FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, October 17, 2025

Tackling Familiar Cyber Threats with Smarter Tools

Source: Independent Banker

Auburn Bank prides itself on being a locally minded institution. The $977 million-asset community bank has clients in every state and even internationally, but its focus is on Auburn, Alabama, says Jerry Siegel, senior vice president and chief technology officer.

The community bank has worked hard to build a good reputation within the community, which is why Siegel also knows that if there's ever a data breach, it won't just be a blip of a news story. It could put the whole bank at risk.

"We're in a small town," he says. "A breach would be more detrimental to us and our customer reputation than if it would be at a larger institution."

Community banks have built their reputation on trust, which can be damaged by a successful cybersecurity attack.

(*Click the heading link to read more.*)

Top News

Identify and Mitigate Potential Compromise of Cisco Devices

Source: Cybersecurity & Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 25-03 in response to an advanced threat actor targeting Cisco Adaptive Security Appliances (ASA) via web services. This is the second emergency directive issued under the Trump Administration. This widespread campaign poses a significant risk to victims' networks by exploiting zero-day vulnerabilities that persist through reboots and system upgrades.

The Emergency Directive mandates that all Federal Civilian Executive Branch Departments and Agencies account for all in-scope devices, collect forensic data, and assess any compromises using CISA-provided procedures and tools. Additionally, they must disconnect end-of-support devices and upgrade those that will remain in service.

“As the lead for federal cybersecurity, CISA is directing federal agencies to take immediate action due to the alarming ease with which a threat actor can exploit these vulnerabilities, maintain persistence on the device, and gain access to a victim’s network," said CISA Acting Director Madhu Gottumukkala. "The same risks apply to any organization using these devices. We strongly urge all entities to adopt the actions outlined in this Emergency Directive."

As federal civilian agencies implement this mandate, CISA will assess and support agency adherence and provide additional resources as required. CISA is committed to using its cybersecurity authorities to gain greater visibility and drive timely risk reduction across federal civilian agencies.

(Click the heading link to read more.)

Emerging Cybersecurity Threats That Could Impact Your Business

Source: Clark Schaefer Consulting

As we approach the end of 2025, the cybersecurity landscape continues to grow in complexity. For IT leaders and decision-makers, staying on top of rising threats is critical to protecting sensitive data, maintaining customer trust, and ensuring business continuity.

We’ve compiled the top risks organizations should prioritize this year and continue to monitor in the years ahead as cyber threats become more sophisticated:

1. AI-Fueled Threats

The use of artificial intelligence (AI) to automate attacks and create highly targeted malware has soared among cybercriminals. These AI-driven threats can adapt in real time, making traditional defenses less effective. Organizations should implement proactive, AI-enhanced monitoring solutions to detect and respond to evolving threats.

2. Ransomware Targeting Critical Infrastructure

Critical infrastructure is in the crosshairs of ransomware attacks, with the intention of causing absolute chaos rather than just financial loss. Recent incidents, such as the Collins Aerospace attack that disrupted European airport operations, highlight the operational and reputational risks. IT and security teams should maintain tested incident response plans, business continuity strategies, and offline backups.

(Click the heading link to read more.)

DHS and CISA Announce Cybersecurity Awareness Month 2025

Source: CISA

The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) announced the official beginning of Cybersecurity Awareness Month 2025. This national campaign, administered by CISA, will give partner agencies and the private sector the tools, support, and information they need to secure the vital services fundamental to our civilization: water, power, communications, food, finance, and more. This year's theme is Building a Cyber Strong America, as CISA gets back on mission to be the nation's leading cybersecurity agency.

This campaign engages with all levels of government and businesses big and small. It calls on everyone – state, local, tribal and territorial (SLTT) governments, small and medium businesses, and entities involved in our supply chains – to take cybersecurity into their own hands to secure the Homeland in a world of constantly-evolving threats.

"Cybersecurity is a critical theater in defending our homeland," said Homeland Security Secretary Kristi Noem. "Every day, bad actors are trying to steal information, sabotage critical infrastructure, and use cyberspace to exploit American citizens. Taking down these threats requires a strong private-public partnership, and the reforms we've implemented at CISA have empowered them to work with all of our partners to take down these threats and make America cyber secure again. This Cybersecurity Awareness Month is the time for us to continue our efforts to build a cyber strong America."

Cyber threats never take a day off. CISA and DHS urge every citizen, government entity, and business to remain vigilant and work to neutralize cyber threats before they cause damage.

(Click the heading link to read more.)

This Channel is Often Regional Banks' Cybersecurity Blind Spot

Source: BAI

In recent years, customers of at least one California financial institution received numerous fraud calls spoofing the bank's actual phone number, asking for debit card numbers, PINs, and other sensitive data. It's not a singular event. Banking leaders there and elsewhere emphasize regularly to customers that the bank would never initiate such requests via phone. Still, customers were unprepared for the barrage of unwanted impersonation robocalls.

While larger financial services firms have prioritized securing their communication channels from robocall fraud, regional and smaller banks have historically faced budget challenges allowing them to keep pace and do the same. This creates a vulnerability gap bad actors can exploit, enabling scammers to launch impersonation attacks where they pose both as bank employees targeting their customers (outbound) or as customers targeting the bank (inbound).

As fraud attempts become more frequent, phishing and spoofing attacks aren't just an IT issue -they're a business risk that directly impacts the customer experience and brand reputation. Regional banks' IT and security leaders must recognize voice fraud as a serious attack vector, one that demands the same level of protection as other core cybersecurity threats.

Evolving fraud tactics exploiting the voice channel

Without proper voice channel authentication measures, smaller and regional banks are unwittingly leaving attack surfaces for bad actors open for fraud. The stakes are high, as recent survey data finds that the voice channel remains core to bank customer engagement: 64% of consumers prefer to engage with their financial services provider via a phone call over any other method (text messaging, apps, website).

(Click the heading link to read more.)