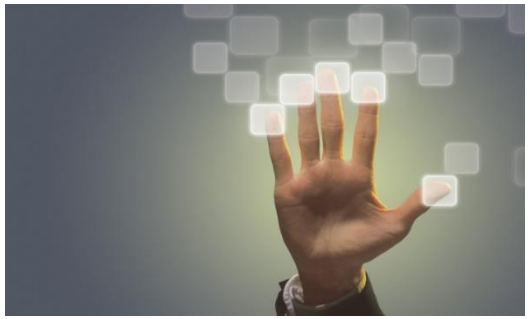
How to Use the 20 Critical Controls in Your Business

DENISE KINSEY, PHD, CISSP, C|CISO

CISSE 2020



Use of these slides

You are permitted to use these slides but credit to the author is **expected and required**

No warranty is made as to the software or its effects suggested herein

Always **backup your data** prior to installing any new programs

D. Kinsey (2018), UH or Kinsey, D. (2018), UH

What are ‘Critical Controls’?

Issues of compliance: diverting effort and attention from ‘correct’ and ‘control’ posture.

In 2008 NSA: need for “offense must inform defense” posture

Identify greatest impact to risk posture

Consortium of US and international agencies, and private sector

SANS coordinated and in 2013 transferred to the Council on CyberSecurity

Why should your business care?

Prioritizing security functions

Focus on ‘What Works’

Subset of NIST SP 800-53 – standard, repeatable, tested

Basis for immediate high-value action

Aids in compliance efforts

The Top 20 Critical Security Controls

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

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

4: Continuous Vulnerability Assessment and Remediation

5: Malware Defenses

6: Application Software Security

7: Wireless Device Control

8: Data Recovery Capability

9: Security Skills Assessment & Appropriate Training to Fill Gaps

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

The Top 20 Critical Security Controls Cont'd

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

12: Controlled Use of Administrative Privileges

13: Boundary Defense

14: Maintenance, Monitoring, & Analysis of Audit Logs

15: Controlled Access Based on the Need to Know

16: Account Monitoring and Control

17: Data Loss Prevention

18: Incident Response and Management

19: Secure Network Engineering

20: Penetration Tests and Red Team Exercises

1: Inventory of Authorized and Unauthorized Devices

"**Actively** manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access."

http://www.sans.org/critical-security-controls/control/1

Davis-Besse Slammer Worm:
http://www.securityfocus.com/news/6767

Redundancy with Control #7 Wireless

Rogue HW Detection

Detecting & Preventing Rogue Devices on a Network : https://www.sans.org/reading-room/whitepapers/wireless/detecting-preventing-rogue-devices-network-1866

NMAP: http://nmap.org

Microsoft Server Health Check: http://technet.microsoft.com/en-us/library/cc768012.aspx

Linux – several choices including Monitorix

http://www.monitorix.org/doc-debian.html

2: Inventory of Authorized and Unauthorized Software

"**Actively** manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."

http://www.sans.org/critical-security-controls/control/2

Risks of using pirated SW

Increase chances software won't function correctly or will fail completely;

Forfeit customer support, upgrades, technical docs, training, and bug fixes;

No warranty to protect business;

Increase risk of exposure to virus that can destroy valuable data;

Software is an outdated version, a beta (test) version, or a nonfunctioning copy;

Significant fines for copyright infringement; and

Embarassment: public and private, negative

http://siia.net/index.php?option=com_content&view=article&id=387:ap-faq&catid=8:anti-piracy-overview

How to Prevent

Know what should be there! (List Authorized)

Restrict access – whitelist

Have an AUP!

Enforce the AUP!

Least Privilege/access on systems

Disable [ctrl] + click

Tools for prevention

Window's AppLocker

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

Tenable SecurityCenter Continuous View (CV)

https://www.tenable.com/products/securitycenter-continuous-view

OS SW License Mgr & Inv. Tools

Snipe IT – Win, Linux, Mac, mobile, web-based: https://snipeitapp.com/

OpenLM – Win, Linux, Mac: https://www.openlm.com/

Streamline - http://audit.assetlabs.com/streamline

SpiceWorks: https://www.spiceworks.com/free-software-inventory-audit-tool/

3: Secure Configs for HW & SW on Mobile Devices, Laptops, Workstations, & Servers

"Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings."

http://www.sans.org/critical-security-controls/control/3

Configuration Managers

Linux:

- Chef: http://gettingstartedwithchef.com/
- Puppet: https://puppetlabs.com/learn?gclid=CIm_5uqZkL0CFZLm7Aod3jAASg
- InfoWorld article that compares the two: http://www.infoworld.com/d/data-center/puppet-or-chef-the-configuration-management-dilemma-215279

Windows:

- Chef: http://gettingstartedwithchef.com/

- How to use Windows PowerShell Desired State Configuration (DSC) : http://www.techrepublic.com/blog/data-center/desired-state-configuration-manage-rapid-change-at-scale-with-constant-failure/

4: Continuous Vulnerability Assessment and Remediation

“Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.”

http://www.sans.org/critical-security-controls/control/4

Vulnerability Resources

Baselining tips & techniques:
http://www.wildpackets.com/use_cases/network_baselining

Wireshark: http://www.wireshark.org/

Angry IP Scanner: (from SourceForge):

http://angryip.org/w/Download

Nessus Vulnerability Scanner:
http://www.tenable.com/products/nessus/select-your-operating-system

Predicting Attack Paths using Nessus
http://www.tenable.com/expert-resources/whitepapers/predicting-attack-paths

5: Malware Defenses

"Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action."

http://www.sans.org/critical-security-controls/control/5

Malware Resources

Tech Republic – 5 Enterprise-ready antivirus solutions: http://www.techrepublic.com/blog/five-apps/five-enterprise-ready-antivirus-systems/1749/

Network World – An evaluation/test of several products: http://www.networkworld.com/news/2013/071213-enterprise-anti-virus-software-test--271765.html

SANS: Source of Malware info: http://www.sans.org/security-resources/malwarefaq/

SANS: Malware Defenses:

http://www.sans.org/critical-security-controls/control.php?id=5

6: Application Software Security

"Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses."

http://www.sans.org/critical-security-controls/control/6

Tips for application SW

Institute version control

Hash all ‘black-box’ solutions (see next slide)

Treat code as an asset – lock up source code!

Limit apps on enterprise systems

In RFPs specifically state expectation

Test and verify all programs

Trust no one and no system

Hash Generators

From SourceForge :

- MD5, SHA-1, SHA-256, Tiger, Whirlpool

  http://md5deep.sourceforge.net/

Cnet's Easy Hash (130 different Hash Functions):

http://download.cnet.com/Easy-Hash/3000-2094_4-10870407.html

Cryptool:http://www.cryptool.org/en/

7: Wireless Device Control

"The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems."

http://www.sans.org/critical-security-controls/control/7

Wireless Tips

Review tips in Control #1

Create AUPs for devices used in the parking lot, grounds, or taken into the employer's facility.

AUP should contain no use of phones as hotspots while at facility.

Netstumbler: http://www.netstumbler.com/downloads/

InSSIDer (need MS .net files): http://www.metageek.net/products/inssider/

8: Data Recovery Capability

"The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it."

http://www.sans.org/critical-security-controls/control/8

Recovery Tips

What can you afford to lose? Determine a BU schedule that works for your business.

Remember all devices – configs, registry, cloud/remote apps.

Have multiple versions

Test all backups!

Belarc Advisor: http://www.belarc.com/

DR Resources

Disaster Recovery Resources:
http://www.disasterrecoveryresources.net/drr/

Disaster Resources for business & community:
http://www.disaster-resource.com/

SANS Disaster Recovery Content – from info, to plans and policy examples:
http://www.sans.org/reading_room/whitepapers/recovery/

Disaster Recovery Plan & Resources from the SBA:
http://buildmybiz.com/material/disaster-recovery-plan/

9: Security Skills Assessment & Appropriate Training to Fill Gaps

---

"For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs."

http://www.sans.org/critical-security-controls/control/9

Gap Training

Council on CyberSecurity:
http://www.counciloncybersecurity.org/practice-areas/people

Free e-book on cybersecurity threats:
http://www.labtechsoftware.com/Landing/security-eBook-ppc/?source=LT-PPC-Google-USCyberSecurity-072613&utm_source=google&utm_medium=cpc&utm_term=it%20security%20solution&gc-lid=CJbO892qkL0CFSJo7AodJ0UAiQ

NIST Special Pub 800-50 Building an Info Tech Security Awareness & Training Program:

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Training ‘must haves’

Continuous

Understandable

Take-aways – pamphlets, guides, posters, etc. for reminding

Everyone included

Relevant and applicable to positions

Compliment the security plan in place

Sign receipt for completion – needed for compliance

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

"Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings."

http://www.sans.org/critical-security-controls/control/10

IDS/IPS

Snort by SourceFire (Cisco) (Try it at home!):

http://www.snort.org/

Whitepaper from TechTarget: How to use Snort:
http://searchsecuritychannel.techtarget.com/tutorial/Snort-Tutorial-How-to-use-Snort-intrusion-detection-resources

OSSEC by TrendMicro:

http://www.ossec.net/

Suricata by DHS & Naval Warfare System Command

http://www.openinfosecfoundation.org/index.php/download-suricata

Additional Resources

Sans Security News:

http://www.sans.org/newsletters/

Drive Wiping: The truth, Darik's Boot & nuke www.dban.org/

Example Security Policies, Examples & Templates:

http://www.sans.org/security-resources/policies/

10 Steps to Creating Your Own IT Security Audit:

http://www.itsecurity.com/features/it-security-audit-010407/

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

"Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers."

http://www.sans.org/critical-security-controls/control/11

All remote access only to legitimate users and services. Best defense: host-based firewalls and port-filtering and scanning tools.

Lockdown ports/protocols/services

What is a protocol analyzer?
http://searchnetworking.techtarget.com/definition/network-analyzer

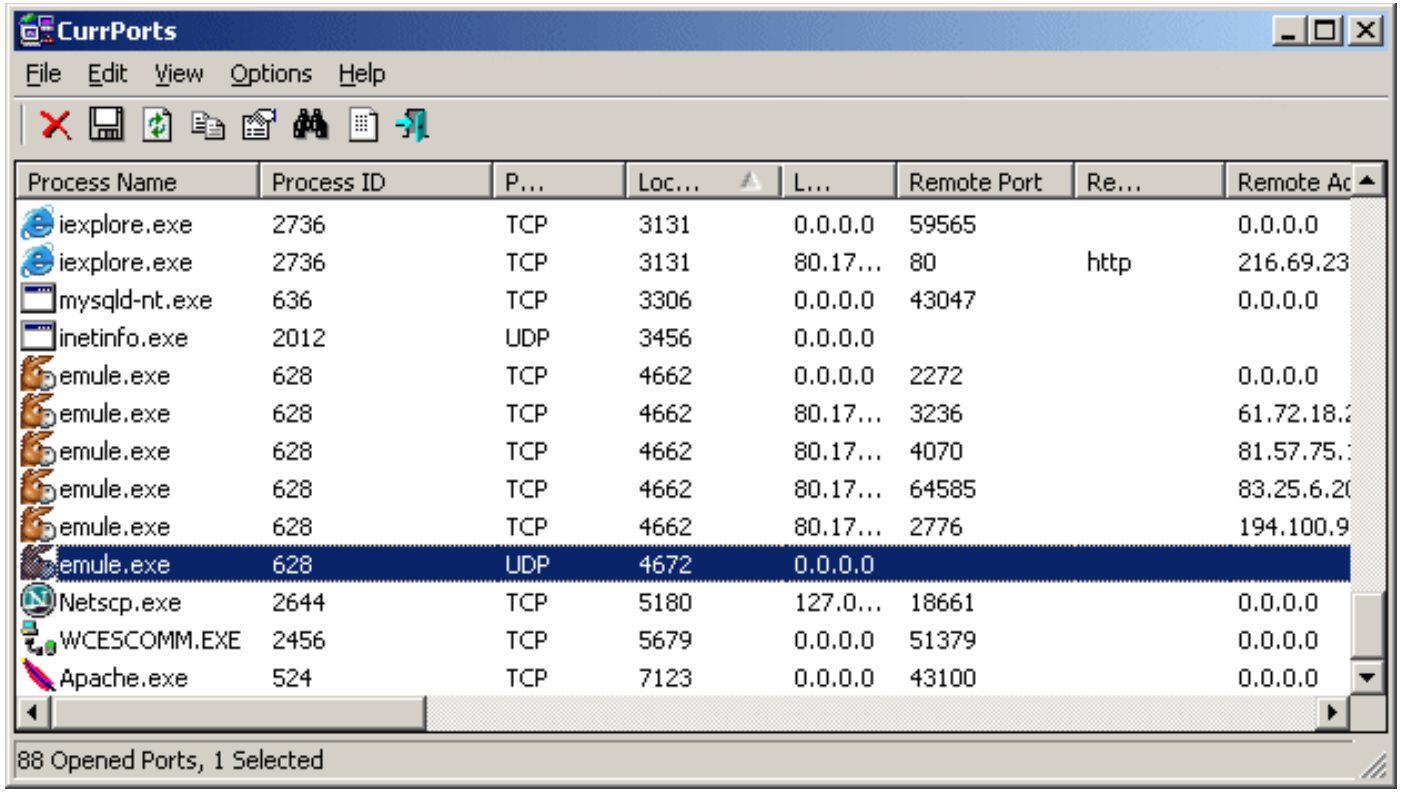
Wireshark: http://www.wireshark.org/

GFI LanGuard:

http://www.gfi.com/land/Home/lanss/port-scanning-sm?adv=13742&loc=18&kwd=7&gclid=CJeVy67zuL8CFUKCMgodexcAJQ

CurrPorts V2.0: http://www.nirsoft.net/utils/cports.html

Screen shot of CurrPorts



More tools for controlling ports/protocols/services

Microsoft SysInternals Suite:

http://technet.microsoft.com/en-us/sysinternals/bb545021.aspx

Easiest ways to manage ports is through a firewall or IDS/IPS (resources supplied in Part 1 for malware).

12: Controlled Use of Administrative Privileges

"The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. "

http://www.sans.org/critical-security-controls/control/12

Protect and validate administrative accounts on desktops, laptops, and servers to prevent attacks.

Resources to limit privilege escalation

Tech Republic article on some of the ways privileges are escalated (Windows and Linux):

http://www.techrepublic.com/blog/it-security/mitigating-the-privilege-escalation-threat/

Great information from OWASP on privilege escalation:

https://www.owasp.org/index.php/Testing_for_Privilege_escalation_%28OWASP-AZ-003%29

13: Boundary Defense

"Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. ."

http://www.sans.org/critical-security-controls/control/13

Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines.

Establish a DMZ

Boundary Defense includes firewall and IPS.

Resources for Boundary Defenses

- Introduction to Firewalls: http://www.firewallinformation.com/

- Firewall information and comparison (hardware and software, stateful vs stateless):

http://searchnetworking.techtarget.com/feature/Choosing-a-next-generation-firewall-Vendor-comparison

IDS/IPS

Snort by SourceFire (Cisco)(Try it at home!):

http://www.snort.org/

Whitepaper from TechTarget: How to use Snort:
http://searchsecuritychannel.techtarget.com/tutorial/Snort-Tutorial-How-to-use-Snort-intrusion-detection-resources

OSSEC by TrendMicro:

http://www.ossec.net/

Suricata by DHS & Naval Warfare System Command

http://www.openinfosecfoundation.org/index.php/download-suricata

14: Maintenance, Monitoring, and Analysis of Audit Logs

“Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack. .”

http://www.sans.org/critical-security-controls/control/14

Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines.

Log Resources

SANS: Logging and Monitoring to Detect Intrusions and Compliance Violations in the Environment:

http://www.sans.org/reading-room/whitepapers/detection/logging-monitoring-detect-network-intrusions-compliance-violations-environment-33985

Recommended Logging for Windows:

http://www.sans.org/security-resources/idfaq/logging-windows.php

6 Categories of Critical Log Information:

http://www.sans.edu/research/security-laboratory/article/6toplogs

15: Controlled Access Based on the Need to Know

"The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification."

http://www.sans.org/critical-security-controls/control/15

Access limited to Need to Know

Prevent attackers from gaining access to highly sensitive data.

Enterprise Access Management

SANS: Adding Enterprise Access Management to Identity Management:

http://www.sans.org/reading-room/whitepapers/analyst/adding-enterprise-access-management-identity-management-35075

ZDNet: Seven ways identity, access management will change in the enterprise: http://www.zdnet.com/seven-ways-identity-access-management-will-change-in-the-enterprise-7000023382/

16: Account Monitoring and Control

“Actively manage the life-cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them. ”

http://www.sans.org/critical-security-controls/control/16

Keep attackers from impersonating legitimate users.

Account Monitoring & Control Tips

Disable any un-used accounts

Delete any invalid accounts and guest accounts

Check what is being logged

They ensure logs are reviewed

For most businesses you can combine this with control #12 - the only difference is the level of access one type of account is expected to have, good procedures should cover both.

Resources

BlogSpot Article: http://id-use.blogspot.com/2016/04/how-to-manage-non-personal-system.html

ComputerHope Article - Managing User Accounts by System:

https://www.computerhope.com/issues/ch001911.htm

17: Data Protection

“The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.”

http://www.sans.org/critical-security-controls/control/17

Stop unauthorized transfer of sensitive data through network attacks and physical theft. (Wireshark!)

Data Protection Tips

Data Protection: At rest, in transit, and in disposal.

Symantec: 8 Tips to Protect your Business and Secure its Data:

http://eval.symantec.com/mktginfo/enterprise/other_resources/b-8_tips_protect_your_business_secure_data.en-us.pdf

HL Chronicle of Data Protection: 5 Tops to Protect your Data:

http://www.hldataprotection.com/2014/01/articles/news-events/5-tips-to-protect-your-privacy-for-data-privacy-day/

18: Incident Response and Management

“Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) 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. .”

http://www.sans.org/critical-security-controls/control/18

Incident Response Tips

Protect the organization's reputation, as well as its information.

Review Disaster Recovery Tips (slides are next)

Understand incident response: 5 tips to make IR work for you:

http://www.csoonline.com/article/2133834/business-continuity/understanding-incident-response-5-tips-to-make-ir-work-for-you.html

Response & Recovery Tips

What can you afford to lose? Determine a BU schedule that works for your business.

Remember all devices – configs, registry, cloud/remote apps.

Have multiple versions

Test all backups!

Belarc Advisor: http://www.belarc.com/

DR Resources

Disaster Recovery Resources:
http://www.disasterrecoveryresources.net/drr/

Disaster Resources for business & community:

http://www.disaster-resource.com/

SANS Disaster Recovery Content – from info, to plans and policy examples: http://www.sans.org/reading_room/whitepapers/recovery/

Disaster Recovery Plan & Resources from the SBA:

http://buildmybiz.com/material/disaster-recovery-plan/

19: Secure Network Engineering

“Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers. ”

http://www.sans.org/critical-security-controls/control/19

Secure Network Engineering Tips

Keep poor network design from enabling attackers

Diagram the network, label it (proprietary), then secure it!

Consider design in all additions

TechTarget: Turning around a bad network: What to do if you inherit one: (Requires free membership to access this article).

http://searchnetworking.techtarget.com/news/1346345/Turning-around-a-bad-network-What-to-do-when-you-inherit-one

Tools to help diagram:

Microsoft Visio:

http://office.microsoft.com/en-us/visio/microsoft-visio-professional-2013-create-professional-diagrams-FX103791368.aspx

Raptor: http://raptor.martincarlisle.com/

20: Penetration Tests and Red Team Exercises

"Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker."

http://www.sans.org/critical-security-controls/control/20

Use simulated attacks to improve organizational readiness.

PenTest Tools & Tips

Back up!!!!!*

Use a virtualized environment first!

Tools include:

- Kali Linux: http://www.kali.org/
- Armitage: http://www.fastandeasyhacking.com/
- Helix: http://www.e-fense.com/products.php
- Metasploit: http://www.metasploit.com/
- Core Impact: http://www.coresecurity.com/core-impact-pro

Any Questions?

dkinsey@central.uh.edu

For slides in PowerPoint format download from CISSE website