Information Technology and Security: Emerging Trends and Audit Considerations

March 5, 2020
Todd Tekancic, CISA
Information Technology and Security: Emerging Trends and Audit Considerations

- KeyBank Overview
- Emerging Technology Trends and Risks
- Critical Focus Areas and Audit Considerations for 2020
  - Cyber & Information Security
  - Business Resilience
  - Public Cloud Environments
  - Robotics Process Automation

Please note that all materials presented here and discussed within represent the view of the speaker and are not necessarily the policy or practices of KeyCorp.
Cleveland-based KeyCorp (KEY) is one of the nation’s largest bank-based financial services companies, with assets of approximately $146 billion.

Key companies provide investment management, retail and commercial banking, consumer finance, and investment banking products and services to individuals and companies throughout the United States and, for certain businesses, internationally.

The company’s businesses deliver their products and services through branches and offices; a network of over 1,500 ATMs; telephone banking centers 800-KEY2YOU® (800-539-2968); and a website, Key.com®, that provides account access and financial products 24 hours a day.
Emerging Technology Trends

Emerging Technologies

- Digital currencies
- Mobile banking products
- Advanced payment technologies
- Internet of things
- Robotics Process Automation

Evolving Threat Landscape

- Blurring malicious actors
- Malicious cyber products and expertise on demand
- Increasing value/profit from exploits
- Increasing use of cyber for political motives
- Complexity of operations

Increased value through greater interconnectivity equals increased risk through greater interconnectivity

Source: Office of the Comptroller of the Currency
Emerging Technology Trends and Risks

• Increasing expectations for speed, security and resilience for delivery of financial services

• Cyber threats continue to proliferate, and are becoming increasingly harder to prevent and detect

• Social engineering and phishing attacks continue to evolve and remain the most significant cause of data breaches

• Many organizations are increasing their reliance on third-party service providers

• Adoption of new technologies, including robotics process automation.

Source: Office of the Comptroller of the Currency
Critical Focus Areas and Audit Considerations

Cyber and Information Security Risks

• Unpatched and end of life systems
• Misconfigured networks and security devices
• Management of privileged access
• Third and fourth-party risks
• Physical security
Critical Focus Areas and Audit Considerations

Audit Considerations for Cyber and Information Security

- Ensure patch levels are current
- Validate IT asset inventory
- Scope and depth of penetration testing and vulnerability testing
- Network and server configuration validation
- Identity and access management processes
- Event logging and management
- Data loss prevention processes
- Review of incident response programs
Critical Focus Areas and Audit Considerations

Organizational, Process, and People Failures Are the Main Source of Critical Breaches

CAUSES OF DATA LOSSES IN 50 MAJOR BREACHES

- Inadequate security technology: 28%
- IT configuration error: 322
- Organizational, process, and people failures: 72%
- Failure to fully implement purchased security products: 146
- Social engineering/“phishing”: 382
- Negligent insider (accidental publication): 21
- Malicious insider: 238
- Physical loss: 16

Sources: Press reports; company statements; BCG analysis.

Source: Cleveland FBI
Breaches by the numbers

The Verizon Data Breach Investigations Report analyzed more than 2,000 confirmed breaches in 2018. Here's a look at the threat actors behind them and the common threads among them.

Who's behind the breaches?

- Outsiders: 69%
- Organized criminal groups: 39%
- Internal actors: 34%
- Actors identified as nation-state or state-affiliated: 23%
- Multiple parties: 5%
- Partners: 2%

What are the commonalities found around breaches?

- Financially motivated: 71%
- Took months or longer to discover: 56%
- Involved phishing: 32%
- Involved use of stolen credentials: 29%
- Motivated by the gain of strategic advantage (espionage): 25%
Critical Focus Areas and Audit Considerations

Business Resiliency and Continuity Management

• Risk appetite for outages
• Accuracy of business impact analysis and corresponding recovery time objectives
• Resilience planning against multiple scenarios
• Thoroughness of business recovery testing activities
• Validation of resiliency capabilities of key third-party dependencies
Audit Considerations for Business Resiliency

• Challenge risk appetite and business impact analysis assumptions along with the corresponding recovery time objectives and recovery point objectives

• Validate adequacy of business recovery test plans and validation of testing activities

• Validation of upstream and downstream dependencies for recovery plans

• Validation of third-party recovery capabilities

• Inclusion of critical third-parties in recovery activities
Critical Focus Areas and Audit Considerations

Usage of Public Cloud Environments

Cloud usage is increasing at a rapid pace for multiple reasons:

- **Cost savings** – No need to pay for large amounts of disk and storage space. No need to buy, install and upgrade pricey software. Easy to scale to fit the needs of the business.

- **Ease of use** – No need to install, download or upgrade software as it is done for you. The cloud offers virtually unlimited storage capacity relative to typical hard drive and server limits. Users can access data and software from virtually anywhere or from any device with an internet connection.

- **Freeing up IT staff** – No need to use valuable IT staff for things like maintaining servers, fixing bugs or taking care of patching and software updates.

Third-party service providers are increasingly leveraging public cloud environments
Audit Considerations for Cloud Environments

• Validate the division of responsibilities
• Review security and access configurations
• Encryption of confidential data
• Design and validation of cloud resiliency controls
• Oversight of cloud provider operations
Robotics Process Automation (RPA)

RPA is evolving rapidly, and is enabling organizations across all industries to effectively automate tasks, streamline process, and increase employee productivity.

Some high-level examples of RPA in use include:

- **Chat Bots** – Computer programs designed to simulate a conversation with human users and quickly provide answers (e.g. Customer Support or FAQs)

- **Digital Labor Bots** – Software configured to interact with computers and applications just like a human would, performing high volume, repetitive processes and tasks (e.g. trade settlement)
Audit Considerations for Robotics Process Automation

- RPA governance framework
- Change management
- Bot availability and performance (SLAs)
- Logical access to bots and bot environments
- Bot access to systems and data
- Data integrity associated with inputs and outputs
Closing Comments and Questions

Thank you!