIPS 199 or at least tag your assets with FIPS 199-specific data formats (you'll probably have to invent one—then open source it, OK?).

PREV PAGE

NEXT PAGE

CONTROL 15: Controlled Access Based on the Need to Know

Improvement Opportunities	Explanation
Focus	Again, I believe a Control should be focused and given that there's a DLP-specific Control (17), the DLP-specific requirements herein should probably be moved. Similarly for the audit logging requirements also found herein.
Tighten notification demands	Allowing 24 hours for notification, especially on sensitive information, seems like too long a timespan. I'd prefer to see as close to "immediate" as you can get.
Key management	There are many ways we rely on cryptography, and, it seems, little guidance in implementing the most important piece—key management. I would really like to see references from Control requirements to good, easy-to-comprehend guidance in this area. Maybe no such guidance exists, in which case, it should.

PREV PAGE

NEXT PAGE

CONTROL 16: Account Monitoring and Control

Critical Security Control Description **Keep attackers from impersonating legitimate users:** Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.

The Upshot:

Key Takeaways

- **Establish an Account Management process**
- **Make a checklist**
- **Do the monitoring**
- **Understand attack state-of-the-art**

Improvement Opportunities

- **Tighten terminology**
- **Combine Control 12 with this one**

PREV PAGE

NEXT PAGE

CONTROL 16: Account Monitoring and Control

Key Takeaways	Explanation
Establish an Account Management process	If you don't already have one, do this (see the second take away). You should be actively managing your accounts. That said, see the ask for Requirement 7. It would be nice to understand how many incidents (resulting in breach or not) have used should-have-been-expired-and-disabled, stale accounts.
Make a checklist	Go through this Control and make a checklist of all the things you need to do for your account management process, prioritize them, then implement them.
Do the monitoring	Pay attention to the requirements that generate reports and require monitoring of account state and usage. Be sure to trend the things you're seeing, because you might pick up on anomalies you simply wouldn't otherwise see.
Understand attack state-of-the-art	If you don't understand how password cracking works and how long it takes (or doesn't take, if you prefer), then read up on the subject. Every time you revisit your credential policies, you should also be revisiting the state of the art for attacks against them. Of course, this advice can be generalized to other areas of your security program.

PREV PAGE

NEXT PAGE

CONTROL 16: Account Monitoring and Control

Improvement Opportunities	Explanation
Tighten terminology	We've found throughout the Controls that terminology can be tricky. It might be pedantic, but that's what matters when audit time comes around, and, more important than that, if you misinterpret "system account" you might just leave your attack surface that much bigger, which you don't want.
Combine Control 12 with this one	It just doesn't make sense to me to have two Controls for what amounts to the same thing—the only difference is the level of access one type of account is expected to have.

PREV PAGE

NEXT PAGE

CONTROL 17: Data Loss Prevention

Critical Security Control Description Stop unauthorized transfer of sensitive data through network attacks and physical theft: Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.

The Upshot:

Key Takeaways

Start small

Grow carefully

Improvement Opportunities

Last time: Key management guidance—*please*

Understand your business

PREV PAGE

NEXT PAGE

CONTROL 17: Data Loss Prevention

Key Takeaways	Explanation
Start small	I know the DLP vendors won't like to hear this, but you can do quite a bit in terms of detection without a "DLP" system. Whatever you do, don't implement DLP without first looking at how you can use proxies, audit logs, and your SIEM solution first. Leverage what you've got.
Grow carefully	Be sure you're measuring not only what this Control wants you to measure, but that you're also measuring how effective the solution is overall for your organization. Are you catching tons of false positives and few true positives? Do you have ways of measuring false negatives? I'm not suggesting that DLP isn't for you, but I wouldn't recommend throwing caution to the wind here.

PREV PAGE

NEXT PAGE

CONTROL 17: Data Loss Prevention

Improvement Opportunities	Explanation
Last time: Key management guidance—*please*	The first requirement here calls for drive encryption software to be deployed on mobile devices. Not only is the term "mobile device" somewhat nebulous (it's at least subject to interpretation), but there is a neglect of key management. I won't mention this shortcoming again, because I don't really want to sound like a broken record (by the way, if you want to feel old—you do, don't you?—ask your kids if they know what that is).
Understand your business	Implementing a DLP-specific solution is not inexpensive. And, it's not resource-free either. Know your business and implement DLP for what matters first.

PREV PAGE

NEXT PAGE

CONTROL 18: Incident Response and Management

Critical Security Control Description **Protect the organization's reputation, as well as its information:** Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

The Upshot:

Key Takeaways

Start

Join the community

Measure well

Improvement Opportunities

Add metrics and tests

PREV PAGE

NEXT PAGE

CONTROL 18: Incident Response and Management

Key Takeaways	Explanation
Start	In my mind, Incident Detection and Response is as important as Asset and Configuration Management. You simply need to do this at some level. Find a group of people in your organization—they don't all need to be in IT, by the way—who are interested and passionate about information security and start. Get some executive buy-in before you start doing anything with authority. Get legal involved for any "special" NDAs the organization might desire for such a team—they may have temporary access to unlimited information, after all.
Join the community	Incidents don't just happen to your organization, they happen to everyone. Know your local, regional, and National CERTs. When you're starting, set the expectation that the organization will share appropriate information with the appropriate external organizations (start with the CERTs). EMC recently released some open source software to help facilitate incident information sharing, so take a look at how you might leverage that.
Measure well	If there's an area that benefits from effective measurement it's this one. If you need some metrics, look for the CIS Security Metrics 1.1.0 and pick up a book or two or three. Hint: Some of these resources have incident-response-specific metrics laid out for you. Even if you're starting small, get metrics in place—they will give you focus and provide you with ammunition to continue the mission.

PREV PAGE

NEXT PAGE

CONTROL 18: Incident Response and Management

Improvement Opportunities	Explanation
Add metrics and tests	There are no metrics presented for Control 18. I'm really dumbfounded by this. See Key Take Away three above.

PREV PAGE

NEXT PAGE

CONTROL 19: Secure Network Engineering

Critical Security Control Description **Keep poor network design from enabling attackers:** Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.

The Upshot:

Key Takeaways

If you're just starting out: DO THIS NOW

If you're just realizing this is good: Take it slow

Get Configuration and Asset Management under control

Improvement Opportunities

Add metrics and tests

Include small-fry guidance

PREV PAGE

NEXT PAGE

CONTROL 19: Secure Network Engineering

Key Takeaways	Explanation
If you're just starting out: DO THIS NOW	If you can get the design secure from the outset, your life will be easier down the road. If you doubt me, ask some veteran IT folk about this. Just strike up a conversation about broad, flat networks and security and see where it takes you.
If you're just realizing this is good: Take it slow	You've been operating without a secure design for a while. Start it slow, but within reason. Look for the most critical business processes you support and secure those. Have a roadmap. Execute. Plan to change.
Get Configuration and Asset Management under control	If you want to react quickly and smoothly, then you're going to want to ensure that you've got a well-oiled machine in place to handle your assets and their configurations.

PREV PAGE

NEXT PAGE

CONTROL 19: Secure Network Engineering

Improvement Opportunities	Explanation
Add metrics and tests	There are no metrics presented for Control 19. Again, dumbfounded here, but perhaps this isn't a mortal sin like the lack of metrics for Control 18. There must be something of use that can be measured here. How about the percentage of network expansion/updates that undergo a security design review?
Include small-fry guidance	From what I hear and read, most of the struggling organizations are small or at least smallish. They may not run a lot of services in-house, and therefore may not have a real need for three tiers. Are there other architectures equally effective for this different case?

PREV PAGE

NEXT PAGE

CONTROL 20: Penetration Tests and Red Team Exercises

Critical Security Control Description **Use simulated attacks to improve organizational readiness:** Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises—all-out attempts to gain access to critical data and systems to test existing defenses and response capabilities.

The Upshot:

Key Takeaways

Contract if you can

If you can't, then do something

Improvement Opportunities

Add metrics and tests

PREV PAGE

NEXT PAGE

CONTROL 20: Penetration Tests and Red Team Exercises

Key Takeaways	Explanation
Contract if you can	My bet is that most organizations don't need to hire a dedicated penetration testing team. Some do. My recommendation is to find a reputable group of people that do this day in and day out. Have some internal security guys geek out with the red team for a while before, during, and after—they'll learn from it. But, you'll probably get more for your dollar by outsourcing this function. Take this with a grain of salt, because your organizational mission and/or industry may dictate otherwise.
If you can't, then do something	Peppered throughout my notes below are some ideas for starting small, again with a group of passionate, willing participants. At the very least the little you're able to accomplish with such a grass roots effort will begin to bring visibility to the purpose of security. Start with things that matter—physical access, social engineering—then move to the trickier domain of logical pen testing.

PREV PAGE

NEXT PAGE

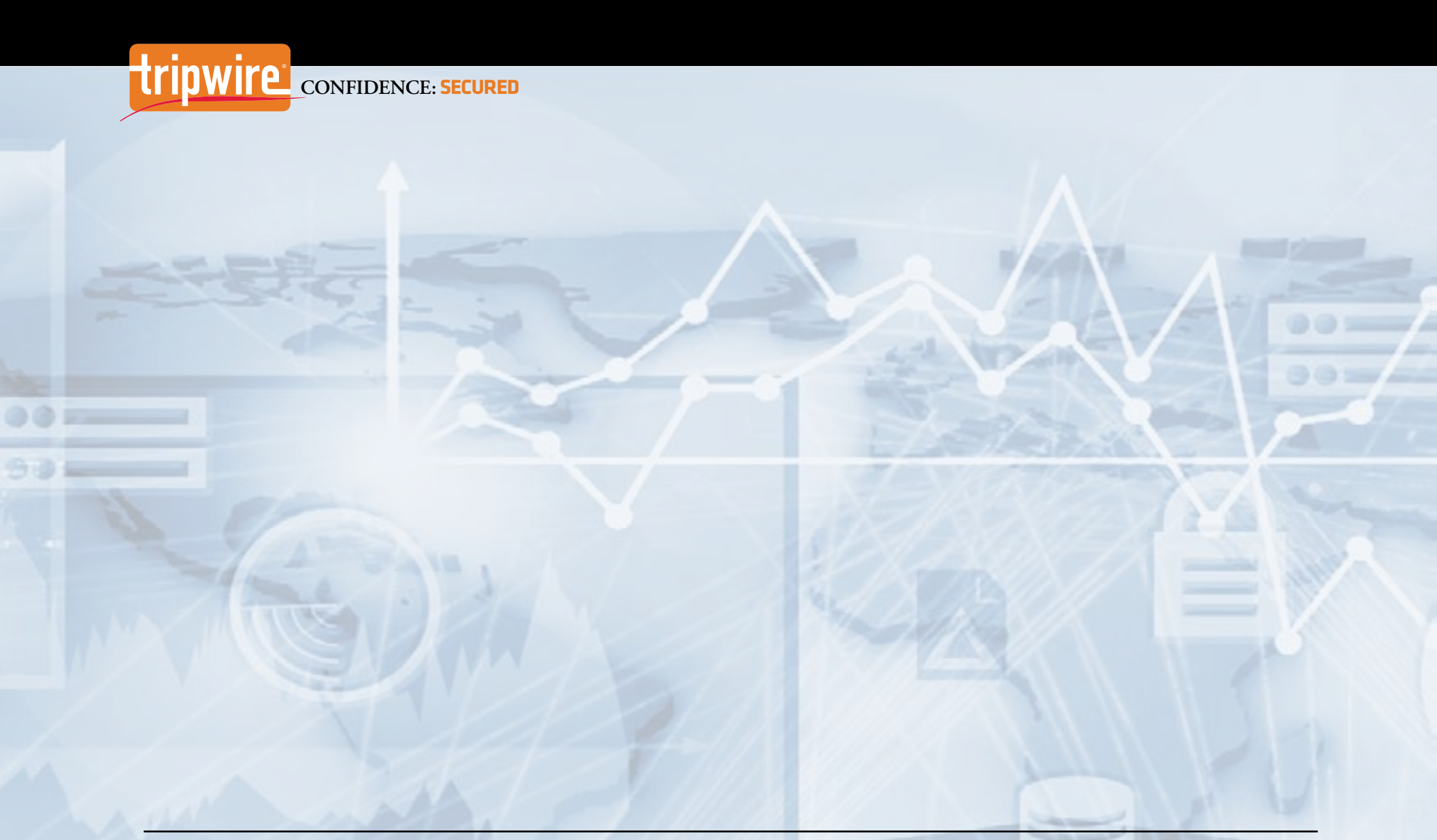
CONTROL 20: Penetration Tests and Red Team Exercises

Improvement Opportunities	Explanation
Add metrics and tests	There are no metrics presented for Control 20. Again.

PREV PAGE

NEXT PAGE

tripwire CONFIDENCE: SECURED



tripwire

Tripwire is a leading provider of advanced threat, security and compliance solutions that enable enterprises, service providers and government agencies to confidently detect, prevent and respond to cybersecurity threats. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business-context, and enable security automation through enterprise integration. Tripwire's portfolio of enterprise-class security solutions includes configuration and policy management, file integrity monitoring, vulnerability management and log intelligence. Learn more at tripwire.com.

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

BREGCSC1a 201310