Preparing for An IT Exam

December 16, 2021

Presenter

Scott Runyan, CPA
Director, Assurance & Business Advisory Services
GBQ
614.947.5291
srunyan@gbq.com

Doug Davidson, CISA
Director of Information Technology Services
GBQ
614.947.5340
ddavidson@gbq.com

Chuck Grigg
IT Consultant
GBQ
248.990.2707
CGrigg@gbq.com

Agenda

- Reality of the Exam Process
- Get Organized
- Anticipate What's Coming
- Review Exam List
- Get Organized
- Checklist
- Be hospitable

Reality of the Exam Process

- All Credit Unions, regardless of size, have to manage IT risk and have a cybersecurity program
- Anything is fair game
- Exam letter findings tend to be a mix of:
  - FFIEC and NCUA concerns – ODFI follows NCUA
  - Individual examiners perspective
- Feels adversarial, but in all reality process is intended to reduce your risk

Anticipate What's Coming

- ODFI uses FFIEC standards/guidelines (NCUA)

- Look to recent NCUA "Letters to Credit Unions and Other Guidance"
  (https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance)

- Pay particular attention to NCUA's 2021 Supervisory Priorities
  (https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/ncuas-2021-supervisory-priorities)

Anticipate What's Coming – NCUA Actions

- NCUA is no longer using AIRES
- NCUA has moved away from ACET as a basis for IT Examinations
- NCUA is "piloting" InTREx-CU, which is an Exam program already in use by the FDIC
- IT Exams will likely continue to focus on the broad principles of sound IT management and Part 748A/B (GLBA and Incident Response)
- No change to ratings components is currently anticipated …
- NCUA is developing MERIT for Exams and will primarily impact Document Request Lists
- NCUA intends to make MERIT available to State Examiners

Anticipate - NCUA's 2021 Supervisory Priorities

Attack Patterns

"Emerging cyber-attacks are a persistent threat to the financial sector, and the likelihood of these threats adversely affecting credit unions and consumers continues to increase because of:

- Advances in **financial technology**;
- An increase in a **remote workforce**; and
- Growing adaptation of **mobile technology** for financial transactions."
- The NCUA continues to promote cybersecurity hygiene in credit unions, and reviews of credit union information systems and assurance programs remain a supervisory priority for the agency.

Anticipate - NCUA's 2021 Supervisory Priorities

Continued emphasis

- NCUA continues to promote **cybersecurity hygiene** in credit unions
- "Reviews of credit union information systems and assurance programs remain a supervisory priority for the agency."
- Building upon its outreach efforts to the industry in 2020, the NCUA will continue to provide guidance and resources to assist credit unions with this critical threat.

See: https://www.ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources

Anticipate - NCUA's 2021 Supervisory Priorities

Risk Assessment

- The FFIEC Cybersecurity Assessment Tool (CAT) **has always been an optional tool** for financial institutions under all FFIEC Agencies (NCUA LCUs 17-CU-01, 17-CU-09).
- NCUA has reprioritized away from performing facilitated Automated Cybersecurity Evaluation Toolbox (ACET) cybersecurity maturity assessments, to piloting the Information Technology Risk Examination for Credit Unions (InTREx-CU) NCUA LCU 21-CU-02.
- InTrex Examination Program states: institutions are not required to use the CAT, and examiners should not criticize management if management chooses to use other appropriate tools, frameworks, or processes to assess a financial institution's cyber risks and cybersecurity preparedness
- IT Risk Assessment must be consistent with GLBA/NCUA Part748A requirements = Threats, Controls, Assets, and Risk Conclusions

Anticipate – Threat Environment

Understand the current "threat environment" (bad things happening) in the FI space.

Suggested source: Verizon Data Breach Investigations Report 2021

Financial and Insurance NAICS 52

Summary

Misdelivery represents 55% of Financial sector errors. The Financial sector frequently faces Credential and Ransomware attacks from External actors.

Frequency	721 incidents, 467 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Basic Web Application Attacks and Social Engineering represent 81% of breaches
Threat Actors	External (56%), Internal (44%), Multiple (1%), Partner (1%) (breaches)
Actor Motives	Financial (96%), Espionage (3%), Grudge (2%), Fun (1%), Ideology (1%) (breaches)
Data Compromised	Personal (83%), Bank (33%), Credentials (32%), Other (21%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (14), Secure Configuration of Enterprise Assets and Software (4), Access Control Management (6)

The Financial Services industry has long been known for rapid changes, including sudden dips, dizzying highs and unforeseen fluctuations (thanks, Reddit users). This vertical has seen quite a diverse set of changes when it comes to the cybersecurity landscape as well. One that we have seen over the last few years has been a convergence of Internal actors and their associated actions with the more famous and nefarious External varieties.

This year, 44% of the breaches in this vertical were caused by Internal actors (having seen a slow but steady increase since 2017) (Figure 104). The majority of actions performed by these folks are the accidental ones, specifically the sending of emails to the wrong people, which represents a whopping 55% of all Error-based breaches (and 13% of all breaches for the year).

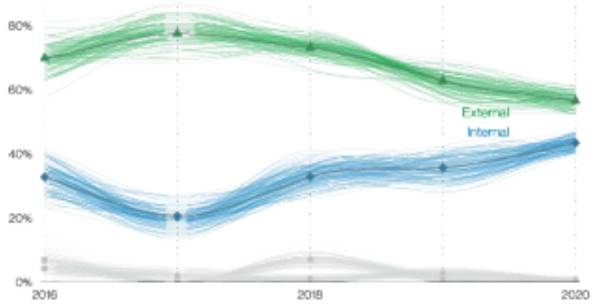


Figure 104. Actors in Finance breaches over time

When we turn our attention to malicious External actors, the Financial industry faces a similar onslaught of Credential attacks, Phishing and Ransomware attacks that we see topping the charts in other industries. With regard to data type, Personal comes in first, followed by Credentials and Bank data, hardly surprising given the focus of the industry.

Finally, this industry continues to be heavily reliant upon external parties for breach discovery. Typically via bad actors making themselves known (38% of the incidents) or notification from monitoring services (36% of incidents).

SEE: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

Review exam list – AS SOON as you get it

- Examiners always send a request list in advance, but advance notification may be short!
- Review as soon as possible – same day if you can.
- Receiving and acting on this list before the exam begins means you can have everything prepared and labeled when they "walk through the door"— virtually or literally.
- Your high level of preparation will make things easier for you and your staff - requiring less searching for things at the last moment - and may even brighten the examiner's disposition.

Get Organized

"More disorganized you look the harder that it is going to go …"

- Chuck Grigg, 2021

- Document throughout the year
- If you say you do it be able to produce a document that shows you do it
- IT Audit as practice run -- If you struggle to get your IT audit firm information you'll struggle to meet the examiner's expectations
- GBQ's biggest obstacle to audit/security assessment success is the information gathering stage where our CU clients meet our information requests … this translates to your exam.

Checklist – Risk / Security Program

- ❑ The Information Security Program is presented to the Board at least annually - Report follows Policy and Guidelines (GLBA/NCUA Part 748A)
- ❑ Employees are required to attend comprehensive information security training (GLBA/NCUA Part 748A)
- ❑ A risk-based IT audit is in place and audits, including security testing, are performed at designated intervals
- ❑ IT Audit and Exam results are tracked and remediated (increased emphasis in recent years)
- ❑ IT Risk Assessment must be consistent with GLBA/NCUA Part748A requirements = Threats, Controls, Assets, and Risk Conclusions
- ❑ FFIEC Cybersecurity Assessment Tool (CAT) - Tool is OPTIONAL, ODFI has been instructing FI's to complete the CAT. NCUA has made the CAT available as ACET (Automated Cybersecurity Evaluation Toolbox).
- ❑ IT Strategic Plan - integrated with Company Strategic plan - initiatives, budgets

Checklist – Cyber health and hygiene

- ❑ Accurate, Complete Network Diagram - Essential!
- ❑ Accurate Inventory of Systems
- ❑ External systems vulnerability and penetration tests occur at least annually (tests of controls)
- ❑ Internal systems vulnerability and penetration tests occur at least annually (tests of controls)
- ❑ Phishing and other social engineering tests of employees occur at least annually (control and tests of controls)
- ❑ A structured vulnerability remediation process is in place
- ❑ Infrastructure and application changes are managed according to a structured change process
- ❑ End-of-Life Systems - Causes much consternation when FI maintains systems after EOL (End of Support)
- ❑ Build/Deployment standards for PCs and Servers (this is relatively new)

Checklist – Vendor Due Diligence

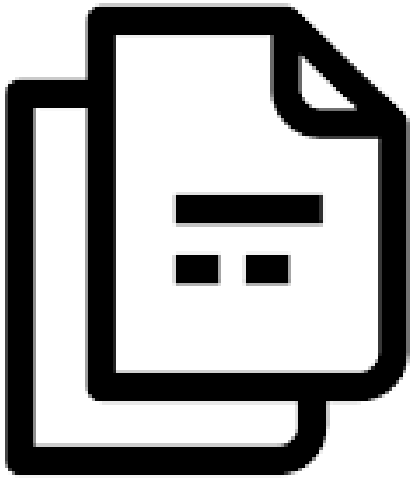
- Vendor due diligence includes financials, audit reports, and appropriate contract terms
- Critical vendors' SOC reports review should document management's review, INCLUDING Complementary User Entity Controls
- Vendor service agreements/SLAs (Even informal contractors and MSPs need contracts)

Checklist – Continuity, Response, Recovery

- ❑ A Security Incident Response Plan is in place and is periodically tested - increased emphasis now placed on testing (GLBA/NCUA Part 748A, 748B)
- ❑ Ransomware layered controls and multiple air-gapped backup sets are created for critical backups
- ❑ A company-wide Business Continuity Plan with a Business Impact Analysis (BIA) is well-developed
- ❑ Recovery capabilities are periodically tested including Core system and Servers
- ❑ Succession Plan for key IT employees

Review previous IT audits

- Examiners often agree with your auditors
- If it is in your audit you can assume the examiner is going to pick on it
- Address audit issues before the examiner visits



Review previous exams

- If you received a Document of Resolution (DOR) from your previous exam, is it completed?

- An examiner may issue a DOR when an unacceptable risk is discovered as part of the exam process. A DOR captures agreements reached between the examiner and the credit union for the timely correction of the identified problem. It includes who is responsible and the time frame for resolution. If you have a previously issued DOR that has not been completed, you should be prepared to explain what actions have been taken to date.

Be hospitable!

Questions?

Presenter

Scott Runyan, CPA
Director, Assurance & Business Advisory Services
GBQ
614.947.5291
srunyan@gbq.com

Doug Davidson, CISA
Director of Information Technology Services
GBQ
614.947.5340
ddavidson@gbq.com

Chuck Grigg
IT Consultant
GBQ
248.990.2707
CGrigg@gbq.com