



Ahead of the Threat: Cyber Landscape Heading Into 2027

Understanding emerging threats and where to focus next.

October 14, 2026



Presenters



Pat Dixon

VP, Sales



Pat Heller

VP, FI Sales



Bill Szumski

*VP, Support &
Security Services*



Adam Ward

*Business
Development
Manager, FI Sales*



Agenda

- The Evolving Threat: Fraud, AI & the Human Element
- Business Email Compromise: How Attackers Exploit Trust
- AI Adoption, Governance & Emerging Risks
- What's Ahead for Security and Compliance
- Open Q&A





The Evolving Threat: Fraud, AI & the Human Element





Cyber Threats Are Becoming More Personal



AI-Driven Scams

Deepfakes and impersonation are making fraud harder to recognize.



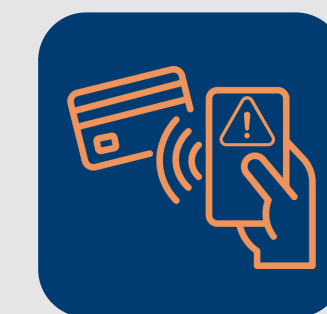
Account Takeovers

Compromised credentials can give attackers access to trusted accounts.



Financial Fraud

Account holders are facing increasingly convincing scams.



Digital Payment Risks

Growing digital wallet adoption creates new fraud prevention challenges.

The Human Defense: Awareness & Education

Technology alone can't prevent every attack. Ongoing employee training and customer education help people recognize threats and stop fraud before it happens.





From Theory to Reality

Real-world examples of cyber threats in action.



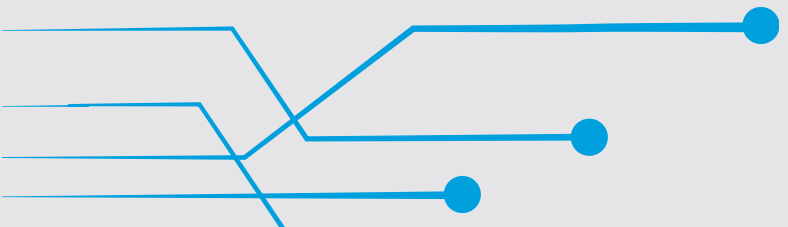
Scenario 1: Voice-Phishing (Vishing) Attack

A major financial technology provider experienced a **voice-phishing (vishing) attack** that led to unauthorized access within its internal corporate environment. **The incident involved an extortion attempt and exposure of personal information affecting FI clients.**



Scenario 2: Business Email Compromise (BEC)

A threat actor impersonated the CEO using a lookalike **.co** domain instead of **.com** and sent the Controller an urgent, confidential wire transfer request. The email appeared authentic, including the CEO's real signature, and resulted in a **~\$300,000 fraudulent transfer.**





Business Email Compromise: How Attackers Exploit Trust





The Path From Compromise to Fraud



These attacks often rely on social engineering rather than malicious attachments or links.





BEC Defense Goes Beyond Email Security

As impersonation tactics become more convincing, layered defenses are essential to staying ahead.



Multi-Factor Authentication

Protect accounts from unauthorized access.



Payment Verification

Confirm changes through a trusted channel.



Employee Awareness

Recognize impersonation and unusual requests.



Account Monitoring

Detect suspicious activity before fraud occurs.





AI Adoption, Governance & Emerging Risks



Poll Question #1

Which AI tools are employees using at your organization?

Select all that apply



- ☐ **Company-approved AI tools (e.g., Microsoft Copilot)**
- ☐ **Personal or free AI tools (e.g., ChatGPT, Claude, Gemini)**
- ☐ **AI features built into existing applications**
- ☐ **Unsure which AI tools are being used**



AI Is Already in Your Business.

Do You Know Where?



Unapproved AI Tools

Employees may be using unapproved AI tools without IT oversight or proper security controls.



Sensitive Data Exposure

Business or customer information may be shared with AI tools, putting sensitive data at risk.



New Security Vulnerabilities

AI tools can introduce new security risks if they aren't properly evaluated, configured, and secured.



You can't manage AI risks you don't know exist.



AI Governance: Five Questions Every Business Should Answer



Building a Foundation for Responsible AI

Clear policies and oversight help businesses adopt AI responsibly, protect sensitive information, and manage risks while maintaining control.

- **Approved Tools:** Which AI tools can employees use?
- **Data Protection:** What information can be shared?
- **Ownership:** Who approves new tools?
- **Monitoring:** How is AI usage tracked?
- **Security:** How will AI access and data be protected?



AI adoption needs clear ownership, policies, and oversight.



Poll Question #2

Which AI governance controls does your organization currently have in place?

Select all that apply



- ☐ **Written AI acceptable use policy**
- ☐ **List of approved AI tools**
- ☐ **Rules for sharing data with AI**
- ☐ **Process for approving and monitoring AI tools**
- ☐ **None of the above**





What's Ahead for Security and Compliance





Building Stronger Defenses Through Action

Identifying Risk Is Only the First Step



A documented remediation process helps turn assessment findings into measurable improvements.





FFIEC CAT Retirement: Choosing Your Next Framework

NIST CSF 2.0

Six functions, now including Govern. Widely recognized and scales to any size.

Best for: A common language with vendors, auditors and the board

CRI PROFILE

Financial-sector version of NIST CSF, mapped to banking regulations and exam expectations.

Best for: Financial institutions that want regulator-mapped controls

CISA CPGS

A short, prioritized set of baseline security practices.

Best for: A quick baseline or gap check



Retired 31 Aug 2025; no single successor is endorsed. Keep a current, maintained assessment.



Staying Ahead of FortiClient VPN Changes



7.4.3

The last version of Fortinet's free VPN-only client. Since 7.4.4 (Sep 2025), no new free agent ships, and current versions need a paid, centrally managed license.

Why It's Time to Review Your Options

- No new features or centralized management
- Oct. 10, 2026: Certificate compatibility issues for older clients
- SSL VPN tunnel mode removed in FortiOS 7.6.3
- Limited visibility into patching and vendor oversight



Staying Ahead of Certificate Renewal Changes



The New TLS Renewal Timeline

Until March 2026

398 days

~1 renewal a year

March 15, 2026

200 days

~2 renewals a year

March 15, 2027

100 days

~4 renewals a year

March 15, 2029

47 days

~8 renewals a year



Why This Matters

The first 200-day certificates expired in October 2026. As renewal cycles shorten, **one missed deadline could disrupt online banking, APIs, or vendor connections.** Manual tracking is no longer enough.



Poll Question #3

How does your organization manage certificate renewals?



- ☐ **Manually, in-house**
- ☐ **Automated, in-house**
- ☐ **Through an external provider**
- ☐ **Combination of internal and external**



Open Q&A

Have a question or a scenario?
Drop them in the chat.



**Ready to stay ahead of
tomorrow's cyber threats?**

Phone 800-228-3628

Website secur-serv.com