CONVERSATIONS
WITH THE ST. LOUIS FED

FEDERAL RESERVE BANK *of* ST. LOUIS
CENTRAL TO AMERICA'S ECONOMY®

CYBERSECURITY
Mission Possible

June 24, 2021

Options to Join

Webinar and audio

- Click on the link: https://www.webcaster4.com/Webcast/Page/584/41594
- Choose to listen with your PC speakers

Webinar and phone

- Click on the link: https://www.webcaster4.com/Webcast/Page/584/41594
- Choose to listen with your phone
- Call-in number: 888-625-5230
- Enter the participant code: **867 690 81#**

Phone only

- Call-in number: 888-625-5230
- Enter the participant code: **867 690 81#**

Questions

- During the call, you can submit questions several ways.
  - **Via webinar chat:** You can submit a question via the **Ask Question** button in the webinar tool. Your question will only be seen by our presenters.
  - **Via email:** conversations@stls.frb.org

Today’s Presenters

- Allen North
  Vice President
  Federal Reserve Bank of St. Louis

- Nathan Goodson
  Supervisory Examiner
  Federal Reserve Bank of St. Louis

- Carey Sharp
  Supervisory Examiner
  Federal Reserve Bank of St. Louis

- Megan Kahlenberg
  Supervisory Officer
  Federal Reserve Bank of St. Louis

Disclaimer

The opinions expressed in the presentations are intended for informational purposes, and are not formal opinions of, nor binding on the Federal Reserve Bank of St. Louis or the Board of Governors of the Federal Reserve System.

Chairman Powell on Cyber Risk

"[C]yber risk is a major focus. Perhaps the major focus in terms of big risks…I would say of the risks that we face, that [cyber] certainly is the largest one."

– 60 Minutes interview (3/10/19)

"[T]he world changes. The world evolves. And the risks change as well. And I would say that the risk that we keep our eyes on the most now is cyber risk…There are cyber-attacks every day on all major institutions now."

– 60 Minutes interview (4/12/21)

Agenda

- Mission Possible – Episodes
  - Takeover [a Zero-Day Tale] – aired 1/2/71
  - The Ransom[ware] – aired 11/5/66
  - Recovery [Service Provider's Woe] – aired 3/17/68
  - The Bank [a Data Loss Story] – aired 10/1/67
- Mission Debrief
- Report In – How We Can Help
- Q&A

Takeover [a Zero-Day Tale] – aired 1/2/71

- Zero-Day Defined
  - Previously unknown vulnerabilities that are targeted and acted upon prior to the vendor knowing that the vulnerabilities exist
- How it Might Affect Your Institution
  - Microsoft Exchange Server (did not affect Exchange Online [a.k.a. O365])
- Impact/Resolution
  - Multi-day systems outage
  - Potential loss of confidential information
  - Vendor patch release – timeliness is important
- URSIT Impact
  - Management + Support and Delivery

The Ransom[ware] – aired 11/5/66

- Bank Profile
  - Core processing and network monitoring: outsourced
  - Email server: in-house
- How it Happened
  - Unpatched Microsoft Exchange server
  - No multi-factor authentication on privilege user account
  - No air-gapped data backups
  - Possible breakdown between monitoring vendor and bank staff
- Impact/Resolution
  - Multi-day systems outage
  - Paid ransom (used firm to negotiate)
- URSIT Impact
  - Support and Delivery

Recovery [Service Provider's Woe] – aired 3/17/68

- What Happened
  - Significant core banking software provider was hit with ransomware
- How It Happened
  - Phishing/spear phishing
  - Lack of data loss prevention (DLP) controls
- Impact/Resolution
  - Core banking, Internet banking, and other services were inaccessible
  - 89 percent of affected services were offline for two business days
    - The remaining 11 percent of services were not restored for another six business days
  - Third-party risk management practices should include ongoing dialogue with higher-risk vendors/service providers
- URSIT Impact
  - Management

The Bank [a Data Loss Story] – aired 10/1/67

- What Happened
  - Loan officer sent customer information to personal email account
  - Activity was discovered after the individual left the organization
- How it Happened
  - Lack of DLP
  - Personal email access
- Impact/Resolution
  - Customer notification required
  - Pending legal review/action
- URSIT Impact
  - Management + Support and Delivery

Mission Debrief – Questions to Consider

- Who is aware of independent technical testing engagements?
- Is incident response a part of our overall testing plan?
- Are there special requirements/clauses within our cyber insurance policies we need to understand when filing a claim?
- How have we implemented multi-factor authentication for privileged users?
- Have we assessed ransomware risks?
- How quickly do we deploy critical security patches?
- Do we have unimpeachable/air-gapped data backups?
- How is our IT audit coverage evolving?
- How are we maturing our cybersecurity posture?

Mission Debrief – Items to Review

- Patch Management Status Reports
- Incident Response/Disaster Recovery Test Results
- Penetration/Vulnerability/Social Engineering Test Results
- IT Audit Reports
- Cybersecurity Assessments
  - Year-over-year comparison of results and maturity levels
- Gramm-Leach-Bliley Act (GLBA) Risk Assessment and Reporting
- Vendor Management Ongoing Monitoring Reports

Report In – How We Can Help

- Federal Reserve Bank of St. Louis Resources
  - IT Supervisory Examiners Nathan Goodson and Carey Sharp
  - Supervisory Officer Megan Kahlenberg
  - Safety & Soundness Supervisory Examiners and Portfolio Examiners

- How to Report Your Incident

- How Your Reporting Helps Other Banks

References

CIS Controls ™

https://www.cisecurity.org/controls/

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework

FFIEC IT Examination Handbooks

https://ithandbook.ffiec.gov/

Incident Reporting Guidance

Federal Reserve Supervisory Letter SR Letter 05-23/CA Letter 05-10, "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice"

Questions

Via webinar chat: You can submit a question via the **Ask Question** button in the webinar tool. Your question will only be seen by our presenters.

Via email: conversations@stls.frb.org