Principle Security.

ORIGINAL RESEARCH · 2026 EDITION

The Credit Union Cyber Incident *Landscape*

What NCUA's incident-reporting data actually says about where credit-union cyber risk lives — 1,072 reports, 13 vendor events, and the examination priorities they shaped.

JULY 2026 · PRINCIPLESEC.COM/RESEARCH · PRINCIPLES FIRST, SECURITY ALWAYS

KEY FINDINGS

Seven in ten incidents weren't about the credit union at all

In the first twelve months of NCUA's 72-hour cyber incident notification rule (September 1, 2023 – August 31, 2024), federally insured credit unions filed **1,072 incident reports**. The defining pattern: the credit union cyber problem is overwhelmingly a **vendor** problem.

1,072
Incident reports in the rule's first year

69%
Traced to third-party service providers (742 reports)

13
Vendor events behind all 742 third-party reports

434
Credit unions impacted by the two largest vendor events alone

46:1
Vendor-related reports vs. ransomware reports

539
Reports in the 12 months ending April 2025 — volume halved as reporting calibrated

Bottom line: when one shared provider stumbles, hundreds of institutions file the same 72-hour report on the same day — and their members feel the same outage. Concentration risk is the sector's defining cyber exposure.

Incident reports by category — year one

Category	Reports	Share
Third party	742	69.2%
ATM / ITM	118	11.0%
Other	101	9.4%
Email compromise	95	8.9%
Ransomware	16	1.5%

VENDOR CONCENTRATION

Thirteen events. Two of them hit 434 credit unions.

The 742 third-party reports collapse into **13 distinct vendor events**. Five events account for 78% of all vendor-related reports; the average event touched **57 institutions**.

Vendor event	Credit unions impacted
Largest	234
Second largest	200
Third largest	55
Fourth largest	50
Fifth largest	40
Remaining 8 combined	163

Counts may include credit unions impacted by multiple events, per NCUA's caveat.

Ransomware is loud. Vendors are lethal.

Ransomware produced just **16 of 1,072 reports (1.5%)** — though stakes per event remain brutal: FBI/CISA put typical demands at **$1–10 million**, and financial services ranks 5th most-targeted among 16 critical infrastructure sectors.

Strip out vendor events, and credit unions' own incidents split largely between **ATM/ITM cyber-fraud (36%)** and **business email compromise (29%)** — operational fraud surfaces, not exotic intrusions.

> **For boards:** the headline threat in the news and the frequent threat in the data are different things. Budget for both — but audit vendor oversight first.

THE EXAMINATION MIRROR

Strong tools, weak programs

Across four years of Information Security Examinations, NCUA reports consistent **strengths** in anti-malware, patching, access controls, policies, and network controls — the things you can buy. Its named **opportunities for improvement**: information security risk assessments, business continuity, incident response programs, and third-party vendor examination — the things you have to *operate*.

The gap is coherent: the sector's biggest reported exposure (vendors) maps directly onto its weakest examined discipline (vendor oversight). NCUA's **2026 supervisory priorities** (Letter 26-CU-01) respond in kind — examiners will assess "governance and risk assessment frameworks, vendor management and oversight, security controls to protect member data" around payment systems — and NCUA's cybersecurity briefing urges boards to **provide for recurring training** and approve the information security program.

Five moves the data argues for

- ✓ **Risk-tier the vendor inventory** and put real evidence requirements on the critical tier — 69% of the sector's incident reports started there.
- ✓ **Wire vendor-incident intake into your 72-hour reporting path** — most reports you will ever file begin with a provider's outage notice, not your own SOC.
- ✓ **Rehearse the reporting decision** before the clock starts: criteria, templates, and a tabletop beat improvisation at 2 a.m.
- ✓ **Fund the programs, not just the tools** — risk assessment, business continuity, and incident response are where examinations consistently find gaps.
- ✓ **Calendar recurring board cybersecurity training** — NCUA guidance calls for it, and the 2026 priorities letter is addressed to your board.

Sources & methodology

NCUA Cybersecurity Board Briefing (Oct 24, 2024); NCUA 2025 Cybersecurity & Credit Union System Resilience Report to Congress (May 2024–Apr 2025; 539 incidents, none systemic, $86T transactions); NCUA 2026 Supervisory Priorities (Jan 14, 2026); FBI IC3 2023 and CISA advisories for sector context. Percentages computed by Principle Security from published figures.

PUT THIS INTO PRACTICE

Your examiners have read this data. Have you?

Principle Security builds the vendor-oversight and incident-reporting programs this landscape demands — from operators who have run credit-union security programs through real examination cycles.

Book a 30-minute intro

info@principlesec.com · +1 (877) 886-0677 · principlesec.com/services/ncua

Full report: principlesec.com/research/credit-union-cyber-incident-landscape