WOLF & COMPANY, P.C.

Cybersecurity: What CFO's Need to Know

William J. Nowik, CISA, CISSP, QSA PCIP

Today's Agenda

- Introduction to Cybersecurity
- How do I measure my readiness
  - FFIEC Cybersecurity Assessment Tool
  - NIST Cybersecurity Framework
- Cybersecurity impact on other risk management programs

Introduction to Cybersecurity

Definitions – Per NIST

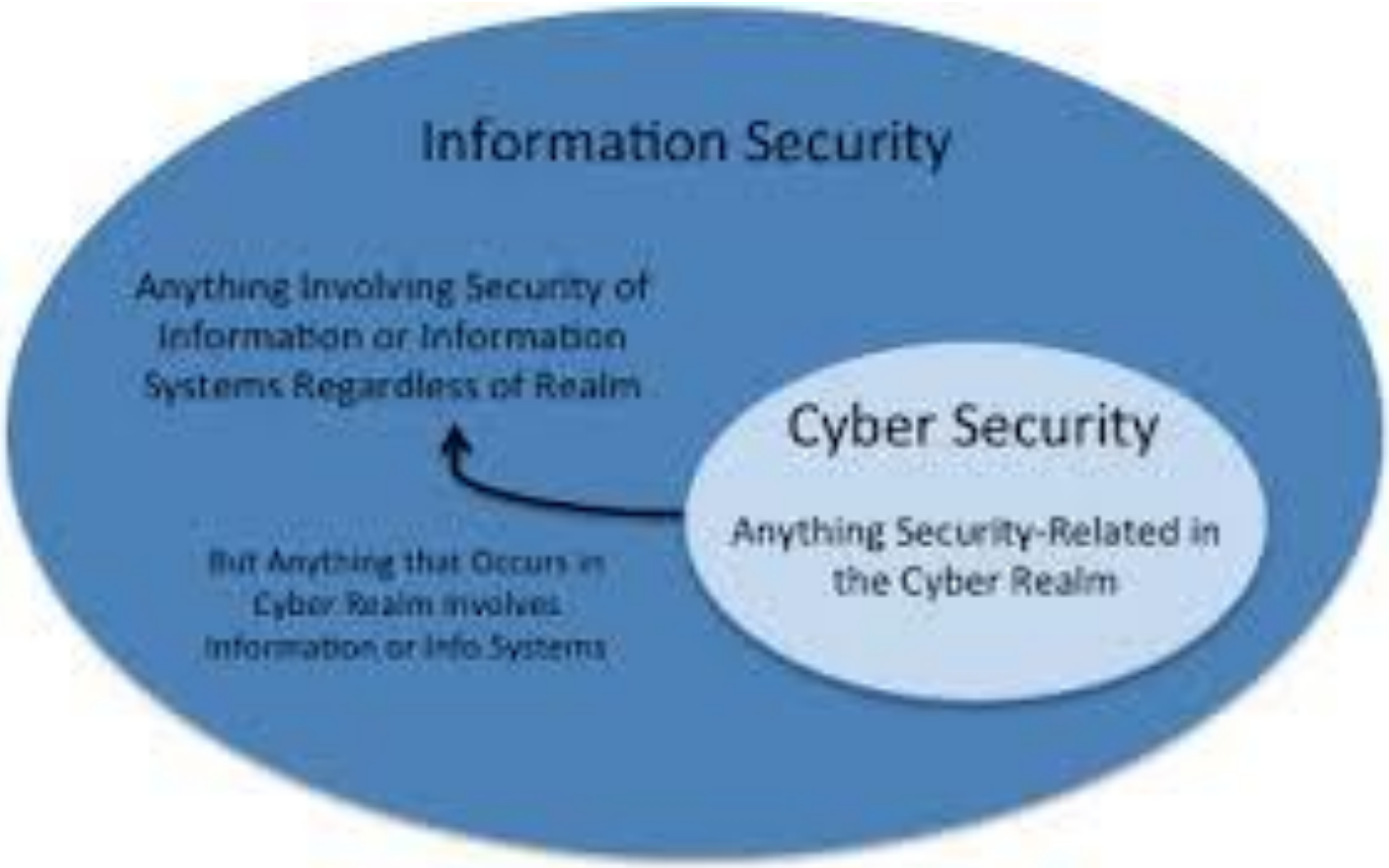
- **Cybersecurity:** The ability to protect or defend the use of cyberspace from cyber attacks.

- **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.

- **Information Security (1):** The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

SOURCE: NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

Definition


Information Security
Anything Involving Security of Information or Information Systems Regardless of Realm
Cyber Security
Anything Security-Related in the Cyber Realm
But Anything that Occurs in Cyber Realm involves Information or Info Systems

Threat Agents & Threats

- Threat Agents
  - **Organized crime**
  - Nation-state and spies
  - Terrorists
  - **Hacktivists**
- Common Cyber Threats to Banks
  - Corporate account takeover (web app attacks)
  - Crimeware - Advanced malware (typically introduced through phishing (email), or web)
  - ATM cash out scams/skimming
  - Denial of Service / Distributed Denial of Service

By Industry

2015 Verizon Data reach Investigation Report

	CRIMEWARE	CYBER-ESPIONAGE	DENIAL OF SERVICE	LOST AND STOLEN ASSETS	MISCELLANEOUS ERRORS	PAYMENT CARD SKIMMERS	POINT OF SALE	PRIVILEGE MISUSE	WEB APPLICATIONS
ACCOMMODATION	1%			1%	2%		91%	5%	1%
ADMINISTRATIVE		9%			27%			45%	18%
EDUCATIONAL	32%	15%		11%	26%			9%	9%
ENTERTAINMENT					13%		73%	7%	7%
FINANCIAL SERVICES	36%			2%	7%	14%		11%	31%
HEALTHCARE	1%	4%		16%	32%		12%	26%	9%
INFORMATION	14%	37%		2%	5%			7%	35%
MANUFACTURING	34%	60%						4%	1%
MINING		14%				7%		79%	
OTHER SERVICES		8%		25%	17%		8%	33%	8%
PROFESSIONAL	25%	52%		2%	10%		5%	4%	4%
PUBLIC	51%	5%		3%	23%			11%	6%
RETAIL	11%					10%	70%	3%	5%

What Banks Need to Know

1. Hackers increasingly have more than one motive and method of attack.
2. The use of memory scraping in data breaches has increased.
3. More cyber threat information is being shared, but there is a need for faster sharing.
4. Too many people still fall for phishing attacks.
5. Old software vulnerabilities are going unpatched.
6. Mobile malware is not statistically significant yet, but it's still a concern.
7. Ongoing Web app attacks point to a need for strong layered security approach.

American Banker Bank Technology News:
http://www.americanbanker.com/news/bank-technology/what-banks-need-to-know-from-verizons-comprehensive-breach-report-1073744-1.html

Examiners want Banks…

- Setting the tone from the top and building a security culture
- Identifying, measuring, mitigating, and monitoring risks
- Developing risk management processes commensurate with the risks and complexity of the institutions
- Aligning cybersecurity strategy with business strategy and accounting for how risks will be managed both now and in the future
- Creating a governance process to ensure ongoing awareness and accountability
- Ensuring timely reports to senior management that include meaningful information addressing the institution's vulnerability to cyber risks

How do you measure readiness?

Current Guidance Available

- FFIEC Cybersecurity Assessment Tool

- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)

Cybersecurity Assessment Tool

- Released in June 2015
- Consistent with the FFIEC Information Technology Examination Handbook and the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Two parts
  - Inherent Risk Profile
  - Cybersecurity Maturity

Inherent Risk Profile Categories

- Technology and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organization Characteristics
- External Threats

Select the most appropriate inherent risk level for each activity, service, or product

Figure 1: Inherent Risk Profile Layout

Risk Levels

Activity, Service, or Product

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

Inherent Risk Profile

- Based on the number of applicable statements in each risk level
- Evaluate each category and determine if it poses additional risk

Maturity Level Domains

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience

- Each domain contains:
  - Assessment factors
  - Contributing components

- Each component contains
  - Declarative Statements that describe an activity that supports the assessment factor at that level of maturity

Maturity Levels Defined

Maturity Levels Defined	
Baseline	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
Evolving	Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.
Intermediate	Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.
Advanced	Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
Innovative	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.

Maturity Levels

Domain

Maturity Level

Assessment Factor

Declarative Statement

Component

			Domain 1: Cyber Risk Management and Oversight
			Assessment Factor: Governance
		Y, N	
OVERSIGHT	Baseline		Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. *(FFIEC Information Security Booklet, page 3)* Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. *(FFIEC Information Security Booklet, page 5)* Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. *(FFIEC Information Security Booklet, page 5)* The budgeting process includes information security related expenses and tools. *(FFIEC E-Banking Booklet, page 20)* Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. *(FFIEC Business Continuity Planning Booklet, page J-12)*
	Evolving		At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity. Cybersecurity tools and staff are requested through the budget process. There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.

Analyzing Results

Cybersecurity Maturity Level for Each Domain	Inherent Risk Levels: Least	Minimal	Moderate	Significant	Most
Innovative					
Advanced					
Intermediate					
Evolving					
Baseline					

Next Steps

- Prepare remediation plans based on gaps identified during the assessment
- Report and communicate regulatory the status
- Reevaluate at least annually or update when there are changes

NIST Cybersecurity Framework

- President issued Executive Order 13636 on February 12, 2013
- NIST Framework for Improving Critical Infrastructure Cybersecurity version 1 publish on February 12, 2014
- Relies and maps to existing standards, guidelines, and practices
  - Describe their current cybersecurity posture
  - Describe their target state for cybersecurity
  - Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
  - Assess progress toward the target state
  - Communicate among internal and external stakeholders about cybersecurity
- Risk-based approach to managing cybersecurity

Framework Components

- Framework Core
  - Functions (Identify, Protect, Detect, Respond, Recover)
  - Categories (i.e. Access control)
  - Subcategories (i.e. Remote access is managed)
  - Information References
- Framework Implementation Tiers
  - Partial (Tier 1)
  - Risk Informed (Tier 2)
  - Repeatable (Tier 3)
  - Adaptive (Tier 4)
- Framework Profiles
  - Current
  - Target
  - Comparison
- Each Framework component reinforces the connection between business drivers and cybersecurity activities

NIST Core Framework

IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery planning
- Improvements
- Communications

Sample Framework Core

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	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3

Impact to other Risk Management Programs?

Vendor Management

- Enhanced Due Diligence and Ongoing Monitoring Activities
  - How do you vet, select and monitoring third party service providers
  - Vulnerability management (i.e. recent SSL vulnerabilities)
  - Integrating Incident Response Plans and Tests
  - Cyber insurance
  - Minimum security standards
  - Minimum vendor management standards (subcontractors)
  - Additional security control environment monitoring other than SOC reports (PCI ROC, PCI AOC, Pen Testing, independent secure code review, NIST CSF etc.)
  - Annual questionnaire
  - Annual review of internal audit plans

Vendor Management

- Contract language
  - Termination clauses
  - Right to audit (required remediation)
  - Require security control environment reports (see previous slide for examples)
  - Minimum security requirements (Encryption, event log retention, etc.)
  - BCP documentation and test results
  - Cyber insurance

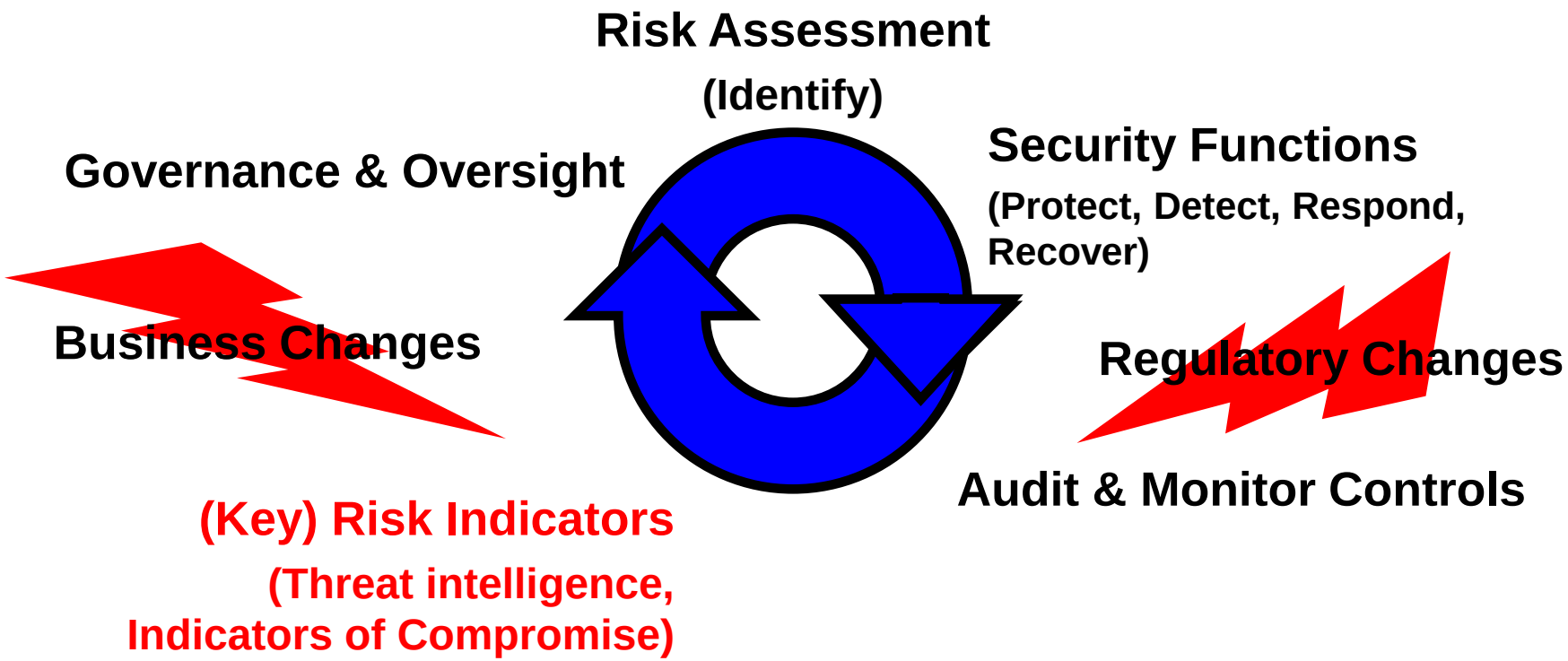
Enhancements To Your BCP

Not enough consideration made to preparing for cyber events

Unique factors of events:

- Customers/Clients affected by cyber incident
- Consideration for employee hit by ID Theft
- Third party providers/suppliers affected by cyber incident
- Transportation affected by cyber incident
- Remote working capabilities affected by cyber incident
  - Consider utilities and availability of employee homes
  - Plan for loss of personnel and key and backup locations for extended periods of time
- Cyber Incident Response Plans should be incorporated to BCP (Destructive malware)

ERM Life Cycle



Key Indicators of Compromise (IOC)

- Key IOC
  - What type of activity would indicate that you have a breach
  - Based on IT operations and processes
  - Security information and event management (SIEM)
    - Logging configuration
    - Correlate events from assets (servers, **workstations**, routers, IDS/IPS, etc…)
    - Network time protocol (NTP) synchronization
  - Incident Response Procedures
    - Known and common events
    - IOC
- Where can I measure IOC's
  - Online banking activity
  - Bank Network
  - Vendor's network (Bitsight)

Technologies to Consider

- Assuming you are blocking and tackling (i.e. patch management, antivirus, firewall, IDS/IPS, user management, configuration management)
  - Network Access Control (NAC)
  - Frequent Vulnerability scanning (at least monthly)
  - Application white listing / behavior analysis
  - Threat intelligence feeds
  - Minimum security standards
  - Next Generation Firewall

Important Resources

FFIEC Cybersecurity guidance-http://www.ffiec.gov/cybersecurity.htm

NIST Cybersecurity Framework-http://www.nist.gov/cyberframework/

Executive Order 13636-http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

FBI InfraGard-https://www.infragard.org/

U.S. Computer Emergency Readiness Team-https://www.us-cert.gov/

U.S. Secret Service Electronic Crimes Task Force-http://www.secretservice.gov/ectf.shtml

Department of Homeland Security-http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program

NY State Department of Financial Services Memo-https://www.njbankers.com/WCM/njbadocs/Operations%20Technology%20Committee/NY%20Cyber%20Security%20Exam%20Process.pdf

Important Resources - CATO

This page has a project tracking tool to track control implementation, sample presentations for bank employees, sample presentations for Bank customers, sample risk assessment, sample notice of fraudulent activity and addition resources: http://www.csbs.org/ec/cato/Pages/catotools.aspx

This page has a link on the bottom “Best Practices for Reducing the Risks of Corporate Account Takeovers” which will open a word document that explains the controls you should have in place in order to meet the layered security approach: http://www.csbs.org/ec/cato/Pages/catorecom.aspx

Questions

William Nowik, CISA, CISSP, QSA, PCIP
Principal IT Assurance Services
Phone: (617) 428-5469
Email: wnowik@wolfandco.com
LinkedIn: wnowik

www.wolfandco.com
www.wolfpacsolutions.com