The Breach Kill Chain and a Layered Security Model

Jeff Sanchez, Managing Director, Protiviti

Dan Hansen, Director, Protiviti

Cybersecurity Essentials – E12

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

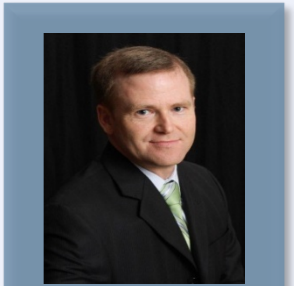
SF ISACA FALL CONFERENCE NOVEMBER 9-11, 2015 HOTEL NIKKO-SAN FRANCISCO

Speakers Today

Jeff Sanchez is a Managing Director in Protiviti's Los Angeles office. He joined Protiviti in 2002 after spending 10 years with Arthur Andersen's Technology Risk Consulting practice.

Jeff has participated in technical consulting and audit projects primarily in the hospitality, gaming, financial services and retail industries. Jeff leads Protiviti's global Data Security and Privacy practice and is a subject-matter expert in the Payment Card Industry Data Security Standard. For the last eight years, Jeff has concentrated on the design and implementation of security and privacy solutions. Jeff is a CIA, CISM, CISA, PA-QSA, CIPP/US and PMP.

jeffrey.sanchez@protiviti.com



Jeffrey Sanchez, Managing Director

Daniel Hansen is a Director in Protiviti's IT Consulting Practice and leads the Security & Privacy practice in the San Francisco Bay Area. He has over 14 years of experience in delivering high value projects in multiple industries focusing on information security, disaster recovery, business continuity, and IT Audit.

Dan is a Certified Information Systems Auditor (CISA), Payment Card Industry Quality Security Assessor (PCI-QSA) and Certified Business Continuity Professional (CBCP).

daniel.hansen@Protiviti.com

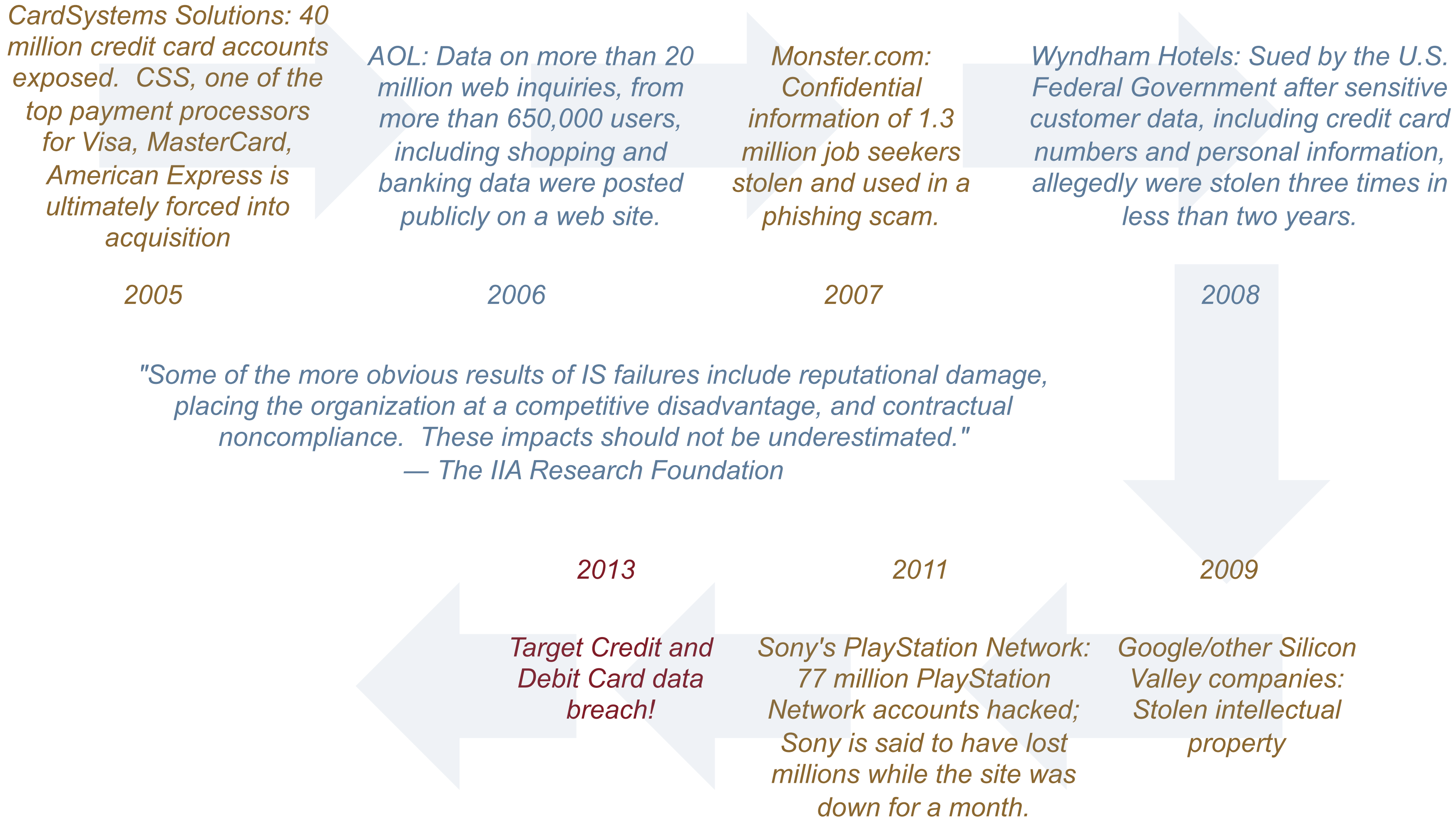
Daniel Hansen, Director

Agenda

Data Breach Overview	3 – 6
Layered Security	7 – 15
Questions	16
Contact	17
Confidentiality Statement and Restriction for Use	18

DATA BREACH OVERVIEW

Large Data Breaches of the Decade



CardSystems Solutions: 40 million credit card accounts exposed. CSS, one of the top payment processors for Visa, MasterCard, American Express is ultimately forced into acquisition

2005

AOL: Data on more than 20 million web inquiries, from more than 650,000 users, including shopping and banking data were posted publicly on a web site.

2006

Monster.com: Confidential information of 1.3 million job seekers stolen and used in a phishing scam.

2007

Wyndham Hotels: Sued by the U.S. Federal Government after sensitive customer data, including credit card numbers and personal information, allegedly were stolen three times in less than two years.

2008

"Some of the more obvious results of IS failures include reputational damage, placing the organization at a competitive disadvantage, and contractual noncompliance. These impacts should not be underestimated."
— The IIA Research Foundation

2009

Google/other Silicon Valley companies: Stolen intellectual property

2011

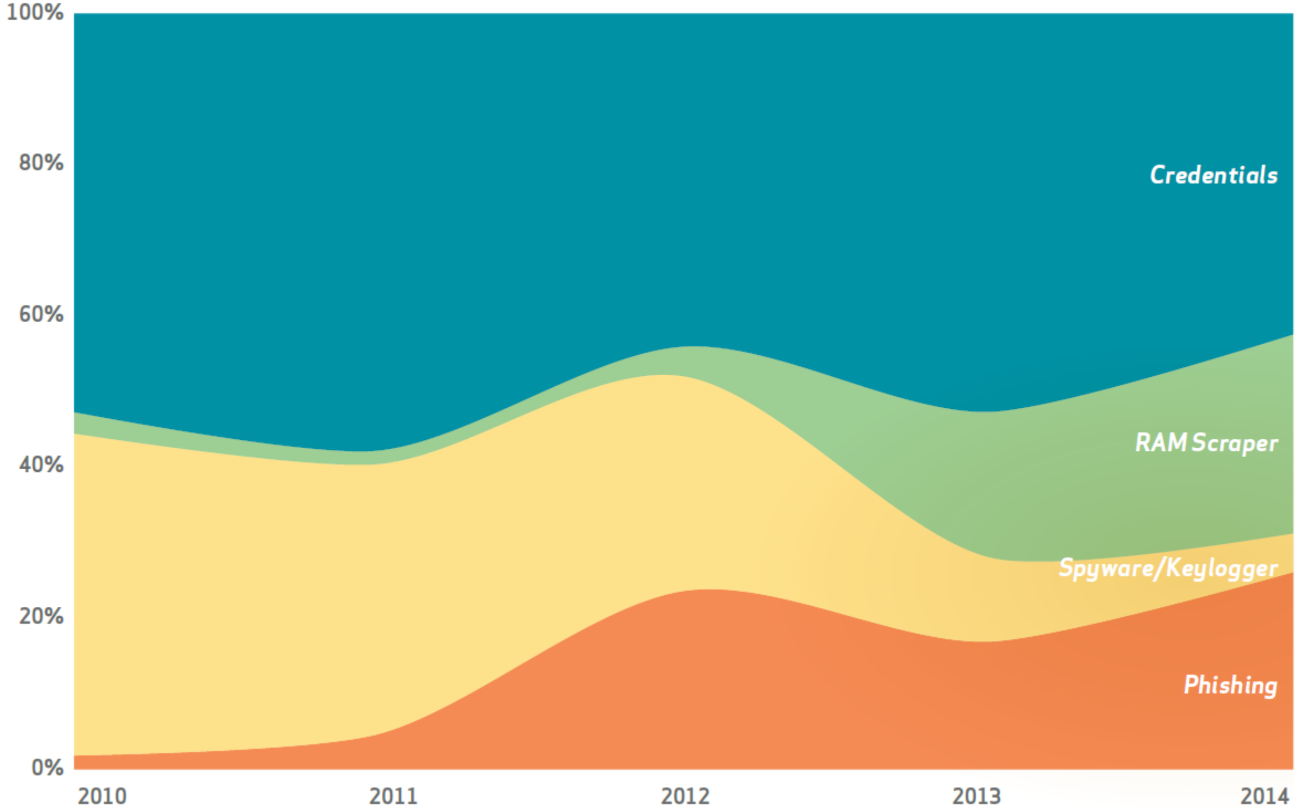
Sony's PlayStation Network: 77 million PlayStation Network accounts hacked; Sony is said to have lost millions while the site was down for a month.

2013

Target Credit and Debit Card data breach!

Source: CNN, NBC, CSO Online

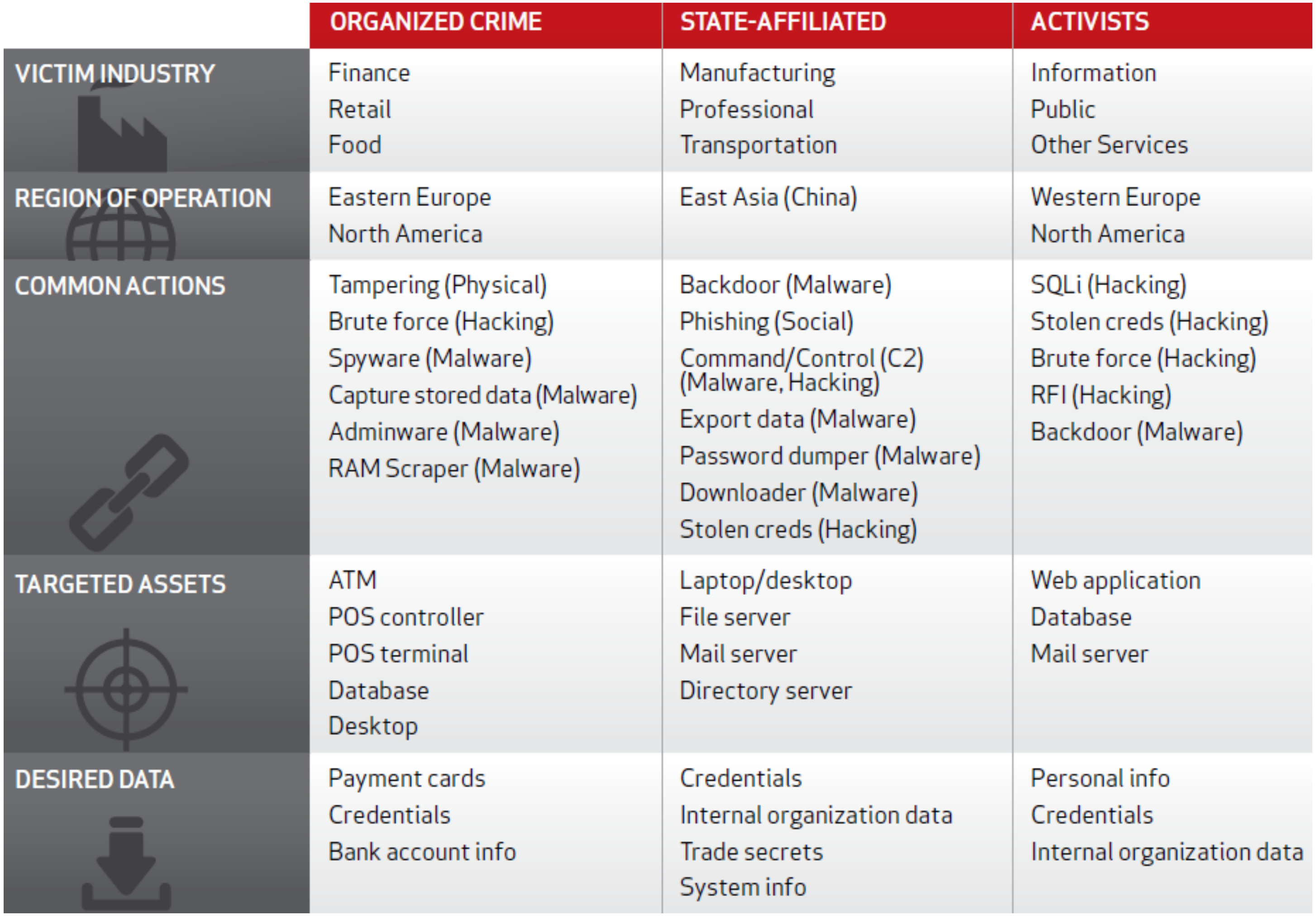
Data Breach Statistics



Significant threat actions over time by percentage.

Source: Verizon

Profiling Threat Actors



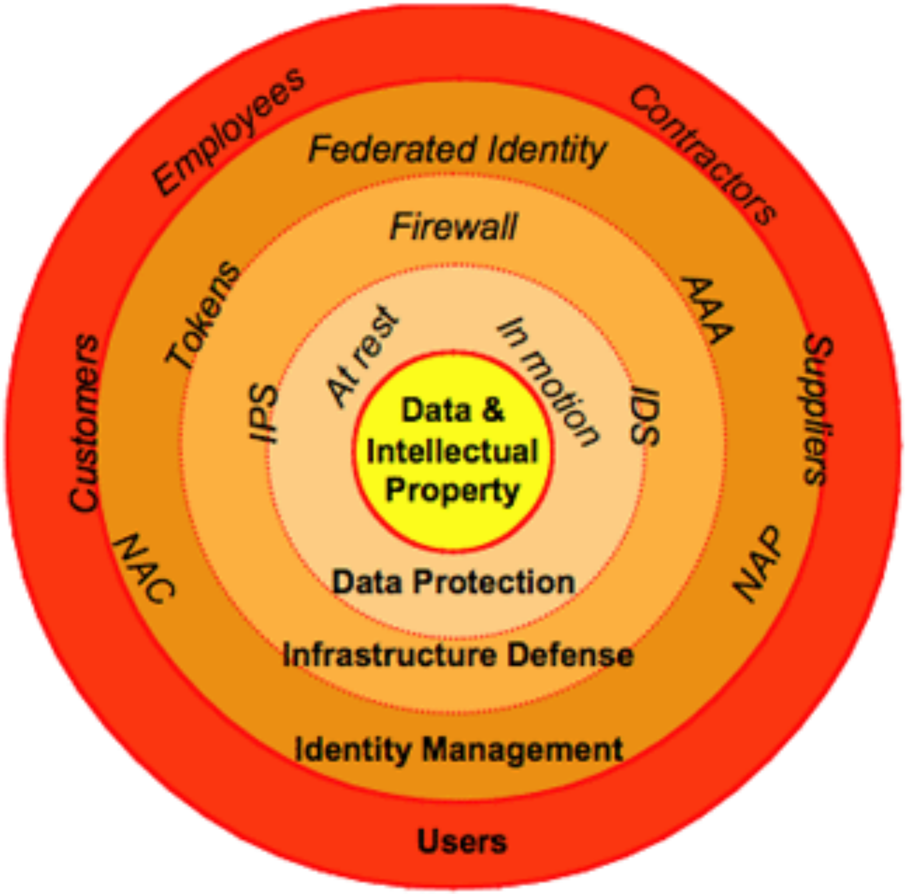
	ORGANIZED CRIME	STATE-AFFILIATED	ACTIVISTS
VICTIM INDUSTRY	Finance Retail Food	Manufacturing Professional Transportation	Information Public Other Services
REGION OF OPERATION	Eastern Europe North America	East Asia (China)	Western Europe North America
COMMON ACTIONS	Tampering (Physical) Brute force (Hacking) Spyware (Malware) Capture stored data (Malware) Adminware (Malware) RAM Scraper (Malware)	Backdoor (Malware) Phishing (Social) Command/Control (C2) (Malware, Hacking) Export data (Malware) Password dumper (Malware) Downloader (Malware) Stolen creds (Hacking)	SQLi (Hacking) Stolen creds (Hacking) Brute force (Hacking) RFI (Hacking) Backdoor (Malware)
TARGETED ASSETS	ATM POS controller POS terminal Database Desktop	Laptop/desktop File server Mail server Directory server	Web application Database Mail server
DESIRED DATA	Payment cards Credentials Bank account info	Credentials Internal organization data Trade secrets System info	Personal info Credentials Internal organization data

Source: Verizon 2013 Report

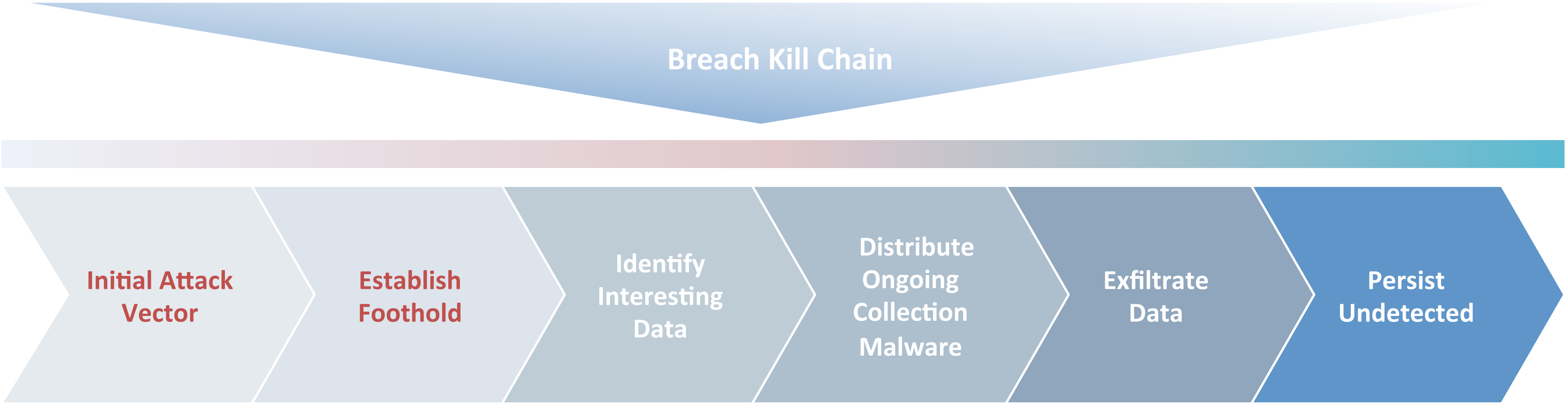
LAYERED SECURITY

Layered Security Model

One Model


Employees
Contractors
Customers
Suppliers
Users
Federated Identity
Tokens
AAA
NAC
NAP
Identity Management
Firewall
IPS
IDS
Infrastructure Defense
At rest
In motion
Data Protection
Data &
Intellectual
Property

Breach Kill Chain



The attack can be disrupted at any point in the kill chain. Ideally, a company will have controls at each point to create a defense in depth strategy. "Cyber kill chain" model shows cyber attacks can and do incorporate a broad range of malevolent actions, from spear phishing and espionage to malware and data exfiltration that may persist undetected for an indefinite period.

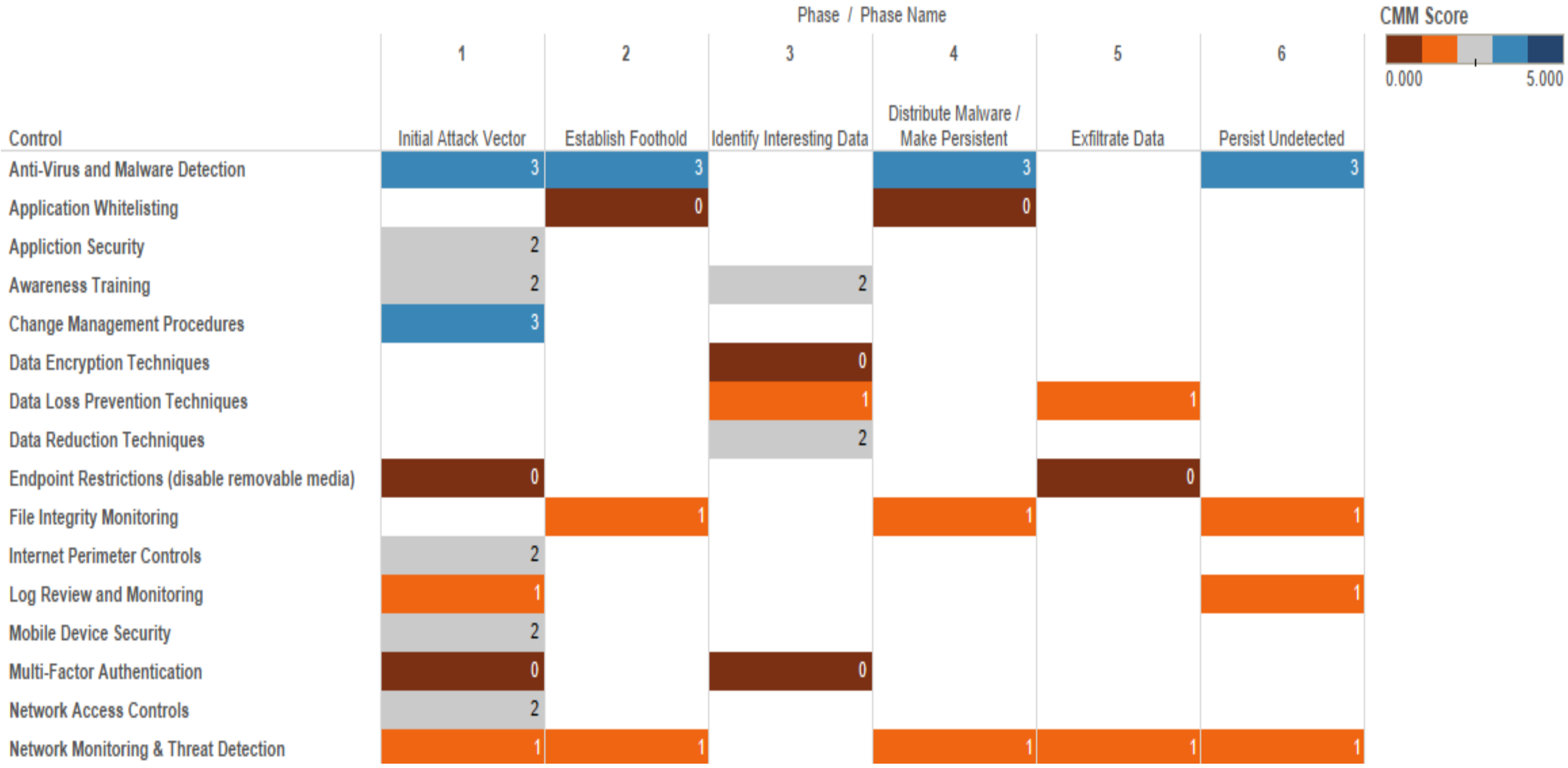
Layered Controls Using Breach Kill Chain

	Phase / Phase Name					
	1	2	3	4	5	6
Control	Initial Attack Vector	Establish Foothold	Identify Interesting Data	Distribute Malware / Make Persistent	Exfiltrate Data	Persist Undetected
Anti-Malware and Malware Detection	X	X		X		X
Application Whitelisting		X		X		
Application Security	X					
Awareness Training	X		X			
Change Management Procedures	X					
Data Encryption Techniques			X			
Data Loss Prevention Techniques			X		X	
Data Reduction Techniques			X			
Endpoint Restrictions (disable removable media)	X				X	
File Integrity Monitoring		X		X		X
Internet Perimeter Controls	X				X	
Log Review and Monitoring	X					X
Mobile Device Security	X					
Multi-Factor Authentication	X		X			
Network Access Control	X					
Network Segmentation			X	X	X	
Outbound Traffic Restrictions & Filtering	X	X		X	X	X
Privileged Account Management		X		X	X	
System Hardening & Secure Build Procedures	X	X		X		
Third Party Access Controls	X					
User Account Security	X					
Vulnerability Management/Patching	X	X		X		
Wireless Controls	X				X	

Australian Signals Directorate Top 4

Mitigation strategy	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Helps Detect Intrusions	Helps Mitigate Intrusion Stage 1: Code Execution	Helps Mitigate Intrusion Stage 2: Network Propagation	Helps Mitigate Intrusion Stage 3: Data Exfiltration
Application whitelisting of permitted/ trusted programs to prevent execution of malicious or unapproved programs including DLL files, scripts and installers.	Medium	High	Medium	Yes	Yes	Yes	Yes
Patch applications (e.g., Java, PDF viewers, Flash, web browsers and Microsoft Office). Patch or mitigate systems with 'extreme risk' vulnerabilities within two days. Use the latest version of applications.	Low	High	High	No	Yes	Possible	No
Patch operating system vulnerabilities. Patch or mitigate systems with 'extreme risk' vulnerabilities within two days. Use the latest suitable operating system. Avoid Windows XP.	Low	Medium	Medium	No	Yes	Possible	No
Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Medium	Medium	Low	No	Possible	Yes	No

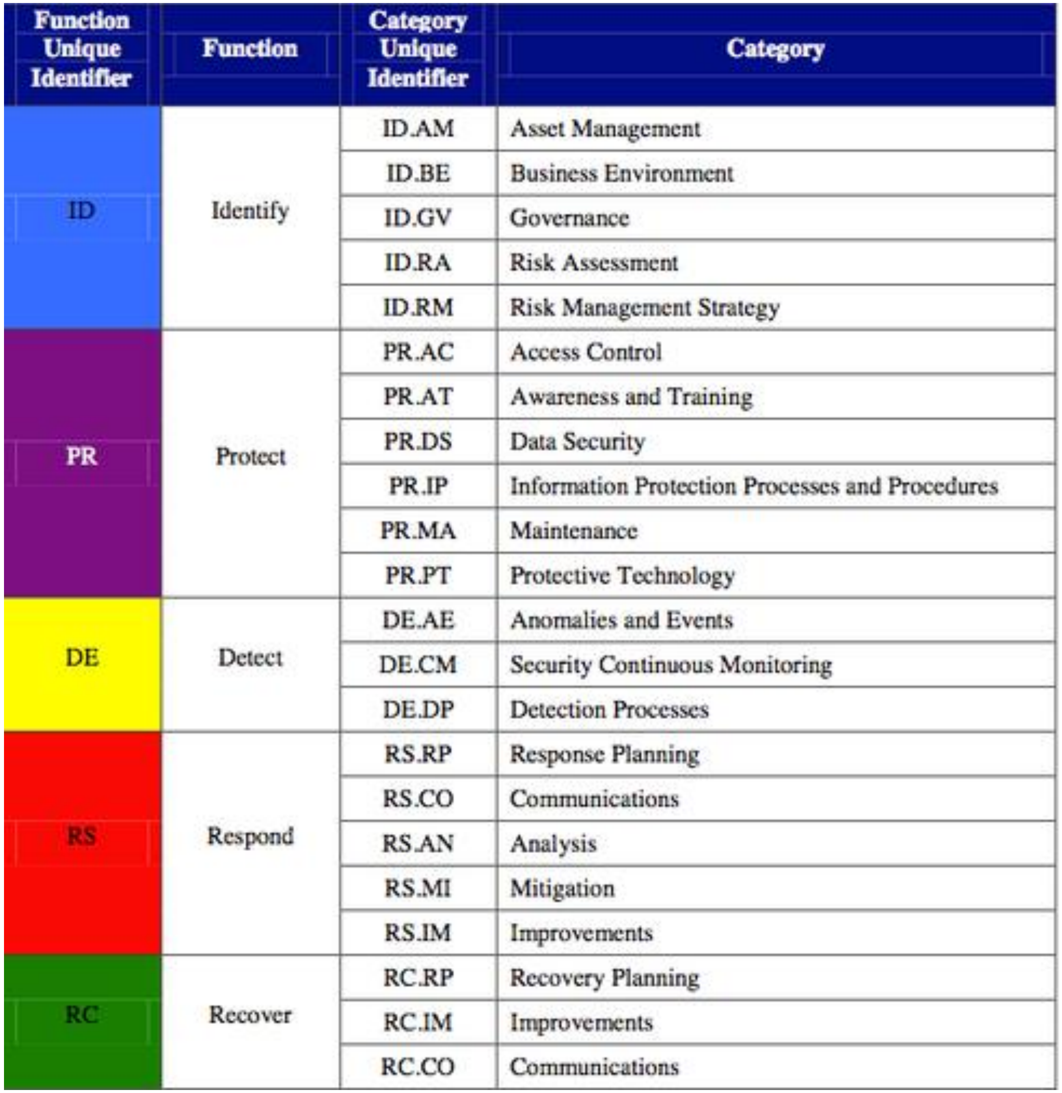
Audit Report Presentation



Phase / Phase Name

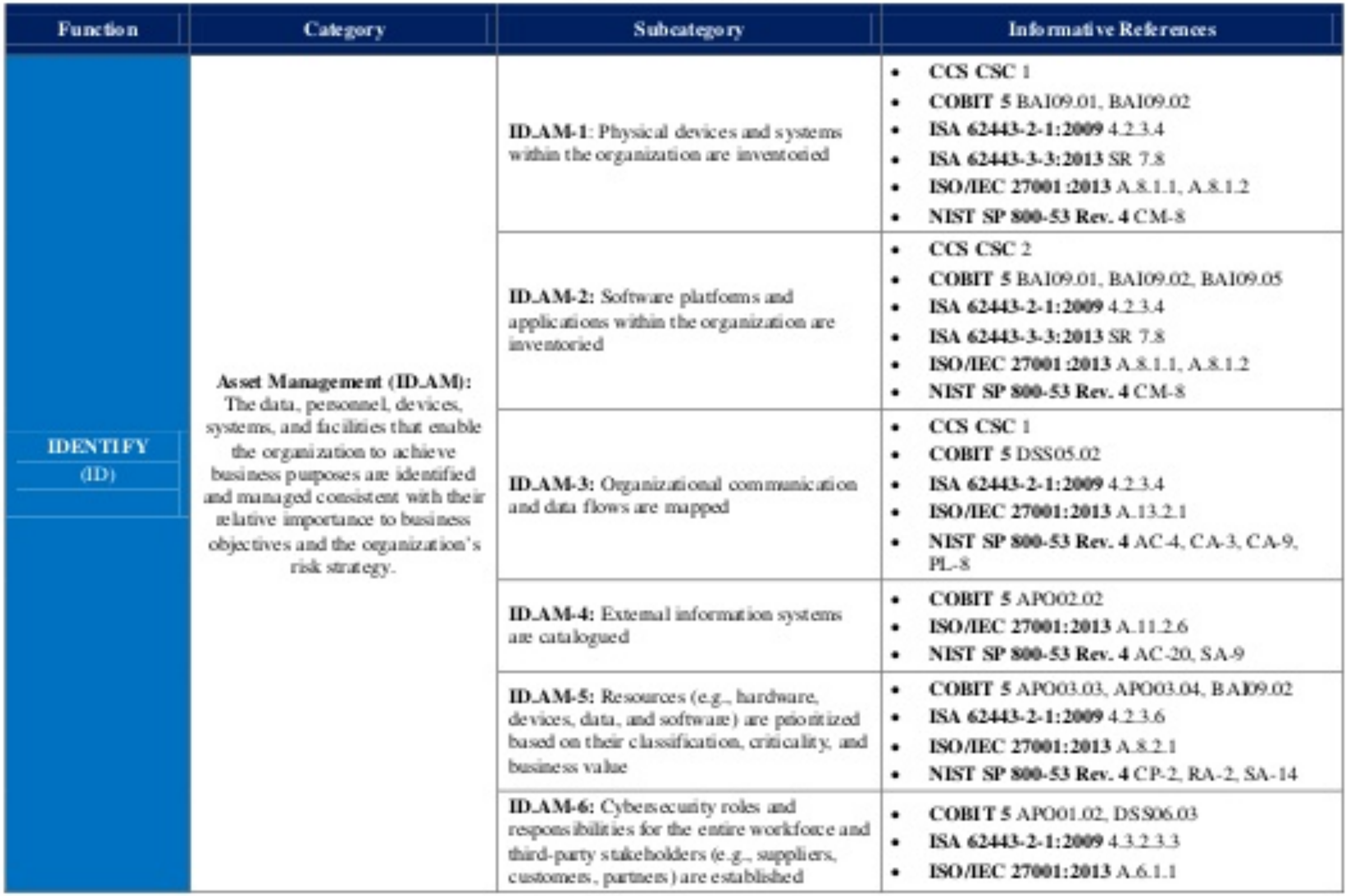
	1	2	3	4	5	6
Control	Initial Attack Vector	Establish Foothold	Identify Interesting Data	Distribute Malware / Make Persistent	Exfiltrate Data	Persist Undetected
Anti-Virus and Malware Detection	3	3		3		3
Application Whitelisting		0		0		
Appliction Security	2					
Awareness Training	2		2			
Change Management Procedures	3					
Data Encryption Techniques			0			
Data Loss Prevention Techniques			1		1	
Data Reduction Techniques			2			
Endpoint Restrictions (disable removable media)	0				0	
File Integrity Monitoring		1		1		1
Internet Perimeter Controls	2					
Log Review and Monitoring	1					1
Mobile Device Security	2					
Multi-Factor Authentication	0		0			
Network Access Controls	2					
Network Monitoring & Threat Detection	1	1		1	1	1

NIST Cyber Security Framework



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Cyber Security Framework



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001 :2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001 :2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

Questions

Contacts

Jeffrey Sanchez

Managing Director
Los Angeles, CA

protiviti®
Risk & Business Consulting.
Internal Audit.

Phone: +1.213.327.1433
jeffrey.sanchez@protiviti.com

Powerful Insights. Proven Delivery.™

Daniel Hansen

Director
San Francisco, CA

protiviti®
Risk & Business Consulting.
Internal Audit.

Phone: +1.415.402.3697
daniel.hansen@protiviti.com

Powerful Insights. Proven Delivery.™