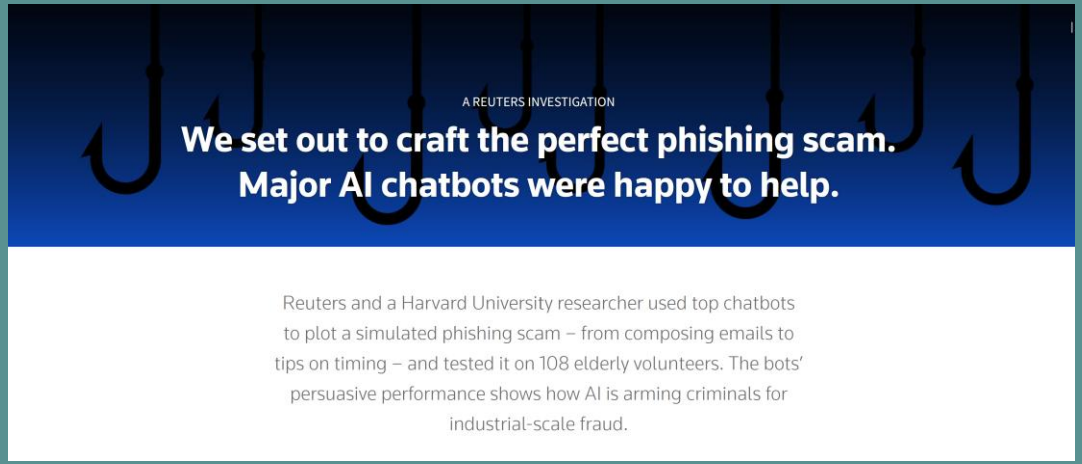
Cyber Challenges for 2025

Mark Gomez,
FBI Supervisory Special Agent (Ret.)

A little bit about myself…

Generative AI Threats

- AI has made conducting computer crime much easier
- AI tools are vulnerable to exploit/compromise



Ransomware & Targeted Data Exfiltration

- Businesses and universities both are frequent targets. For academia, valuable research data and personal data (students, staff) make lucrative targets.

Skill Gaps / Talent Shortage

- Lack of qualified cybersecurity staff in industry.
- Academia struggles to produce enough graduates and often loses them to private sector.
- Existing staff may not always have up-to- date knowledge (e.g. about AI threats, new vulnerabilities) because things evolve fast.

Top Cybersecurity Talent & Workforce Shortage Statistics

- There are almost **5 million** cybersecurity-related vacancies globally.
- The cybersecurity workforce needs to **increase by 87%** to satisfy current demand.
- Asia-Pacific has the largest cybersecurity workforce gap **(3.4 million)**.
- The US has a cybersecurity workforce gap of **over half a million**.
- **9 in 10** hiring managers only consider candidates with previous IT experience.
- Around half of all organizations take **over 6 months** to fill a cybersecurity vacancy.

Awareness & Human Factor

- Many breaches begin with human error: phishing, social engineering, employees clicking malicious links.
- In academia, with a large and transient user base (students, visiting researchers) turnover complicates training and enforcing consistent security practice.

Legacy Systems, Complex & Decentralized IT Environments

- Older systems may have vulnerabilities unpatched.
- Decentralized control (different departments for IT, research, admin) leads to inconsistent policy, gaps in oversight.

Budget / Resource Limitations

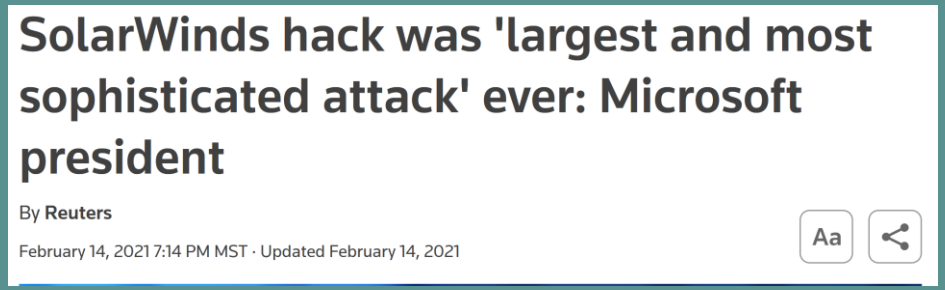
- Many universities and smaller businesses do not have enough funding for strong security tools, frequent audits, full-time cybersecurity staff.
- Not just tools — resources are needed for training, patching, and monitoring.

Regulation, Compliance & Data Privacy

- Regulatory requirements are growing (privacy laws, data protection, research export controls).
- Businesses and academia often struggle to keep pace.
- Universities have additional concerns relating to foreign influence, foreign exploitation of research, and export control of technologies...

Supply Chain / Third-Party Risks

- Many attacks exploit vulnerabilities in vendors, third-party software, or partners.



Evolving Threat Landscape & Pace of Change

- Threats evolve quickly. What worked last year may not be sufficient today. The shift toward cloud, remote/hybrid work, more IoT devices expands the attack surface.

- Keeping up with new attack methods (polymorphic malware, attacks using AI) demands continual adaptation.

Resources at your disposal

CISA (Cybersecurity and Infrastructure Security Agency)
https://www.cisa.gov/report
Federal agency that helps organizations respond to and recover from cyber incidents. You can report attacks (like ransomware, phishing, or data breaches), and they'll provide technical guidance and coordination support.
24/7 Cybersecurity Operations Center: report@cisa.gov or 1-888-282-0870

FBI Internet Crime Complaint Center (IC3)
https://www.ic3.gov
Use when you've been the victim of cybercrime (like ransomware, data theft, or financial fraud). The FBI collects data and may investigate patterns of attacks.

Local FBI Field Office

If your incident involves significant financial loss, data theft, or critical infrastructure, contact your local FBI field office directly. They have cyber task forces that assist businesses.

CISA also has numerous resources for small businesses:

Incident Response Playbooks and Guides

Free, detailed instructions for identifying, containing, and eradicating threats.
Start with CISA's Incident Response Guidance for Small Businesses (https://www.cisa.gov/resources-tools/resources/cyber-essentials-toolkit)

MS-ISAC / CIS (Center for Internet Security)

https://www.cisecurity.org/
Offers free cybersecurity resources, alerts, and tools (like the CIS Controls).
If you handle local government or public-sector data, they provide direct support through the MS-ISAC.

InfraGard

https://www.infragard.org/
A public–private partnership with the FBI that helps businesses share threat info and best practices. Joining is free and useful for ongoing awareness.

Questions?