NetCov

Two Mondays Two Outcomes

Bill Goldin
Senior VP, Cybersecurity

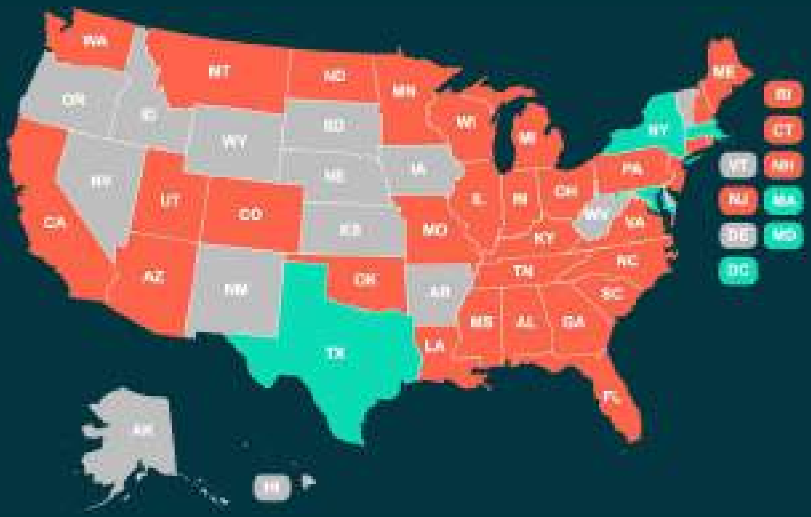
By the Numbers

1996 COMPANY FOUNDED

350+ STAFF MEMBERS

50K+ SUPPORTED USERS

185+ CREDIT UNIONS SERVED

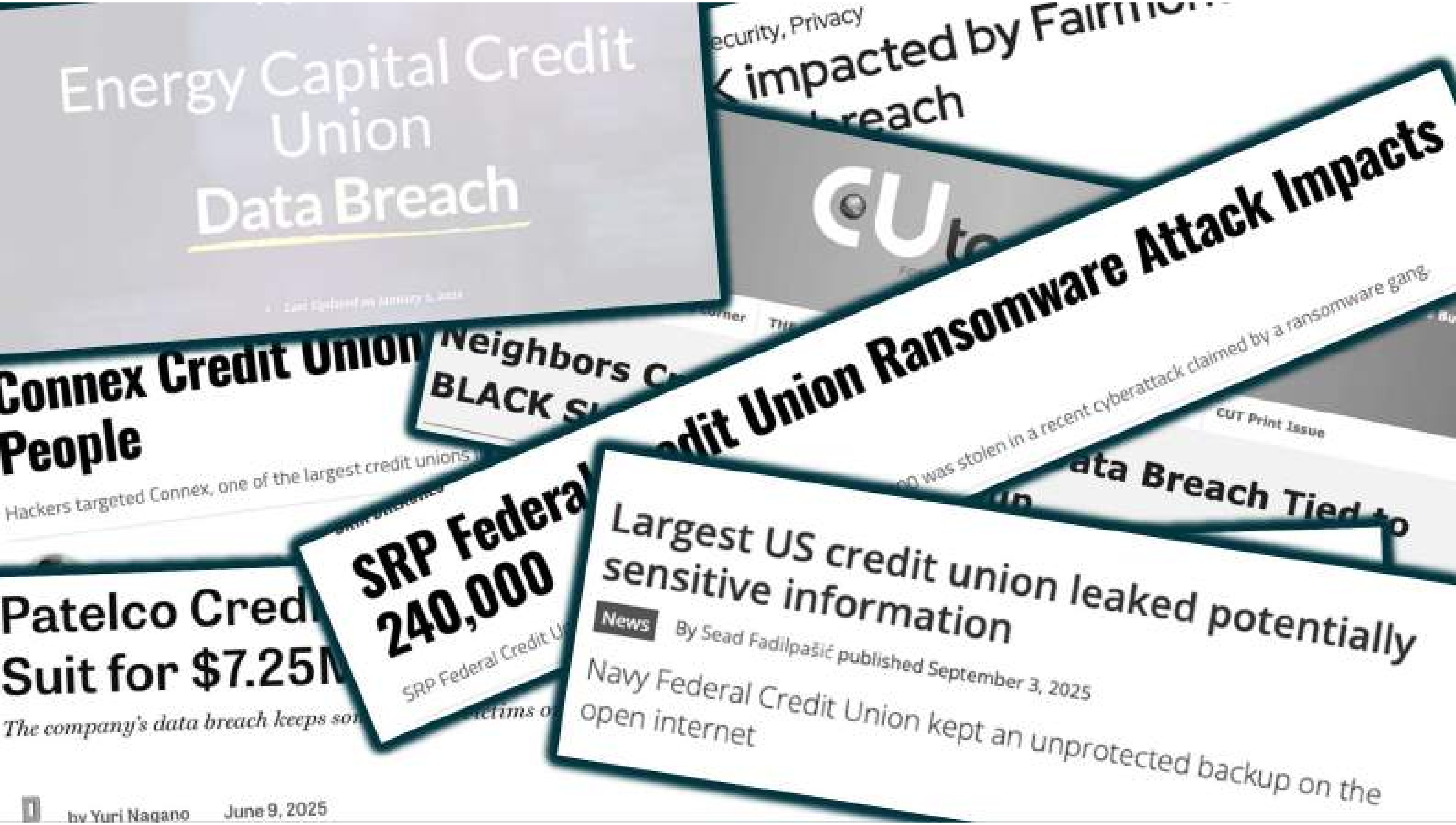


We're **strategically staffed** nationally, with team members in 35 states and the District of Columbia, in addition to our **five offices** in Boston, New York, Baltimore, Fort Worth and Washington, D.C.

G 4.9/5 ★★★★★ bizratings.com 9.6/10 ★★★★★ GLASSDOOR 4.4/5 ★★★★★

Today's Agenda

1. Ransomware Headlines: Recent CU Incidents
2. Two Mondays: Two Organizations, Two Very Different Outcomes
3. What Happened Next: Impact, Response, Recovery
4. Lessons Learned: Three Key Takeaways
5. Ransomware Preparedness Checklist
6. Running an Effective Ransomware Tabletop



Energy Capital Credit Union Data Breach

Last Updated on January 5, 2024

ecurity, Privacy

K impacted by Fairmon
breach

CU to

orner

TH

Connex Credit Union
People

Hackers targeted Connex, one of the largest credit unions

Neighbors C
BLACK S

dit Union Ransomware Attack Impacts

00 was stolen in a recent cyberattack claimed by a ransomware gang

CUT Print Issue

ata Breach Tied to

Patelco Cred
Suit for $7.25M

The company's data breach keeps so *ictims o*

by Yuri Nagano June 9, 2025

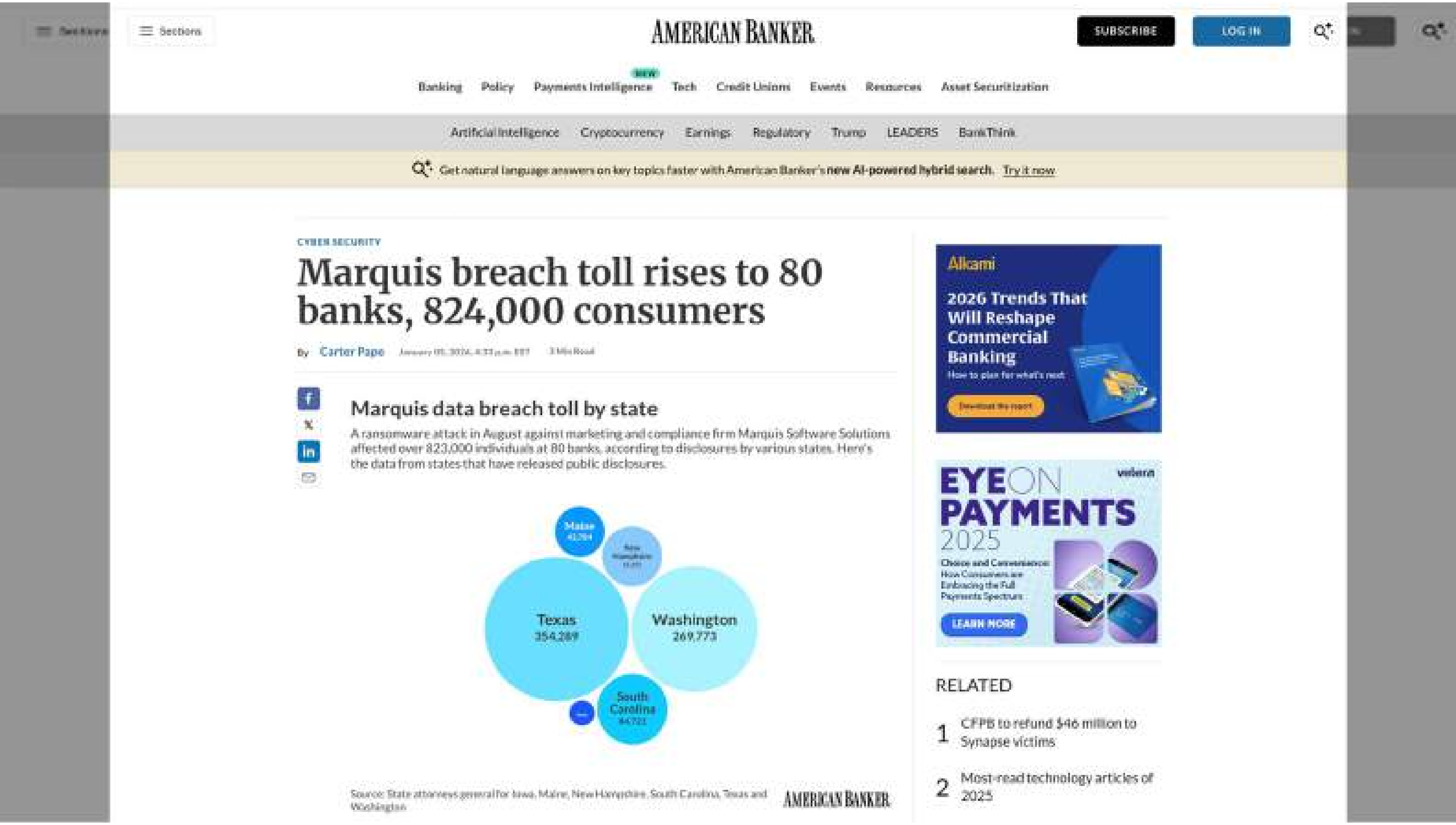
SRP Federal
240,000

SRP Federal Credit U

Largest US credit union leaked potentially sensitive information

News By Sead Fadilpašić published September 3, 2025

Navy Federal Credit Union kept an unprotected backup on the open internet



Get natural language answers on key topics faster with American Banker's **new AI-powered hybrid search.** Try it now

CYBER SECURITY

Marquis breach toll rises to 80 banks, 824,000 consumers

By Carter Pape January 05, 2026, 4:33 p.m. EST 3 Min Read

Marquis data breach toll by state

A ransomware attack in August against marketing and compliance firm Marquis Software Solutions affected over 823,000 individuals at 80 banks, according to disclosures by various states. Here's the data from states that have released public disclosures.

Source: State attorneys general for Iowa, Maine, New Hampshire, South Carolina, Texas and Washington

AMERICAN BANKER

RELATED

1 CFPB to refund $46 million to Synapse victims

2 Most-read technology articles of 2025

NetCov

Pop Quiz!

Put your **hands** in the **air** for **Ransomware!**

NetCov

Storytime: Tale of 2 Mondays

Bill Goldin

Senior VP, Cybersecurity

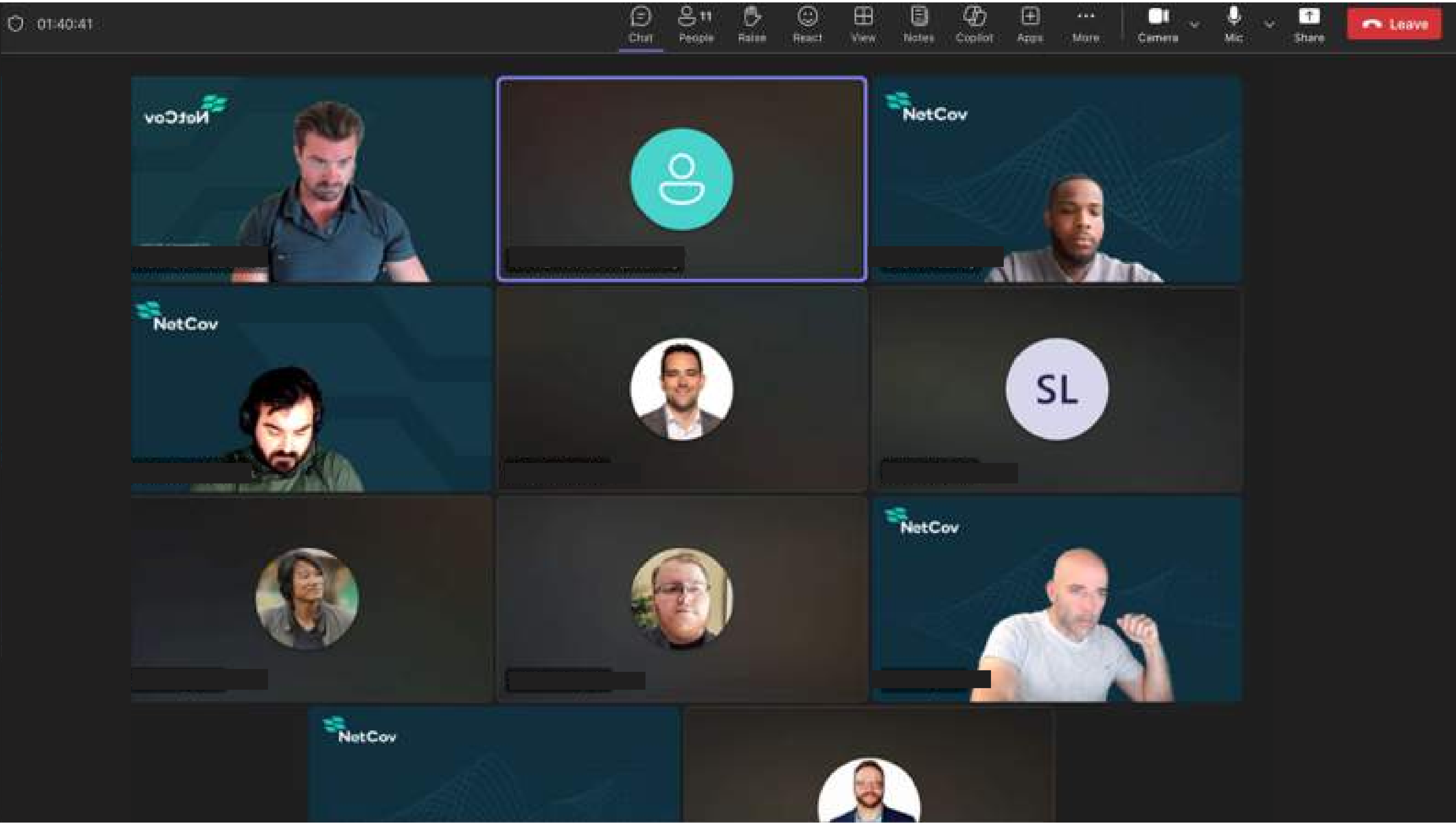
About Blindside Enterprises

- ✓ **Service** industry
- ✓ **300** employees
- ✓ **5** offices
- ✓ **2** internal IT staff members
- ✓ Recently **acquired**

THIS IS FINE
RANSOMWARE

Decision Time – What Will You Choose?

Cyber insurance route
Start the restore


01:40:41
Chat
People 11
Raise
React
View
Notes
Copilot
Apps
More
Camera
Mic
Share
Leave
NetCov
[redacted]
[redacted]
[redacted]
NetCov
NetCov
[redacted]
[redacted]
SL
[redacted]
[redacted]
[redacted]
NetCov
NetCov
NetCov

The Rest of the Week

Tuesday ⇨

Wednesday ⇨

Thursday ⇨

Friday!

Blindside's
Business Impact

- ✓ **5** days of downtime
- ✓ **110,000** files encrypted
- ✓ **Hundreds** of coordinated hours
- ✓ Significant **revenue** impact
- ✓ **2-3 weeks** full of restores, password changes, etc.
- ✓ **400 hours** of NetCov time

About Pragmatic

- ✓ **Manufacturing** industry
- ✓ **600** employees
- ✓ **7** offices
- ✓ **5** internal IT staff members

THE
PRAGMATIC
CORPORATION
PRAGMATIC
CORPORA

The Bigger Picture

- ✓ We had one client hit hard but **three others like "The Pragmatic Corp"**

- ✓ **MDR** service to the rescue!

- ✓ **NOC team** reviewed over **400 firewalls** and disabled all affected SSL VPN access as we worked on **"Blindside Enterprises"**

“From the moment your team reacted to the initial breach and flawlessly executed the lockdown, to gaining a clear picture of the situation, you didn’t miss a beat or flinch despite the enormity of the challenge.

This **could have been a complete disaster** for us, and without a doubt, **the NetCov team played the biggest role in preventing that from happening**.

Thank you. Thank you. Thank you.”

-- Senior Manager, IT Infrastructure & Security
(Blindside Enterprises)

Lessons Learned

1

2

3

Ransomware Preparedness Checklist

Governance & Policy

□ Ensure an **Incident Response Plan (IRP)** includes ransomware-specific scenarios

□ Define **roles and responsibilities** for executives, IT, compliance, and communications

□ Confirm **regulatory reporting requirements** (NCUA, FFIEC, state laws).

Ransomware Preparedness Checklist

Backup Strategy

❑ Maintain **offline, immutable backups** of critical systems and data

❑ Test **backup restoration** at least quarterly

❑ Store backups in **multiple locations** (on-prem and cloud)

Ransomware Preparedness Checklist

Access Controls

- □ Enforce **MFA** for all privileged accounts and remote access
- □ Implement **least privilege** and regular access reviews
- □ Disable unused accounts promptly

Ransomware Preparedness Checklist

Patch & Vulnerability Management

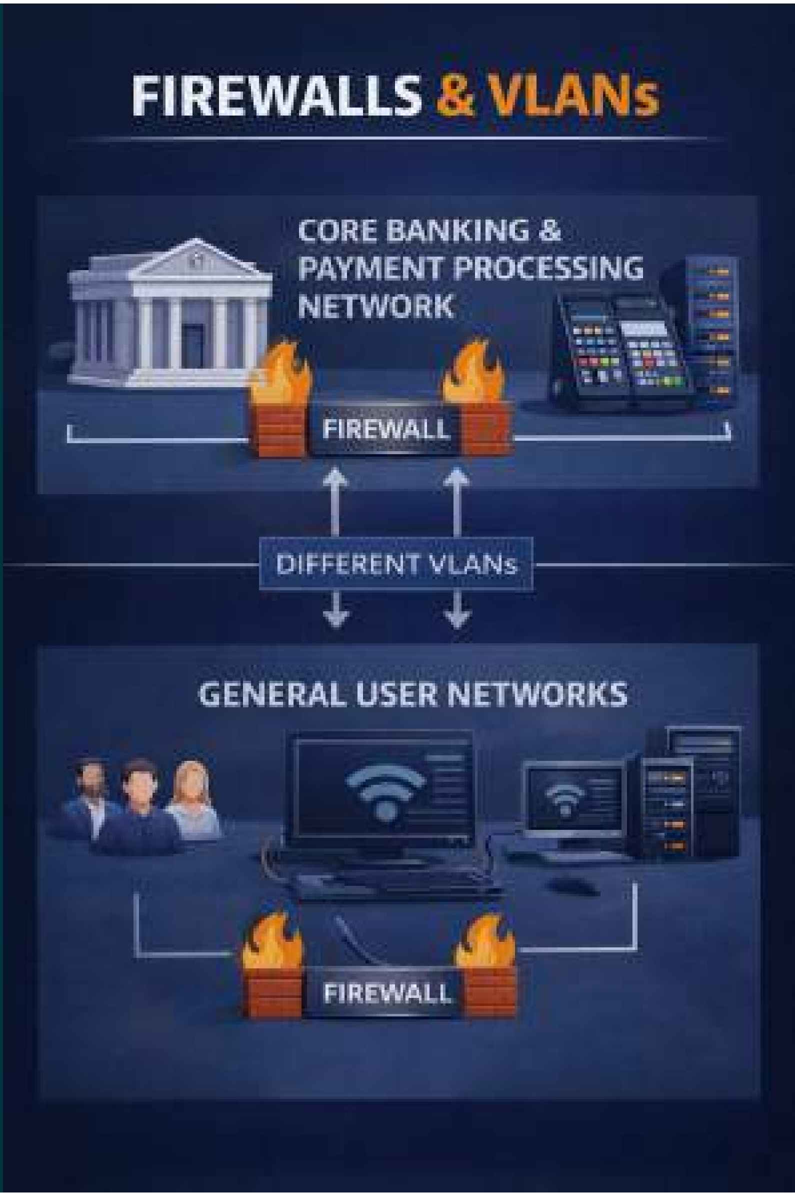
□ Apply **critical patches** within 24–48 hours

□ Run **regular vulnerability scans** and remediate findings quickly

Ransomware Preparedness Checklist

Network Segmentation

- ❑ Separate **critical systems** (core banking, payment processing) from general user networks
- ❑ Limit **lateral movement** with internal firewalls and VLANs



Ransomware Preparedness Checklist

Email & Endpoint Security

- □ Deploy **advanced email filtering** and sandboxing
- □ Enable **EDR/XDR solutions** for real-time threat detection
- □ Block **macro-enabled attachments** and suspicious file types

Ransomware Preparedness Checklist

User Awareness

- □ Conduct **phishing simulations** quarterly
- □ Train staff on **reporting suspicious activity** immediately

Report Suspicious Activity
1. Be Alert for Suspicious Emails
2. Report Strange Behavior
3. Follow Security Procedures

Ransomware Preparedness Checklist

Incident Response Readiness

□ Maintain **contact lists** for law enforcement, regulators, and cyber insurance

□ Pre-arrange **forensic and legal support**

□ Validate **cyber insurance coverage** for ransomware events

Ransomware Preparedness Checklist

24/7/365 Security event log Monitoring

- □ Confirm all **Networking equipment** is monitored (firewalls, switches, WAPs, etc.)
- □ **Eyes on glass** at all times to review security events before they become Incidents
- □ Make sure you have **1 year of retention** for logs
- □ SaaS, On-prem, and Cloud are all centrally logged

Ransomware Attack Detected!
72:16:47
Pay Ransom to Decrypt Files!
RANSOMWARE ATTACCK
Ransomware
TABLETOP
INCIDENT RESPONSE

Tips for Running a Ransomware Tabletop Exercise

Before the Exercise

- □ **Define objectives:** e.g., test decision-making, communication flow, regulatory compliance

- □ **Select a realistic scenario**: ransomware encrypts the core banking system and demands payment

- □ **Invite cross-functional participants**: IT, compliance, operations, legal, communications, executive leadership

Tips for Running a Ransomware Tabletop Exercise

During the Exercise

- ❑ **Simulate timeline pressure:** escalate events every 15 -30 minutes

- ❑ **Include injects:** Regulator requests update, Member complaints on Social Media, Local media inquiry about service outage

- ❑ **Force critical decisions:** Pay ransom or not? Notify Members now or later? Engage Law enforcement

Tips for Running a Ransomware Tabletop Exercise

After the Exercise

- ❑ Conduct a hot wash immediately.
- ❑ Document gaps and lessons learned.
- ❑ Update IRP and playbooks based on findings
- ❑ Put together a plan to address the gaps

You will **always pay** for cybersecurity: **proactively** or **reactively**

NetCov

Thanks for joining! Swing by **Booth #820** to say hello, talk shop and get to know **our amazing team**!

Alicia Dzurenko
Sr. Account Executive

Steven Koss
Account Executive

Bill Goldin
SVP, Cybersecurity

#PEOPLEBEFORETECH