CSBS Ransomware Self-Assessment Tool, Version 2.0

Housekeeping

- This meeting is being recorded. The recording and deck will be provided in a follow-up email.
- To minimize background noise, all attendees are on mute.
- Questions will be taken via the **WebEx Chat** function. Send chats to **all panelists**.
- Q&A session at the end of the presentation.

Presentation Outline

- Today's Ransomware Threat Environment
- Drivers for Version 2.0 / Lessons Learned Studies
- Overview of Version 2.0
- Question & Answer

Today's Speakers

Commissioner Charles Cooper
Texas Department of Banking

Phillip Hinkle
Texas Department of Banking

Robert Kahl
FDIC

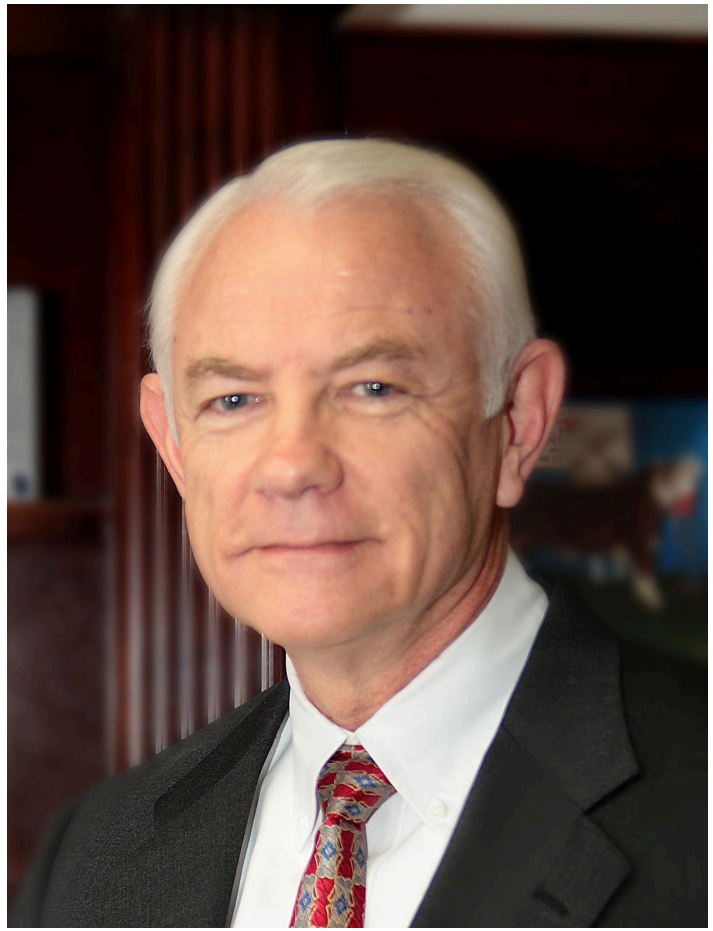
Christopher J. Furlow
Texas Bankers Association

Brad Robinson
CSBS

Mary Beth Quist
CSBS

Introduction

Commissioner Charles Cooper
Texas Department of Banking



Today's Ransomware Threat Environment

- Ransomware remains the **most visible** cyber threat
- Threats are enhanced due to ongoing geopolitical conflicts
- According to Chainalysis, victims have paid ransomware groups $449.1 million in the first six months of 2023. At the current pace, the total figure for 2023 could hit $898.6 million.
- Cyber criminal groups are adopting effective new tactics
    - Reliance on various extortion tactics to maximize impact
    - Foregoing encryption to focus on data theft

Sources:
Splunk: The State of Security 2023
Ransomware Attacks Are on the Rise, Again | WIRED
IBM's 2023 Cost of a Data Breach Report

What Does This Mean for the Financial Sector?

- Technological evolution = more potential attack surfaces
- Ultimately, every organization is at risk
- For the unprepared, the consequences can be severe
    - Damage to brand reputation
    - Regulatory consequences
    - Impacts to operations
    - Failure of the institution
- Ransomware can present an existential threat to the institution

Drivers for Version 2.0

- Changes needed to address changing threat environment and bad actor tactics
  - Increased geopolitical threat environment
  - Double and triple extortion techniques
  - Data exfiltration (without encryption)
- Changes needed to address changing bank environments and controls
  - Increased emphasis on multi-factor authentication (MFA)
  - More scrutiny on other controls, such as cloud security, incident response planning, vendor access to systems, and employee training and awareness

FDIC Ransomware Horizontal Review

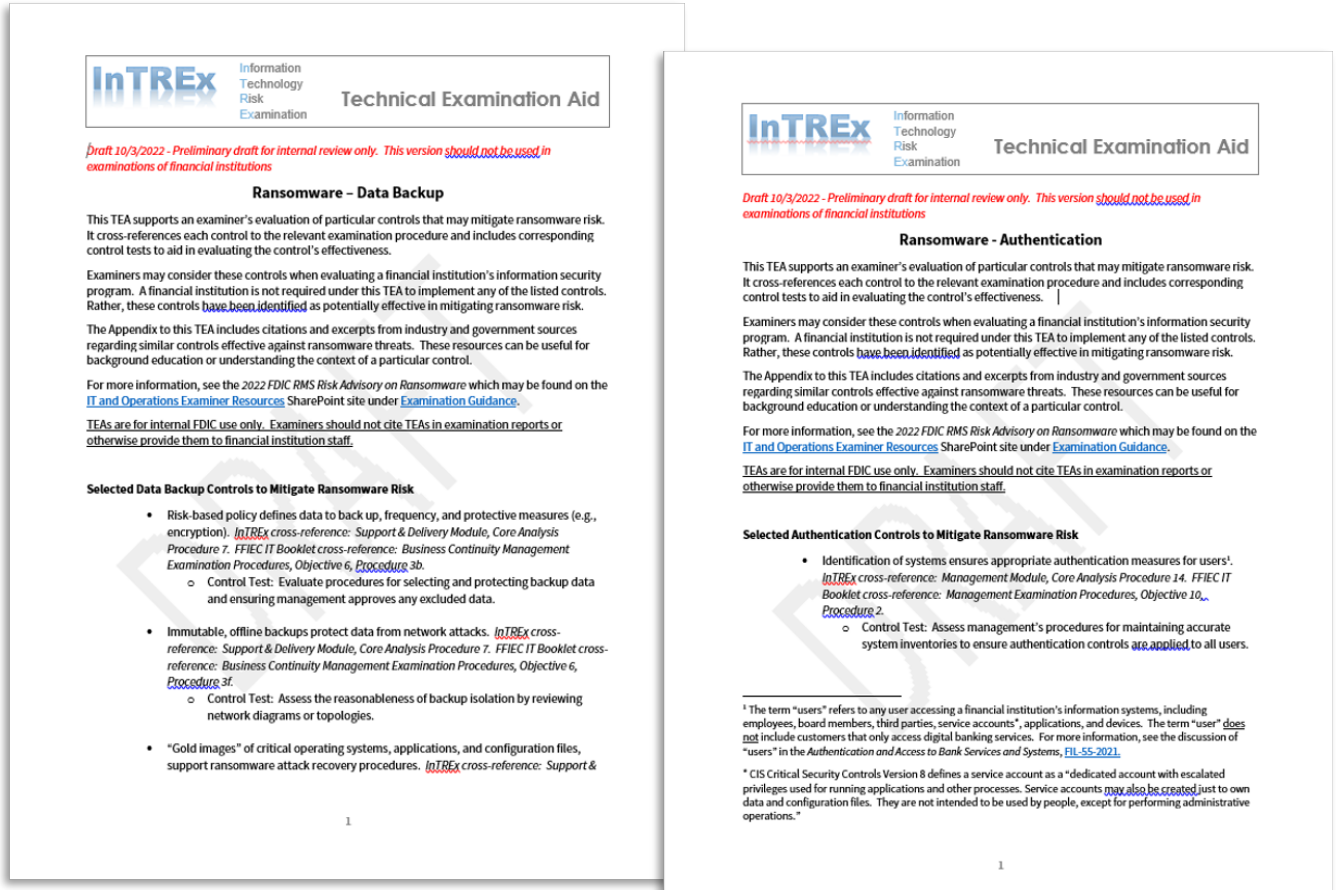
Background

- Searched FDIC and other agency databases for ransomware attacks over a two-year period (June 2019-May 2021).
- Identified 36 ransomware attacks of interest at FDIC-supervised institutions.
- The FDIC reviewed forensic reports from, and conducted interviews with, attacked financial institutions.

What Controls Make a Difference In Defense?

Internet (HTTP) Address Filtering	Logging	Operating System Hardening
Multifactor Authentication	Preventing Unauthorized Executables and Macros (including PowerShell)	Least Privilege Implementation
Backup Isolation and Viability	Network Segmentation	Intrusion Detection System / Intrusion Prevention System Implementation

Resulting Supervisory Adjustments



InTREx Information Technology Risk Examination — Technical Examination Aid

Draft 10/3/2022 - Preliminary draft for internal review only. This version should not be used in examinations of financial institutions

Ransomware – Data Backup

This TEA supports an examiner's evaluation of particular controls that may mitigate ransomware risk. It cross-references each control to the relevant examination procedure and includes corresponding control tests to aid in evaluating the control's effectiveness.

Examiners may consider these controls when evaluating a financial institution's information security program. A financial institution is not required under this TEA to implement any of the listed controls. Rather, these controls have been identified as potentially effective in mitigating ransomware risk.

The Appendix to this TEA includes citations and excerpts from industry and government sources regarding similar controls effective against ransomware threats. These resources can be useful for background education or understanding the context of a particular control.

For more information, see the *2022 FDIC RMS Risk Advisory on Ransomware* which may be found on the IT and Operations Examiner Resources SharePoint site under Examination Guidance.

TEAs are for internal FDIC use only. Examiners should not cite TEAs in examination reports or otherwise provide them to financial institution staff.

Selected Data Backup Controls to Mitigate Ransomware Risk

- Risk-based policy defines data to back up, frequency, and protective measures (e.g., encryption). *InTREx cross-reference: Support & Delivery Module, Core Analysis Procedure 7. FFIEC IT Booklet cross-reference: Business Continuity Management Examination Procedures, Objective 6, Procedure 3b.*
  - Control Test: Evaluate procedures for selecting and protecting backup data and ensuring management approves any excluded data.
- Immutable, offline backups protect data from network attacks. *InTREx cross-reference: Support & Delivery Module, Core Analysis Procedure 7. FFIEC IT Booklet cross-reference: Business Continuity Management Examination Procedures, Objective 6, Procedure 3f.*
  - Control Test: Assess the reasonableness of backup isolation by reviewing network diagrams or topologies.
- "Gold images" of critical operating systems, applications, and configuration files, support ransomware attack recovery procedures. *InTREx cross-reference: Support &*

1

InTREx Information Technology Risk Examination — Technical Examination Aid

Draft 10/3/2022 - Preliminary draft for internal review only. This version should not be used in examinations of financial institutions

Ransomware - Authentication

This TEA supports an examiner's evaluation of particular controls that may mitigate ransomware risk. It cross-references each control to the relevant examination procedure and includes corresponding control tests to aid in evaluating the control's effectiveness.

Examiners may consider these controls when evaluating a financial institution's information security program. A financial institution is not required under this TEA to implement any of the listed controls. Rather, these controls have been identified as potentially effective in mitigating ransomware risk.

The Appendix to this TEA includes citations and excerpts from industry and government sources regarding similar controls effective against ransomware threats. These resources can be useful for background education or understanding the context of a particular control.

For more information, see the *2022 FDIC RMS Risk Advisory on Ransomware* which may be found on the IT and Operations Examiner Resources SharePoint site under Examination Guidance.

TEAs are for internal FDIC use only. Examiners should not cite TEAs in examination reports or otherwise provide them to financial institution staff.

Selected Authentication Controls to Mitigate Ransomware Risk

- Identification of systems ensures appropriate authentication measures for users[1]. *InTREx cross-reference: Management Module, Core Analysis Procedure 14. FFIEC IT Booklet cross-reference: Management Examination Procedures, Objective 10, Procedure 2.*
  - Control Test: Assess management's procedures for maintaining accurate system inventories to ensure authentication controls are applied to all users.

[1] The term "users" refers to any user accessing a financial institution's information systems, including employees, board members, third parties, service accounts*, applications, and devices. The term "user" does not include customers that only access digital banking services. For more information, see the discussion of "users" in the *Authentication and Access to Bank Services and Systems*, FIL-55-2021.

* CIS Critical Security Controls Version 8 defines a service account as a "dedicated account with escalated privileges used for running applications and other processes. Service accounts may also be created just to own data and configuration files. They are not intended to be used by people, except for performing administrative operations."

1

Lessons Learned From Ransomware Attacks

- Study was conducted of victims of ransomware attacks
- Purpose of the study was to guide needed updates to the R-SAT
- The study covered the four-year period between January 1, 2019, and December 31, 2022
    - Multiple state banking departments participated in the study
    - A written report is available for review

Lessons Learned From Ransomware Attacks

- Key findings from the study:
  - Most victims had not used the R-SAT to guide their risk mitigation, but ALL began using it fully after the incident
  - Multi-factor authentication (MFA) was implemented by all victims after the incident, if they weren't using it
  - Monitoring "hyper-local", as well as traditional social media, is important to manage misinformation and maintain consumer confidence

Lessons Learned From Ransomware Attacks

- Additional observations from the study:
  - Expanding cloud usage requires greater awareness of where data is located, as well as which services are cloud-based
  - Ransomware tactics are changing and now include double and triple extortion techniques, sometimes with accompanying DDoS attacks
  - Controversial practices: Paying an extortion fee for the promise of silence from a criminal emboldens them to continue targeting the banking industry

R-SAT Version 2.0: Overview

- New version has the same general look and format as Version 1.0
- Still follows the NIST Framework
    - Identify
    - Protect
    - Detect
    - Respond
    - Recover
- Expanded from 16 questions to 20 questions

R-SAT Version 2.0: Notable Changes

- Increased emphasis on multi-factor authentication (MFA)
  - Now an expanded, stand-alone question
  - New sub-question emphasizing whether the institution relies on stronger application-based or phishing-resistant methods
  - More options to identify where and how MFA is applied
  - New sub-question identifying areas where MFA implementation is not planned or has been deferred

R-SAT Version 2.0: Notable Changes

- Identification and management awareness of any data, including cloud-based data, housed in locations outside of the US (new question)
    - Potentially subject to different privacy regulations of other countries
    - GDPR, PIPEDA, etc.
- Increased emphasis and detail on employee awareness and security training
    - Types of training offered
    - Frequency of training offerings (new sub-question)
    - Phishing test exercises and use of testing results (new question)
    - Employee briefings on emerging ransomware threats (new question)

R-SAT Version 2.0: Notable Changes

- Increased clarity on identifying systems or activities processed or performed internally, outsourced to a third party, or a combination of the two
- Identification of systems or activities that are based in a cloud environment
- Review of cyber framework gap analysis (new sub-question)
- Checklist of services potentially available through cyber insurance policies
- Narrative requesting identification of vendors that do not have ransomware-related controls in place
- Procedures to validate the sterility of data backups prior to restoration to prevent reinfection.

R-SAT Version 2.0: Notable Changes

- Identification of any ransomware threats and risks identified in risk assessments that have not been appropriately remediated or mitigated to an acceptable risk level (new sub-question)
- Identification of new preventative controls
    - Patch management
    - Controls governing removeable media use
    - Controls ensuring changing of default hardware and software settings
    - Implementation of jump box (bastion host) or administrative VLAN
    - Procedures for resetting or replacing user authentication credentials

R-SAT Version 2.0: Notable Changes

- Identification of new or reworded Incident Response Plan considerations
  - Alternative strategies for connecting to third parties
  - Escalation procedures for activating BCP/DR plans
  - Social media monitoring for public awareness
  - Notification of state and federal regulators (in accordance with regulatory requirements)
  - Immediate notification of federal law enforcement
  - Threat hunting
  - “Out-of-band” communications procedures
  - Board discussions of ransom payments prior to payment

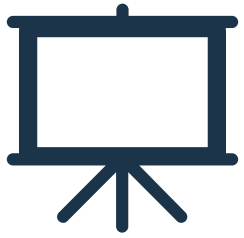
R-SAT Version 2.0: Notable Changes

- Considerations for third parties engaged in the event of an attack
  - Identification of any third parties to be engaged (new question)
  - Do prearranged service contracts or, at a minimum, contact information exist so that legal and contract issues do not delay the institution's response?
  - Does the institution or does the institution require third parties, including insurance companies, to promptly engage with law enforcement (new sub-question)
  - Pre-approval of third parties by the bank's cyber insurance provider (new sub-question)

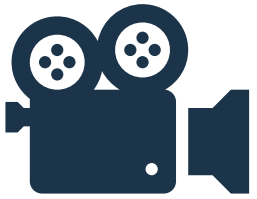
Banker's Perspective

Christopher J. Furlow
President & CEO
Texas Bankers Association

Thanks for listening!



You'll get the presentation via email



And the recording too!

Questions?