Southeast Bankers Outreach Forum

High Priority Risks: *Cybersecurity*

Date: September 21, 2015

Presented by: Tony DaSilva, AAP, CISA

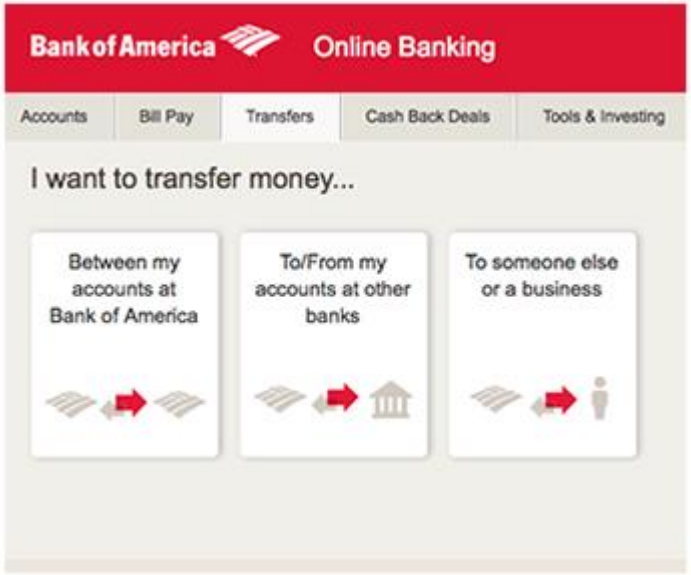
FEDERAL RESERVE BANK *of* ATLANTA

The opinions expressed are those of the presenter and are not those of the Federal Reserve Bank of Atlanta, the Federal Reserve System, or its Board of Governors.

TOPICS

- Electronic Banking
- Cybercrime
- Fraud
- Data Breaches
- Cybersecurity
- FFIEC “CAT”

ELECTRONIC BANKING



ELECTRONIC BANKING

- Account Activity
- Internal Transfers
- Bill Pay
- RDC
- ACH
- Wire Transfer
- External Transfers
- Mobile Payments
- New Accounts

OPPORTUNITY !

CYBERCRIME

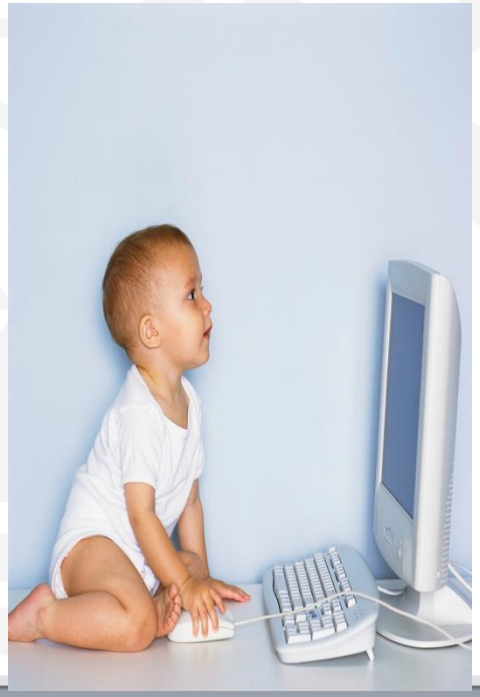
Cybercrime is a well-funded, organized business with sophisticated technology. It is driven by a powerful combination of actors ranging from organized crime, nation states, and decentralized cyber gangs. They executed recent massive credit card and identity data breaches, using this data to profit from all types of fraud—card not present, account takeover, and new account creation–across all businesses across all regions.

CYBERCRIME – WHERE & WHY?

- Where do cyber attacks come from?
- What is the motivation?
  - Ideology – making a political statement
  - Extortion – demand for payment to avoid website attack
  - Competition – disrupt a competitors online services
  - Fraud – used as a tool to aid in unauthorized financial gain

TRENDS

DENIAL OF SERVICE ATTACK



DoS & DDoS

WHAT IS A DENIAL OF SERVICE ATTACK?

- **Objective(s):**
  - **Render a service unavailable**
  - **Cripple the infrastructure**
- **Typical targets:**
  - **Bank**
  - **Credit card payment servicers**
- **Mode of attack: Saturate the target with external requests for connectivity or communication**

DISTRIBUTED DOS (DDOS)

- A DDoS attack is performed when hundreds, or possibly thousands, of computers simultaneously request services or bandwidth from the same target computer.
- The attack is executed with networks of computers which are controlled by malicious software which has been installed on a user's computer.
- The antivirus detection rate for botnet malware is less than 40 percent. For additional information, visit: https://zeustracker.abuse.ch/index.php.

DEVELOPING CONCERNS

- Bank service providers as possible future targets
- Overload of key service providers attempting to mitigate the effects of DDoS attacks
- Attacks moving down to banks of lower asset size and with potentially less capability for managing the attacks
- DDoS attacks being used as a diversion while fraudulent wire transfers are being transmitted

PAYMENTS CYBERCRIME

ACH & Wire Transfers

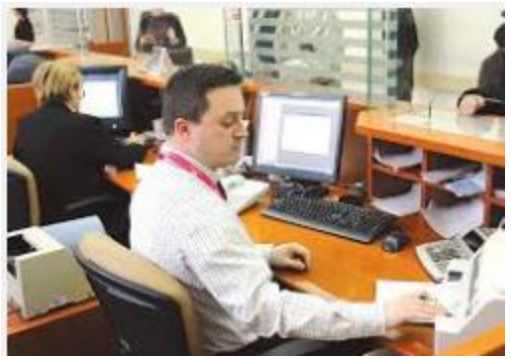
HOW DO CYBER CRIMINALS GAIN ACCESS?

- Deception via DDoS
- Spam
- Phishing attempts
- Spoofed web pages
- Popup ads and warnings
- Malware (Trojans, worms, etc.)
- Theft (laptops, thumb drives, etc.)
- Email attachments
- Downloads
- Social mediums

PROTECT THE BANK

From:

- Vendors
- Customers
- Employees



READILY AVAILABLE MAYHEM

- Botnet malware development kits are available for purchase over the internet.
- The most recent versions may cost less than two thousand dollars.
- Older versions can be obtained for a few hundred dollars or for free.
- Botnet administrators also lease their botnets on a per-project basis.
- The DDoS attack application software called Low Orbit Ion Cannon is available for free download from sourceforge.net.

JUST A FEW EXAMPLES

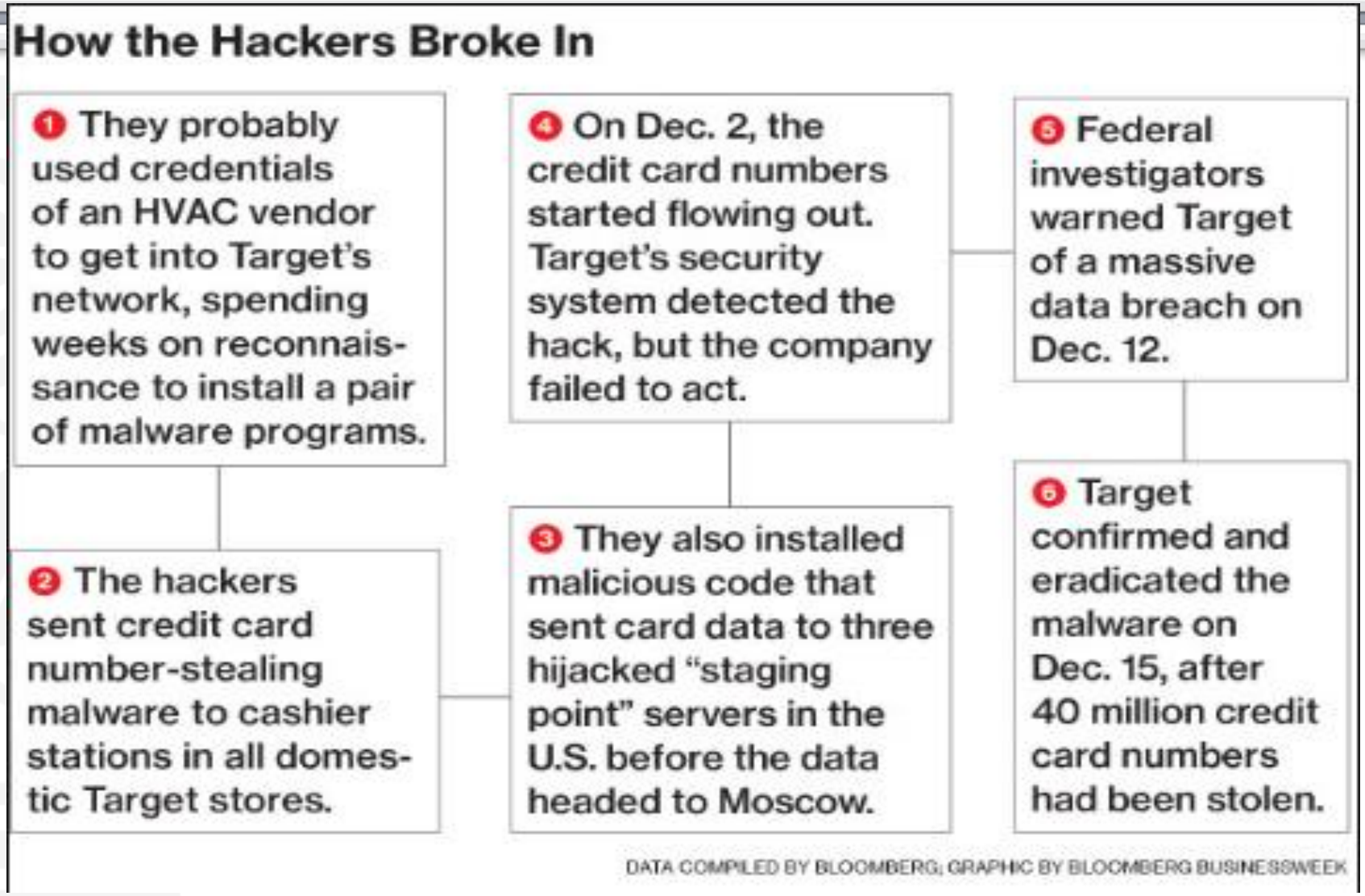
- SpyEye– A Zeus variant that "wakes-up" and steals credentials in real time.
- OddJob–Keeps online sessions open after logout by the user
- Tatanga– Caused a screen freeze or displays a "please wait" message as it conducts transactions in the background.
- Zeus Mitmo– Steals SMS one-time passwords via social engineering. Can utilize smishing to get user to download malware that forwards SMS messages
- Ramnit Worm – It was paired with source code from the Zeus botnet, and began targeting financial institution and has the ability to "bypass two-factor authentication and transaction signing systems."

VAWTRAK

- Banking malware strain known as Vawtrak, which compromises commonly used URLs by injecting them with code. This allows the hackers to steal online banking credentials as they are input on the bank's website.
- Vawtrak ranks as the "single most dangerous threat" among botnet-based cybercrime malware strains on the market today.
- While Vawtrak's crimeware-as-a-service model, better known as CaaS, has been around since about 2006, researchers say the crime rings that manage this type of service have perfected their techniques, affording them the ability to adapt their attacks for specific targets.
- Some of the most notable U.S. banking institutions that have been targeted by this attack so far include Bank of America, Wells Fargo, Capital One Financial Corp., Citigroup and JPMorgan Chase.

BANK INFO SECURITY®

DATA BREACHES


How the Hackers Broke In
1 They probably used credentials of an HVAC vendor to get into Target's network, spending weeks on reconnaissance to install a pair of malware programs.
2 The hackers sent credit card number-stealing malware to cashier stations in all domestic Target stores.
3 They also installed malicious code that sent card data to three hijacked "staging point" servers in the U.S. before the data headed to Moscow.
4 On Dec. 2, the credit card numbers started flowing out. Target's security system detected the hack, but the company failed to act.
5 Federal investigators warned Target of a massive data breach on Dec. 12.
6 Target confirmed and eradicated the malware on Dec. 15, after 40 million credit card numbers had been stolen.
DATA COMPILED BY BLOOMBERG; GRAPHIC BY BLOOMBERG BUSINESSWEEK

WHO

- **Law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses.**

- **Eastern European organized crimes groups are believed to be predominantly responsible for the activities that are also employing witting and unwitting accomplices in the United States (money mules) to receive, cash and forward payments from thousands to millions of dollars to overseas locations via popular money and wire transfer services.**

PROOF

- **Eastern Europe is proudly refining its reputation as the world's top cyber thief place of business, as a group of Russian thieves was accused Tuesday (Aug. 5, 2014) of what is possibly the largest high-tech swindle to date. The take? About 1.2 billion usernames and passwords in addition to more than 500 million E-mail addresses, according to a report in The New York Times.**

- **The haul included "confidential material gathered from 420,000 websites, including household names, and small Internet sites."**

The FBI's $3 million 'wanted' poster for Evgeniy Mikhailovich Bogachev.

How much money would it take for you to rat out a member of a Russian organized crime gang?

Russian Ring Blamed for Retail Breaches

by Tracy Kitten

A sophisticated hacking group in Eastern Europe with ties to banking Trojans like Carberp has now been linked to attacks waged against 16 U.S. retailers. Could U.S. banks be the next big targets?

BANK INFO SECURITY ENEWS

ENEWS@BANKINFOSECURITY.COM

FEBRUARY 16, 2015

Cybercrime Gang: Fraud Estimates Hit $1B

Experts Say Anunak/Carbanak Malware Attacks Still Underway

By Mathew J. Schwartz

A notorious cybercrime gang continues to target financial services firms and retailers. A new report estimates that the Anunak - a.k.a. Carbanak - gang has now stolen up to $1 billion from banks in Russia, the United States and beyond, in part by using "jackpotting" malware that infects ATMs and which attackers can use to issue cash from ATMs, on demand.

$1 MILLION STOLEN IN PAST MONTH

In a blog posted April 2, IBM senior threat researcher John Kuhn, notes that The Dyre Wolf malware has been used to steal more than $1 million from businesses within the past month.

What's so concerning about attacks waged with The Dyre Wolf malware is that they involve sophisticated social engineering and, in some cases, even distributed-denial-of-service attacks, security experts say.

It's also clear, they say, that the fraudsters behind The Dyre Wolf malware attacks are extremely knowledgeable about banking institutions' back-end systems and online-banking platforms.

ANTI-MALWARE TECHNOLOGIES USED TODAY

Signatures

- Traditionally, a characteristic sequence of bytes used to identify a particular piece of malware. But anti-malware solutions today make extensive use of generic signatures to detect large numbers of malware belonging to the same malware family.

Heuristic analysis

- This is used to detect new, unknown threats. It includes the use of a signature that identifies known malicious instructions, rather than a specific piece of malware. It also refers to the use of a sandbox (a secure virtual environment created in memory) to examine how the code will behave when it is executed on the real computer.

Behavioral analysis

- This involves monitoring the system in real time to see how a piece of code interacts with the computer. The more sophisticated system watchers don't just look at code in isolation, but track its activities across different sessions, as well as looking at how it interacts with other processes on the computer.

ANTI-MALWARE TECHNOLOGIES USED TODAY

Whitelisting

Historically, anti-malware solutions have been based on identifying code that is known to be malicious, i.e. 'blacklisting' programs. Whitelisting takes the opposite approach, blocking it if it is not in the list of acceptable programs.

Vulnerability scanning

Since cybercriminals make extensive use of vulnerabilities in applications, it makes sense to be able to identify those applications on a system that are vulnerable to attack, allowing businesses or individuals to take remedial action. Some solutions also include a real time scan of a computer, to block the use of zero-day vulnerabilities.

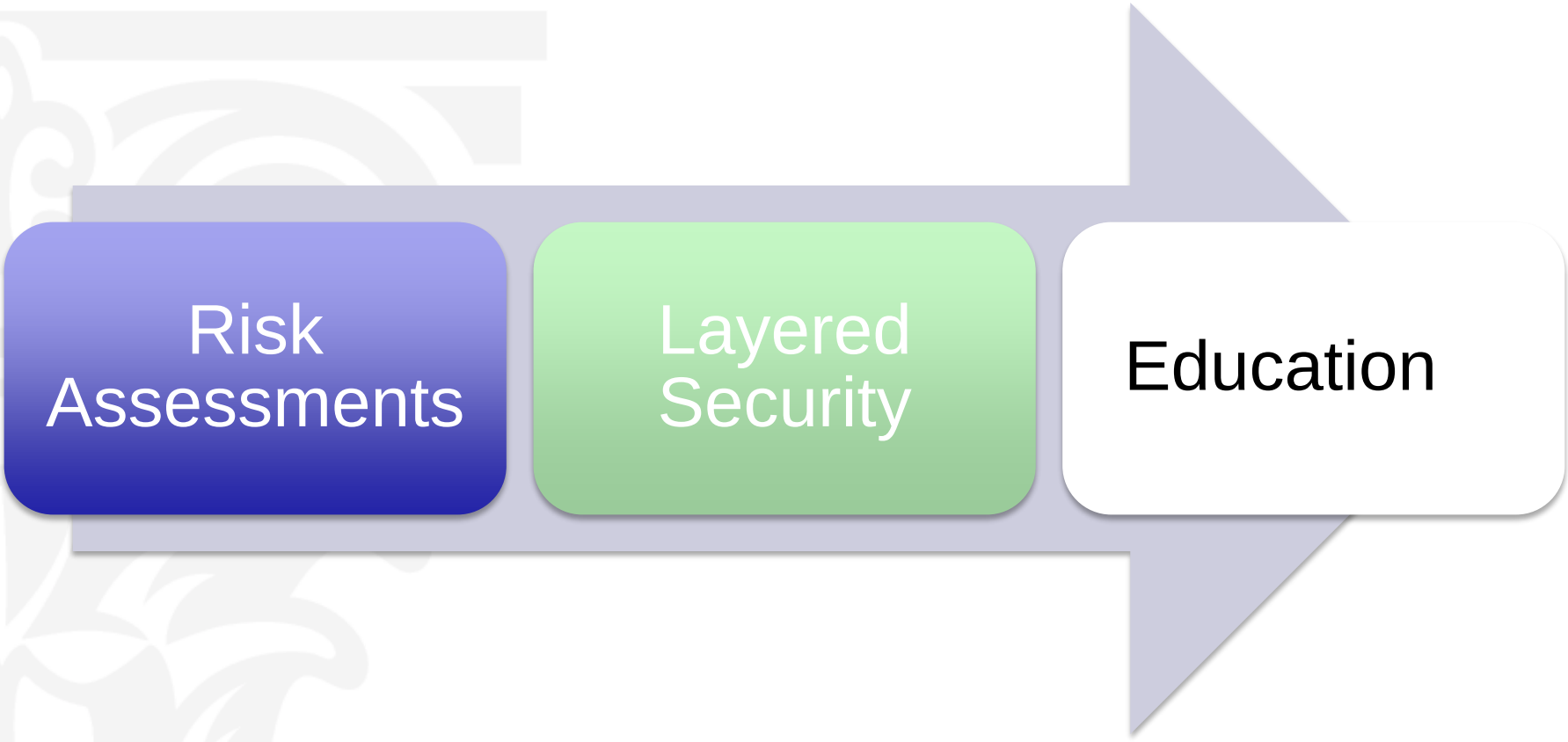
REGULATORY GUIDANCE

THE FFIEC GUIDANCE SUPPLEMENT

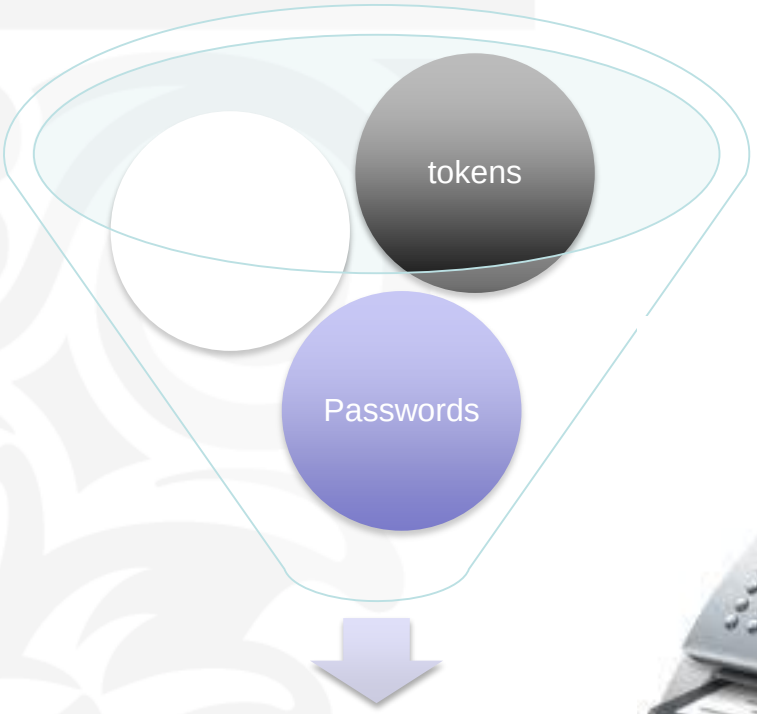
Effective 1/1/2012:

On June 28th, 2011 the Federal Financial Institutions Examination Council (FFIEC) released a supplement to the 2005 "Authentication in an Internet Banking Environment" guidance that describes the measures financial institutions should take to protect Internet banking customers from online fraud.

THREE PRIMARY REQUIREMENTS
FFIEC GUIDANCE – EFFECTIVE JANUARY 1, 2012



OUT-OF-BAND



SR 15-3 FEBRUARY 6, 2015
"STRENGTHENING THE RESILIENCE OF OUTSOURCED TECHNOLOGY SERVICES"

- ***Third-party management*** **addresses a financial institution's responsibility to control the business continuity risks associated with its TSPs and their subcontractors.**
- ***Third-party capacity*** **addresses the potential impact of a significant disruption on a third-party servicer's ability to restore services to multiple clients.**
- ***Testing with TSPs*** **addresses the importance of validating business continuity plans with TSPs and provides considerations for a robust third-party testing program.**
- ***Cyber resilience addresses aspects of BCP unique to disruptions caused by cyber events.***

CYBERSECURITY
FFIEC GUIDANCE

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

February 12, 2014

CYBERSECURITY

The process for managing cyber threats and vulnerabilities and for protecting information and information systems by identifying, defending against, responding to, and recovering from attacks.

CYBERSECURITY FRAMEWORK

The Framework Core consists of five concurrent & continuous functions:

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

SR 15-9
FFIEC CYBERSECURITY ASSESSMENT TOOL

Overview for Chief Executive Officers and Boards of Directors

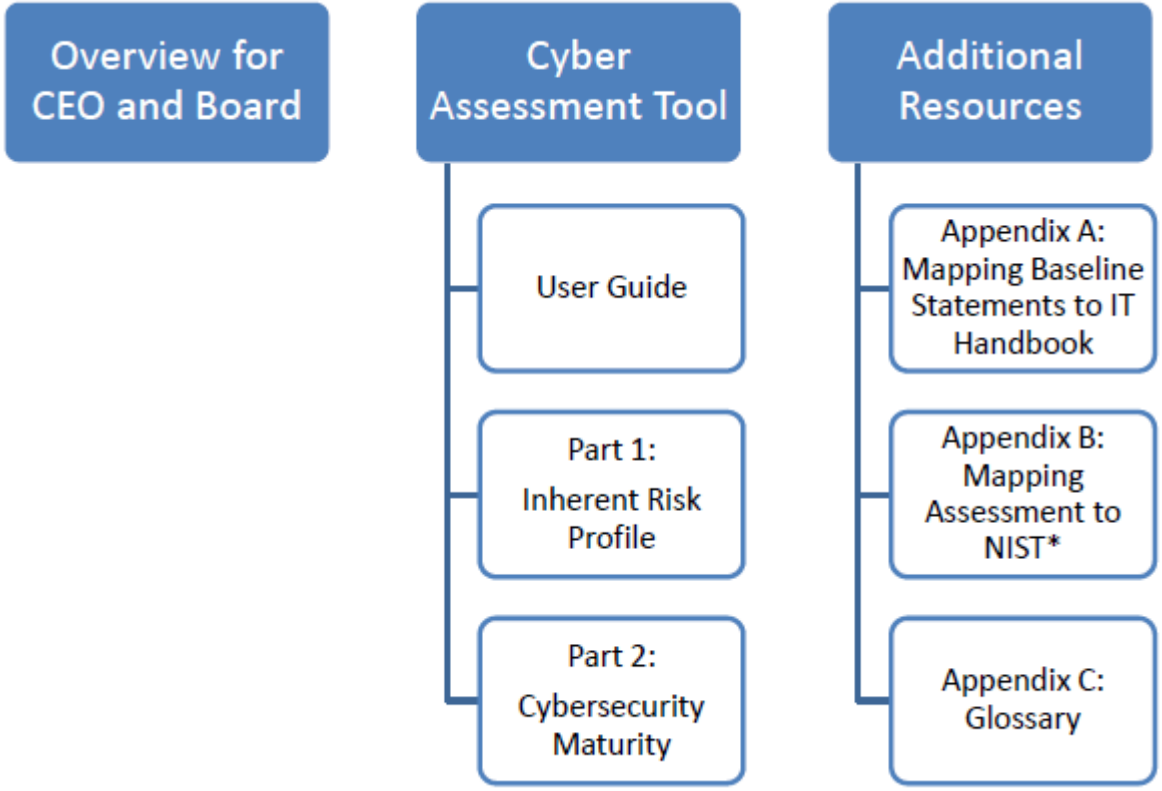
In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council(FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity preparedness. *The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time.* The Assessment incorporates cybersecurity-related principles from the *FFIEC Information Technology (IT) Examination Handbook* and regulatory guidance, and concepts from other industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

BENEFITS TO THE INSTITUTION

For institutions using the Assessment, management will be able to enhance their oversight and management of the institution's cybersecurity by doing the following:

- **Identifying factors contributing to and determining the institution's overall cyber risk.**
- **Assessing the institution's cybersecurity preparedness.**
- **Evaluating whether the institution's cybersecurity preparedness is aligned with its risks.**
- **Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.**
- **Informing risk management strategies.**

ASSESSMENT TOOL COMPONENTS



BOARD OF DIRECTORS

- Directors need to understand and approach as an ERM issue, not just an IT issue.
- Directors should understand the legal implications of cyber-risks
- Boards should have adequate access to cybersecurity expertise
- Discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda
- Directors should set the expectation that management will establish an enterprise wide, cyber-risk management framework
- Discussions of cyber-risks between boards and senior managers should include identification of which risks to avoid, accept, mitigate, or transfer.

CEO AND BOARD OF DIRECTORS - CAT

- Develop a plan to conduct the Assessment.
- Lead employee efforts during the Assessment to facilitate timely responses from across the institution.
- Set the target state of cybersecurity preparedness that best aligns to the board of directors' (board) stated (or approved) risk appetite.
- Review, approve, and support plans to address risk management and control weaknesses.
- Analyze and present results for executive oversight, including key stakeholders and the board, or an appropriate board committee.
- Oversee the performance of ongoing monitoring to remain nimble and agile in addressing evolving areas of cybersecurity risk.
- Oversee changes to maintain or increase the desired cybersecurity preparedness.

ASSESSMENT'S PARTS AND PROCESS

The Assessment consists of two parts:

1. **Inherent Risk Profile**
2. **Cybersecurity Maturity**

Upon completion of both parts, management can evaluate whether the institution's inherent risk and preparedness are aligned.

INHERENT RISK PROFILE –RISK CATEGORIES

Technologies and Connection Types

- Certain types of connections and technologies may pose a higher risk depending on the complexity and maturity, connections, and the nature of the specific technology products or services.

Delivery Channels

- Various delivery channels for products and services may pose a higher inherent risk depending on the nature of the specific product or service offered.

Online/Mobile Products and Technology Services

- Different products and technology services offered by institutions may pose a higher risk depending on the nature of the specific product or service offered.

Institution Characteristics

- The current size and strategic plans for institution growth may contribute to inherent risk.

External Threats

- The volume and type of attacks (attempted or successful) impact an institution's inherent risk exposure.

INHERENT RISK PROFILE –RISK LEVELS

Least Inherent Risk

- An institution with a Least Inherent Risk Profile generally has very limited use of technology, few computers, applications, systems, and no connections. The variety of products and services are limited.

Minimal Inherent Risk

- An institution with a Minimal Inherent Risk Profile generally has limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services.

Moderate Inherent Risk

- An institution with a Moderate Inherent Risk Profile generally uses technology that may be complex in terms of volume and sophistication.

Significant Inherent Risk

- An institution with a Significant Inherent Risk Profile generally uses complex technology in terms of scope and sophistication. The institution offers high-risk products and services that may include emerging technologies.

Most Inherent Risk

- An institution with a Most Inherent Risk Profile uses extremely complex technologies to deliver myriad products and services. Many of the products and services are at the highest level of risk, including those offered to other institutions. New and emerging technologies are utilized across multiple delivery channels.

Part 1: Inherent Risk Profile – Example 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 prototype (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 is logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; moderate 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)

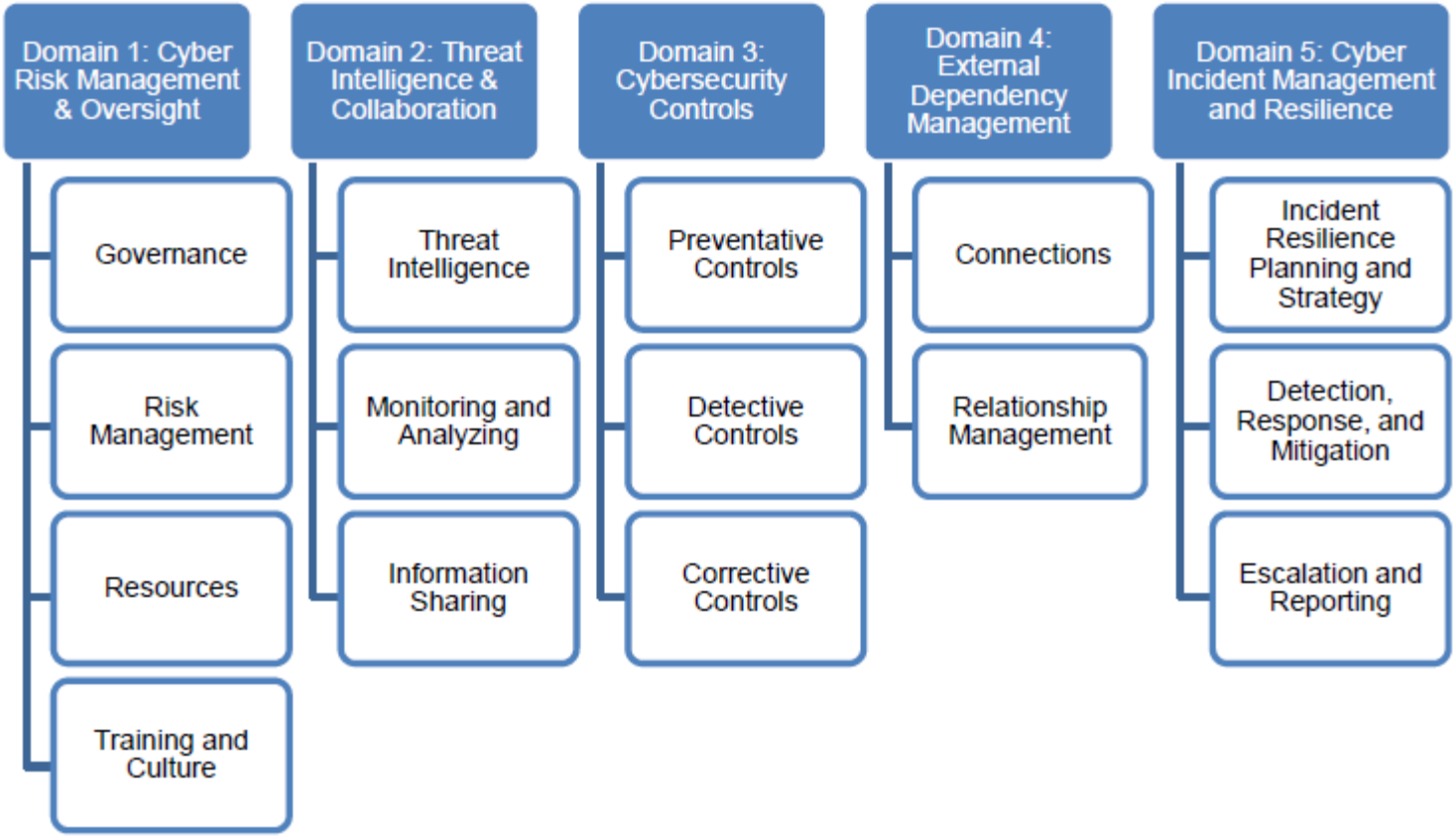
THE 5 DOMAINS

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

Note:

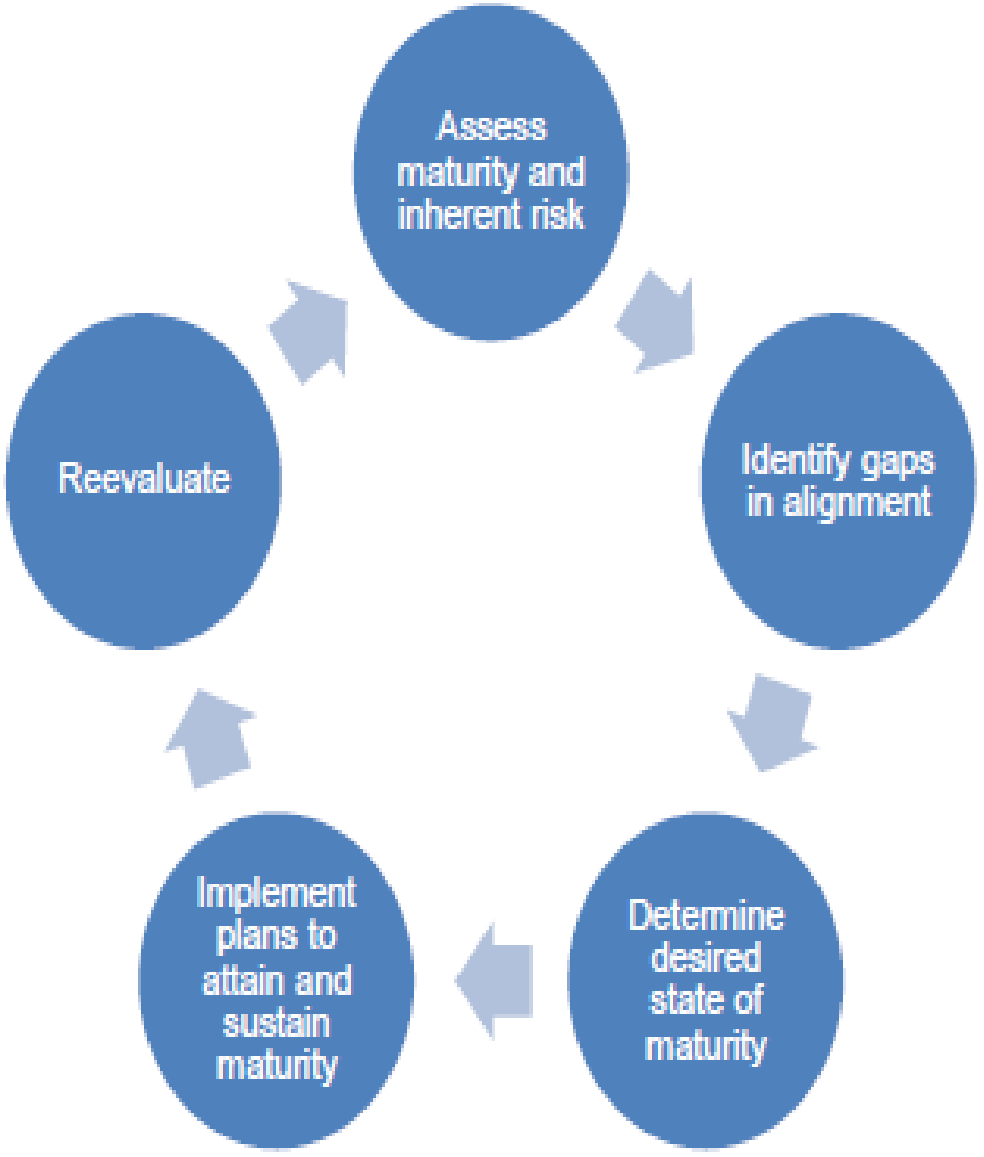
The domains include assessment factors and contributing components. Within each component, declarative statements describe activities supporting the assessment factor at each maturity level. Management determines which declarative statements best fit the current practices of the institution.

FIVE DOMAINS & ASSESSMENT FACTORS



STEPS

1. Complete Part One: Inherent Risk Profile
2. Complete Part Two: Cybersecurity Maturity Assessment
3. Determine appropriate target maturity level
4. Identify any gaps between current and desired states
5. Develop implementation plans based on identified gaps

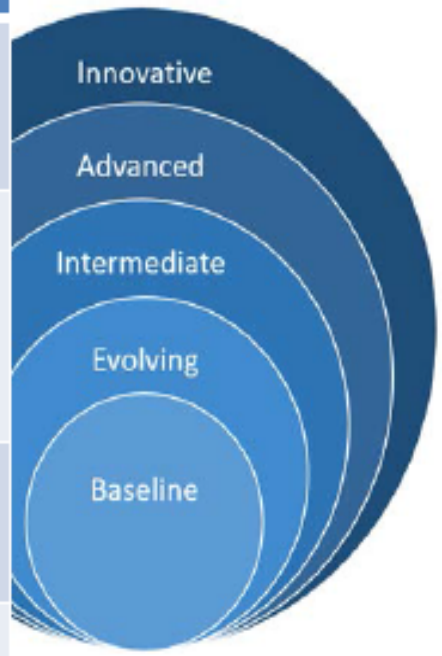


CYBERSECURITY MATURITY

- How effective are the institution's risk management activities and controls identified in the Assessment?
- Are there more efficient or effective means for attaining or improving the institution's risk management and controls?
- What third parties does the institution rely on to support critical activities?
- What is the process to oversee third parties and understand their inherent risks and cybersecurity maturity?
- How does management validate the type and volume of attacks?
- Is the institution sharing threat information with peers, law enforcement, and critical third parties through information-sharing procedures?

Maturity Assessment – Maturity Levels

Baseline	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in guidance. It includes compliance-driven objectives. Management has reviewed and evaluated guidance.
Evolving	Evolving maturity is characterized by additional formality of documented procedures and policies which 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 the lines of business. Risk management processes are automated and include continuous process improvement. Accountability for risk decisions by front-line businesses is formally assigned.
Innovative	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.



SIX-STEP CYBER THREAT INTELLIGENCE PROCESS FOR FINANCIAL INSTITUTIONS

1. Know your SPECIFIC threats and vulnerabilities.
2. *Establish outside sources of threat intelligence for your threats.*
3. Actively and continuously adjust your security controls and monitoring as appropriate to mitigate those threats.
4. Have detailed incident plans for responses to the threats, and update these plans periodically as appropriate.
5. Actively adjust your intelligence-gathering goals to address the changes in your threats and risks.
6. Additionally conduct a cyber threat analysis as part of your overall risk management governance and compliance program.

THREAT INTELLIGENCE INFORMATION SOURCES

Government and Institutional Resources

- Federal Bureau of Investigation (FBI)
  - Infragard
- United States Secret Service (USSS)
  - Electronic Crimes Task Force
- Department of Homeland Security (DHS)
  - United States Computer Emergency Readiness Team (US-CERT)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Financial Crimes Enforcement Network (FinCEN)
- Common Vulnerability Enumeration Database (CVE)
- National Vulnerability Database

Sector, Industry and Technology-Focused Resources

- Financial Services-Information Sharing and Analysis Center (FS-ISAC)
- Competitors, partners, and financial industry associations
- Industry news sites, e.g. krebsonsecurity.com, bankinfosecurity.com
- Information security sector sites, e.g. Internet Storm Center, Open Threat Exchange (OTX), ATLAS
- Managed security service providers (MSSPs) – blogs and feeds

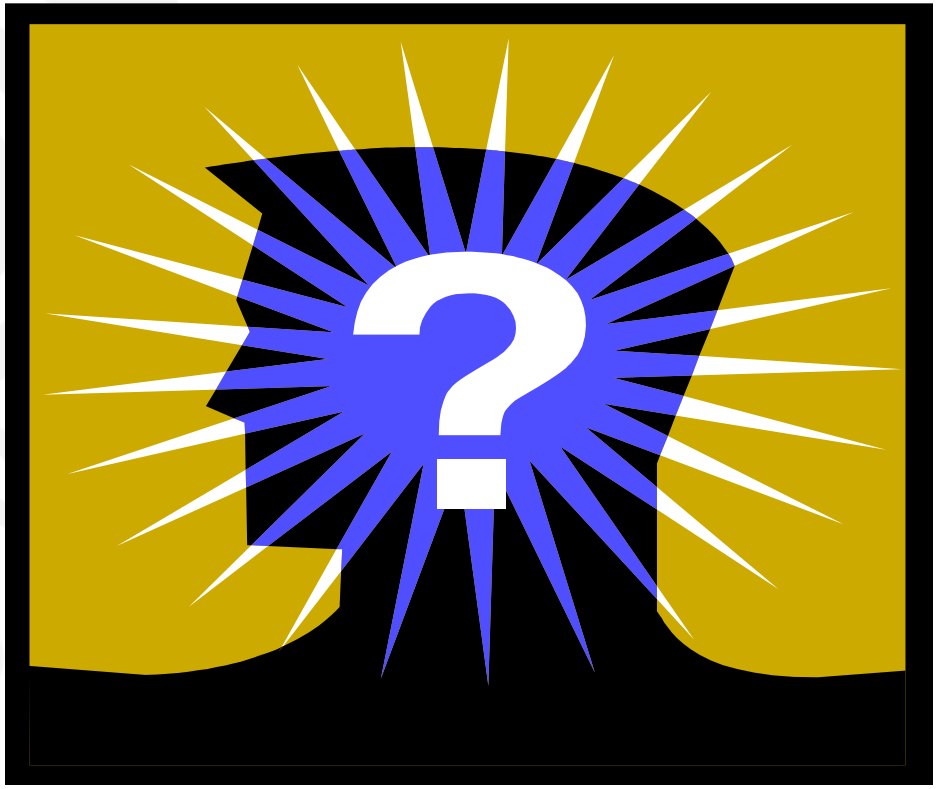
FFIEC Cyber Security

- Main Site: https://www.ffiec.gov/cybersecurity.htm
- Board/Senior Management Video: http://youtu.be/t1ZgWKjynXI
- Observations: https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf

SUMMARY

- Understand your inherent risk relating to cybersecurity
- Monitor and manage sufficient awareness of continuing and emerging threats and vulnerabilities
- Ensure you have established a dynamic control environment
- Understand the responsibilities of third parties and manage them effectively
- Test your BCP and DR plans against cybersecurity scenarios
- Involve the Board of Director and Senior Management to provide oversight

QUESTIONS



DOMAIN DEFINITIONS

GOVERNANCE

The Cyber Governance, Leadership and Resources domain focuses on whether management has implemented oversight and accountability, policies, procedures, and controls that will effectively prevent and detect internal and external cyber threats. Governance, leadership, and resource management are the foundation of a robust cyber risk management program. In order to be able manage the ever changing threat landscape, organizations will need to identify the necessary metrics, monitoring and reporting mechanisms to provide for sustained improvement in preventative and detective controls.

CULTURE & TRAINING

The purpose of Security Culture & Training is to ensure employees and third parties (i.e. customers, third party providers) understand cybersecurity and to promote individual awareness and to foster a culture where cybersecurity is integrated into all aspects of the financial institution. The extent of cybersecurity and cyber risk training should aid staff in self-identifying cyber risks. Cybersecurity must be seen as part of core business and not as something added to existing tasks. Cybersecurity needs to be everyone's responsibility in an organization. On-going targeted training must be provided to staff and management at all levels to increase enterprise awareness.

RISK MANAGEMENT

The purpose of Cyber Risk Management is to identify, analyze, and mitigate cyber-security threats and risks to critical information and technology assets and services. Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. Organizations can then determine the acceptable level of risk for delivery of services, i.e., their risk tolerance.

CYBER RESILIENCE

Cyber Resilience is crucial because it reflects an institution's ability to prevent an impact from, or recover systems and processes following, cyber incidents of all types and levels of impact. If cyber resilience is not properly managed, a financial institution's recovery from a cyber incident may be unnecessarily delayed, may lead to financial and legal repercussions, or the inability to recover at all. Cyber resilience is derived from the maturity and integration of the individual disciplines of crisis management, incident response, business continuity, and disaster recovery. A primary objective is to minimize service disruptions to a financial institution's critical and public facing systems, and to effectively contain such incidents.

CYBERSECURITY CONTROLS

Institutions must vigorously defend their networks and systems from a variety of internal and external threats. They must also be prepared to detect and prevent damaging follow-on attack activities inside a network that has already been compromised. The goal of such controls is to protect critical assets, infrastructure, and information by strengthening a bank's defensive posture through continuous, automated protection and monitoring of information technology infrastructure to reduce exploits and minimize the need for recovery efforts.

EXTERNAL DEPENDENCY

Identifying dependencies involves establishing and maintaining a comprehensive understanding of the key external relationships required for the delivery of the function. Managing dependency risk includes approaches, such as independent testing, access review, scanning for vulnerabilities, and reviewing demonstrable evidence from the third party that a secure process (to include connectivity) has been established and is being followed. Contracts binding the utility to a relationship with a partner or vendor for products or services should be reviewed and approved for cybersecurity risk mitigation, such as contract language that establishes vendor responsibilities for meeting or exceeding specified cybersecurity standards or guidelines. Service level agreements can specify monitoring and audit processes to verify that vendors and service providers meet cybersecurity and other performance measures.

VULNERABILITY MANAGEMENT

Vulnerability management is a risk management approach to identifying vulnerabilities within an organization's operating environment and mitigating threats and exploits against the organization. Vulnerabilities are most often thought as an unintentional software flaws, however vulnerabilities can be represented by flaws with technical infrastructure, business processes, and human resource behavior and third-party relationships. A vulnerability management program provides the ability to identify, analyze, prioritize and remediate/mitigate vulnerabilities to minimize the risk to the organization. A critical component of a vulnerability management program is patch management which address flaws within the computer software operated by the organization. The identification, analysis and application of software patches helps close existing vulnerabilities or "holes" within a particular software program that could otherwise be exploited by an attacker. Another key component of a vulnerability management program is testing.

INCIDENT MANAGEMENT

The purpose of Cyber Incident Management is to establish processes to identify,, analyze cyber events, and determine an organizational response. Cybersecurity incident management involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events. Computer security incident management is a specialized form of incident management, the primary purpose of which is the development of a well understood and predictable response to damaging events and cyber events. Cyber incident management is an administrative function of responding to cyber events that can affect computer assets, networks and information systems.

THREAT INTELLIGENCE

The purpose of Threat Intelligence & Collaboration is to actively discover and analyze information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture. Sound relationships with security experts in relevant government and private sector organizations can serve as avenues for obtaining best practices, current and emerging threat information, and potential software and hardware vulnerabilities. Information sharing as such should build good on-going relationships that continue both in "peace time" and "war time", which builds trust. This would help to gather information about potential cyber-attacks; and also, in the event of a cyber incident, timely communication with stakeholders, in particular with relevant authorities, would be of critical importance.

FOR MORE INFORMATION

FBI Alert: Fraudulent ACH Transfers

http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm

FDIC Special Alert: Fraudulent Electronic Funds Transfers

http://www.fdic.gov/news/news/SpecialAlert/2009/sa09147.html

FDIC Special Alert SA-185-2009 Fraudulent Funds Transfer Schemes

http://www.fdic.gov/news/news/SpecialAlert/2009/sa09185.html

NACHA Bulletin: Corporate Account Takeovers

http://www.nacha.org/docs/NACHA%20Operations%20Bulletin%20-%20Corporate%20Account%20Takeover%20-%20December%202,%202009.pdf

FOR MORE INFORMATION

- FFIEC IT Handbooks
  http://ithandbook.ffiec.gov
- FFIEC Cybersecurity Awareness Web Site
  http://ffiec.gov/cybersecurity.htm
- Financial Stability Oversight Council 2015 Annual Report
  http://www.treasury.gov/initiatives/fsoc/studies-reports/Pages/2015-Annual-Report.aspx
- The FDIC's "Cyber Challenge: A Community Bank Cyber Exercise"
  http://www.fdic.gov/regulations/resources/director/technical/cyber/cyber/htm
- Financial Services-Information Sharing and Analysis Center (FS-ISAC) www.fsisac.com/
- United States Computer Emergency Readiness Team (US-CERT)
  www.us-cert.gov/
- InfraGard
  www.infragard.org/
- U.S. Secret Service Electronic Crimes Task Force www.secretservice.gov/ectf.shtml
- The Top Cyber Threat Intelligence Feeds
  www.thecyberthreat.com/cyber-threat-intelligence-feeds/

REGULATORY GUIDANCE

- SR 15-3: Strengthening the Resilience of Outsourced Technology Services
- SR 15-9: FFIEC Cybersecurity Assessment Tool
- SR 12-14: Revised Guidance on Supervision of Technology Service Providers
- SR 11-9: Interagency Supplement to Authentication in an Internet Banking Environment
- SR 09-2: FFIEC Guidance Addressing Risk Management of Remote Deposit Capture
- SR 06-13: Q&A Related to Interagency Guidance on Authentication in an Internet Banking Environment

REGULATORY GUIDANCE CONTINUED

- SR 05-23: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- SR 05-19: Interagency Guidance on Authentication in an Internet Banking Environment
- FFIEC Risk Management of Remote Deposit Capture
- FFIEC Information Security Booklet
- SR 01-15: Standards for Safeguarding Customer Information
- SR 01-11: Identity Theft and Pretext Calling—(attachment) Interagency Guidelines Establishing Standards for Safeguarding Customer Information

VENDOR RESOURCES & REFERENCES

- Trusteer
- ThreatMetrix
- Akamai
- enews@bankinfosecurity.com