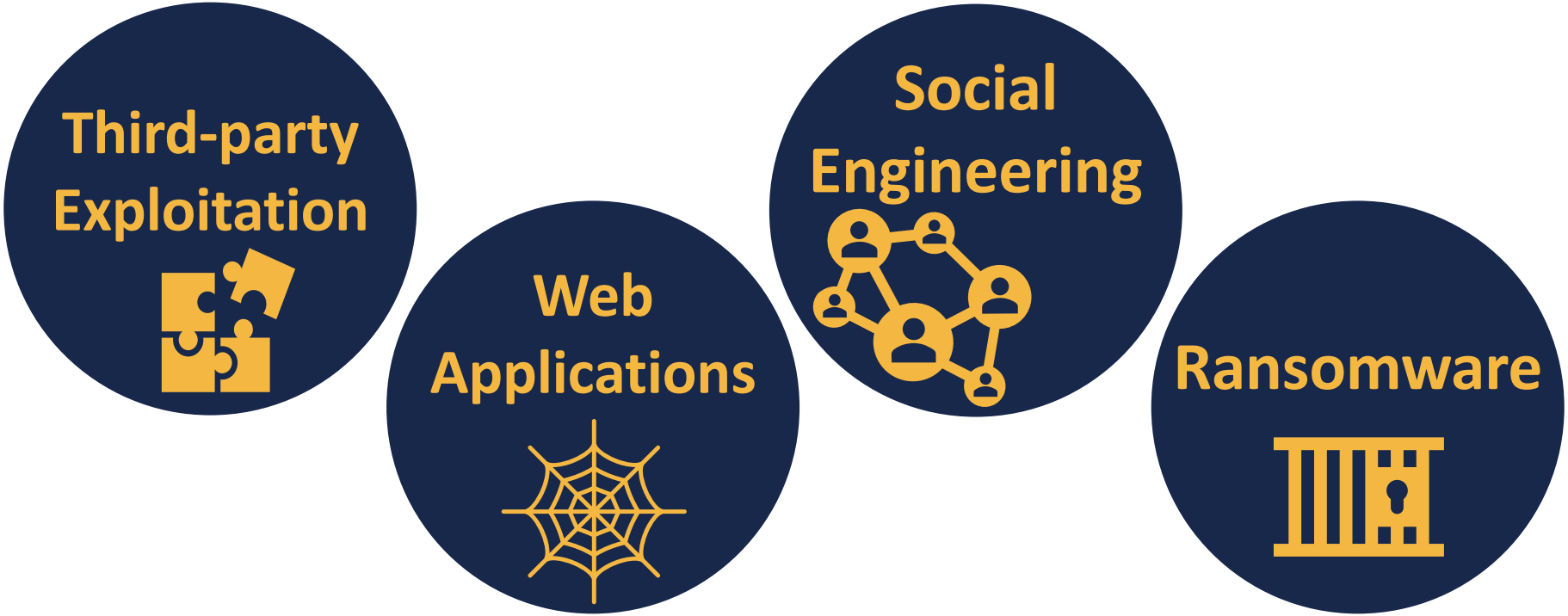
Cybersecurity Briefing

October 24, 2024

Overview

- Hacking Economics
- Cybersecurity Support Resources
- Cyber Incident Reporting
- Information Security Examination Program
- NCUA Cybersecurity Resources

Hacking Economics



Free Cybersecurity Support

- **Cybersecurity and Infrastructure Security Agency**
  - Regional Cybersecurity Expert
  - Cyber Hygiene - Vulnerability Scanning
  - Known Exploited Vulnerabilities
  - Automated Information Sharing Feed
- **U.S. Treasury**
  - Automated Threat Information Feed (OCCIP-Coord@treasury.gov)
  - Office of Intelligence and Analysis – T-Suite
- **U.S. Cyber Command**
  - UNDERADVISEMENT Threat Intel Sharing

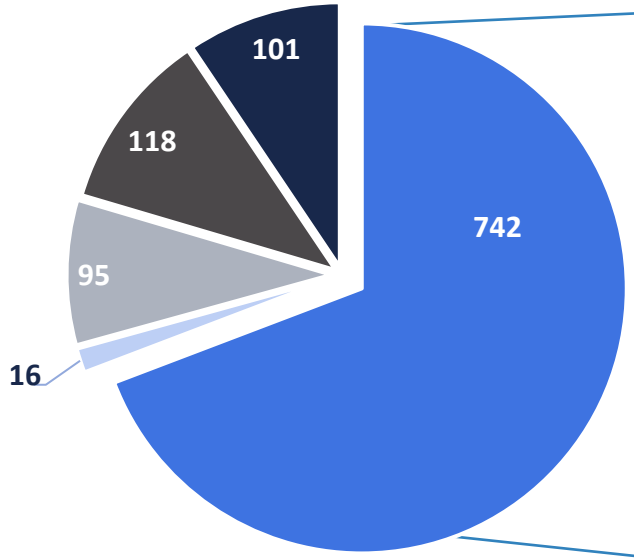
Trends Across the Credit Union System

- Outages caused by third-party service providers
- Ransomware attacks
- Business email compromises
- ATMs

Credit Union Reports and Third-Party Provider Incidents

Incident Reports = 1,072

Sep 1, 2023 - Aug 31, 2024



- 742 incident reports related to third-parties, grouped into 13 specific events.

Third-Party Events (13)	Impacted # of Credit Unions
Largest	234
Second Largest	200
Third Largest	55
Fourth Largest	50
Fifth Largest	40
Remaining 8 Combined	163*
Total	742*

*Count may include one or more of the same credit unions impacted by multiple events.

■ Third Party ■ Ransomware ■ Email Compromise ■ ATM ■ Other

Ransomware

- **The Financial Services Sector is the 5th most targeted sector out of the Nation's 16 critical infrastructure sectors.[1]**
- **Ransom demands are on average between $1 million and $10 million.[2]**
- **Credit unions should be prepared to respond to a ransomware incident.**

[1] FBI's Internet Crimes Complaint Center 2023 IC3 Annual Report

[2] FBI and CISA joint Ransomware notification update 8/7/2024 #StopRansomware: Blacksuit (Royal) Ransomware | CISA

Business Email Compromise and ATMs

- **Business email compromises**
  - 29% of reported credit union cyber incidents (not third-party related)
- **Cyber and fraud issues for ATMs/ITMs**
  - 36% of reported credit union cyber incidents (not third-party related)

Cyber Incident Reporting – Lessons Learned

- **Information sharing is critical**
- **Report all cyber incidents**
  - —Report when a third party provides an outage alert or notification (other than for planned maintenance)
- **Update NCUA throughout the lifespan of an incident**

Cyber Incident Reporting – What is reportable?

Within 72 hours a credit union must report a cyber incident as defined in the rule as:

- A substantial loss of confidentiality, integrity, or availability of a network or member information system that results from the unauthorized access to or exposure of sensitive data, disrupts vital member services, or has a serious impact on the safety and resiliency of operational systems and processes.
- A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities.
- A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise of a credit union service organization, cloud service provider, or other third-party data hosting provider or by a supply chain compromise.

Cyber Incident Reporting – What's Next

- **NCUA is implementing a new cyber incident reporting webform**

To report a cyber security incident, please complete the following form below in it's entirety.

Note: Please **DO NOT** provide samples of malicious code in this form.

New or Modified Incident

*Is this a New, Modified, or Corrected Cyber Incident report?

New

Reportable Cyber Incident Details

The credit union has experienced a Cyber Incident resulting in:

Check all that apply.

- A substantial loss of confidentiality, integrity, or availability of a network or member information system.
- A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities.
- A disruption of business operations or unauthorized access to sensitive data facilitated through, a compromise of a credit union service organization, cloud service provider, or other third-party data hosting provider or by a supply chain compromise.

Description of the event:

Add Attachments

Max file size = 5MB

Information Security Examination (ISE) Program

- **Implemented in February 2023**
- **Strengths**
  - — Anti-virus/malware
  - — Patching
  - — Access controls
  - — Policies and procedures
  - — Network security controls

Information Security Examination (ISE) Program

- **Opportunities for improvement**
  - — Information security risk assessments
  - — Business continuity programs
  - — Incident response programs
  - — Examinations of third-party vendors

Board of Director Engagement in Cybersecurity Oversight

- Provide for recurring training
- Approve information security program
- Oversee operational management
- Ensure effective incident response planning and resilience

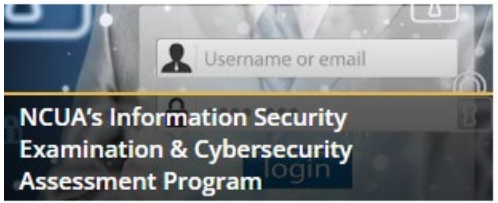
NCUA Cybersecurity Resources

- **Automated Cybersecurity Evaluation Toolbox (ACET)**
  - The ACET helps credit unions
    - Identify and measure inherent risk
    - Evaluate cybersecurity maturity over time
  - Free to download from NCUA.gov
  - Completely voluntary

NCUA Cybersecurity Resources

Cybersecurity Resources

- NCUA's Information Security Examination and Cybersecurity Assessment Program
- ACET and Other Assessment Tools
- Supply Chain Risk Management (SCRM)
- Catastrophic and Incident Reporting
- NCUA's Regulations and Guidance
- References & Resources



www.ncua.gov/cybersecurity