

# 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



# The Good...



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

ASPEN  
SECURITY  
FORUM

HOME ABOUT AGENDA SPEAKERS & MODERATORS ATTEND MULTIMEDIA

Media

MULTIMEDIA LIVE VIDEOS PHOTOS TRANSCRIPTS

[RETURN TO NEWS >>](#)

## MICHAEL CHERTOFF: PRACTICE SAFE CYBER HYGIENE

1101101001011010110101010101010101111010101101010101010101101  
1101101001011010110101010101010101111010101101010101010101101  
1101101001011010110101010101010101111010101101010101010101101  
1101101001011010110101010101010101111010101101010101010101101  
1101101001011010110101010101010101111010101101010101010101101  
1101101001011010110101010101010101111010101101010101010101101  
1101101001011010110101010101010101111010101101010101010101101

INFOSEC  
INSTITUTE

TOPICS ▾ CONTRIBUTORS CONTENT ARCHIVES ▾ JOB BOARD



CYBER SECURITY  
SUMMIT

# The Bad – Framework Fallacy

SANS

Critical Security Controls:  
From Adoption to Implementation

## A SANS Analyst Survey

Written by James Tarala  
Advisor: Tony Sager

September 2014

“...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.”

KPMG

cutting through complexity

ADVISORY

The five most  
common cyber  
security mistakes

Management's  
perspective on cyber  
security



John Hermans  
KPMG Cyber Security Lead Partner

Gerben Schreurs  
Partner KPMG Forensic

4

Mistake: “Cyber security compliance is all about effective monitoring”

Reality: The ability to learn is just as important as the ability to monitor

“...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.”

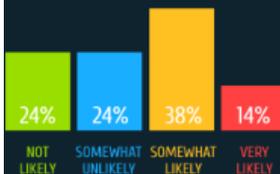
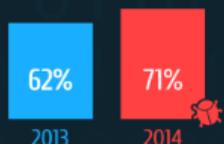


CYBER SECURITY  
SUMMIT

# The Ugly...

## RISING CYBERATTACKS

71% of respondents' networks were breached in 2014, up from 62% the prior year.



## SINKING EXPECTATIONS

More than half (52%) of respondents believe a successful cyberattack is likely in 2015, up from 39% the prior year.

## CYBERSECURITY CONFIDENCE DOWN AS CYBERATTACKS RISE



# 2015 CYBERTHREAT DEFENSE REPORT<sup>SM</sup>

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.

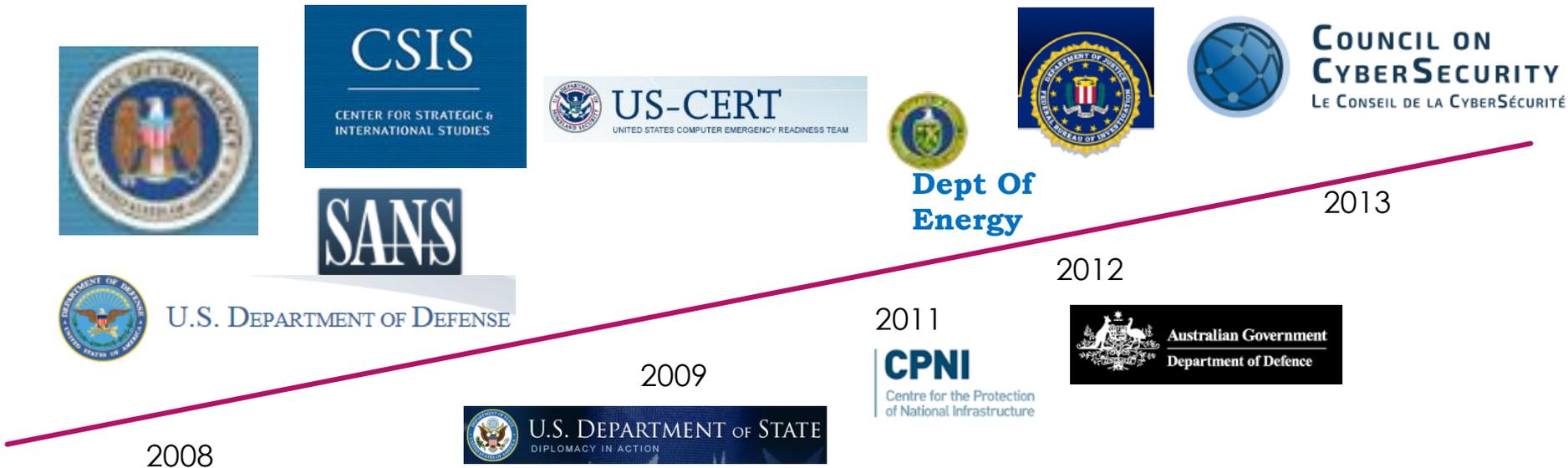
May 2014 | by Tucker Bailey, Andrea Del Miglio, and Wolf Richter

“...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..."



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

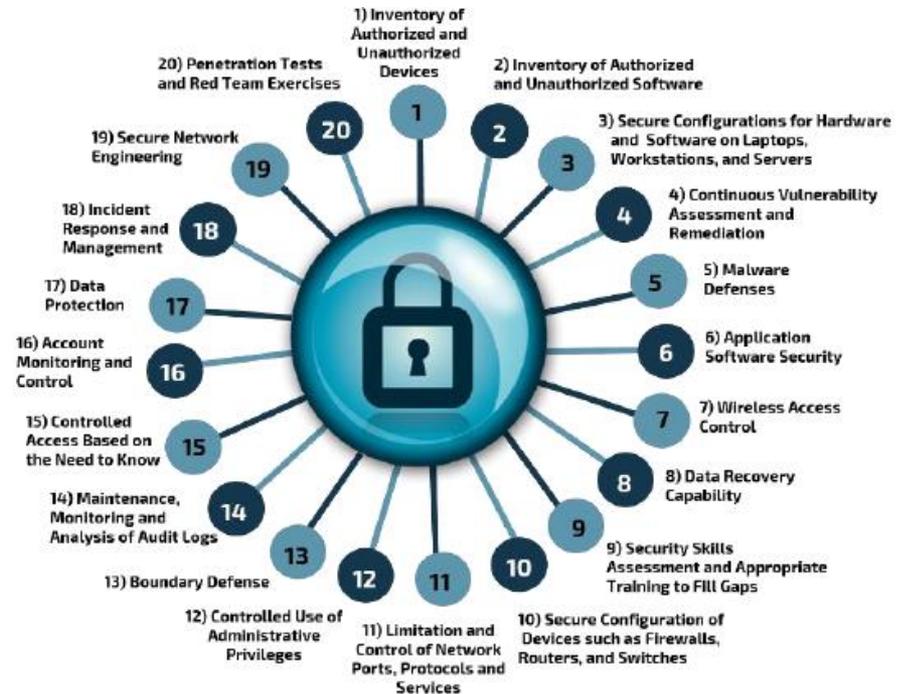
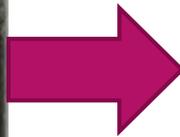
Annual Report



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

The Critical Security Controls  
for  
Effective Cyber Defense  
Version 5.1



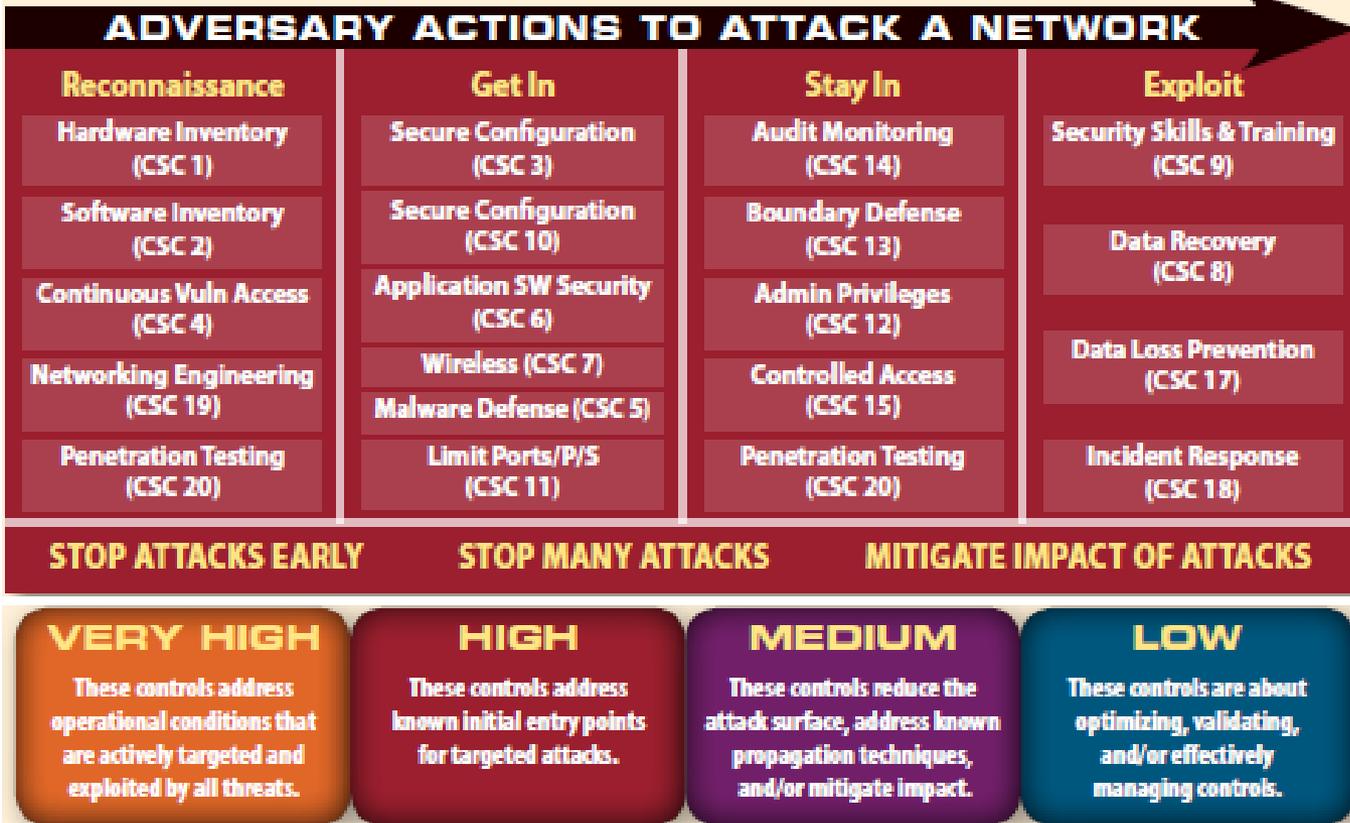
CYBER SECURITY  
SUMMIT

# 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



# 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 Assess (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.			
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



# Automation



**TREND MICRO**  
Securing Your Journey to the Cloud

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

trendmicro.com



## 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.

**THE CRITICAL SECURITY CONTROLS SOLUTION PROVIDERS**

Map of vendors to controls including: Acronis, LogRhythm, Qualys, Symantec, etc.

## Splunk and the SANS Top 20 Critical Security Controls

BeyondTrust Solution Mapping to the Critical Security Controls

	BeyondTrust Platform Vulnerability Mgmt.	BeyondTrust Network Security Scanner	BeyondTrust Patch Manager	BeyondTrust for Windows	BeyondTrust Identity Mgmt.	BeyondTrust Auditor	BeyondTrust Password Safe	BeyondTrust Endpoint Protection	BeyondTrust 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	○	○	○	○	○	○	○	○	○



### CRITICAL CONTROL PROTECTION PRIORITIES

	HARDEN DEFENSES			ENHANCE DETECTION			REDUCE IMPACT					
Data Breaches	02	03	04	05	01	14	16	09	08	12	17	13
Targeted Attacks	02	03	04	05	06	11		20	12	17	13	15
Web-Based Attacks	02	03	04	05	06				01	14	16	
Safeguarding Web Servers	02	03	04	05	06	10	11		01	14	16	18
Mobile Threats	02	03	04	05	06	07			01			08
Malware Threats	02	03	04	05	06				01	14	16	09
Spam + Phishing	02	05			01	09	20		12	13		
Bots	02	03	04	05	06				01	14	18	



The Security Intelligence Company

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



CYBER SECURITY SUMMIT

# Sub Controls – Accelerate assimilation and Implementation

<p>CSC 3-5</p>	<p>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.</p>	<p>Quick win</p>	<p><b>QUICK WIN:</b> Provides Significant risk reduction without major financial, technical or architectural changes</p>
<p>CSC 3-6</p>	<p>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.</p>	<p>Visibility/Attribution</p>	<p><b>VISIBILITY and ATTRIBUTION:</b> Improves process, arch, tech to monitor and detect threats</p>
<p>CSC 3-7</p>	<p>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.</p>	<p>Configuration/Hygiene</p>	<p><b>CONFIG/HYGIENE:</b> Decrease number and magnitude of security vulnerabilities</p>
<p>CSC 3-9</p>	<p>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.</p>	<p>Advanced</p>	<p><b>ADVANCED:</b> Max security, harder to deploy</p>

# for Effective Cyber Defense

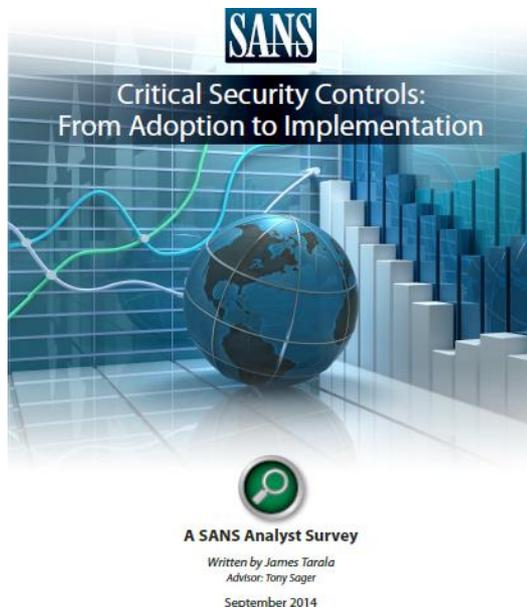
CRITICAL SECURITY CONTROL	DESCRIPTION	MAPPINGS TO THE CRITICAL SECURITY CONTROLS (V5.0A)									
		NIST CORE FRAMEWORK	PCI DSS 3.0	ISO 27002: 2013	DHS CDM PROGRAM	ASTIANUM TOP 35	GCHQ 10 STEPS	UK CYBER ESSENTIALS	UK ICO PROTECTING DATA	NIST 800-53 REV4*	
<b>1</b> Inventory of Authorized and Unauthorized 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 CA-8 IA-3: SA-4	SC-17 SI-4 PM-5
<b>2</b> 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 CA-8 SA-4 SC-18	CA-10 CA-11 SI-4 PM-5	SC-34
<b>3</b> 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 CA-8 CA-9 CA-10 CA-11 CA-12 CA-13 CA-14 CA-15 CA-16 CA-17 CA-18 CA-19 CA-20 CA-21 CA-22 CA-23 CA-24 CA-25 CA-26 CA-27 CA-28 CA-29 CA-30 CA-31 CA-32 CA-33 CA-34 CA-35 CA-36 CA-37 CA-38 CA-39 CA-40 CA-41 CA-42 CA-43 CA-44 CA-45 CA-46 CA-47 CA-48 CA-49 CA-50 CA-51 CA-52 CA-53 CA-54 CA-55 CA-56 CA-57 CA-58 CA-59 CA-60 CA-61 CA-62 CA-63 CA-64 CA-65 CA-66 CA-67 CA-68 CA-69 CA-70 CA-71 CA-72 CA-73 CA-74 CA-75 CA-76 CA-77 CA-78 CA-79 CA-80 CA-81 CA-82 CA-83 CA-84 CA-85 CA-86 CA-87 CA-88 CA-89 CA-90 CA-91 CA-92 CA-93 CA-94 CA-95 CA-96 CA-97 CA-98 CA-99 CA-100	SC-14 SC-15 SC-16 SC-17 SC-18 SC-19 SC-20 SC-21 SC-22 SC-23 SC-24 SC-25 SC-26 SC-27 SC-28 SC-29 SC-30 SC-31 SC-32 SC-33 SC-34 SC-35 SC-36 SC-37 SC-38 SC-39 SC-40 SC-41 SC-42 SC-43 SC-44 SC-45 SC-46 SC-47 SC-48 SC-49 SC-50 SC-51 SC-52 SC-53 SC-54 SC-55 SC-56 SC-57 SC-58 SC-59 SC-60 SC-61 SC-62 SC-63 SC-64 SC-65 SC-66 SC-67 SC-68 SC-69 SC-70 SC-71 SC-72 SC-73 SC-74 SC-75 SC-76 SC-77 SC-78 SC-79 SC-80 SC-81 SC-82 SC-83 SC-84 SC-85 SC-86 SC-87 SC-88 SC-89 SC-90 SC-91 SC-92 SC-93 SC-94 SC-95 SC-96 SC-97 SC-98 SC-99 SC-100
<b>4</b> 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
<b>5</b> 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 17 22	Removable Media Controls Malware Protection	Malware Protection		CA-7 SC-39 SC-44	SI-3 SI-4 SI-8
<b>6</b> 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.A5 A.12.1.4 A.14.2.1 A.14.2.8 - A.14.2.8	Vulnerability Management	24		SQL Injection	SA-13 SA-15 SA-16 SA-17	SA-20 SA-21 SA-22 SA-23 SA-24 SA-25 SA-26 SA-27 SA-28 SA-29 SA-30 SA-31 SA-32 SA-33 SA-34 SA-35 SA-36 SA-37 SA-38 SA-39 SA-40 SA-41 SA-42 SA-43 SA-44 SA-45 SA-46 SA-47 SA-48 SA-49 SA-50 SA-51 SA-52 SA-53 SA-54 SA-55 SA-56 SA-57 SA-58 SA-59 SA-60 SA-61 SA-62 SA-63 SA-64 SA-65 SA-66 SA-67 SA-68 SA-69 SA-70 SA-71 SA-72 SA-73 SA-74 SA-75 SA-76 SA-77 SA-78 SA-79 SA-80 SA-81 SA-82 SA-83 SA-84 SA-85 SA-86 SA-87 SA-88 SA-89 SA-90 SA-91 SA-92 SA-93 SA-94 SA-95 SA-96 SA-97 SA-98 SA-99 SA-100	
<b>7</b> Wireless Access Control	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), 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 CA-2 IA-3 SC-8	SC-17 SC-40 SI-4
<b>8</b> 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 HP-4	
<b>9</b> 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 SI-11 SI-16 PM-13 PM-14 PM-15
<b>10</b> 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 CA-7 CA-9	CA-2 CA-3 CA-5 CA-6 CA-8 CA-9 CA-10 CA-11 CA-12 CA-13 CA-14 CA-15 CA-16 CA-17 CA-18 CA-19 CA-20 CA-21 CA-22 CA-23 CA-24 CA-25 CA-26 CA-27 CA-28 CA-29 CA-30 CA-31 CA-32 CA-33 CA-34 CA-35 CA-36 CA-37 CA-38 CA-39 CA-40 CA-41 CA-42 CA-43 CA-44 CA-45 CA-46 CA-47 CA-48 CA-49 CA-50 CA-51 CA-52 CA-53 CA-54 CA-55 CA-56 CA-57 CA-58 CA-59 CA-60 CA-61 CA-62 CA-63 CA-64 CA-65 CA-66 CA-67 CA-68 CA-69 CA-70 CA-71 CA-72 CA-73 CA-74 CA-75 CA-76 CA-77 CA-78 CA-79 CA-80 CA-81 CA-82 CA-83 CA-84 CA-85 CA-86 CA-87 CA-88 CA-89 CA-90 CA-91 CA-92 CA-93 CA-94 CA-95 CA-96 CA-97 CA-98 CA-99 CA-100
<b>11</b> 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 3 12	Network Security		Decommissioning of software or services Unnecessary Services	AC-4 CA-7 CA-9 CA-2	CA-2 CA-3 CA-5 CA-6 CA-8 CA-9 CA-10 CA-11 CA-12 CA-13 CA-14 CA-15 CA-16 CA-17 CA-18 CA-19 CA-20 CA-21 CA-22 CA-23 CA-24 CA-25 CA-26 CA-27 CA-28 CA-29 CA-30 CA-31 CA-32 CA-33 CA-34 CA-35 CA-36 CA-37 CA-38 CA-39 CA-40 CA-41 CA-42 CA-43 CA-44 CA-45 CA-46 CA-47 CA-48 CA-49 CA-50 CA-51 CA-52 CA-53 CA-54 CA-55 CA-56 CA-57 CA-58 CA-59 CA-60 CA-61 CA-62 CA-63 CA-64 CA-65 CA-66 CA-67 CA-68 CA-69 CA-70 CA-71 CA-72 CA-73 CA-74 CA-75 CA-76 CA-77 CA-78 CA-79 CA-80 CA-81 CA-82 CA-83 CA-84 CA-85 CA-86 CA-87 CA-88 CA-89 CA-90 CA-91 CA-92 CA-93 CA-94 CA-95 CA-96 CA-97 CA-98 CA-99 CA-100

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.

# CSC Adoption



## 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



## 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

What barriers inhibit your adoption of the Critical Security Controls?  
(Check all that apply.)

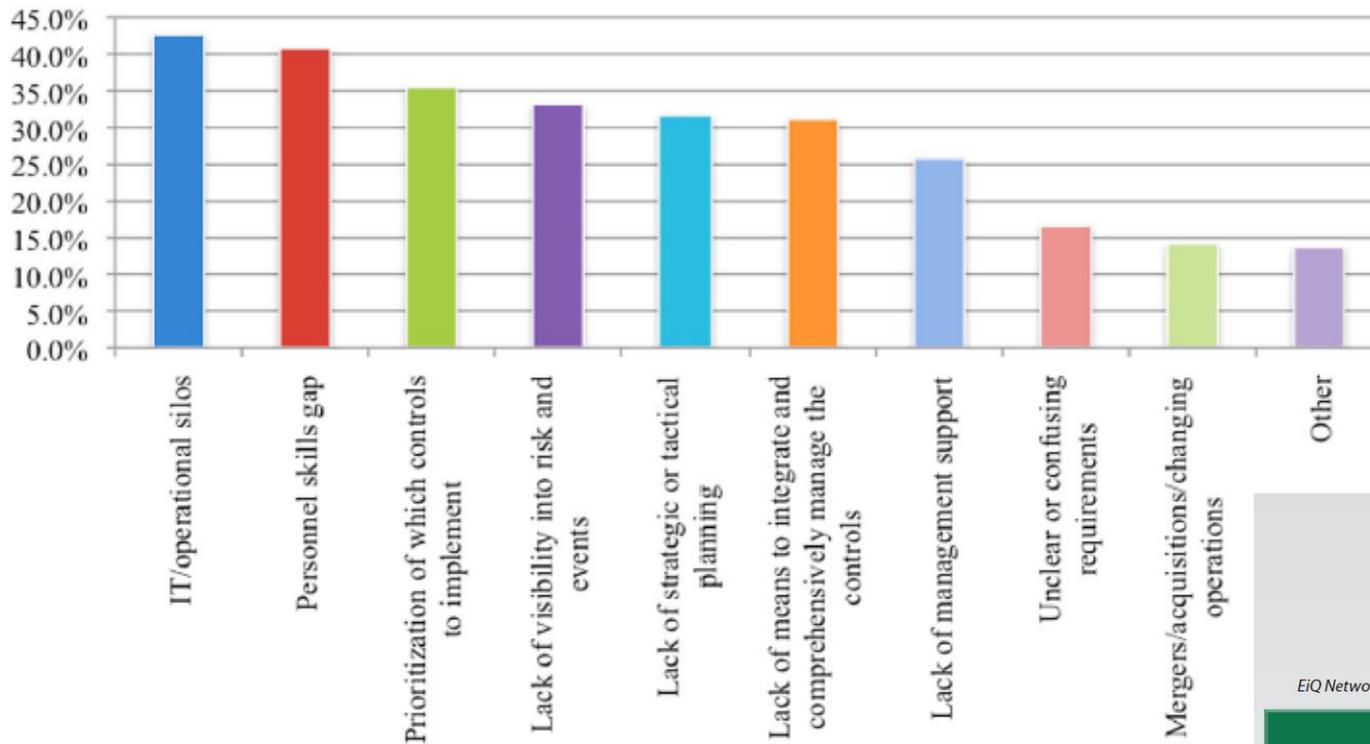


Figure 7. Barriers to Adopting the Critical Security Controls



Sponsored by  
EiQ Networks, FireEye, IBM, Symantec and Tenable Network Security

**SANS 2013 Critical Security Controls Survey**  
**Moving From Awareness to Action**

June 2013

A SANS Whitepaper

Written by: John Pescatore



**CYBER SECURITY  
SUMMIT**



AA FONT SIZE + PRINT AP PHOTO/PABLO MARTINEZ MONSIVAI

## The Next Wave of Cyberattacks Won't Steal Data — They'll Change It

SEPTEMBER 10, 2015 BY PATRICK TUCKER

America's intelligence chiefs say data that goes missing may become the least of our cyber worries. [Cyber](#)

[Intelligence](#)

The big attacks that have been disclosed so far in 2015 involved the theft of data, and a lot of it. Some 21 million

▶ 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."



# 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

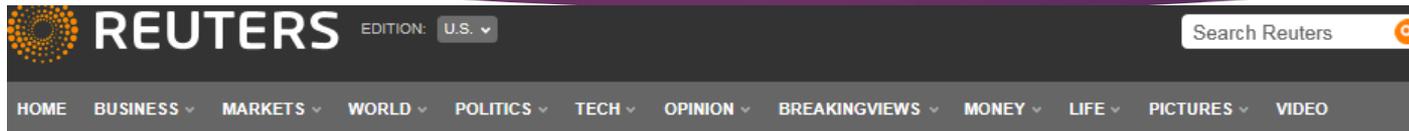


- ▶ Date Aug 31, 2015
- ▶ Decision by Third Court of Appeals in the event of such an Information Technology System hack, the U.S. Federal Trade Commission has authority to investigate the company and charge it with unfair trade practices for failure to protect customers from the theft of on-line data
- ▶ 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



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

**info** security

13 OCT 2015 NEWS

STRATEGY | INSIGHT | TECHNOLOGY

Cyber-Insurance Premiums Rocket

Tara Seals **US/North America News Reporter, Infosecurity Magazine**

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



MARSH RISK  
MANAGEMENT RESEARCH

## Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise

- ▶ 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



Lee Trieu

Web and mobile application developer, Information Security, Cyber security, Mobile security, M2M and IOT

Follow

## Cyber insurance premiums increase

Oct 14, 2015 | 70 views | 3 Likes | 0 Comments



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)
<b>Control 5:</b> 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
<b>Control 6:</b> 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	
<b>Control 7:</b> 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
<b>Control 8:</b> 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](http://www.systemexperts.com)  
1.800.748.4000  
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

© Copyright 2011 SystemExperts Corporation. All rights reserved.



**CYBER SECURITY  
SUMMIT**

# 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



Avalution's Perspective  
On Business Continuity & IT Disaster Recovery

[Insights](#) · [Advice](#) · [Trends](#) · [Best Practices](#) · [Common Issues & Solutions](#)

[Home](#) [About Avalution](#) [BCM 101](#) [Consulting Services](#) [Software Solutions](#)

Posted on December 5, 2013 by Stacy Gardner

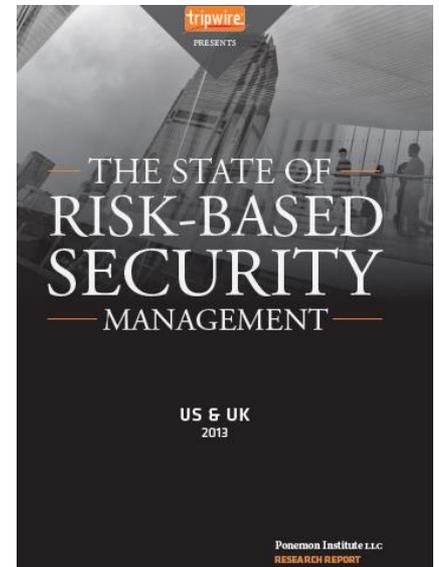
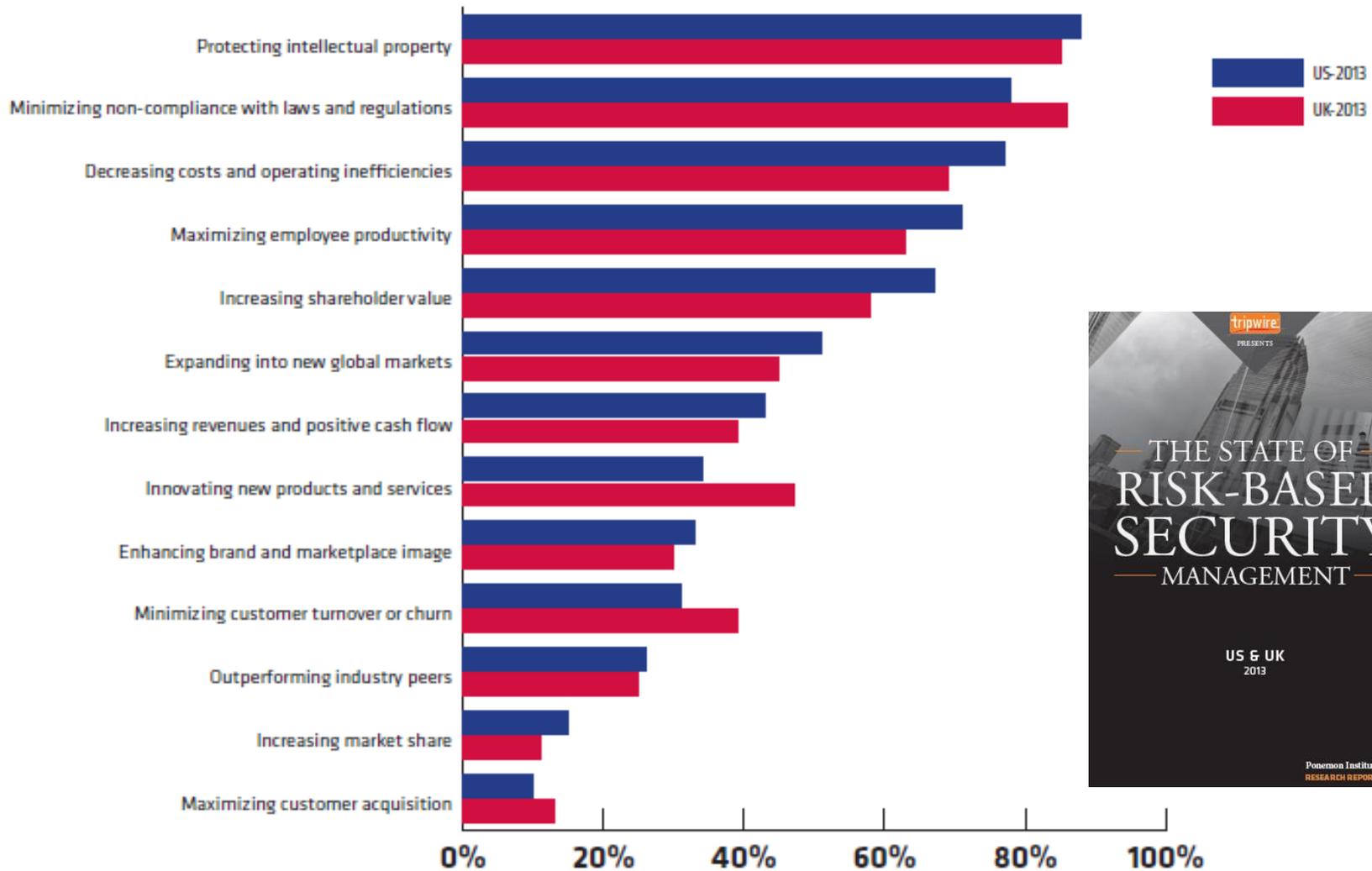
[← Previous](#) [Next →](#)

**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®**



**CIS  
CRITICAL  
SECURITY  
CONTROLS**



**Critical Security Controls**

Critical Security Controls for Effective Cyber  
Defense



**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 Cyber Security.<sup>1</sup>



CYBER SECURITY  
SUMMIT

I had the opportunity to converse with two executives of Tripwire, Ambyr O'Donnell, VP, General Counsel & Corporate Secretary and Kelly Lang, Chief Financial Officer to obtain their perspectives about the role of security in creating a standard of due care.

"Because there is no firmly established standard of due care in security, you have the option of waiting for regulators to dictate what you should do, or be more proactive about how to properly protect your organization," says Lang.

So what does good security hygiene looks like? What should the role of security be in risk management and creating an organizational standard of due care?

When lawyers talk about due care, it is often in the context of liability for negligence claims. In layman's terms, 'due care' can be thought of as the amount of attention that an ordinary and reasonable person would have exercised in order to prevent a foreseeable bad thing from happening.

In addition, part of directors' and officers' fiduciary duties includes a duty of care. The duty of care requires that directors and officers act prudently in overseeing the business, in light of reasonably available information.

O'Donnell comments that security, like all risk management, is fundamentally a corporate governance concern. Directors and officers must appropriately inform themselves before making corporate decisions.

In today's business and legal environment, it is appropriate for corporate leadership to have in-depth discussions about how security considerations factor into assessing operational risk, corporate performance, compliance and brand protection.

In addition, public companies have certain disclosure obligations related to cyber security risks, as affirmed in the [US Securities and Exchange Commission guidelines in 2011](#).

"Cybersecurity is nebulous for many, so it's hard to put your finger on it," says Lang.

### Security Configuration Management For Dummies

Download Now

## Business Reasons to implement Security Cont

### Latest Security News

NHS-Approved Apps Sending Unencrypted Medical Info Over the Web, Finds Study SEP 25, 2015

US Navy Develops New System to Protect Ships Against Cyber Attacks SEP 24, 2015

Healthcare Industry Is Four Times More Likely to Be Impacted by Advanced Malware than Other Industries SEP 24, 2015

Study: US IT Pros Less Confident in Board's Cybersecurity Literacy Than UK Counterparts SEP 23, 2015

UK Government Creates £500,000 Fund to Improve IT Security Education, Skills SEP 23, 2015



## 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 Cyber Security, et

