Critical Security Controls

COL Stef Horvath

MNARNG

Oct 21, 2015

CYBER SECURITY SUMMIT

Agenda

- Security Controls – the Good, the Bad, the Ugly
- Emerging Security Controls – Critical Security Controls
  - Methodology and Contributors
  - Supporting Vendors
- Barriers
- Distinct Advantages
  - Prioritized, highly focused set of actions
  - Regulatory
  - Insurance
  - Business Efficiencies

CYBER SECURITY SUMMIT

The Good…

INTERNET SECURITY ALLIANCE

SOPHISTICATED MANAGEMENT OF CYBER RISK

Maintaining Focus on Good Cyber Hygiene

- Date: May 2013
- "…conventional wisdom - 80% of cyber incursions prevented or substantially mitigated using good cyber hygiene."
- Verizon and US Secret Service conducted forensic analysis of hundreds of cyber security breaches going back to 2008, proving conventional wisdom wrong
- Employing well known and comparatively inexpensive cyber security best practices could have prevented or mitigated damage for 97% of cyber events.

CYBER SECURITY SUMMIT

More on Cyber Hygiene

The good

CYBER SECURITY SUMMIT

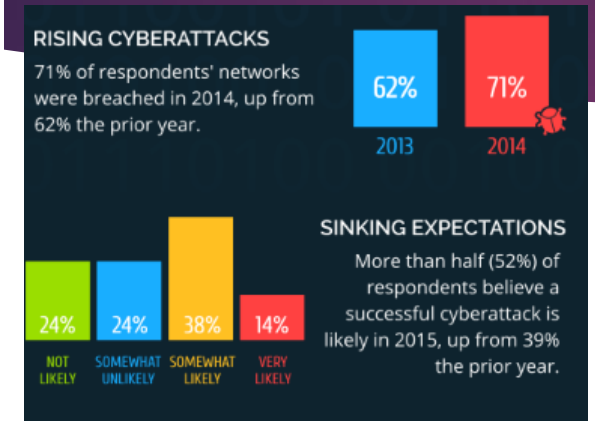
The Bad – Framework Fallacy

"…the information assurance industry has developed best practices and frameworks, but many times ***implementing these frameworks became cumbersome and served only to provide information for compliance reports—instead*** of being used to block attacks against information systems."

"…counter productive to view compliance as the ultimate goal of the cyber security policy." "Only an organization capable of understanding external developments and incident trends and use this insight to inform policy and strategy will be successful in the long term."

CYBER SECURITY SUMMIT

The Ugly…



CYBEREDGE GROUP **2015 CYBERTHREAT DEFENSE REPORT**
NORTH AMERICA & EUROPE

Article | *McKinsey Quarterly*

The rising strategic risks of cyberattacks

McKinsey&Company

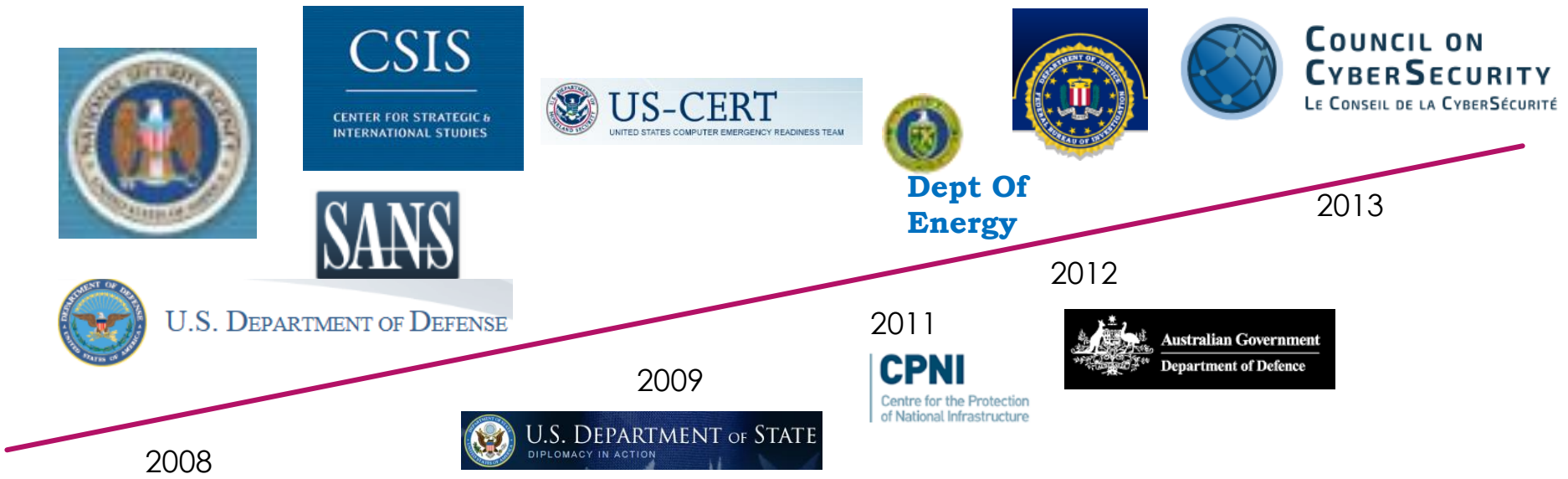
Research by McKinsey and the World Economic Forum points to a widening range of technology vulnerabilities and potentially huge losses in value tied to innovation.

May 2014 | by Tucker Bailey, Andrea Del Miglio, and Wolf Richter

"…most technology executives believe that they are losing ground to attackers."

CYBER SECURITY SUMMIT

Critical Security Controls – Where did they come from



"offense must inform defense"
"first fix the known bads."

"The strength of the Critical Controls is that they reflect the combined knowledge of actual attacks and effective defenses of experts in the many organizations…"

CYBER SECURITY SUMMIT

Conquer the Top 20 critical security controls.
Build on industry-leading coverage for the "Quick Wins" in the Top 5.

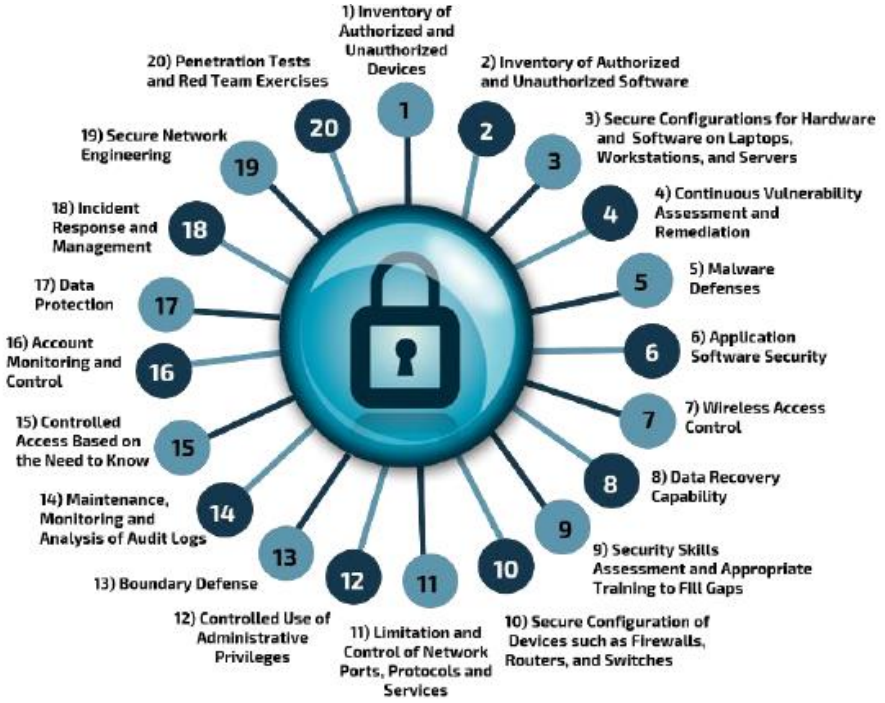
From the "fog of more" to organized cybersecurity strategy

2014

Annual Report

Council on CyberSecurity
Le Conseil de la CyberSécurité

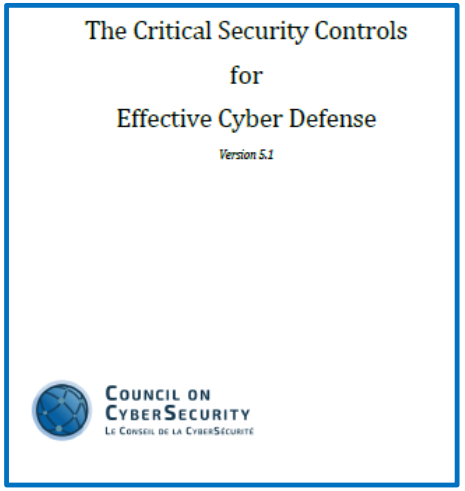
The "Fog of More"



CYBER SECURITY SUMMIT

5 Tenets of an Effective Cyber Defense System

- **Offense Informs Defense** – use knowledge of actual attacks; use only controls known to stop actual attacks
- **Prioritization** – Invest first in controls that provide greatest risk reduction
- **Metrics** – Establish common metrics shared language with for Executives, IT specialists, auditors
- **Continuous Diagnostic and Mitigation** – continuous measurement to validate effectiveness of current security measures
- **Automation** – Automate defenses to achieve reliable, scalable and continuous measurements



CYBER SECURITY SUMMIT

Offense Informs Defense/Prioritization

NSA's Attack Mitigation View Of The 20 Critical Controls

The National Security Agency categorized the 20 Critical Controls both by their attack mitigation impact and by their importance.

Categories of Attack Mitigation

Critical Security Controls

Src: 2013 SANS CSC Poster

Continuous Diagnostic and Mitigation (CDM) – DHS CDM Program

Five actions that can prevent 80% of attacks

Reconnaissance	Get In
Hardware Inventory (CSC 1)	Secure Configuration (CSC 3)
Software Inventory (CSC 2)	Secure Configuration (CSC 10)
Continuous Vuln Access (CSC 4)	Application SW Security (CSC 6)
Networking Engineering (CSC 19)	Wireless (CSC 7)
Penetration Testing (CSC 20)	Malware Defense (CSC 5)
	Limit Ports/P/S (CSC 11)

CENTER FOR INTERNET SECURITY

1. Inventory authorized and unauthorized devices;
2. Inventory authorized and unauthorized software;
3. Develop and manage secure configurations for all devices;
4. Conduct continuous (automated) vulnerability assessment and remediation; and
5. Actively manage and control the use of administrative privileges.

VERY HIGH

These controls address operational conditions that are actively targeted and exploited by all threats.

CYBER SECURITY SUMMIT

Metrics - Mapping to VERIS 2013 Threats

Mapping the Critical Security Controls (CSC) v4.0 to the Verizon VERIS 2013 Threats - Executive Summary

VERIS 2013 Report Threats	Gap Analysis	Matching Controls	Match to Top Seven Human Risks (HR)
Controls that would help mitigate each of the VERIS threats.		CSC 1.1-10, 9.1-6	
1. Tampering (alter physical form or function)	* Threat is partially addressed.	CSC 1.6, 3.13	
2. Backdoor (enable remote access)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14, 13.1-14	
3. Use of stolen authentication credentials	Threat is completely addressed.	CSC 14.1-11, 15.1-5	HR-1/HR-4
4. Export data to another site or system	Threat is completely addressed.	CSC 10.1-7, 13.1-14, 17.1-8	
5. Use of Backdoor or C2 channel	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14, 13.1-14	
6. Phishing (or any type of *ishing)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14, 13.1-14	HR-1 / HR-3
7. Command and control (C2)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14, 13.1-14	
8. Downloader (pull updates or other malware)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14	
9. Brute force or password guessing attacks	Threat is completely addressed.	CSC 14.1-11, 15.1-5	HR-4
10. Spyware, keylogger or form-grabber (capture user input or activity)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14	
11. Capture data stored on system disk	Threat is completely addressed.	CSC 14.1-11, 15.1-5, 17.1-8	
12. System or network utilities (e.g., PsTools, Netcat)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14	
13. Abuse of system access privileges	Threat is completely addressed.	CSC 12.1-14, 14.1-11, 15.1-5, 16.1-12	*Note 1*
14. Ram scraper or memory parser (capture data from volatile memory)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14	
15. Use of unapproved hardware or devices	Threat is completely addressed.	CSC 1.1-12, 17.1-8	*Note 1*
16. SQL injection	Threat is completely addressed.	CSC 6.1-9	*Note 2*

CYBER SECURITY SUMMIT

Automation

TREND MICRO
Securing Your Journey to the Cloud

The Enterprise Fights Back Series (Part III): Building an Incident Response Team

trendmicro.com

tenable network security

Tenable for the 20 Critical Security Controls

Conquer the Top 20 critical security controls.

Build on industry-leading coverage for the "Quick Wins" in the Top 5.

Splunk and the SANS Top 20 Critical Security Controls

beyondtrust

BeyondTrust Solution Mapping to the Critical Security Controls

	BeyondInsight Platform*	Retina CS Enterprise Vulnerability Mgt.	Retina Network Security Scanner	BeyondInsight	PowerBroker for UNIX & Linux	PowerBroker for Windows	PowerBroker Identity Services	PowerBroker Auditor	PowerBroker Password Safe	PowerBroker Endpoint Protection	BTU Training / Services
1: Inventory of Devices	●	●	●	●	○	○	○	○	○	○	○
2: Inventory of Software	●	●	●	○	○	○	○	○	○	○	○
3: Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, & Servers	●	●	●	○	●	●	◒	○	◒	●	○
4: Continuous Vuln. Assessment & Remediation	●	●	●	●	○	◒	○	○	○	●	○
5: Malware Defenses	○	●	○	○	○	○	○	○	○	●	○
6: Application Software Security	◒	◒	○	○	○	○	○	○	○	◒	○
7: Wireless Device Control	○	◒	◒	○	○	○	○	○	○	◒	○
8: Data Recovery Capability	○	○	○	○	○	○	○	○	○	○	○
9: Security Skills Assessment and Appropriate Training to Fill Gaps	○	○	○	○	○	○	○	○	○	○	●
10: Secure Configurations for Network Devices (e.g., Firewalls, Routers, & Switches)	◒	◒	◒	○	◒	○	○	○	◒	○	○
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 Need to Know	●	◒	○	○	●	●	●	●	●	◒	○
16: Account Monitoring and Control	●	●	●	○	●	●	●	●	●	○	○
17: Data Loss Prevention	◒	◒	◒	○	○	◒	○	○	○	◒	○
18: Incident Response and Management	○	○	○	○	○	○	○	○	○	○	○
19: Secure Network Engineering	○	○	○	○	○	○	○	○	○	○	○
20: Penetration Tests & Red Team Exercises	◒	◒	◒	◒	○	○	○	○	○	○	●

LogRhythm
The Security Intelligence Company

Combining Security Intelligence and the Critical Security Controls:
A Review of LogRhythm's SIEM Platform

SANS

CYBER SECURITY SUMMIT

Sub Controls – Accelerate assimilation and Implementation

CSC 3-5	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.	Quick win
CSC 3-6	Negotiate contracts to buy systems configured securely out of the box using standardized images, which should be devised to avoid extraneous software that would increase their attack surface and susceptibility to vulnerabilities.	Visibility/Attribution
CSC 3-7	Do all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.	Configuration/Hygiene
CSC 3-9	Implement and test an automated configuration monitoring system that measures all secure configuration elements that can be measured through remote testing using features such as those included with tools compliant with Security Content Automation Protocol (SCAP), and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects, (where applicable), and new services running on a system.	Advanced

QUICK WIN: Provides Significant risk reduction without major financial, technical or architectural changes

VISIBILITY and ATTRIBUTION: Improves process, arch, tech to monitor and detect threats

CONFIG/HYGIENE: Decrease number and magnitude of security vulnerabilities

ADVANCED: Max security, harder to deploy

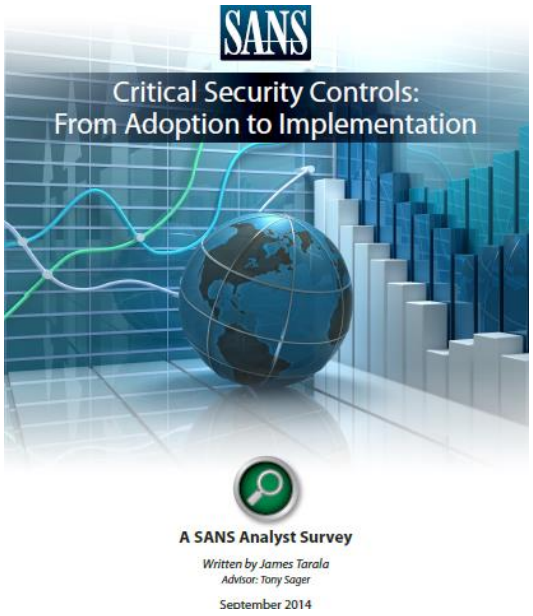
for Effective Cyber Defense

CRITICAL SECURITY CONTROL	DESCRIPTION	MAPPINGS TO THE CRITICAL SECURITY CONTROLS (V5.0A)								
		NIST CORE FRAMEWORK	PCI DSS 3.0	ISO 27002: 2013	DHS CDM PROGRAM	AUSTRALIAN TOP 35	GCHQ 10 STEPS	UK CYBER ESSENTIALS	UK ICO PROTECTING DATA	NIST 800-53 REV4*
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.	ID.AM-1 ID.AM-3 PR.DS-3	2.4	A.8.1.1 A.9.1.2 A.13.1.1	Configuration Settings Management	1 14 17			Inappropriate locations for processing data	CA-7 CM-8 IA-3: SA-4 SC-17 SI-4 PM-5
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.	ID.AM-2 PR.DS-6		A.12.5.1 A.12.6.2	Hardware Asset Management Software Asset Management				Decommissioning of software or services	CA-7 CM-2 CM-8 CM-10 CM-11 SA-4 SC-18 SC-34 SI-4 PM-5
3 Secure Configurations for Hardware and Software	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.	PR.IP-1	2.2 2.3 6.2 11.5	A.14.2.4 A.14.2.8 A.18.2.3	Configuration Settings Management	2-5 21	Secure Configuration	Secure Configuration Patch Management	Inappropriate locations for processing data	CA-7 CM-2 CM-3 CM-5 CM-6 CM-7 CM-8 CM-9 MA-4 MA-5 SA-4 SC-34 SI-2 SI-4
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.	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.MI-3	6.1 6.2 11.2	A.12.6.1 A.14.2.8	Vulnerability Management	2-3		Patch Management	Software Updates	CA-2 CA-7 RA-5 SC-34 SI-4 SI-7
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.	PR.PT-2 DE.CM-4 DE.CM-5	5.1 - 5.4	A.8.3.1 A.12.2.1 A.13.2.3		7 26 17 30 22	Removable Media Controls Malware Protection	Malware Protection		CA-7 SC-39 SC-44 SI-3 SI-4 SI-8
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.	PR.DS-7	6.3 6.5 - 6.7	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6 - A.14.2.8	Vulnerability Management	24			SQL Injection	SA-13 SA-15 SA-16 SA-17 SA-20 SA-21 SC-39 SI-10 SI-11 SI-15 SI-16
7 Wireless Access 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.		4.3 11.1	A.10.1.1 A.12.4.1 A.12.7.1			Monitoring Network Security			AC-18 AC-19 CA-3 CA-7 CM-2 IA-3 SC-8 SC-17 SC-40 SI-4
8 Data Recovery Capability	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.	PR.IP-4	4.3 9.5 - 9.7	A.10.1.1 A.12.3.1						CP-9 CP-10 MP-4
9 Security Skills Assessment and 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.	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	12.6	A.7.2.2	Security-Related Behavior Management	28	User Education & Awareness			AT-1 AT-2 AT-3 AT-4 SA-11 SA-16 PM-13 PM-14 PM-16
10 Secure Configurations for Network Devices	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.	PR.AC-5 PR.IP-1 PR.PT-4	1.1 - 1.2 2.2 6.2	A.9.1.2 A.13.1.1 A.13.1.3	Configuration Settings Management Boundary Protection	2 3 10	Secure Configuration Network Security	Boundary firewalls and internet gateways Secure Configuration Patch Management	Software Updates Inappropriate locations for processing data	AC-4 CA-3 CM-2 CM-3 CM-5 CM-6 CM-8 PM-4 SC-24 SI-4
11 Limitation and Control of Network Ports	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.	PR.AC-5 DE.AE-1	1.4	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	Boundary Protection	2 13 3 27 12	Network Security		Decommissioning of software or services Unnecessary Services	AC-4 CA-7 CA-9 CM-2 CM-6 CM-8 SC-20 SC-21 SC-22 SC-41 SI-4

Src: SANS CSC Fall 2014 Poster

CYBER SECURITY SUMMIT

3 Major Reasons for adopting CSCs



- Implementing the CSCs is the **fastest and most cost effective way** to focus security staffs and budgets on the high payback areas TO achieve **cyber risk reduction**
- They facilitate cooperation between IT security and audit staffs - **broad consensus on the security processes and tools** that are absolutely necessary to prevent or mitigate actual cyber threats.
- Provide the **focus and clarity needed to gain top management support** and budget approval.

CYBER SECURITY SUMMIT

CSC Adoption

BANK INFO SECURITY®

Defense Strategies for Advanced Threats: Breaking the Cyber Kill Chain with SANS 20 Critical Security Controls

Presented by Solutionary 60 minutes 0 Comments

Twitter Facebook LinkedIn Credit Eligible

- **Fastest and most cost effective way** to achieve cyber risk reduction

tripwire

Using the Top 20 Critical Security Controls to Get your CFO's Attention

CINDY VALLADARES

OCT 16, 2013 | IT SECURITY AND DATA PROTECTION

- Provide the **focus and clarity** needed to gain top management support and budget approval.

CYBER SECURITY SUMMIT

Barriers to implement Controls

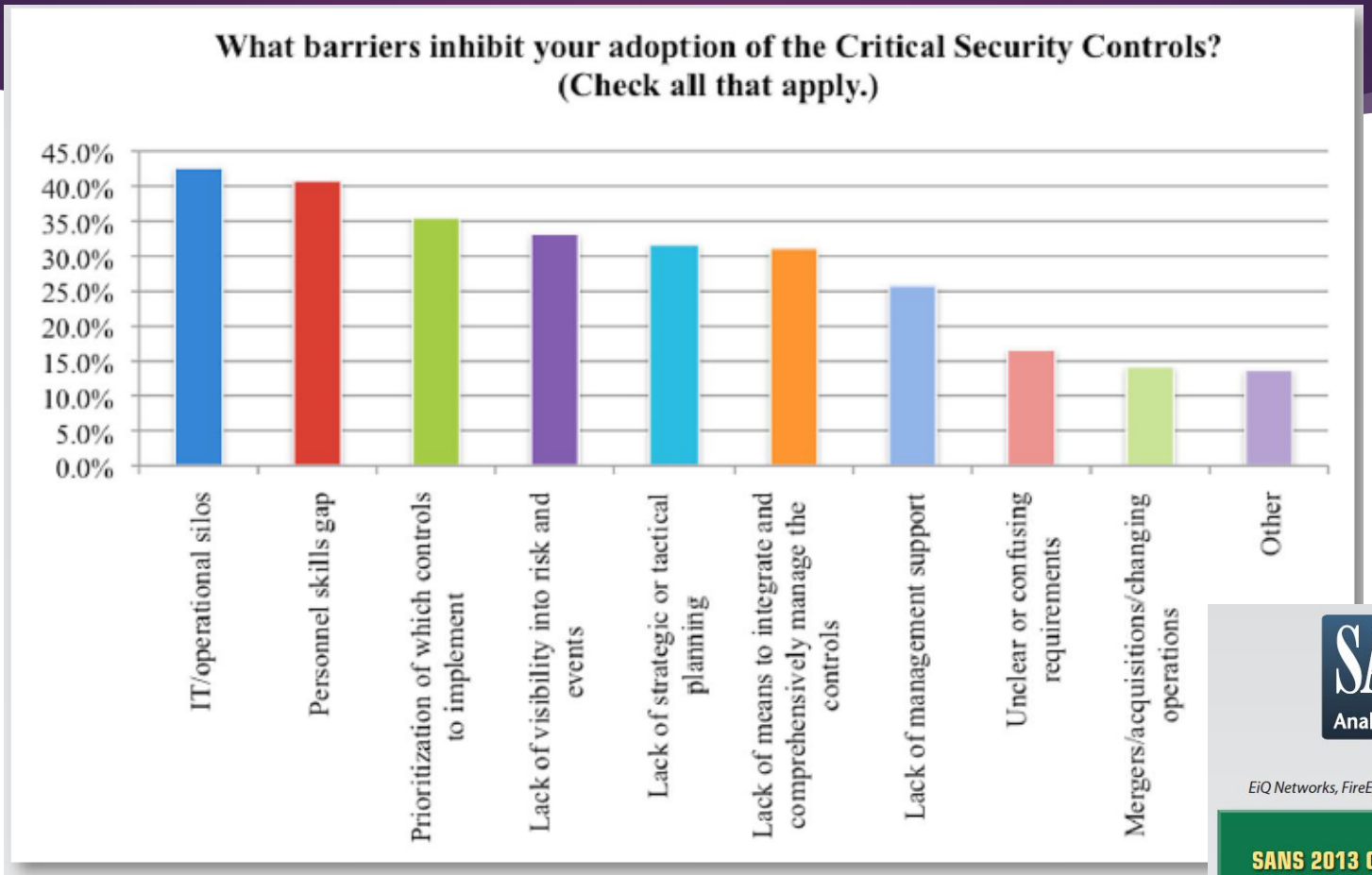
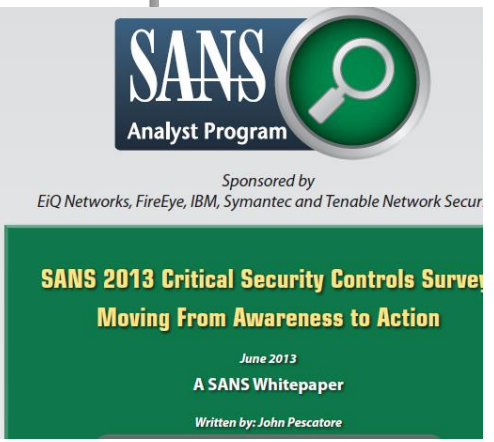
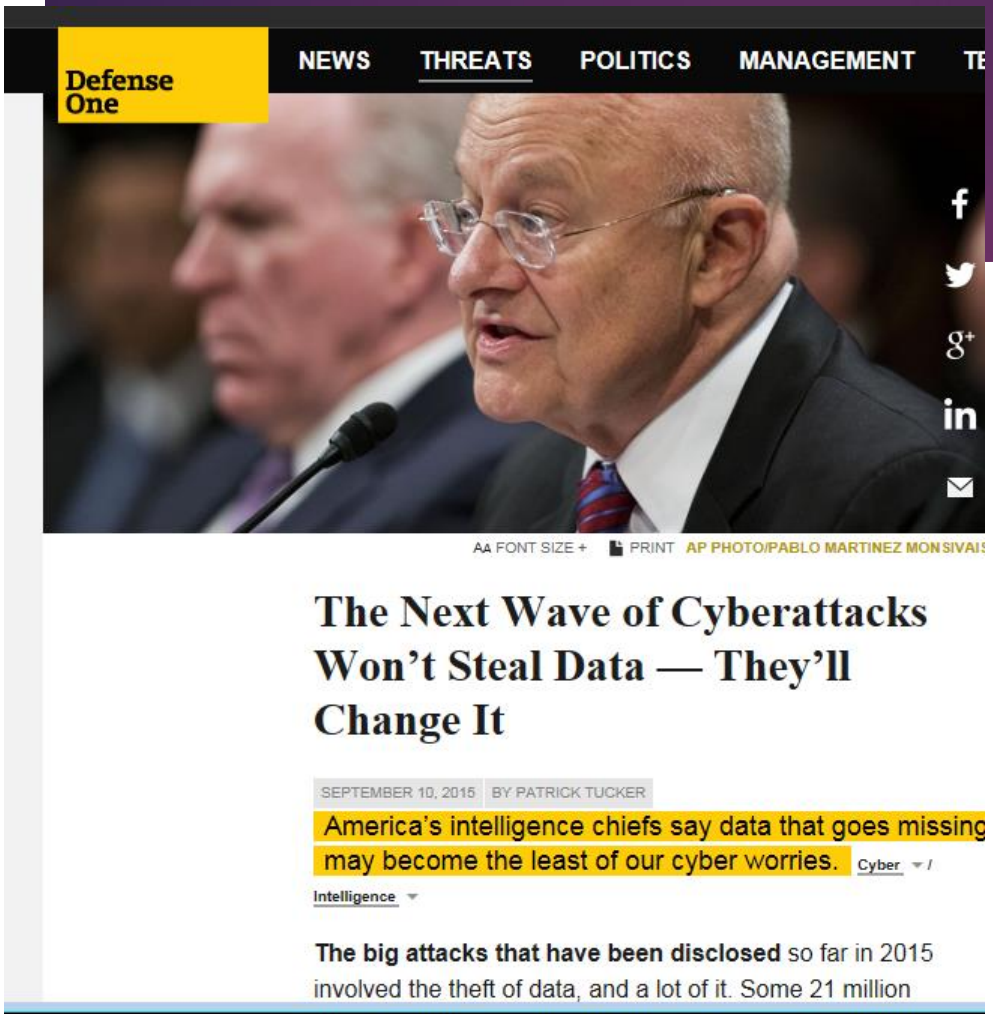


Figure 7. Barriers to Adopting the Critical Security Controls



CYBER SECURI
SUMMIT



- Date: September 10, 2015
- America's top spies concerned with direct manipulation of data
- Future attacks to compromise integrity of data changing perceptions of what is real and what is not.
- "Decision making by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving."

CYBER SECURITY SUMMIT

Distinct Advantage – Regulatory Protection

3:06 pm ET
Aug 31, 2015 GUEST VOICES

What CIOs Need to Know About the FTC Cybersecurity Ruling

ARTICLE COMMENTS (7)

CYBERSECURITY FEDERAL TRADE COMMISSION

Email Print

By RICHARD RAYSMAN AND FRANCESCA MORRIS

- Date Aug 31, 2015
- Decision by Third Court of Appeals in the event of such an Information Technology System hack, the U.S. Federal Trade Commission has authority to investigate the company and charge it with unfair trade practices for failure to protect customers from the theft of on-line data
- Authors explained CIOs should act defensively to mitigate the company's exposure
  - Compliance with NIST Cyber Security Framework – becoming a de facto standard of cybersecurity for US regulators
  - **Critical Security Controls – proactively align with NIST Core Framework**

CYBER SECURITY SUMMIT

Data breach class action litigation


REUTERS EDITION: U.S. Search Reuters

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS MONEY LIFE PICTURES VIDEO

Alison Frankel

The 7th Circuit just made it a lot easier to sue over data breaches

By Alison Frankel | July 21, 2015

Tags: DATA | HACKING | TARGET

- Date: July 21, 2015
- 7th Circuit Court of Appeals last week reinstated a lawsuit against Neiman Marcus over a 2013 data breach in which hackers stole credit card information from as many as 350,000 customers.

CYBER SECURITY SUMMIT

Cyber Insurance

3:06 pm ET
Aug 31, 2015 GUEST VOICES

What CIOs Need to Know About the FTC Cybersecurity Ruling

ARTICLE COMMENTS (7)

CYBERSECURITY FEDERAL TRADE COMMISSION

Email Print

By RICHARD RAYSMAN AND FRANCESCA MORRIS

- Useful checklist for CIOs to bolster defenses
- CIOs should review the company's cybersecurity policy to ensure that it provides the necessary coverage in the event of a hack

CYBER SECURITY SUMMIT

Cyber Insurance Premiums Increasing Significantly

REUTERS EDITION: U.S.

INSIGHT-Cyber insurance premiums rocket after high-profile attacks

BOSTON | BY JIM FINKLE

- Date: Oct 2015
- Prompted Increase in cyber premiums for some companies
- Insurers are increasing deductibles and limiting Coverage

infosecurity STRATEGY | INSIGHT | TECHNOLOGY

13 OCT 2015 NEWS

Cyber-Insurance Premiums Rocket

Tara Seals US/North America News Reporter, Infosecurity Magazine

- Date: Oct 2015
- From Recent attacks, insurers have data to assess risk
- Financial risk to a company goes beyond initial clean up and identity
- Increase in lawsuits filed against breached companies increase financial impact

CYBER SECURITY SUMMIT

Distinct Advantage – Reduce Cyber Premiums

- March 2015
- Volatile Cyber Premiums 2014
- Renewal Rate Increase for some clients
- Expansion in Regulation and Litigation
- Heightened due diligence from underwriters on company's information security policies
  - Encryption
  - EMV (credit card technology)
  - Formal Incident Response Plans to protect data

THOMAS REAGAN
Cyber Practice Leader
ROBERT PARISI
Cyber Product Leader

CYBER SECURITY SUMMIT

Distinct Advantage - Cyber Insurance Premiums

- Date: Oct 2015
- **Reduce your premiums; implement best-practice information security procedures**
- International standard ISO 27001 sets out the requirements of a best-practice information security management system (ISMS)
- **CSC aligns to ISO 27002**
- ISO 27001 describes Information Security Mgmt System, 27002 has the details on control implementation

CYBER SECURITY SUMMIT

Looking at the SANS 20 Critical Security Controls

SANS 20 Critical Security Controls	NIST SP 800-53 (control numbers)	ISO 27002 (control heading numbers)
Control 5: Boundary Defense	AC-17	10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2
	AC-20	7.1.3, 8.1.1, 8.1.3, 10.6.1, 10.8.1, 11.4.1, 11.4.2
	CA-3	6.2.1, 6.2.3, 10.6.1, 10.8.1, 10.8.2, 10.8.5, 11.4.2
	IA-2	11.3.2, 11.5.1, 11.5.2, 11.5.3
	IA-8	10.9.1, 11.4.2, 11.5.1, 11.5.2
	RA-5	12.6.1, 15.2.2
	SC-7	6.2.1, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 10.10.2, 11.4.5, 11.4.6
	SC-18	10.4.2
	SI-4	10.10.2, 13.1.1, 13.1.2
	PM-7	None
Control 6: Maintenance, Monitoring & Analysis of Security Audit Logs	AC-17	10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2
	AC-19	10.4.1, 11.1.1, 11.4.3, 11.7.1
	AU-2	10.10.1, 10.10.4, 10.10.5, 15.3.1
	AU-3	10.10.1
	AU-4	10.10.1, 10.3.1
	AU-5	10.3.1, 10.10.1
	AU-6	10.10.2, 10.10.5, 13.1.1, 15.1.5
	AU-8	10.10.1, 10.10.6
	AU-9	10.10.3, 13.2.3, 15.1.3, 15.3.2
	AU-12	10.10.1, 10.10.4, 10.10.5
	SI-4	10.10.2, 13.1.1, 13.1.2
Control 7: Application Software Security	CM-7	None
	RA-5	12.6.1, 15.2.2
	SA-3	12.1.1
	SA-4	12.1.1, 12.5.5
	SA-8	10.4.1, 10.4.2, 11.4.5, 12.5.5
	SI-3	10.4.1
	SI-10	12.2.1, 12.2.2
Control 8: Controlled Use of Administrative Privileges	AC-6	6.1.3, 8.1.1, 11.1.1, 11.2.2, 11.4.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.3
	AC-17	10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2
	AC-19	10.4.1, 11.1.1, 11.4.3, 11.7.1
	AU-2	10.10.1, 10.10.4, 10.10.5, 15.3.1

SystemEXPERTS
LEADERSHIP IN SECURITY & COMPLIANCE

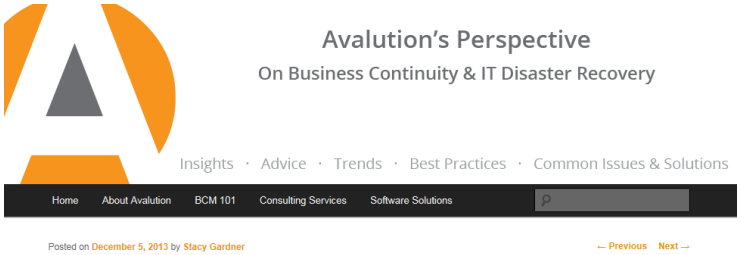
www.systemexperts.com
1.888.749.9000
info@systemexperts.com

Looking at the SANS 20 Critical Security Controls

Mapping the SANS 20 to NIST 800-53 to ISO 27002
by Brad C. Johnson

Distinct Advantages - Business

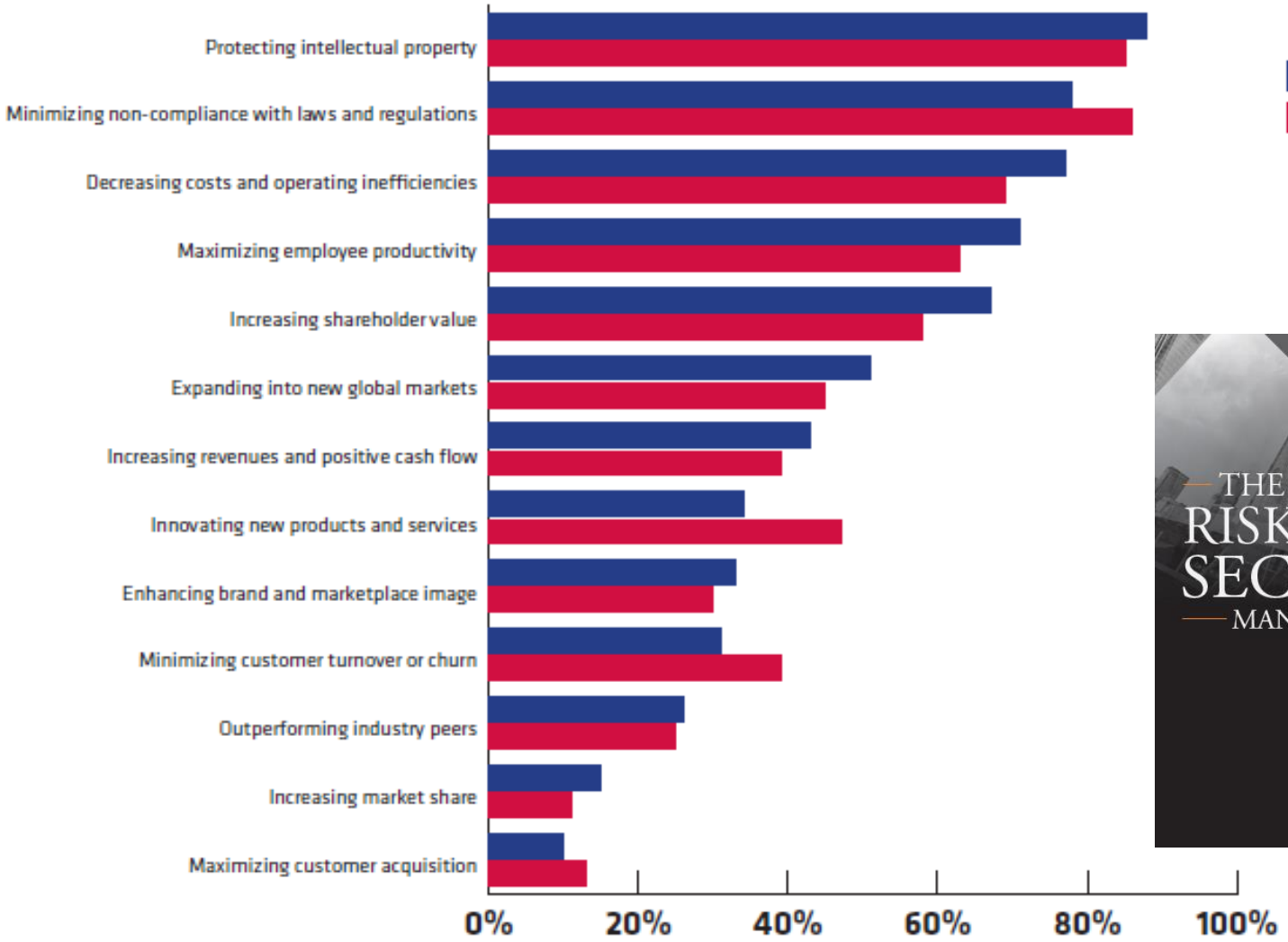
- Control IT Business Management (Cost saving measures)
  - Asset control & accountability – licensing and end of life replacement
  - Software metering – licensing
  - Prioritizing Data for Security will drive prioritization of Data Backups and Disaster Recovery

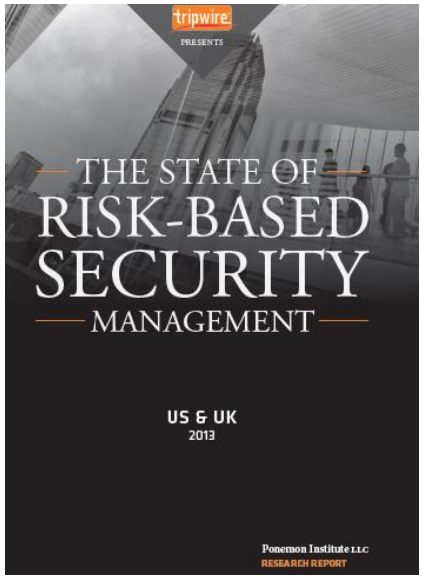


Integrating Cyber Security and Business Continuity

CYBER SECURITY SUMMIT

FIGURE 2-2. Critical business objectives met by risk-based security management





CYBER SECURITY SUMMIT

Where To Find ALL the Answers

COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

Center for Internet Security®

SANS

CIS CRITICAL SECURITY CONTROLS

Critical Security Controls

Critical Security Controls for Effective Cyber Defense

SANS WHAT WORKS In Internet Security

CYBER SECURITY SUMMIT

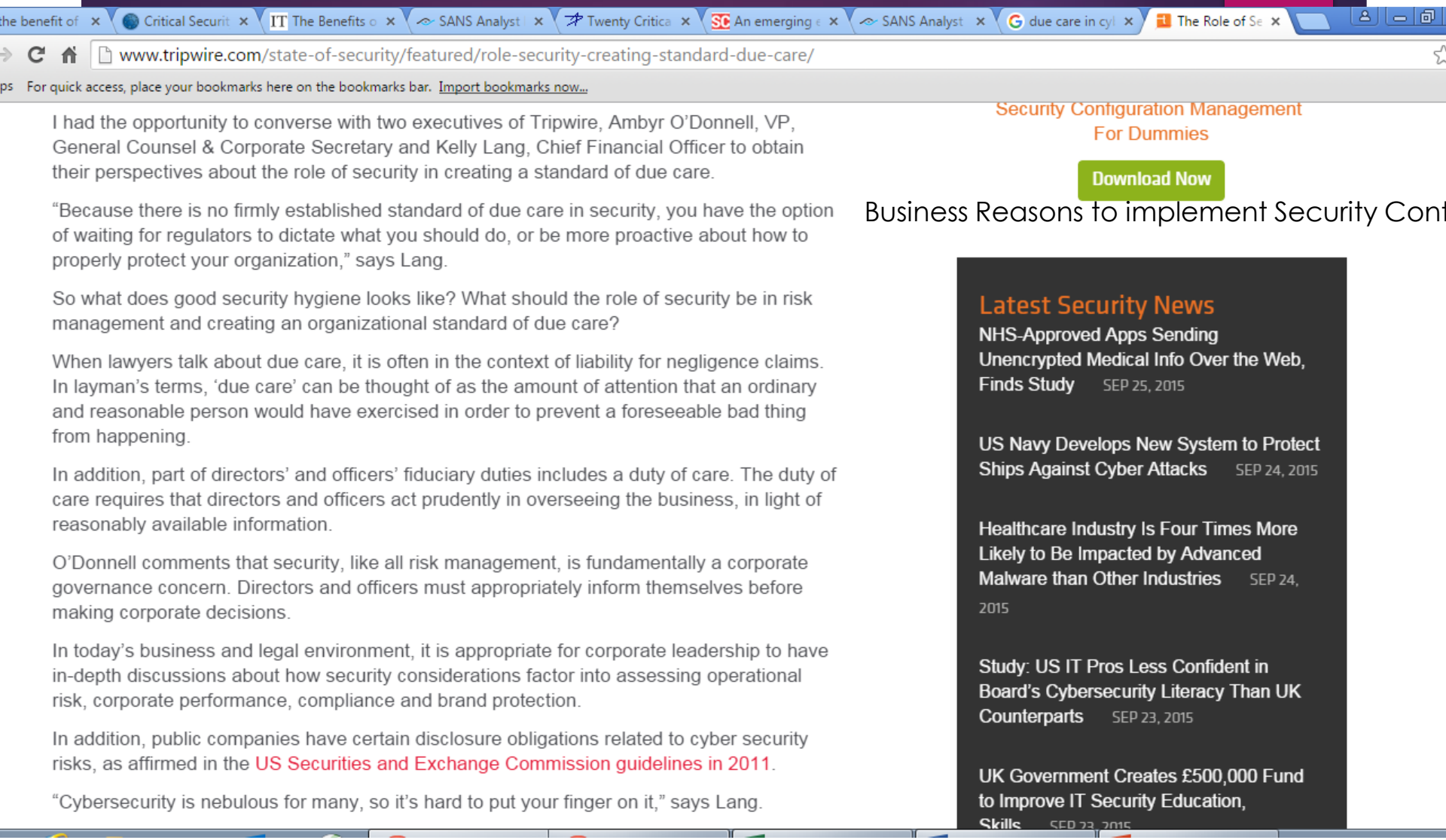
The Controls… are working

This Country may be turning the corner on cybersecurity! The National Governors Association, the Atlantic Council, Zurich Insurance, the Center for Internet Security, the MS-ISAC, and other major nationwide institutions are all calling for basic cybersecurity hygiene, specifically using the Critical Security Controls. And 14 of the 20 leading security vendors have aligned part or all of their product offerings with the Critical Security Controls. Clearly we are witnessing the beginning of a movement.

The Honorable Jane Holl Lute,

recently Deputy Secretary of the U.S. Department of Homeland Security and Chair of the Council on CyberSecurity.1

CYBER SECURITY SUMMIT



CYBER SECURITY SUMMIT

Protect your Brand

Contrary to common belief, there is such a thing as bad PR. Both interviewees agree that keeping your brand untarnished is a top priority when setting security goals. Companies in all industries want to do business with trusted partners. A company's value cannot be optimized unless the market views the company as secure and trustworthy.

Foster a Culture of Security

Risk appetite differs from organization to organization. Having both the appropriate tone from the top and consistently conveying that tone through the ranks creates a more security-aware culture.

As Lang comments: "If my boss cares about security, I better start focusing on it as well." It is important not only to understand the threats and vulnerabilities to the corporate environment, but also the costs required to mitigate those potential risks.

Know your Crown Jewels: What and Where

A few months ago I interviewed security executives to ask for tips to improve information security risk management practice. There was a consensus that assessing the importance of your assets was key, as Eric Cowperthwaite, former CISO commented, "If I don't know what it is that I need to protect on behalf of my organization, I can't possibly be successful in going beyond foundational due diligence security.:

However, as Erin Jacobs, former CSO for UCB commented, "What's important to the Board is not necessarily what's important to the business units. And what's important to the business units might be different to what's important to security teams."

Lang and O'Donnell agreed that identifying key assets and critical infrastructure is fundamental to any security program.

Create/Update your Incident Response Plans

POPULAR FEATURED RECENT


The Top 10 Tips for Building an Effective Security Dashboard
SEPTEMBER 23, 2015


'Ghost Push' Malware Infects 600K Android Users Daily, Say Security Researchers
SEPTEMBER 22, 2015


Hackers Have Stolen Almost Six Million US Government Fingerprints
SEPTEMBER 24, 2015


It's 2AM – Do You Know Who Your Smartphone is Talking to?
SEPTEMBER 23, 2015


Seven Years of Cyber

This Country may be turning the corner on cybersecurity! The National Governors Association, the Atlantic Council, Zurich Insurance, the Center for Internet Security, the MS-ISAC, and other major nationwide institutions are all calling for basic cybersecurity hygiene, specifically using the Critical Security Controls. And 14 of the 20 leading security vendors have aligned part or all of their product offerings with the Critical Security Controls. Clearly we are witnessing the beginning of a movement.

The Honorable Jane Holl Lute,
recently Deputy Secretary of the U.S. Department of Homeland Security and Chair of the Council on CyberSecurity.[1]