What to Expect At Your Next Regulatory Exam

Tony DaSilva, AAP, CISA
Federal Reserve Bank of Atlanta

The opinions expressed are those of the presenters and are not those of the Federal Reserve Banks, the Federal Reserve System, or its Board of Governors.

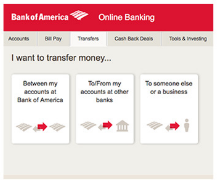
Topics

- ❖ Electronic Banking
- ❖ Payments
- ❖ Cybercrime
- ❖ Fraud
- ❖ Cybersecurity
- ❖ FFIEC “CAT” Tool
- ❖ FFIEC Payments
- ❖ Updated InTREx

2

Electronic Banking

Now and the Future (*No Going Back)*



Bank of America Online Banking

Accounts | Bill Pay | Transfers | Cash Back Deals | Tools & Investing

I want to transfer money...

Between my accounts at Bank of America

To/From my accounts at other banks

To someone else or a business

3

Electronic Banking

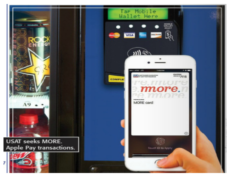
- ❖ Account Activity
- ❖ Internal Transfers
- ❖ Bill Pay
- ❖ RDC
- ❖ ACH
- ❖ Wire Transfer
- ❖ External Transfers
- ❖ Mobile Payments
- ❖ New Accounts
  - ❖ Deposits, Loans, (Fintech), etc.

4

Retail Payments

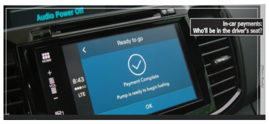
- ➢ Checks/Remote Deposit Capture
- ➢ Remotely Created Checks
- ➢ ACH FedACH® Services
- ➢ Card Products (Debit, Credit, Stored Value)
- ➢ Merchant Acquiring VISA MasterCard
- ➢ Mobile Financial Services

5



PAYMENT DEVICE TYPES

Device-wise, digital payments today are mainly performed with card, smartphone, tablet or PC. Joining these will be the emerging new category of wearable devices – such as smart watches and contactless wristbands.



In-car payments:
Who'll be in the driver's seat?

6

FIS
(NYSE: FIS)
D+H
EBANQ
Automated Systems, Inc
NexorONE
jack henry & ASSOCIATES INC.
TEMENOS
fiserv.

OPPORTUNITY!

FOR COMMUNITY BANKS

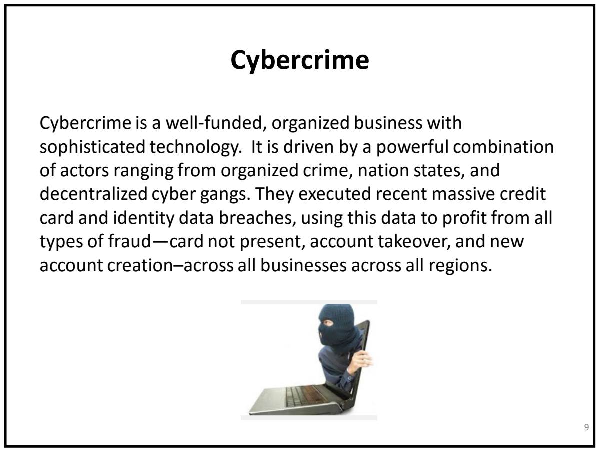
7

CYBER CRIME

Also an OPPORTUNITY !

Bad guys follow the path of least resistance and most profit.

8



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.

9

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

Threats & Consequences

- Third Party, Vendor, and Cloud
- Malware
- Ransomware
- Data Corruption
- Data Destruction
- Distributed Denial of Service (DDoS)
- Payment Account Takeovers
- Mobile Application Vulnerabilities
- Social Engineering

Trends

Ongoing Concerns

- ❖ Bank service providers as continued targets ✓
- ❖ Overload of key service providers attempting to mitigate the effects of DDoS attacks ✓
- ❖ Attacks moving down to banks of lower asset size with potentially less capability for managing the attacks ✓
- ❖ DDoS attacks being used as a diversion while fraudulent wire transfers are being transmitted (and other fraudulent/malicious transactions) ✓

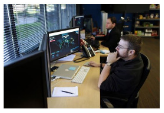
Payments Cybercrime

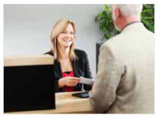
ACH & Wire Transfers

Protect the Bank

From:

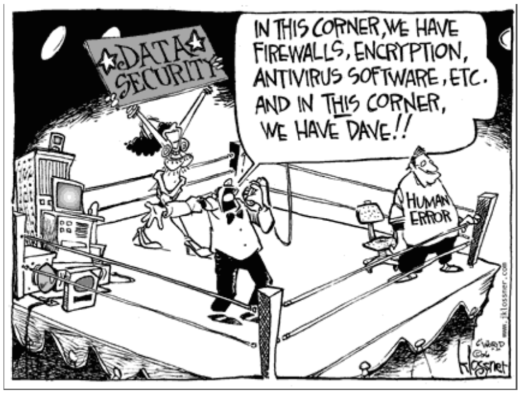
- ❖ Vendors
- ❖ Customers
- ❖ Employees





People the Weak Link

- ❖Whether they come from email, the web, social media, or mobile apps, today's cyber attacks have one thing in common—they all target people.
- ❖Cyber criminals have shifted tactics. Rather than relying solely on technical exploits, today's attacks fool humans into becoming unwitting accomplices, infecting systems, stealing credentials, and transferring funds.

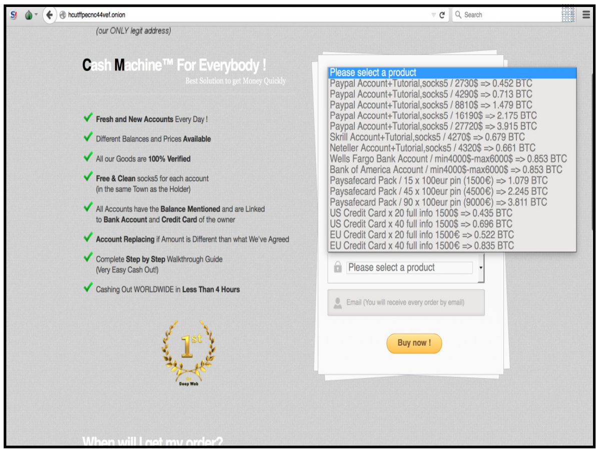

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

Dark Web

THE TOR DARK WEB MAY BE REFERRED TO AS ONIONLAND.

TOR

Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms".



(our ONLY legit address)

Cash Machine™ For Everybody !

Best Solution to get Money Quickly

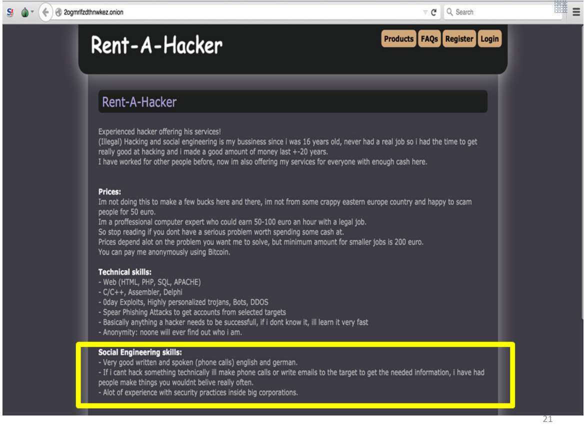
- ✓ **Fresh and New Accounts** Every Day !
- ✓ Different Balances and Prices **Available**
- ✓ All our Goods are **100% Verified**
- ✓ **Free & Clean** socks5 for each account (in the same Town as the Holder)
- ✓ All Accounts have the **Balance Mentioned** and are Linked to **Bank Account** and **Credit Card** of the owner
- ✓ **Account Replacing** if Amount is Different than what We've Agreed
- ✓ Complete **Step by Step** Walkthrough Guide (Very Easy Cash Out!)
- ✓ Cashing Out WORLDWIDE in **Less Than 4 Hours**

Please select a product
Paypal Account+Tutorial,socks5 / 2730$ => 0.452 BTC
Paypal Account+Tutorial,socks5 / 4290$ => 0.713 BTC
Paypal Account+Tutorial,socks5 / 8810$ => 1.479 BTC
Paypal Account+Tutorial,socks5 / 16190$ => 2.175 BTC
Paypal Account+Tutorial,socks5 / 27720$ => 3.915 BTC
Skrill Account+Tutorial,socks5 / 4270$ => 0.679 BTC
Neteller Account+Tutorial,socks5 / 4320$ => 0.661 BTC
Wells Fargo Bank Account / min4000$-max6000$ => 0.853 BTC
Bank of America Account / min4000$-max6000$ => 0.853 BTC
Paysafecard Pack / 15 x 100eur pin (1500€) => 1.079 BTC
Paysafecard Pack / 45 x 100eur pin (4500€) => 2.245 BTC
Paysafecard Pack / 90 x 100eur pin (9000€) => 3.811 BTC
US Credit Card x 20 full info 1500$ => 0.435 BTC
US Credit Card x 40 full info 1500$ => 0.696 BTC
EU Credit Card x 20 full info 1500€ => 0.522 BTC
EU Credit Card x 40 full info 1500€ => 0.835 BTC

Please select a product

Email (You will receive every order by email)

When will I get my order?



Rent-A-Hacker

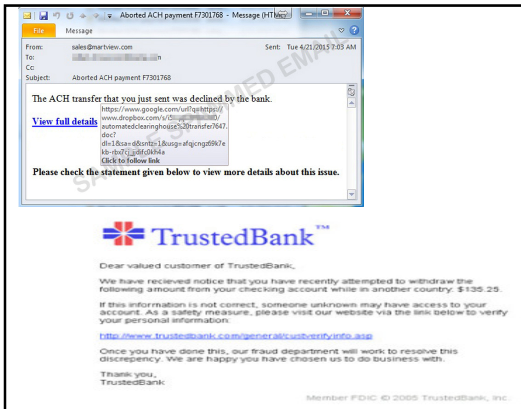
Rent-A-Hacker

Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my bussiness since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
I have worked for other people before, now im also offering my services for everyone with enough cash here.

Prices:
Im not doing this to make a few bucks here and there, im not from some crappy eastern europe country and happy to scam people for 50 euro.
Im a proffessional computer expert who could earn 50-100 euro an hour with a legal job.
So stop reading if you dont have a serious problem worth spending some cash at.
Prices depend alot on the problem you want me to solve, but minimum amount for smaller jobs is 200 euro.
You can pay me anonymously using Bitcoin.

Technical skills:
- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successfull, if i dont know it, ill learn it very fast
- Anonymity: noone will ever find out who i am.

Social Engineering skills:
- Very good written and spoken (phone calls) english and german.
- If i cant hack something technically ill make phone calls or write emails to the target to get the needed information, i have had people make things you wouldnt belive really often.
- Alot of experience with security practices inside big corporations.



Aborted ACH payment F7301768 - Message (HTML)

From: sales@martview.com
Sent: Tue 4/21/2015 7:03 AM
To: [redacted]
Cc:
Subject: Aborted ACH payment F7301768

The ACH transfer that you just sent was declined by the bank.

View full details

https://www.google.com/url?q=https://www.dropbox.com/s/i5[redacted]0/automatedclearinghouse%20transfer7647.doc?dl=1&sa=d&sntz=1&usg=afqjcngz69k7ekb-rbx7cj_jjdifc0kh4a
Click to follow link

Please check the statement given below to view more details about this issue.

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

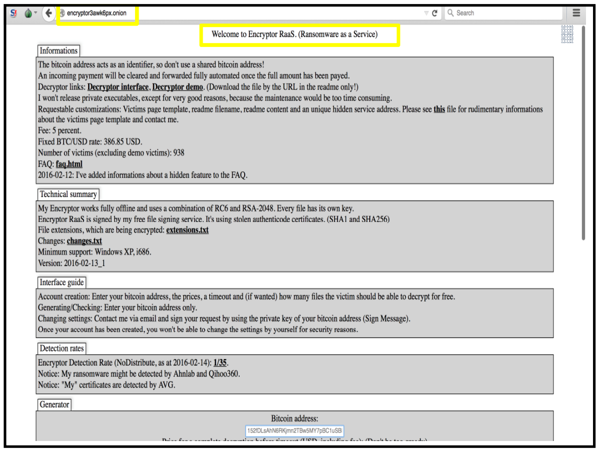
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Ransomware

- Ransomware can:

❖ Prevent you from accessing Windows.
❖ Encrypt files so you can't use them.
❖ Stop certain apps from running (like your web browser).
❖ Ransomware will demand that you pay money (a "ransom") to get access to your PC or files. We have also seen them make you complete surveys.
❖ There is no guarantee that paying the fine or doing what the ransomware tells you will give access to your PC or files again.



Welcome to Encryptor RaaS. (Ransomware as a Service)

Informations

The bitcoin address acts as an identifier, so don't use a shared bitcoin address!
An incoming payment will be cleared and forwarded fully automated once the full amount has been payed.
Decryptor links: **Decryptor interface**, **Decryptor demo**. (Download the file by the URL in the readme only!)
I won't release private executables, except for very good reasons, because the maintenance would be too time consuming.
Requestable customizations: Victims page template, readme filename, readme content and an unique hidden service address. Please see **this** file for rudimentary informations about the victims page template and contact me.
Fee: 5 percent.
Fixed BTC/USD rate: 386.85 USD.
Number of victims (excluding demo victims): 938
FAQ: **faq.html**
2016-02-12: I've added informations about a hidden feature to the FAQ.

Technical summary

My Encryptor works fully offline and uses a combination of RC6 and RSA-2048. Every file has its own key.
Encryptor RaaS is signed by my free file signing service. It's using stolen authenticode certificates. (SHA1 and SHA256)
File extensions, which are being encrypted: **extensions.txt**
Changes: **changes.txt**
Minimum support: Windows XP, i686.
Version: 2016-02-13_1

Interface guide

Account creation: Enter your bitcoin address, the prices, a timeout and (if wanted) how many files the victim should be able to decrypt for free.
Generating/Checking: Enter your bitcoin address only.
Changing settings: Contact me via email and sign your request by using the private key of your bitcoin address (Sign Message).
Once your account has been created, you won't be able to change the settings by yourself for security reasons.

Detection rates

Encryptor Detection Rate (NoDistribute, as at 2016-02-14): **1/35**.
Notice: My ransomware might be detected by Ahnlab and Qihoo360.
Notice: "My" certificates are detected by AVG.

Generator

Bitcoin address:
152fDLsAhN6RKjmn2TBw5MY7pBC1uSB

2016 Bangladesh Bank Heist

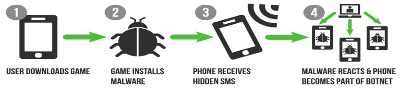
In February 2016, instructions to steal US$951 million from Bangladesh Bank, the central bank of Bangladesh, were issued via the SWIFT network. Five transactions issued by hackers, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20 million traced to Sri Lanka (since recovered) and $81 million to the Philippines (about $18 million recovered). The Federal Reserve Bank of NY blocked the remaining thirty transactions, amounting to $850 million, at the request of Bangladesh Bank. It was identified later that Dridex malware was used for the attack.[

Dridex

- Investigators have linked malware used by Russian and eastern European cybergangs to a string of bank heists that culminated in the record-breaking theft of US$81 million from Bangladesh's central bank. The gangs operate in Russia and former parts of the Soviet Union, including Moldova and Kazakhstan.
- Dridex, which is used to identify the malware and the group that uses it, is spread through e-mail that infiltrate computers and harvest information like user names and passwords which are used to gain access to privileged networks.
- First spotted in 2014, Dridex is one of the most serious online threats facing consumers and businesses, said security firm Symantec. The disciplined and highly organized gang behind the malware operates in many ways like an ordinary company, following a Monday-to-Friday work week and even taking time off for Christmas.

The Next Risk: Mobile Malware

- **Mobile malware has been growing in popularity:**
  - Primarily targets Android platform.
  - Some early attacks were against BlackBerry.
- **Malware for attacker financial gain:**
  - Simple message service (SMS) to premium-rate-short code, bills victim (up to $50/message).
  - Zeus Trojan intercepts SMS messages for banking authentication systems.
- **Malware for advertising delivery (search engine poisoning)**
- **Malware for location tracking and piracy attacks**


1
USER DOWNLOADS GAME
2
GAME INSTALLS MALWARE
3
PHONE RECEIVES HIDDEN SMS
4
MALWARE REACTS & PHONE BECOMES PART OF BOTNET

Source: Trustwave, Inc.

Regulatory Guidance
&
Updated InTREx Examination Program

Cybersecurity

FFIEC Guidance

Federal Financial Institutions Examination Council

SR 15-9
FFIEC Cybersecurity Assessment Tool

Overview for Chief Executive Officers and Boards of Directors

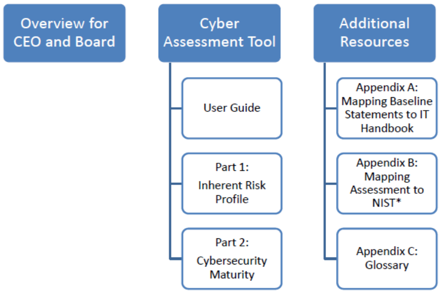
In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council(FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity preparedness. *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



Overview for CEO and Board

Cyber Assessment Tool

- User Guide
- Part 1: Inherent Risk Profile
- Part 2: Cybersecurity Maturity

Additional Resources

- Appendix A: Mapping Baseline Statements to IT Handbook
- Appendix B: Mapping Assessment to NIST*
- Appendix C: Glossary

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.

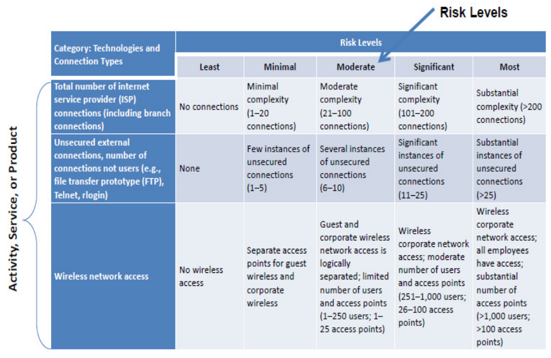
Significant Inherent Risk

- 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)

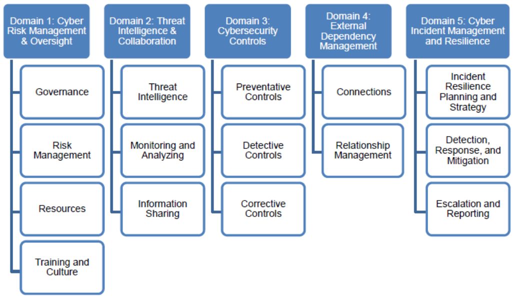
The 5 Domains

- ❖ 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.

37

Five Domains & Assessment Factors

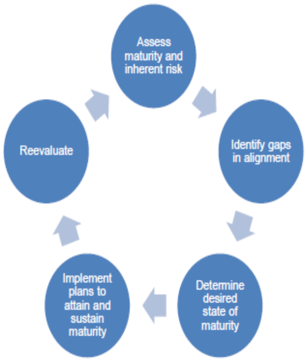


- Domain 1: Cyber Risk Management & Oversight
  - Governance
  - Risk Management
  - Resources
  - Training and Culture
- Domain 2: Threat Intelligence & Collaboration
  - Threat Intelligence
  - Monitoring and Analyzing
  - Information Sharing
- Domain 3: Cybersecurity Controls
  - Preventative Controls
  - Detective Controls
  - Corrective Controls
- Domain 4: External Dependency Management
  - Connections
  - Relationship Management
- Domain 5: Cyber Incident Management and Resilience
  - Incident Resilience Planning and Strategy
  - Detection, Response, and Mitigation
  - Escalation and Reporting

38

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



Assess maturity and inherent risk

Identify gaps in alignment

Determine desired state of maturity

Implement plans to attain and sustain maturity

Reevaluate

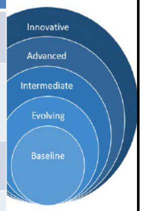
39

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?

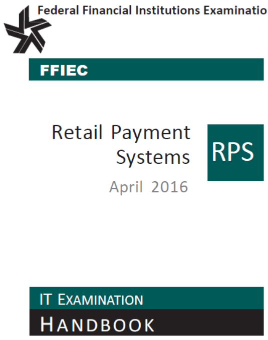
Maturity Assessment – Maturity Levels

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.



Federal Financial Institutions Examination Council

FFIEC

Retail Payment Systems

April 2016

RPS

IT EXAMINATION HANDBOOK

FFIEC Retail Payment Systems Examination Handbook

- Revised April 2016
- The FFIEC IT Examination Handbook (IT Handbook), "Retail Payment Systems Booklet" (booklet), provides guidance to examiners, financial institutions, and technology service providers (TSPs) on identifying and controlling risks associated with retail payment systems and related banking activities.

Financial Institutions

- Financial institutions accept, collect, and process a variety of payment instruments and participate in clearing and settlement systems. In some cases, financial institutions perform all of these tasks.
- However, independent third parties are increasingly involved in this process, introducing new risks that affect the security of financial institutions.

Electronic Payments

- Recently, a number of new payment instruments have emerged that are largely or wholly electronic.
- Electronic payment systems offer efficiency gains by allowing for rapid and convenient transmission of payment information among system participants.
- However, the emergence of a new payment mechanism can also enable the rapid propagation of fraud, money laundering, and operational disruption if data is compromised.

Emerging Technologies

- The booklet includes a new section that covers some emerging technologies in retail payment systems.
- Additional emphasis is placed on the need for improved operational, credit, legal, and compliance risk processes for retail payment products, especially for the deployment of remote and Internet-based check and ACH capture systems.

Risk Mitigation

Risk Management Methods:

- Policies, standards, and risk limits
- Underwriting, due diligence, & oversight
- Contracts and agreements
- Transaction limits and controls
- Risk monitoring and reporting
- Audit and Control Testing

Example

Mitigate Operational Risk from Fraud by:

- Ensuring proper due diligence including background checks
- Using fraud detection software to filter suspicious activity
- Verification/validation of transmission
- Strict adherence to credit and other related policies
- Ensuring that credit originators require pre-funding or more in-depth financial analysis and underwriting
- Ensuring appropriate limits are in place
- Establishing adequate reserves for debit originators
- Complying with *NACHA* and Operator rules/regulations
- Requiring and enforcing updated agreements for all originators and third-party senders
- Monitoring activity and exceptions reports on a daily basis

Examinations

- Examiners use the Tier I and Tier II Retail Payment Systems examination procedures to evaluate the policies and procedures, business processes, personnel, and internal control systems of financial institutions and technology service providers.
- Retail payment system services include checks and share draft item processing, bankcards, payment cards, ACH, EFT/POS networks, electronic bill payment, person-to-person (P2P) and account-to-account (A2A) payment systems, and many other products and services resulting from emerging advances in technology.

Examination Scope

- The examination scope should be based upon the risk profile of the financial institution or the technology service provider.
- The risk profile is determined through an assessment of the entity’s risk environment and quality of risk management practices.

Additionally

- ➢Appendix A: Examination Procedures
- ➢Appendix B: Glossary
- ➢Appendix C: Schematic of Retail Payments Access Channels & Payments Method
- ➢Appendix D: Laws, Regulations, and Guidance
- ➢Appendix E: Mobile Financial Services

52

Mobile Financial Services

Mobile financial services (MFS) are the products and services that a financial institution provides to its customers through mobile devices. The mobile channel provides an opportunity for financial institutions of all sizes to increase customer access to financial services and decrease costs. Although the risks from traditional delivery channels for financial services continue to apply to MFS, the risk management strategies may differ.

53

Appendix E: MFS

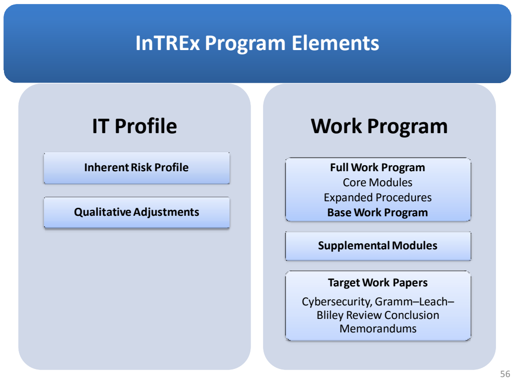
The appendix addresses the following:

- ➢MFS Technologies
- ➢Risk Identification
- ➢Risk Measurement
- ➢Risk Mitigation
- ➢Monitoring and Reporting

54

Updated InTREx Program

- The program has been revised to:
  - eliminate duplicative examination procedures, particularly in the cybersecurity and the information security standards work programs;
  - further risk focus examination procedures;
  - increase the flexibility for scoping supervisory activities;
  - include foreign banking organizations' U.S. branches and agencies with less than $50 billion in U.S. assets and savings and loan holding companies (SLHC) with less than $50 billion in consolidated assets in the population of Federal Reserve-supervised entities for which InTREx is used for evaluating IT-related risks; and
  - implement a consistent approach for Federal Reserve staff in assigning URSIT ratings.



InTREx Program Elements

IT Profile

Inherent Risk Profile

Qualitative Adjustments

Work Program

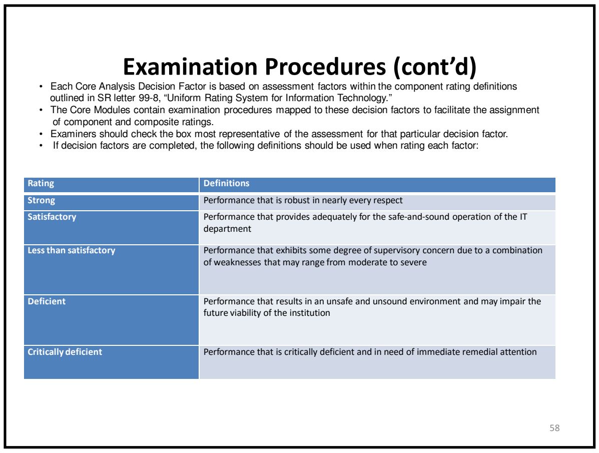
Full Work Program
Core Modules
Expanded Procedures
Base Work Program

Supplemental Modules

Target Work Papers
Cybersecurity, Gramm–Leach–Bliley Review Conclusion Memorandums

IT Profile Key Features

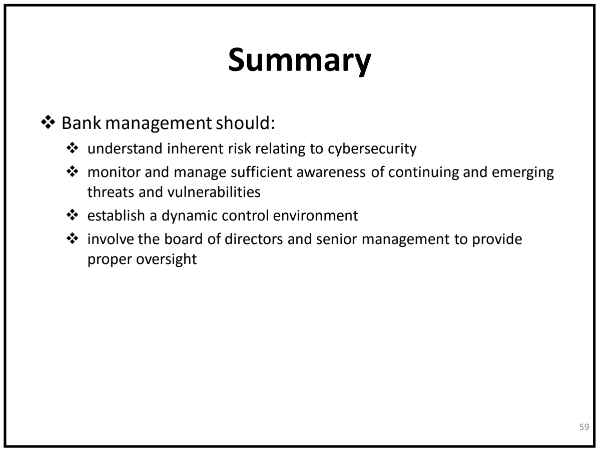
- Q & A Format
- Significant risk areas considered
  - Core Processing
  - Networking
  - Online Banking
  - Software Development and Technology Planning Activities
  - Responses to Software and Services Request list
- Gross technology profile score
- Qualitative adjustments
  - Unique characteristics
  - Previous examination ratings and findings
  - Enforcement actions;
  - Fraud red flags and/or customer or examiner complaints about data accuracy;
  - Concerns raised during offsite surveillance;
  - Critical service provider concerns
  - Reliance on a dominant TPSP
  - Mergers/acquisitions



Examination Procedures (cont’d)

- Each Core Analysis Decision Factor is based on assessment factors within the component rating definitions outlined in SR letter 99-8, “Uniform Rating System for Information Technology.”
- The Core Modules contain examination procedures mapped to these decision factors to facilitate the assignment of component and composite ratings.
- Examiners should check the box most representative of the assessment for that particular decision factor.
- If decision factors are completed, the following definitions should be used when rating each factor:

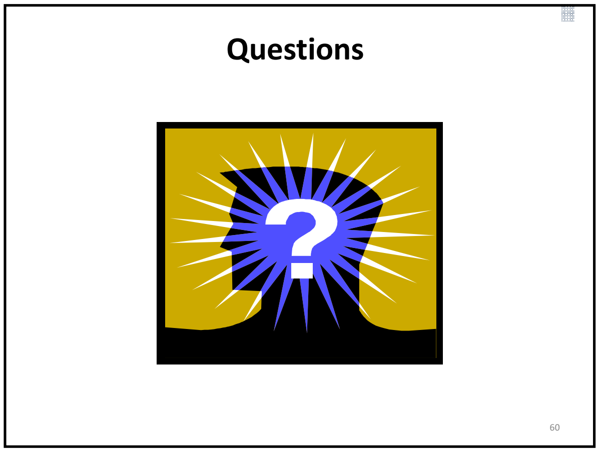
Rating	Definitions
Strong	Performance that is robust in nearly every respect
Satisfactory	Performance that provides adequately for the safe-and-sound operation of the IT department
Less than satisfactory	Performance that exhibits some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe
Deficient	Performance that results in an unsafe and unsound environment and may impair the future viability of the institution
Critically deficient	Performance that is critically deficient and in need of immediate remedial attention



Summary

❖ Bank management should:

- ❖ understand inherent risk relating to cybersecurity
- ❖ monitor and manage sufficient awareness of continuing and emerging threats and vulnerabilities
- ❖ establish a dynamic control environment
- ❖ involve the board of directors and senior management to provide proper oversight



Questions

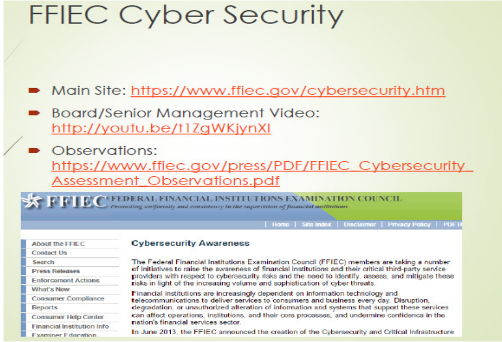
Threat Intelligence Information Sources

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

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions
Home | Site Index | Disclaimer | Privacy Policy | PDF H
About the FFIEC
Contact Us
Search
Press Releases
Enforcement Actions
What's New
Consumer Compliance
Reports
Consumer Help Center
Financial Institution Info
Examiner Education

Cybersecurity Awareness

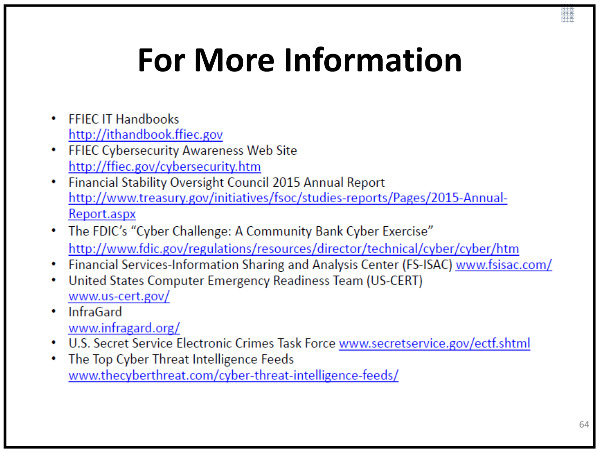
The Federal Financial Institutions Examination Council (FFIEC) members are taking a number of initiatives to raise the awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats.

Financial institutions are increasingly dependent on information technology and telecommunications to deliver services to consumers and business every day. Disruption, degradation, or unauthorized alteration of information and systems that support these services can affect operations, institutions, and their core processes, and undermine confidence in the nation's financial services sector.

In June 2013, the FFIEC announced the creation of the Cybersecurity and Critical Infrastructure

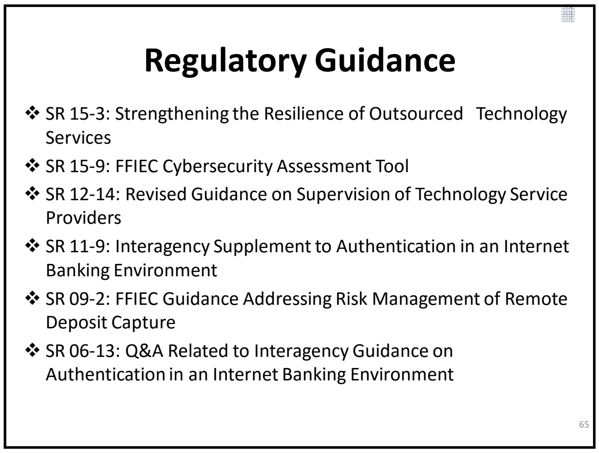
For More Information

- 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



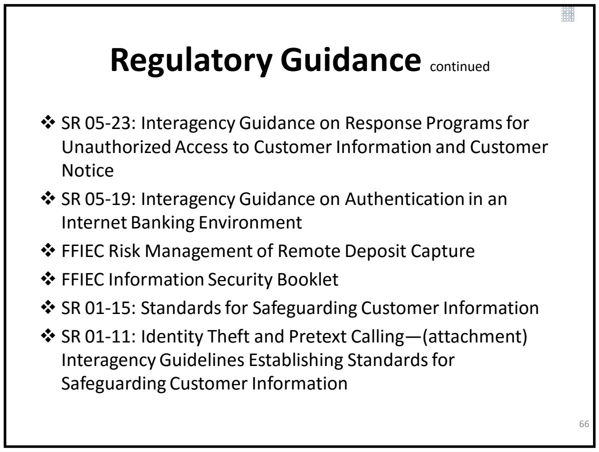
For More Information

- 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/



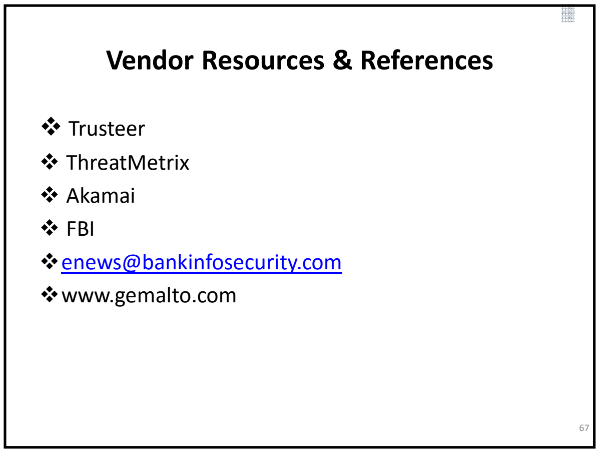
Regulatory Guidance

- ❖ 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
- ❖ FBI
- ❖ enews@bankinfosecurity.com
- ❖ www.gemalto.com

67