PURE IT

# Key Principles of Incident Response

Steve Koinm – CISSP, CCSK, SAS-AP – CISO Pure IT Credit Union Services


# Steve Koinm

## CISSP, CCSK, SAS-AP

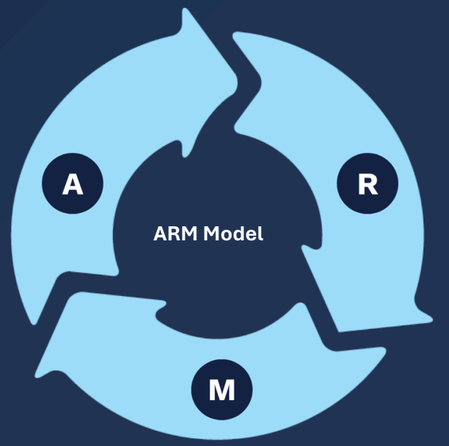
CISO, Co-Founder, and VP of Professional Services
Steve.koinm@pureitcuso.com

- Serves as the internal CISO for Pure IT Credit Union Services and as a virtual CISO or CIO to many clients
- Active in providing assessments and roadmaps for credit unions in People, Process, Technology, and Business Management
- An advisor to credit union Boards who need to provide a credible challenge to their technology teams and a regular speaker at security and credit union industry conferences throughout the country
- Advisory Board Member of the National Credit Union Information Sharing and Analysis Organization (NCU-ISAO).

PURE IT

**Our mission:** To bring credit unions more cost-effective, cutting-edge, and business-enabling technology.

- Infrastructure & Operations Assessments,
- IT Projects, implementation and remediation
- Complete IT Managed Services
- CISO, CIO, CTO, Executive Advisory Services




**Assess. Remediate. Manage**

PURE IT

# Questions?

Email questions to info@leagueinfosight.com

“By failing to prepare,
you are preparing to fail.”

- Ben Franklin

# “There is no ‘I’ in team, but there is an ‘I’ in win.”

**- Nick Saban**

# CREDIT UNION INDUSTRY CYBER & FRAUD RISK MONTHLY EXECUTIVE SUMMARY

NCU-ISAO

## AUGUST 2024

## KEY TAKEAWAYS

A problematic update at CrowdStrike caused an IT outage that impacted a wide range of companies around the world. The root cause of the outage was a rapid response update in channel file 291 that was pushed overnight on July 19th. The file included null-byte information that caused Windows machines to go into a blue-screen error loop. Because computers would not boot, the fix also required physical access to the machine, which further compounded the timeline of the outage.

### Notable News & Breaches

A failed sensor update from CrowdStrike caused Windows computers around the world to crash and show the infamous "Blue Screen of Death (BSOD)." Some credit unions and their providers had parts of their operations disrupted until the corrupted file could be removed. This was especially challenging for some businesses, as the fix could not be administered remotely.

### Government & Regulatory Updates

The U.S. Treasury Department's FinCEN has proposed updates to anti-money laundering (AML) and countering the financing of terrorism (CFT) compliance obligations. The update includes

NCU-ISAO

## Advisories

Daily Advisory email

Monthly 1 page for the board

Member Alerts

Physical Security Alerts

Intelligence Gathering

Annual Tabletop Exercise

## Working Groups

Fraud

Generative AI

Physical Security

Risk & Compliance

Threat Briefings

## Slack Community

Countermeasures & Best Practices

Fraud Intel

Generative AI

Physical Security

Risk & Compliance

Threat Intel

## Darkweb Monitoring

BIN Monitoring

Check Monitoring

Chatter

Exploits and Malware Blogs

PURE IT

NCU-ISAO

## Membership Fees

501(c)(6) Non-Profit

Less than $100M - $250/yr.
$100M to $250M - $500/yr.
$250M to $500M - $1,000/yr.
$500M TO $1B - $2,500/yr.
Over $1B - $5,000/yr.

PURE IT

| | Ransomware | Cocaine Trafficking in 1992 |
|---|---|---|
| Revenue/Unit | $140,000/attack | $60,000/kilo |
| Operating Costs/Unit | $2,500/attack* | $5,000/kilo |
| Profit Margin | 98% | 91% |
| Arrests/Unit | .0008** | .50 |
| Deaths/Unit | 0 | .25 |
| Barriers to Entry | None | Very High |

**Estimate based on reported costs of network access credentials, and amount of hours a threat actor expends on the average attack*

***Estimated roughly 25,000 ransomware attacks of impact in 2020. Research found evidence of less than 20 total arrests globally.*

The barriers to entry in Cybercrime are LOW. The risks to Cybercrime are LOW. The likelihood to be killed are near zero!

Easy cloud hosting

Anonymous delivery

24/7 global access

PURE IT

# Preparation

Constantly under attack, Always monitoring

**Prevention**

Reasonable Controls  - Point in time

**Relevant**

IR Requires Commitment to keep it updated

**Incident Response is not Disaster Recovery**

Much more than DR.  It is migration, preparation, response, and management.

**Not just Cyber Incidents**

Broad coverage for different types of incidents.

PURE IT

# Detection and Analysis

Playbooks for common incident vectors

## Fraud

ATM

Check

Zelle

## Malware

Local Workstation

Remote User

## Phishing

Credential Harvesting

BEC

## Third Party

Notification

Compromised Member Data

Service Unavailable

PURE IT

# Manage

What is the loop through the incident?

**Containment**

**Eradication**

**Recovery**

PURE IT

# Post Incident

- Lessons Learned
- Root Cause Analysis
- Incident Reporting

PURE IT

# Root Cause Analysis

## Identifiable

Need to have the data to be able to make this determination

## Specific

Not a generalization

## Could Stop Recurrence

Would enable a change in the incident

## Ability to Fix

There are resources to fix the issue and make the change

PURE IT

# Post Incident

- Lessons Learned
- Root Cause Analysis
- Incident Reporting

PURE IT

# Questions?

# CU Intersect 2024

- Cybersecurity conference made for credit unions
- Hosted by Pure IT and NCU-ISAO
- Topics include
  - Emerging **technologies** like AI, physical hacking tools, and SASE
  - **Security** considerations for credit unions of all sizes: how can we keep member data protected?
  - The latest **resiliency** solutions and strategies


PURE IT

# Thank you!

PURE IT

info@pureitcuso.com
281-378-7737
pureitcuso.com

Connect with us on social media!