Tabletop Exercise - Threats to Your Credit Union

Mike Bechtel

information security director

Disclaimer

The information contained herein has been prepared for general informational purposes only and is not offered as and does not constitute legal advice or legal opinions. You should not act or rely on any information contained herein without first seeking the advice of your legal counsel.

No copy or use of this presentation should occur without the permission of Vizo Financial. Vizo Financial retains all intellectual property interests associated with this presentation. Vizo Financial makes no claim, promise, or guarantee of any kind about the accuracy, completeness, or adequacy of the content of the presentation and expressly disclaims liability for errors and omissions in such content.

"Tabletop Exercise - Threats to Your Credit Union" discussed in this presentation is the current version with effective date of 6/1/2026.

The comments today are my own and not necessarily those of Vizo Financial or the Vizo Financial membership.

Overview – IR Steps

- **Preparation** – Playbook & IR Team & Training
- **Identification** – Monitoring & Triage
- **Containment** – Short Term Isolation & Temporary Workaround
- **Eradication** – RCA & Removal
- **Recovery** – Restoration & Validation
- **Lessons Learned** – Review & Future Improvement

Overview – Take Home Goals

- Identify Gaps in Your Plans
- Clarify Roles in Your IR Team
- Improve Coordination Between IR Team Members
- Assess Information Flow During Incident

Overview – Today's Goals

- No pressure, it's not real
- Freedom to take risks and see where they go
- Open discussion & collaborate on solutions
- The goal is not to solve the mystery, it's to learn something along the way.

Overview – Goals

Directions

- You will get enough details to work the scenario, but not enough to solve the problem
- Teams at each table will work together on how you would respond to the situation as presented
- You are the IR Team; you have decision making power
- You will be given seven minuets of time after each set of phase updates to work with you team
- We will come together as a group at the end of each phase to review as a larger group

Background Information

- State Charted Credit Union since 1980.
- 100 Employees including internal IS, IT and Help Desk.
- Main office has a branch, Executive team and an operations department located in the downtown area.
- 6 additional satellite branches across three nearby counties.

Background Information

- The Credit Union recently completed a migration to a hybrid Core Processing environment consisting of both on-premises servers and cloud-hosted services. The implementation includes several AI-enabled features that are used across the environment:
  - AI-assisted fraud scoring
  - Automated transaction anomaly detection
  - AI-driven member service chatbot
  - AI-based loan decision support
  - Predictive account risk analytics

Background Information

- The platform is integrated with the Credit Union's existing:
  - Online Banking Platform
  - Mobile Banking Platform
  - ACH Processing / Wire Transfers
  - Debit Card Processing
  - Member Services Call Center Systems

Let’s Begin

Phase 1

- Member Services begins receiving increased calls from the membership reporting:
  - Debit cards are being declined when funds are available
  - ACH processing is being delayed
  - Online banking accounts are seeing increased lockouts
  - Duplicate fraud alerts
- Branch operations report intermittent connectivity loss between on-premises teller systems and cloud-hosted core services.

Phase 1

- Fraud Operations Reports:
  - A sharp decrease in fraud cases being flagged
  - Unusual approval patterns for high-risk wire transfers
  - AI fraud recommendations conflicting with analyst assessments
- IT / IS teams identify abnormal outbound traffic originating from on-premises servers connected to the new Core Processor environment.

Phase 1 – Discussion Questions

- Who did you notify first?
- What thresholds trigger incident escalation?
- Is this issue treated as operational, fraud-related, vendor-related, or cyber-related?
- What logs and data are reviewed across cloud and on-premises systems?
- Did you engage the vendor?
- What monitoring exists for AI model integrity?

Phase 2

- Information Security finds evidence that a recent software update introduced unauthorized code into the AI environment.
- Security Monitoring Reveals:
  - Unknown processes running on on-premises servers
  - Changes to AI fraud model thresholds
  - Unexpected outbound encrypted traffic to unfamiliar cloud infrastructure
  - Suspicious API activity between cloud AI services and internal banking servers

Phase 2

- The vendor contacts you and states:
  - A legitimate was applied to the cloud and on premises systems. But also acknowledges that several other financial institutions are reporting similar anomalies following the same update deployment.

Phase 2 – Discussion Questions

- Who has authority to disable vendor access?
- What systems are/can be isolated?
- When is law enforcement / Regulators / contacted?
- Does the Credit Union activate its cyber insurance policy?
- What contractual obligations exist with the vendor?

Phase 3

- The CEO receives a call from a local news outlet asking whether the Credit Union was impacted by a widespread software supply chain attack affecting multiple financial institutions.
- At the same time:
  - Fraud losses are currently at $250,000
  - Multiple commercial members cannot process payroll
  - NCUA is aware of other CUs being impacted and is requesting a status briefing
  - Core Processor vendor issues an emergency advisory recommending immediate containment actions
  - Industry websites and ISAC groups begin distributing indicators of compromise

Phase 3

- The vendor contacts you and states:
  - The AI fraud model was updated automatically three days ago
  - This software update, distributed during routine platform maintenance, was compromised before deployment
  - The change management process does not require Credit Union approval
  - The Vendor’s software integrity validation controls failed to detect the malicious modification
  - The Vendor’s logs for tracking model decisions are no longer available

Phase 3 – Discussion Questions

- Do you send a message to the public, or to members?
- Does your organization have sufficient AI policy and controls?
- Who owns accountability for AI decisions?
- What evidence is needed for regulators?
- How are potentially discriminatory or inaccurate AI actions assessed?

Phase 4

- A ransomware note appears on an on-premises server connected to the Core Processor environment.
  - Attackers claim that member and Credit Union data has been exfiltrated
  - The threaten to release both member and credit union financial data within 72 hours if not paid
- Simultaneously:
  - Cloud-hosted AI services begin failing integrity checks
  - API integrations between branch systems and cloud services become unusable

Phase 4

- The vendor contacts you and states:
  - Confirms the compromise which originated from a downstream 3rd party software supplier used within their development pipeline.

Phase 4 – Discussion Questions

- What are your recovery priorities?
- How are member impacts minimized?
- What manual processes are activated?
- What criteria determine restoration approval?
- How is the integrity of AI models validated before reuse?

Threat Scenario Summary

A sophisticated threat actor (APT) compromises a third-party software supplier used by your Core Processor vendor. Malicious code was inserted into a trusted software update package distributed to all financial institutions.

The Credit Union's AI Core systems automatically deployed the update to both the cloud-hosted AI services and the on-premises systems during a scheduled maintenance window.

Over the next several days, the malicious update establishes persistence, manipulates AI-assisted fraud scoring behavior, captured sensitive data, and created unauthorized communication channels between internal systems and attacker-controlled infrastructure.

Debrief Questions

- What were your top priorities?
- What worked well during the exercise?
- What areas did you struggle with?
- What can you take away from this to update your Playbook?

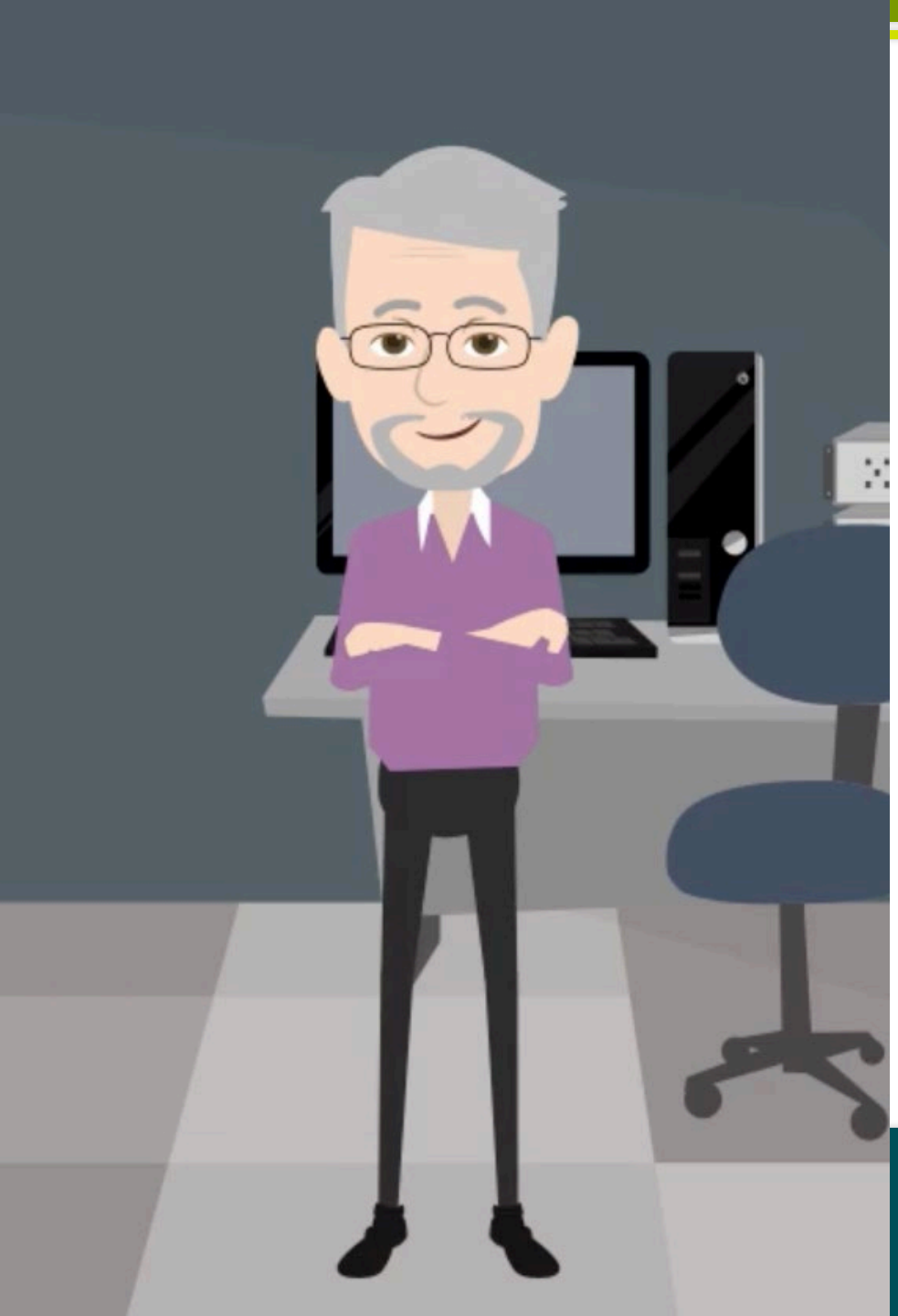
Debrief Questions

- Who is at fault for the breach? (CU or Vendor)
- What's an item you learned from another CU at your table?
- Are you using AI at your CU and how did this help you prepare for issues?

Questions to Take Home

- Where is your DR plan and IR playbook?
  - Digital or Physical
- Who is on your IR team?
  - Listed by name or position?
- How are you dealing with Change Management processing from third party vendors?
- What additional training, policies or controls will you be adding at your CU?

Questions?



Contact Information

- **Michael Bechtel**
- *Information Security Director*
- mbechtel@vfccu.org
- Toll-Free (800) 622-7494 ext. 1101
- Website: www.vfccu.org/solutions_mobile/risk_management.html