

Failure of Cyber Security Controls: Review of Security Research Reports and the Security Controls that Fail

Rebecca Snevel, Managing Consultant, RGP

Professional Strategies – S32



Agenda

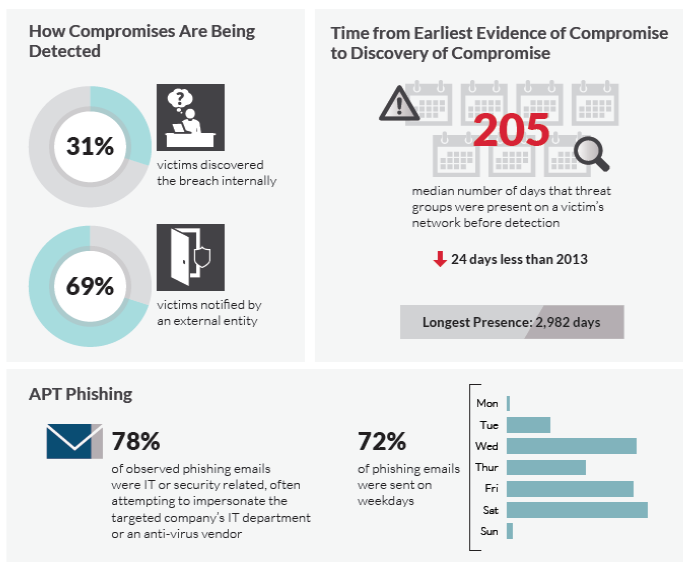
- Overview of 2015 Breaches
- Cyber Security Terminology
- Review of Threat Reports
- Risk and Threat Assessment
- Cyber Security Frameworks
- Overview of the Top 20 Critical Security Controls for Effective Cyber Defense
- Cyber Risk Insurance
- Performing Vendor/Third Party Security Assessments

OVERVIEW OF 2015 BREACHES



Overall View of Cyber Security

- Significant Cyber Security threats exist and every day there are thousands of attacks. Security professionals often say, 'it's not if, but when' there will be a threat
 - Symantec's 2014 Internet Security Threat Report highlights a 91% increase in targeted attacks and a 62% increase in the number of breaches
 - Verizon's 2015 Annual Data Breach Investigation Report states
 - 2,122 confirmed data breaches
 - 79,790 security incidents
 - FireEye's M-Trends 2015 (see below)



2015 Breaches (so far)

CYBER SECURITY TERMINOLOGY



Terminology

- The National Institute of Standards and Technology (NIST) has issued NISTIR (NIST Interagency Reports) 7298 Revision 2 with the following terms defined:
 - **Cybersecurity**
 - The ability to protect or defend the use of cyberspace from cyber attacks.
 - **Cyberspace**
 - A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
 - **Cyber Attack**
 - An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
 - **Cyber Incident**
 - Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

Terminology (con't)

– Risk

- The level of impact on
 - Organizational operations (including mission, functions, image or reputation)
 - Organizational assets,
 - Individuals,
 - Other organizations, or
 - the Nation....resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

– Threat

- Any circumstance or event with the potential to adversely impact on
 - Organizational operations (including mission, functions, image or reputation)
 - Organizational assets,
 - Individuals,
 - Other organizations, or
 - the Nation...via unauthorized access, destruction, disclosure, modification of information and/or denial of service
- The potential source of an adverse event

Verizon's 2015 Data Breach Investigations Report

- Breach Trends
- Phishing
- Vulnerabilities
- Mobile
- Malware
- Industry Profiles
- Incident Classification Patterns

Trustwave's Global Security Report

- Key Insights
- Data Compromise
- Threat Intelligence
- Regional Perspectives

Cisco's 2015 Annual Security Report

- Key Discoveries
- Threat Intelligence
- Security Capabilities Benchmark Study
- Geopolitical and Industry Trends

Symantec's Internet Security Report

- Mobile Devices and The Internet of Things
- Web Threats
- Social Media and Scams
- Targeted Attacks
- Data Breaches and Privacy
- eCrime and Malware

Aon and Ponemon's 2015 Global Cyber Impact Report



- Underinsurance of information assets (based on value, probable maximum loss and likelihood)
- Disclosure of a material loss of PP&E and information asset differs
- Reluctance to purchase cyber insurance coverage
- 37% of the respondent's experienced a material or significantly disruptive security exploit or data breach
- Cyber risk experience

RISK AND THREAT ASSESSMENT



Threat Analysis

1

INFORMATION ASSETS

- INTELLECTUAL PROPERTY
- CUSTOMER INFORMATION
- BUSINESS PARTNERS
- FINANCIAL INFORMATION
- EMPLOYEE INFORMATION
- BUSINESS STRATEGIES

2

THREATS

THREAT SOURCE

- ADVERSARIAL
 - INDIVIDUAL
 - GROUP
 - ORGANIZATION
 - NATION-STATE
- ACCIDENTAL
- STRUCTURAL
- ENVIRONMENTAL

THREAT EVENTS

- RECONNAISSANCE
- ATTACK TOOLS
- CONDUCT AN ATTACK

3

ATTACK SURFACE AND VECTORS

ATTACK SURFACE

- CYBER
- PHYSICAL
- DECEPTION

ATTACK VECTORS

- WEB
- EMAIL
- WIRELESS
- MOBILE
- SOCIAL NETWORKING
- MALWARE

4

VULNERABILITIES

- IDENTIFICATION
- RESOLUTION
- INFORMATION SHARING

5

OBJECTIVES

- FINANCIAL
- REPUTATION
- PRIVACY
- REGULATORY
- AVAILABILITY

QUESTIONS TO CONSIDER

☐

Have the information assets to be protected been identified?

☐

Who and what are the threats and vulnerabilities?

☐

What is the value to the organization?

☐

What can be done to minimize loss or exposure to the loss or damage?

Threats

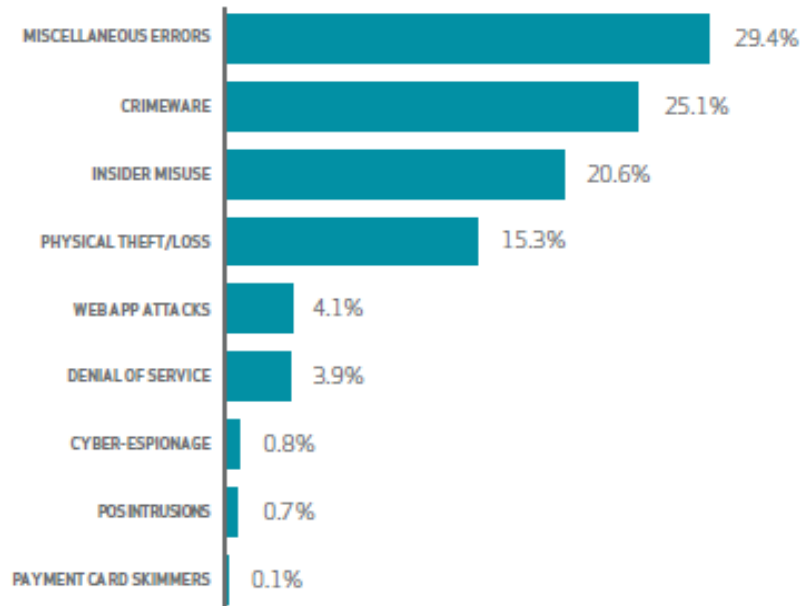
- According to Verizon's 2015 Annual Data Breach Investigation Report, threat 'actors' have remained fairly consistent over the past four years.



Internal vs. External Threats

Incident Classification Patterns

During the production of the 2013 DBIR we had the crazy idea that there must be a way to reduce the majority of attacks into a handful of attack patterns and proved out our theory with great success in the 2014 DBIR. We used the same hierarchical clustering technique on the 2015 corpus and—lo and behold—it worked again (data science FTW!).



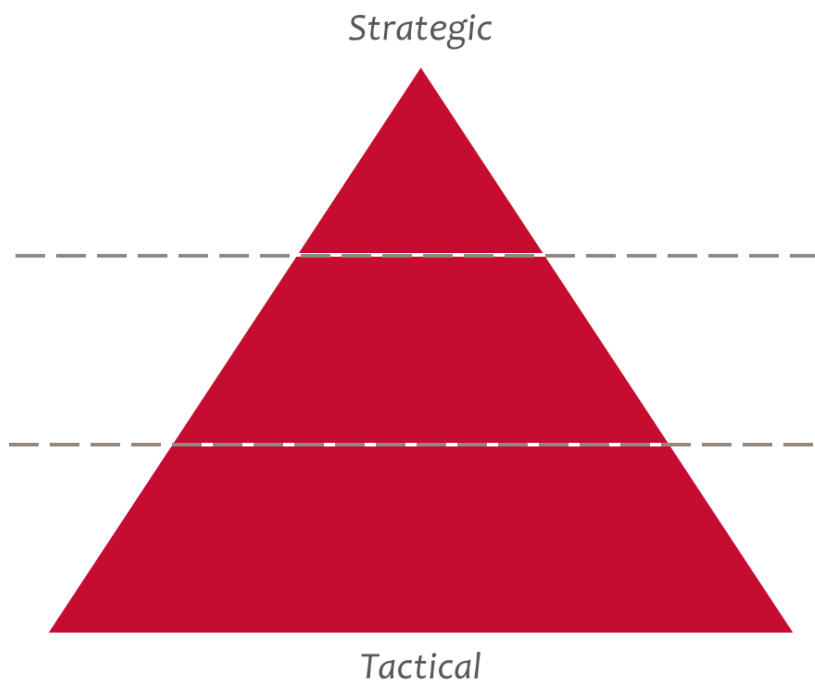
96%

WHILE WE SAW MANY CHANGES IN THE THREAT LANDSCAPE IN THE LAST 12 MONTHS, THESE PATTERNS STILL COVERED THE VAST MAJORITY OF INCIDENTS (96%).

Cyber Security –Security Threats

- **Specific Threats May Include:**
 - Phishing
 - Spear Phishing
 - Malware
 - Counterfeit or tampered hardware
 - Communication interception
 - Denial of Service
 - Social Engineering
 - Human error
 - Leak of sensitive information
 - Hardware failure
 - Lack of IT controls
 - Weather related issues (i.e. hurricane, tornado, flood)

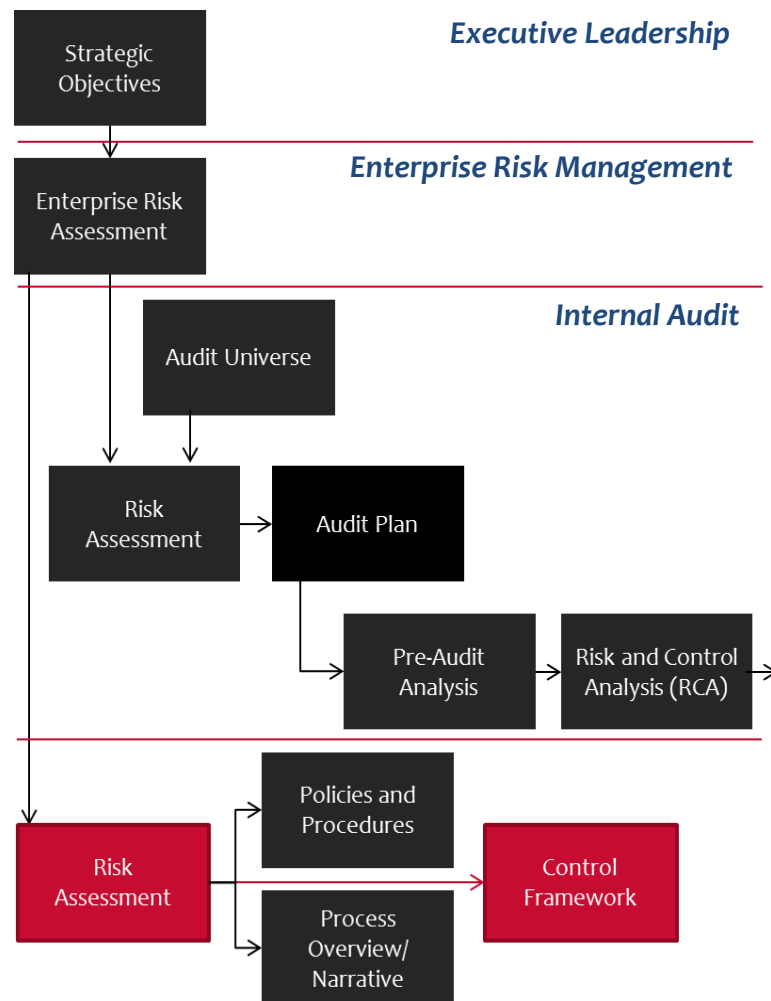
Risk and Threat Assessment



Source: NIST Special Publication 800-39

- RGP recommends integrating the Risk and Threat Assessment activities with the organization's overall Enterprise Risk Management approach and processes

Example Enterprise Risk Management Process Flow



Risk and Threat Assessment – Tier 1

Strategic

Tier 1: Business Objectives and Organizational Structure (Organization)

- Business Entity Risk Assessment
- Business Capability (and Enabling Technology) Risk Assessment

RATING RISK

Risk Severity Rating Matrix

		Likelihood						Key
		Remote < 1% chance to occur	Highly Unlikely 1% to 5% chance to occur	Unlikely 5% to 10% chance to occur	Possible 10% to 50% chance to occur	Likely 50% to 99% chance to occur	Almost Certain > 99% chance to occur	
Impact	Catastrophic	H	H	S	S	E	E	Low
	Critical	M	M	H	S	S	E	Medium
	Major	M	M	M	H	S	S	High
	Serious	L	M	M	M	H	S	Severe
	Moderate	L	L	M	M	M	H	Extreme
	Minor	L	L	L	M	M	M	

Risk Impact Rating Categories

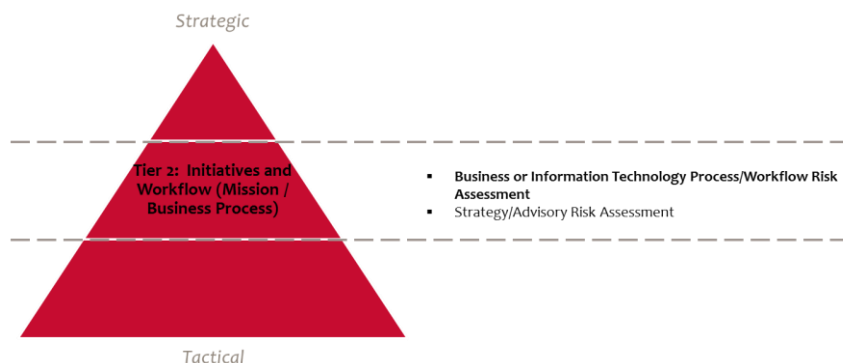
- Impact to Personnel
- Financial Impact
- Reputation Damage, Service Interruption, or Customer Interruption
- Breach of Law, Criminal Prosecution, or Civil Action
- Impact to Community and Social and Cultural Heritage
- Impact to Natural Environment

Tactical

Sources: NIST Special Publication 800-39 and IT Leadership Exchange.

- Tier 1: Business Objectives and Organizational Structure ('Organization' in NIST)
- Top-down assessments of an entity designed to surface top risks
- Output typically bubbles up to ERM and board-level reports
- Information Security normally works with the business to identify major risk categories and enterprise risk appetite

Risk and Threat Assessment – Tier 2



Sources: NIST Special Publication 800-39 and IT Leadership Exchange.

CSC 1: Inventory of Authorized and Unauthorized Devices	Overall Risk Likelihood	Level of Impact	Management Strategy	CSC Details	Mitigation Actions	Overall Status
	High	High	Manage			
	High Level Control Strategy					
Unauthorized assets could be deployed on the SMSG Network	Inventory of information technology assets is performed on a quarterly basis.			<ul style="list-style-type: none">- Assets are tracked through an automated asset inventory discovery tool- An automated asset inventory discovery tool is used to build a preliminary asset inventory of systems- Tool scans through network address ranges and passive tools that identify hosts based on analyzing traffic	Implement an automated asset discovery tool to identify authorized and unauthorized assets on the SMSG Network	
	Serial numbers for meters are documented and tracked in a perpetual inventory as part of the Advanced Meter Infrastructure.					
	Serial numbers for meters are documented and tracked in a perpetual inventory as part of the Advanced Meter Infrastructure.					
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Overall Risk Likelihood	Level of Impact	Management Strategy	CSC Details	Mitigation Actions	Overall Status
	High	Medium	Manage			
	High Level Control Strategy					
Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers are not secured	Standard, hardened operating system images are used for all servers, workstations and laptops			<ul style="list-style-type: none">- Deploy secure standard configurations for operating systems- Implement automated patching tools and processes for both applications and for operating system software- Review administrative privileges to ensure access is restricted to very few users and authorization is appropriately restricted	<ul style="list-style-type: none">- Implement an automated patching tool- Implement automated patching tools and processes- Review administrative privileges to ensure access is restricted to very few users and authorization is appropriately restricted	
	Corporate policy requires all systems to be patched to current levels					
	Administration users are limited					

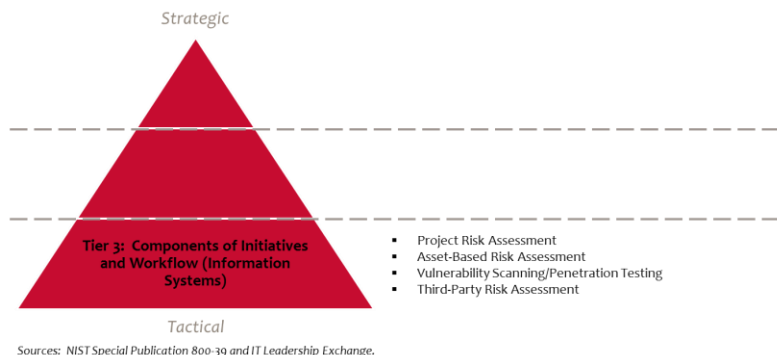
• Tier 2: Initiatives and Workflow (Mission / Business Process in NIST)

- As the responsibility of Information Security has evolved from not only identifying and assessing risk of various technologies and ensuring effective controls are designed and operating effectively to be acting as a true advisor to risk owners to provide information to support business decisions.
- To accomplish this level of detail, RGP recommends the Risk Assessment be performed for a sequence of activities that will efficiently and effectively surface items for business and information technology processes, workflow and controls

Risk and Threat Assessment - Tier 3

Tier 3: Components of Initiatives and Workflow (Information Systems in NIST)

- Targeted assessments of new projects, existing technology assets, such as applications, infrastructure, or IT systems, to identify, assess and document risk
- Detailed control activities are assessed for the design of control activities mitigate risk to an acceptable level



Audit Section: ##### End-User Information Security							
I. KEY PROCESS INFORMATION		II. RISK INFORMATION	III. CONTROL INFORMATION		IV. TEST OF CONTROLS		
Key process End-User Information Security	Risks	Control to Mitigate Risk	Key Control?	Previous Control Reference	Audit Program	Tested in SOX Testing ?	Test W/P Ref
Logical Access							
Logical Access							

CYBER SECURITY FRAMEWORKS



Cyber Security Risk Assessment Approach



Cybersecurity Framework

- In 2013, President Obama issued the Executive Order 13636 [“Improving Critical Infrastructure Cybersecurity”](#) in the 2013 State of the Union.
 - On February 12, 2014, the Obama Administration announced the launch of the [Cybersecurity Framework](#)
 - Each component reinforces the connection between business drivers and cybersecurity activities
 - The Framework Core is a set of cybersecurity activities are grouped by five functions: Identify, Protect, Detect, Respond, Recover
 - Profiles can help organizations align their cybersecurity activities with business requirements, risk tolerances, and resources
 - Tiers provide a mechanism for organizations to view their approach and processes for managing cyber risk.



Cybersecurity Framework Details

•The five functions of the Framework Core (Identify, Protect, Detect, Respond, Recover) include:

- 22 Categories
- 356 Sub-Categories

Function	Category	Subcategory	Informative References
	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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Cyber Security Frameworks

- **There are a number of frameworks that provide guidance on Cyber Security:**
 - ISO International Standards Organization (including the 2700 series)
 - NIST National Institute of Standards and Technology
 - NIST Special Publications (800 Series) includes 166 ‘documents’
 - NIST’s Framework for Improving Critical Infrastructure Cybersecurity
 - ITIL Information Technology Infrastructure Library
 - Standard of Good Practice published by the Information Security Forum (ISF)
 - Trust Services Principles
 - Control frameworks may include Committee of Sponsoring Organizations (COSO)
 - Control Objectives for Information Technology (COBIT)
 - Various Regulatory and Industry requirements and frameworks

OVERVIEW OF THE TOP 20 CRITICAL SECURITY CONTROLS FOR EFFECTIVE CYBER DEFENSE



List of Top 20 Critical Security Controls

Count	Top 20 Most Critical Security Controls
1	CSC 1: Inventory of Authorized and Unauthorized Devices
2	CSC 2: Inventory of Authorized and Unauthorized Software
3	CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4	CSC 4: Continuous Vulnerability Assessment and Remediation
5	CSC 5: Malware Defenses
6	CSC 6: Application Software Security
7	CSC 7: Wireless Access Control
8	CSC 8: Data Recovery Capability
9	CSC 9: Security Skills Assessment and Appropriate Training to Fill Gaps
10	CSC 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11	CSC 12: Controlled Use of Administrative Privileges
12	CSC 13: Boundary Defense
13	CSC 15: Controlled Access Based on the Need to Know
14	CSC 16: Account Monitoring and Control
15	CSC 17: Data Protection
16	CSC 18: Incident Response and Management
17	CSC 19: Secure Network Engineering
18	CSC 11: Limitation and Control of Network Ports, Protocols, and Services
19	CSC 14: Maintenance, Monitoring, and Analysis of Audit Logs
20	CSC 20: Penetration Tests and Red Team Exercises

<https://www.sans.org/critical-security-controls/>

National Security Agency/ Central Security Service



- The National Security Agency/Central Security Service (NSA/CSS) has provided information to U.S. decision makers and military leaders for over 50 years
- The Central Security Service was established in 1972 to promote a full partnership between NSA and the cryptologic elements of the armed forces
- NSA/CSS products and services to the Department of Defense, the Intelligence Community, government agencies, industry partners, and select allies and coalition partners
- NSA/CSS delivers critical strategic and tactical information to war planners and war fighters

Background of the Critical Security Controls for Effective Cyber Defense

- History
 - In 2008, the Office of the Secretary of Defense asked the National Security Agency for help in prioritizing the myriad security controls that were available for cybersecurity.
 - The request went to NSA because NSA best understood how cyber attacks worked and which attacks were used most frequently. The request came at a moment when the theme "offense must inform defense" had become a White House mantra for cybersecurity.
- The Goal of the Critical Controls
 - The goal of the Critical Controls is to protect critical assets, infrastructure, and information by strengthening your organization's defensive posture through continuous, automated protection and monitoring of your sensitive information technology infrastructure to reduce compromises, minimize the need for recovery efforts, and lower associated costs.

Top 20 Critical Security Controls

Count	Top 20 Most Critical Security Controls
1	CSC 1: Inventory of Authorized and Unauthorized Devices
2	CSC 2: Inventory of Authorized and Unauthorized Software
3	CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4	CSC 4: Continuous Vulnerability Assessment and Remediation
5	CSC 5: Malware Defenses
6	CSC 6: Application Software Security
7	CSC 7: Wireless Access Control
8	CSC 8: Data Recovery Capability
9	CSC 9: Security Skills Assessment and Appropriate Training to Fill Gaps
10	CSC 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11	CSC 12: Controlled Use of Administrative Privileges
12	CSC 13: Boundary Defense
13	CSC 15: Controlled Access Based on the Need to Know
14	CSC 16: Account Monitoring and Control
15	CSC 17: Data Protection
16	CSC 18: Incident Response and Management
17	CSC 19: Secure Network Engineering
18	CSC 11: Limitation and Control of Network Ports, Protocols, and Services
19	CSC 14: Maintenance, Monitoring, and Analysis of Audit Logs
20	CSC 20: Penetration Tests and Red Team Exercises

CSC 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.
 - CSC 1-1 Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s).
 - CSC 1-2 Deploy dynamic host configuration protocol (DHCP) server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information.
 - CSC 1-3 Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
 - CSC 1-4 Maintain an asset inventory of all systems that has an Internet protocol (IP) address on the network and must also include data on whether the device is a portable and/or personal device.
 - CSC 1-5 Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.
 - CSC 1-6 Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.
 - CSC 1-7 Utilize client certificates to validate and authenticate systems prior to connecting to the private

CSC 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.
 - CSC 2-1 Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system
 - CSC 2-2 Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses
 - CSC 2-3 Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system
 - CSC 2-4 Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops and include the version number and patch level
 - CSC 2-5 The software inventory systems must be integrated with the hardware asset inventory
 - CSC 2-6 Dangerous file types (e.g., .exe, .zip, .msi) should be closely monitored and/or blocked
 - CSC 2-7 Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment
 - CSC 2-8 Configure client workstations with non-persistent, virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis
 - CSC 2-9 Deploy software that only provides signed software ID tags

CSC 3: Secure Configuration

- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
 - CSC 3-1 Establish and ensure the use of standard secure configurations of your operating systems
 - CSC 3-2 Implement automated patching tools and processes for both applications and for operating system software
 - CSC 3-3 Limit administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system
 - CSC 3-4 Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise
 - 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
 - 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
 - CSC 3-7 Do all remote administration of servers, workstation, network devices, and similar equipment over secure channels.
 - CSC 3-8 Utilize file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered
 - 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
 - CSC 3-10 Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis. Configuration/Hygiene

CSC 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
 - CSC 4-1 Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities
 - CSC 4-2 Correlate event logs with information from vulnerability scans
 - CSC 4-3 Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners
 - CSC 4-4 Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis
 - CSC 4-5 Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe
 - CSC 4-6 Carefully monitor logs associated with any scanning activity and associated administrator accounts
 - CSC 4-7 Compare the results from back-to-back vulnerability scans
 - CSC 4-8 Measure the delay in patching new vulnerabilities and ensure that the delay is equal to or less than the benchmarks set forth by the organization
 - CSC 4-9 Evaluate critical patches in a test environment before pushing them into production on enterprise systems
 - CSC 4-10 Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets

CSC 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.
 - CSC 5-1 Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality
 - CSC 5-2 Employ anti-malware software that offers a remote, cloud- based centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machine
 - CSC 5-3 Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares
 - CSC 5-4 Configure systems so that they automatically conduct an anti- malware scan of removable media when inserted
 - CSC 5-5 Scan and block all e-mail attachments entering the Quick Win organization’s e-mail gateway if they contain malicious code or file types that are unnecessary for the organization’s business
 - CSC 5-6 Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc.
 - CSC 5-7 Limit use of external devices to those that have a business need
 - CSC 5-8 Ensure that automated monitoring tools use behavior-based anomaly detection to complement traditional signature-based detection.
 - CSC 5-9 Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature- based detection to identify and filter out malicious content
 - CSC 5-10 Implement an incident response process that allows the IT support organization to supply the security team with samples of malware running on corporate systems that do not appear to be recognized by the enterprise’s anti-malware software
 - CSC 5-11 Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains

CSC 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.

- CSC 6-1 For all acquired application software, check that the version is supported by the vendor.
- CSC 6-2 Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks
- CSC 6-3 For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats
- CSC 6-4 Test in-house-developed and third-party-procured web applications for common security weaknesses
- CSC 6-5 Do not display system error messages to end-users
- CSC 6-6 Maintain separate environments for production and nonproduction systems
- CSC 6-7 Test in-house-developed web and other application software for coding errors and potential vulnerabilities
- CSC 6-8 (NEW) For acquired application software, examine the product security process of the vendor (history of vulnerabilities, customer notification, patching/remediation)
- CSC 6-9 For applications that rely on a database, use standard hardening configuration templates
- CSC 6-10 Ensure that all software development personnel receive training in writing secure code for their specific development environment
- CSC 6-11 For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.

CSC's and Incidents

- Verizon mapped the Critical Security Controls to incidents

CSC	DESCRIPTION	PERCENTAGE	CATEGORY
13-7	2FA	24%	Visibility/Attribution
6-1	Patching web services	24%	Quick Win
11-5	Verify need for Internet-facing devices	7%	Visibility/Attribution
13-6	Proxy outbound traffic	7%	Visibility/Attribution
6-4	Web application testing	7%	Visibility/Attribution
16-9	User lockout after multiple failed attempts	5%	Quick Win
17-13	Block known file transfer sites	5%	Advanced
5-5	Mail attachment filtering	5%	Quick Win
11-1	Limiting ports and services	2%	Quick Win
13-10	Segregation of networks	2%	Configuration/Hygiene
16-8	Password complexity	2%	Visibility/Attribution
3-3	Restrict ability to download software	2%	Quick Win
5-1	Anti-virus	2%	Quick Win
6-8	Vet security process of vendor	2%	Configuration/Hygiene

How Organizations Are Applying the Controls

- Dozens of early adopters of the Critical Controls have shared their experiences and lessons learned with the Consortium for Cybersecurity Action (CCA). A pattern has emerged of steps common to many organizations that have made substantial progress in reducing risk using the Critical Controls:
 - Step 1. Perform Initial Gap Assessment - determining what has been implemented and where gaps remain for each control and sub-control.
 - Step 2. Develop an Implementation Roadmap - selecting the specific controls (and sub-controls) to be implemented in each phase, and scheduling the phases based on business risk considerations.
 - Step 3. Implement the First Phase of Controls - identifying existing tools that can be repurposed or more fully utilized, new tools to acquire, processes to be enhanced, and skills to be developed through training.
 - Step 4. Integrate Controls into Operations - focusing on continuous monitoring and mitigation and weaving new processes into standard acquisition and systems management operations.
 - Step 5. Report and Manage Progress against the Implementation Roadmap developed in Step 2. Then repeat Steps 3-5 in the next phase of the Roadmap.

Cybersecurity Framework

Function	Category	Function	Category
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.	PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
IDENTIFY (ID)	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	PROTECT (PR)	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	PROTECT (PR)	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
IDENTIFY (ID)	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
IDENTIFY (ID)	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	PROTECT (PR)	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
		PROTECT (PR)	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Cybersecurity Framework

Function	Category
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.
DETECT (DE)	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
DETECT (DE)	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
RESPOND (RS)	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
RESPOND (RS)	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
RESPOND (RS)	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Function	Category
RESPOND (RS)	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
RECOVER (RC)	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
RECOVER (RC)	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Proposed Solution - Approach



High Level Approach



High Level Approach



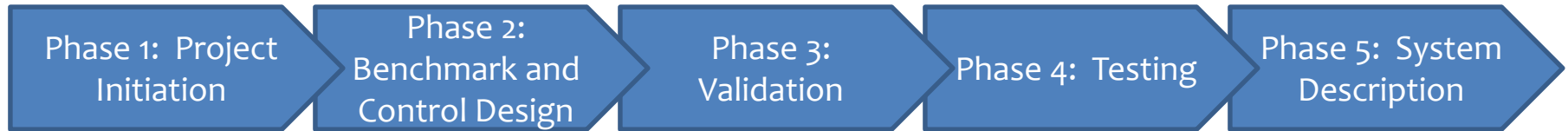
Key Considerations Outside of Information Technology

- Keep security at the top of mind for the Executive Team
- Ensure appropriate internal controls, including operational and compliance, have been designed and are operating as intended
 - Be aware of phishing attacks
 - Involvement in testing of applications
 - Role in Information Security approvals, provisioning and de-provisioning
- Evaluate the Security Posture periodically and against the current landscape
- Consider monitoring threats real time (dashboard)
- Understand the role of Data Loss Prevention
- Periodic Vulnerability Assessments are not be enough to protect
- Ensure data classification policies and procedures
 - Identify the categories of data
 - Classify data
 - Map the data throughout the lifecycle

Approach for Assessing Security Controls



Example SOC2 Key Activities and Deliverables





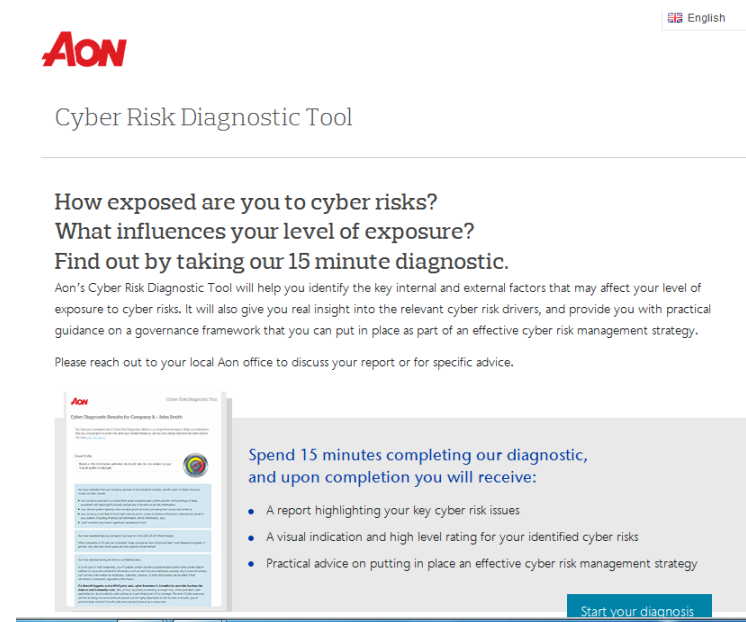
Cyber Risk Insurance

Cyber Risk

- RGP and Aon Insurance have established a partnership on Cyber Risk insurance services
- Who should be concerned about Cyber Risk exposure?
 - Gather, maintain and/or share private information
 - High dependency on electronic processes
 - Engage with business partners
 - Subject to regulatory status, including HIPAA and PCI
 - Part of the nation's critical infrastructure
 - Subject to SEC Cyber Disclosure Guidance of 2011
- What is the scope of coverage?
 - 3rd party coverage
 - Wrongful disclosure
 - Failure to guard against threats (e.g. hackers, virus, DOS)
 - Security or privacy breach regulatory proceedings
 - 1st party coverage
 - Network business interruption
 - Intangible property
 - Breach response/management costs
 - Cyber extortion
 - Loss of income due to failure of network security

Aon's Approach to Cyber Risk Insurance

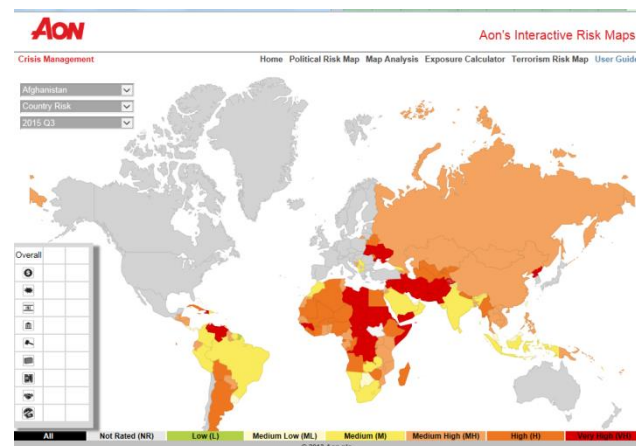
- Aon's Approach is a combination of
 - Risk management and brokering expertise
 - Data and analytics
 - Advisory and consulting services
 - Technology and tools
- The objective is to help clients protect their organization and empower results through
 - Understanding risk
 - Managing risk
 - Where appropriate, transfer risk
- The Aon Approach includes
 - Strategic Meetings/Discussion
 - Submission Development
 - Marketplace Leverage
 - Strategic Negotiations and Placement



The screenshot displays the Aon Cyber Risk Diagnostic Tool interface. At the top, the Aon logo is visible on the left, and a language selector set to 'English' is on the right. Below the logo, the title 'Cyber Risk Diagnostic Tool' is centered. The main content area poses the question 'How exposed are you to cyber risks? What influences your level of exposure?' and encourages users to 'Find out by taking our 15 minute diagnostic.' It provides a brief description of the tool's purpose: to identify internal and external factors affecting cyber risk exposure and provide practical guidance on governance frameworks. A note at the bottom of this section asks users to reach out to their local Aon office for further advice. Below this text, there is a visual representation of the diagnostic tool's output, showing a list of cyber risks and a corresponding report. To the right of this visual, a box states 'Spend 15 minutes completing our diagnostic, and upon completion you will receive:' followed by three bullet points: 'A report highlighting your key cyber risk issues', 'A visual indication and high level rating for your identified cyber risks', and 'Practical advice on putting in place an effective cyber risk management strategy'. A 'Start your diagnosis' button is located at the bottom right of the interface.

Aon's Thought Leadership

- In the 2015 Global Risk Management Survey, five of the top 10 risks are related to security and privacy issues
 - Damage to reputation/brand (1)
 - Regulatory/legislative changes (3)
 - Business interruption (7)
 - Third-party liability (8)
 - Computer crime (9)
- When asked to assess and rate their organizations' preparedness, the average score was 6.72 of 10 with 57% falling to the 'need for improvement' category
- Additional thought leadership is available on www.aon.com





Performing Vendor/Third Party Security Assessments

Third-Party (Vendor) Oversight - Background

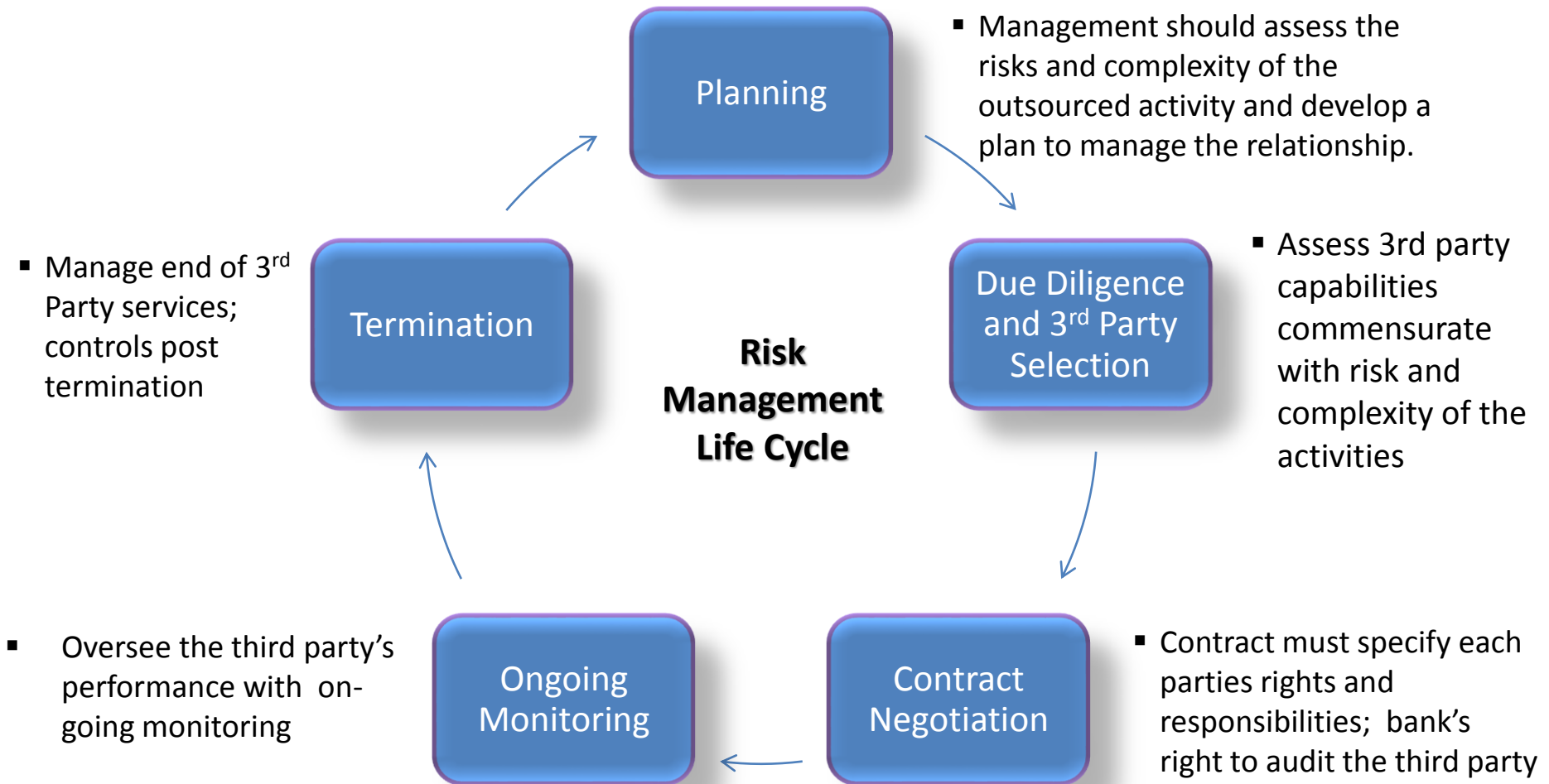
- U.S. companies are facing increased regulatory scrutiny of the processes, systems and controls used in monitoring and managing risks associated with “significant” third-party vendors.
 - These risks include both risks to the institution’s business and solvency as well as the institution’s protection of its customers from financial harm.
 - Recent trends are driving regulators to look at vendor risk more closely:
 - Greater overall interest in operational risk from third parties
 - Greater interest in compliance risk
 - Increased outsourcing and use of sub-contractors
 - Focus on protecting customer and employee confidential information
 - Increased vendor access
 - Vendor Security is the weakest link
 - Shared technical infrastructure
 - Costly and difficult to detect- vendor related breaches and disruption.
 - The new guidance introduces a “life cycle” approach to third-party risk management, requiring comprehensive oversight throughout each phase of a bank’s business arrangement with third parties, including consultants, joint ventures, affiliates, subsidiaries, payment processors, computer network and security providers.

Third-Party (Vendor) Relationships Defined

- A third-party relationship could be considered “significant” if:
 - The relationship has a material effect on the institution’s revenues or expenses
 - They store, access, transmit, or performs transactions on sensitive customer information
 - They significantly increases the institution’s geographic market
 - They provide a product or perform a service involving lending or card payment transactions
 - They provide a product or perform a service that covers or could cover a large number of consumers
 - They provide a product or perform a service that implicates several or higher risk consumer protection regulations
 - They are involved in deposit taking arrangements such as affinity arrangements
 - They market products or services directly to institution customers that could pose a risk of financial loss to the individual

OCC Guidance *

Oversight of third-party (Vendor) providers is a critical area in managing enterprise risks. Regulators look for formal programs with structured controls throughout the lifecycle.



RGP 3rd Party/Vendor Oversight Methodology

RGP supports the development and implementation of Third-Party Oversight strategies to ensure that vendor risks are identified and managed.



Critical Success Factors

- Senior management buy-in and communication
- Understand inherent risks of relationship
- Engage cross-functional stakeholders
- Contracts cover required points
- Establish ongoing assessment and performance monitoring
- Broad communication and training

Thank You!



Trust in, and value from, information systems

San Francisco Chapter



SF ISACA FALL CONFERENCE

NOVEMBER 9-11, 2015

HOTEL NIKKO-SAN FRANCISCO