FFIEC

Executive Leadership of Cybersecurity

What Today's CEO Needs To Know About the Threats They Don't See

Presented by
Federal Financial Institutions Examination Council (FFIEC)
Cybersecurity and Critical Infrastructure Working Group
May 7, 2014

Let's Get Started

- **Welcome / Some background on today's session**
- **Dial-in Information (this session is being recorded)**
  - Call-in number: 888-625-5230
  - Conference code: 37906091
- **Webinar Link**
- **How we'll take questions**
  - Email us at askthefed@stls.frb.org
  - Chat feature in the webinar

- **FFIEC members include:** (http://www.ffiec.gov)
  - Board of Governors of the Federal Reserve System
  - Consumer Financial Protection Bureau
  - Federal Deposit Insurance Corporation
  - National Credit Union Administration
  - Office of the Comptroller of the Currency
  - State Liaison Committee

Disclaimer: The opinions expressed in this presentation are intended for informational purposes, and are not formal opinions of, nor binding on, the FFIEC or its members.

Welcome from Thomas J. Curry

FFIEC Chairman / Comptroller of the Currency

Agenda

Topics

- Current Threats
- Cyber Risk Management
- Public/Private Partnerships

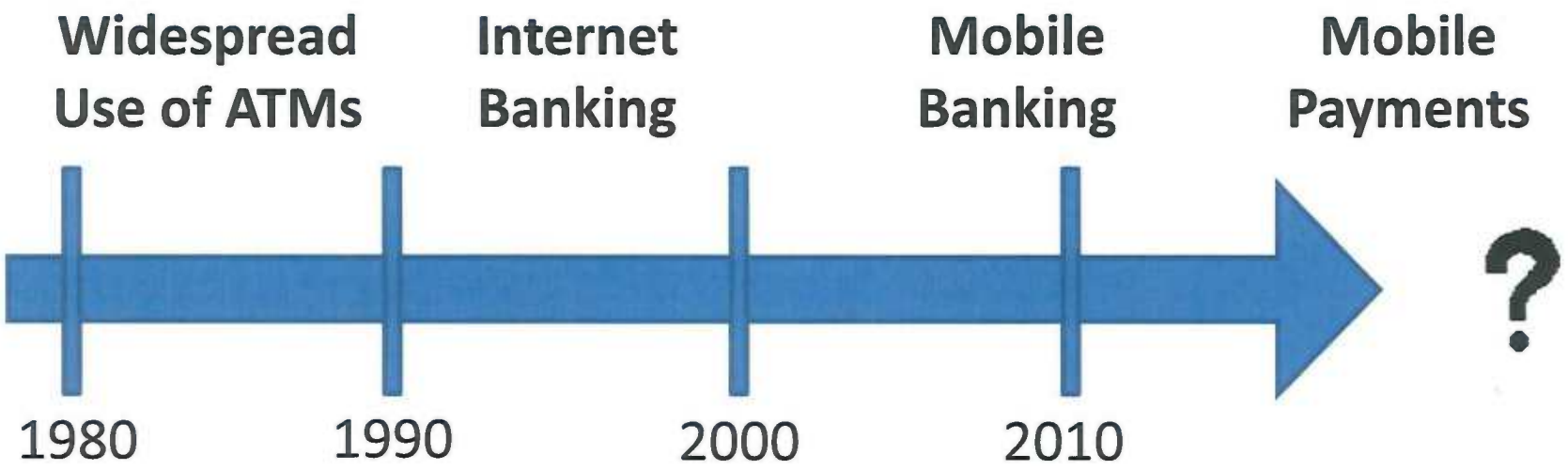
Presenters

- Matt Biliouris, NCUA
- Phillip Hinkle, Texas Department of Banking
- Chris Olson, FRB
- Bill Nelson, FS-ISAC
- Doreen Eberley, FDIC

Why an Information Technology (IT)/Cyber Webinar for CEOs?

- More frequent attacks on smaller institutions
- Cyber attacks are increasing in sophistication
- Not just an IT problem

Evolution of Technology in Financial Services



Current Threats

- Who are the Threat Actors?
  - Nation-states, hacktivists, organized criminals, insiders

What is their <u>Motivation</u>?

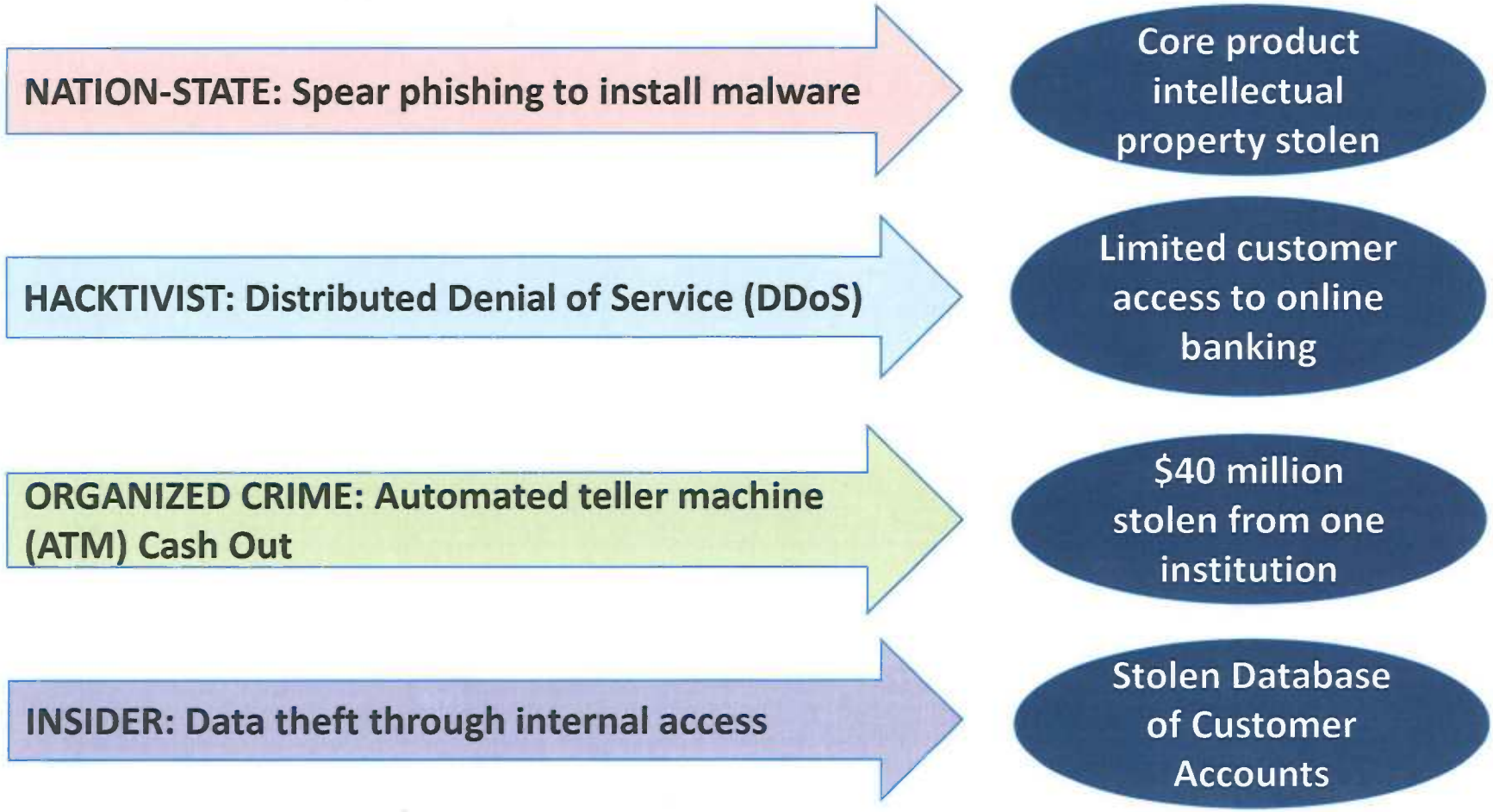
- **Espionage**
- **Fraud**
- **Disruption**
- **Destruction**
- **Social or political message**
- **Undermining reputation or overall confidence**
- **Building Reputation/recruiting**
- **War**

What are their <u>Capabilities</u>?

- **Technical**
- **Infrastructure**
- **Knowledge**
- **Financial**
- **Legal**

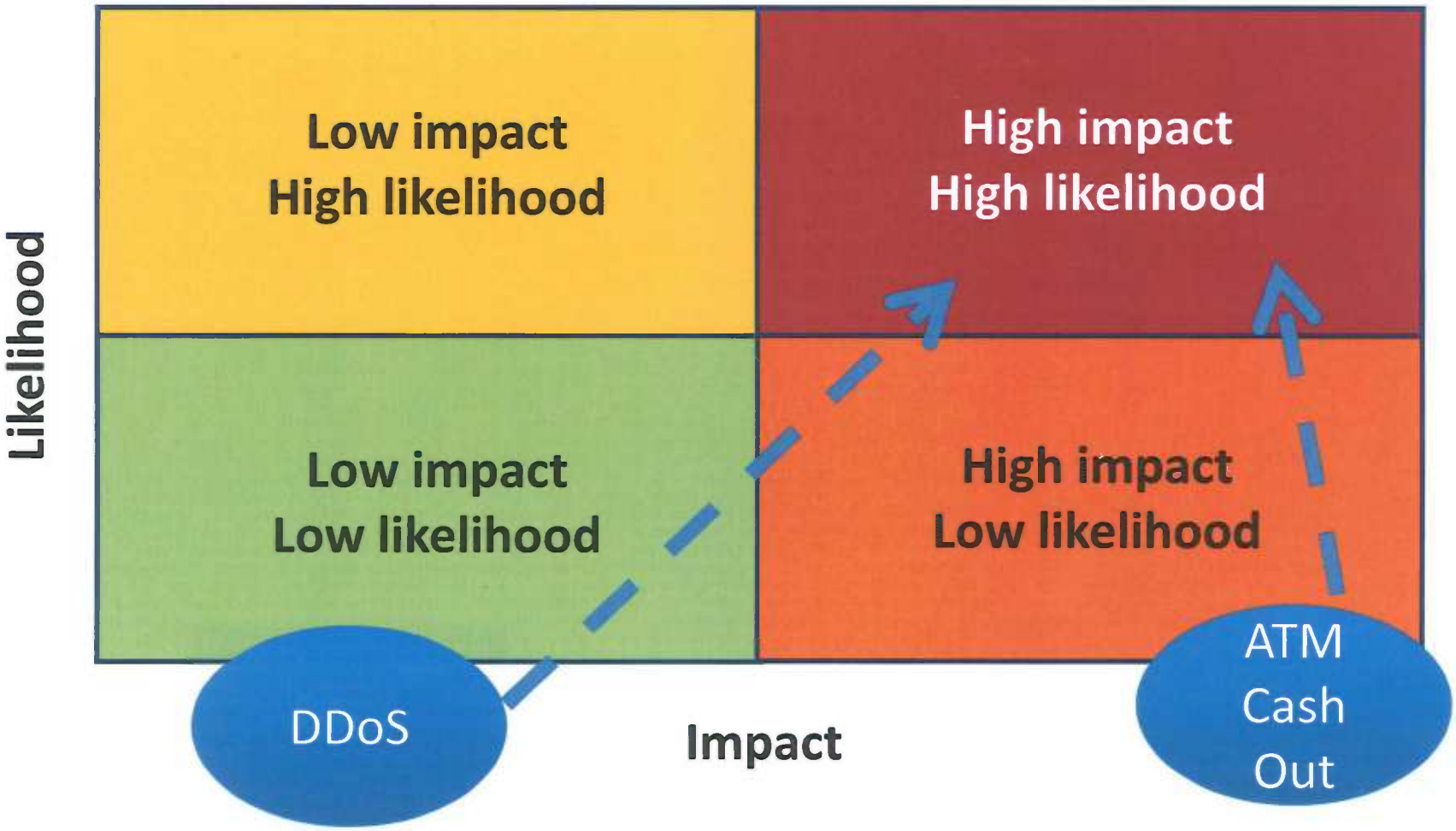
Current Threats (continued)

What Is The Impact?



Current Threats (continued)

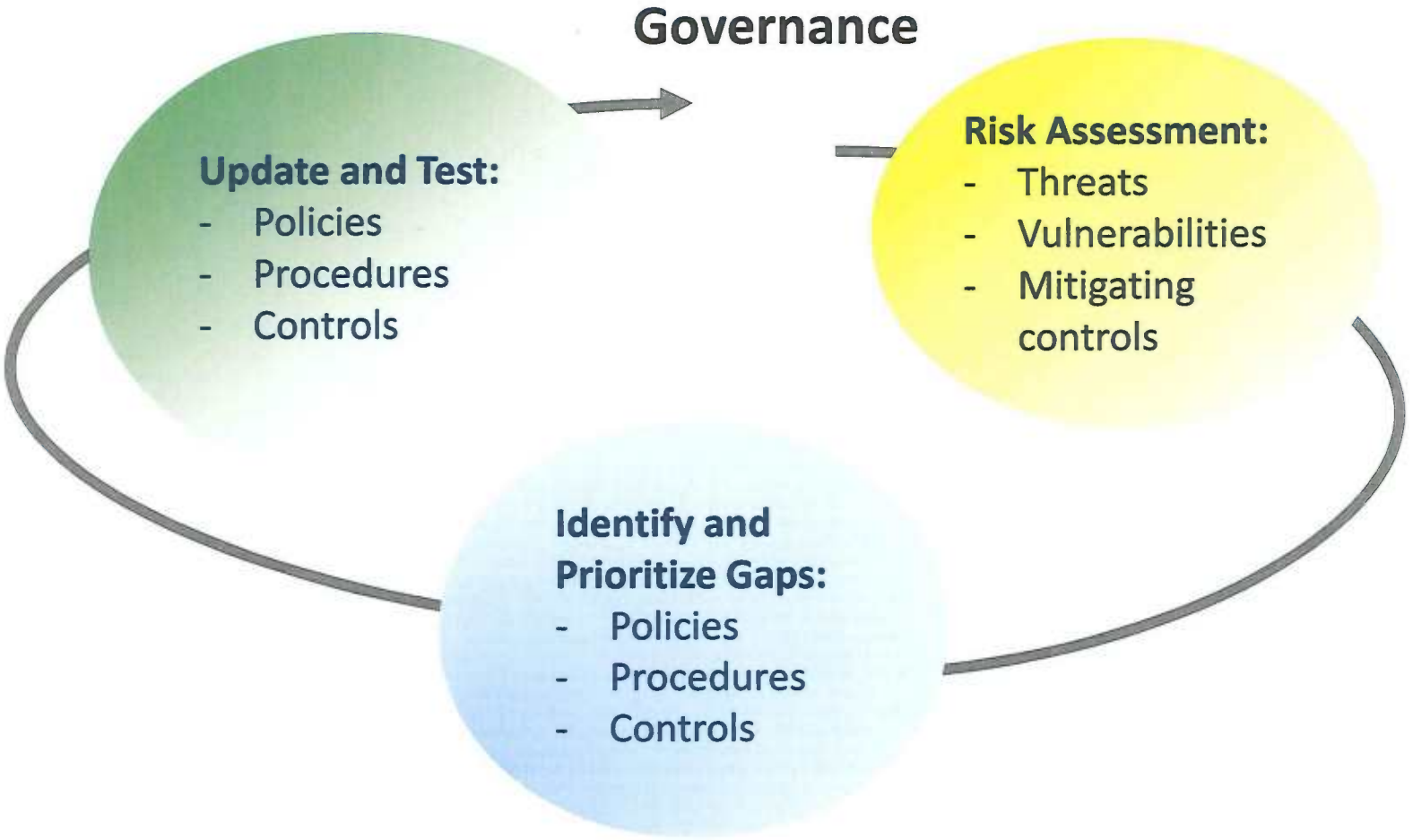
What are the sector-wide risk trends?



Cyber Risk Management

- Governance
- Threat intelligence
- Third-party/vendor management
- Incident response and resilience

Cyber Risk Management (continued)



Current Threat Example: ATM Cash Out

Cyber Risk Management (continued)

Governance Key Takeaway

- How is the staff at my institution providing me with accurate and timely information about our risks and our ability to mitigate them, so that I can prioritize our resource allocations and inform the board of directors?

Cyber Risk Management (continued)

Threat Intelligence

- Internal Resources
  - Internal audit reports
  - Fraud detection tools
  - Anti-Money Laundering/Office of Foreign Assets Control/Bank Secrecy Act tools
- External Resources
  - Financial Services Information and Sharing Analysis Center (FS-ISAC)
  - Federal Bureau of Investigation (FBI) – InfraGard
  - United States Secret Service (USSS) – Electronic Crimes Task Forces
  - Conferences
  - Vendor Reports

Current Threat Example: Account Takeover and Wire Fraud

Cyber Risk Management (continued)

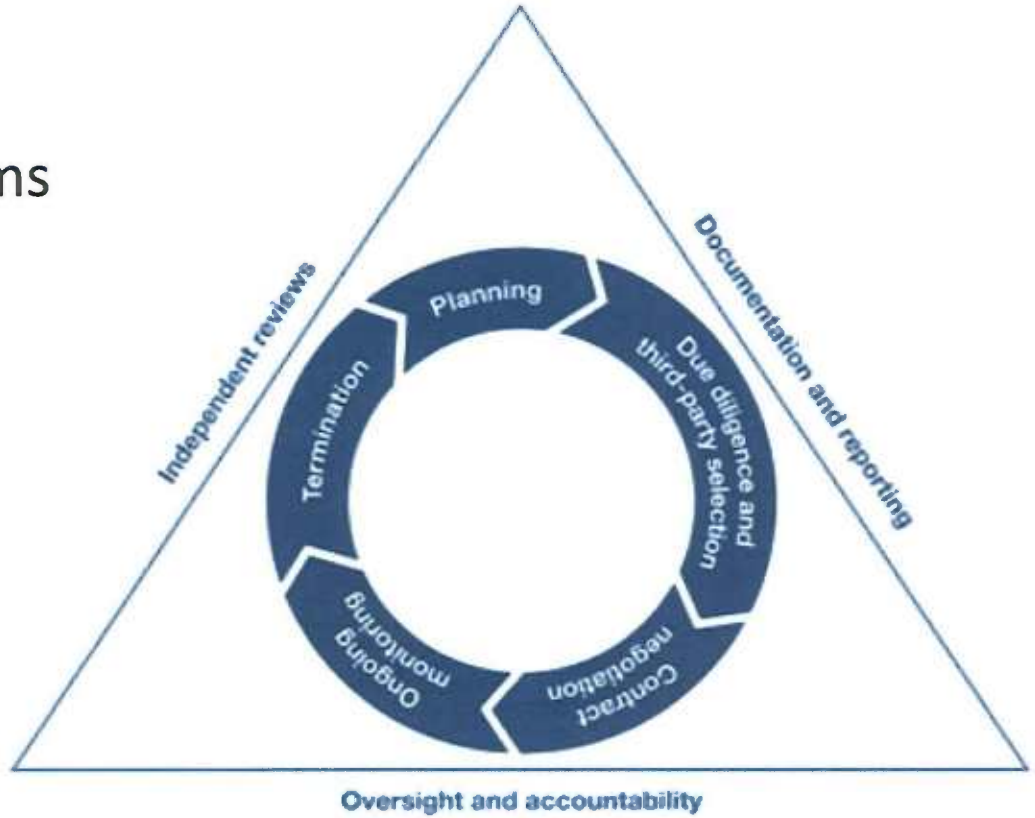
Threat Intelligence Key Takeaway

- How is my organization identifying and monitoring cyber threats and attacks both to my institution and to the sector as a whole? How is this information used to inform my risk assessment process?

Cyber Risk Management (continued)

Third-Party Relationships

- Risks
  - Connectivity of systems
  - User access
- Controls
  - Initial due diligence
  - Monitoring



Current Threat Example: Software End of Life

Source: OCC

Cyber Risk Management (continued)

Third-Party Relationships Key Takeaway

- How are we managing the third-party relationship risk management life cycle at our institution to ensure that we are selecting the best third parties and identifying, monitoring, and mitigating the risk exposure for third parties?

Cyber Risk Management (continued)

Incident Response and Resilience

- Preparation
  - Incident response plan and policy
  - Incident response team
- Escalation: internal
- Notification: external

Current Threat Example: Distributed DDoS Attacks

Cyber Risk Management (continued)

Incident Response and Resilience Key Takeaway

- How often is my institution testing its plans to respond to a cyber attack? Do these tests include our key internal and external stakeholders?

Key Takeaways

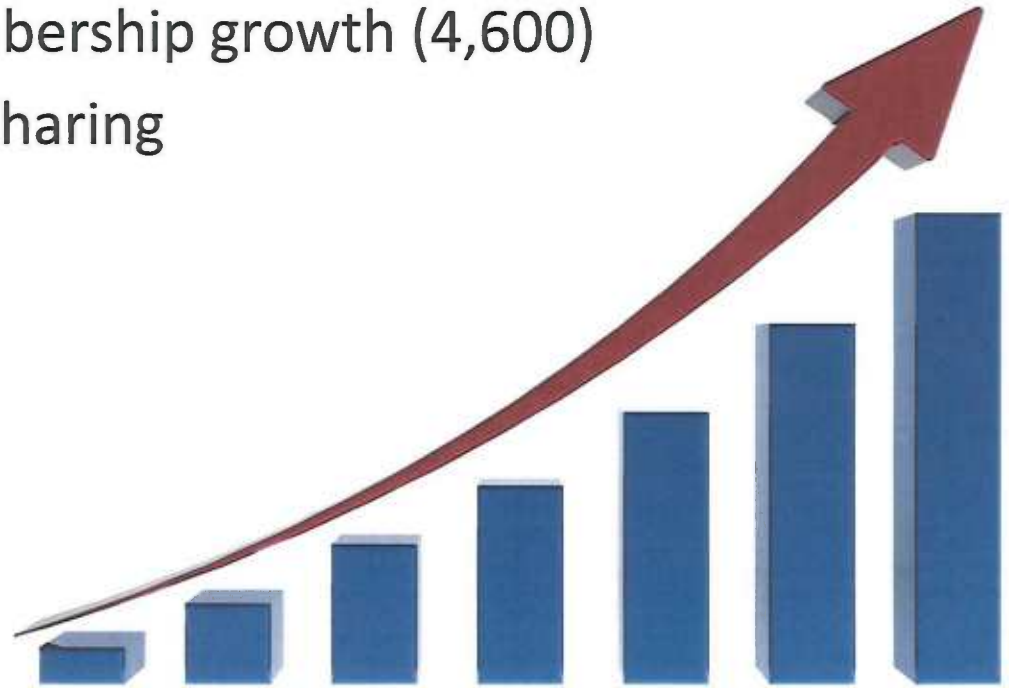
- Set the tone from the top and build a security culture
- Identify, measure, mitigate and monitor risks
- Develop risk management processes commensurate with your institution's level of risk and complexity
- Align IT strategy with business strategy and account for how risks will be managed both now and in the future
- Create a governance process to ensure ongoing awareness and accountability
- Ensure reports to you and your board are meaningful and timely with metrics on the institution's vulnerability to cyber risks and **potential business impacts**

FS-ISAC

The following individual is not an employee of an FFIEC member and the presentation includes the opinions of the FS-ISAC and do not represent those of the FFIEC.

FS-ISAC Overview

- A nonprofit private-sector initiative formed in 1999
- Designed/developed/owned by financial services industry
- Sharing thousands of threat indicators per month
- Double-digit membership growth (4,600)
- Expanded global sharing



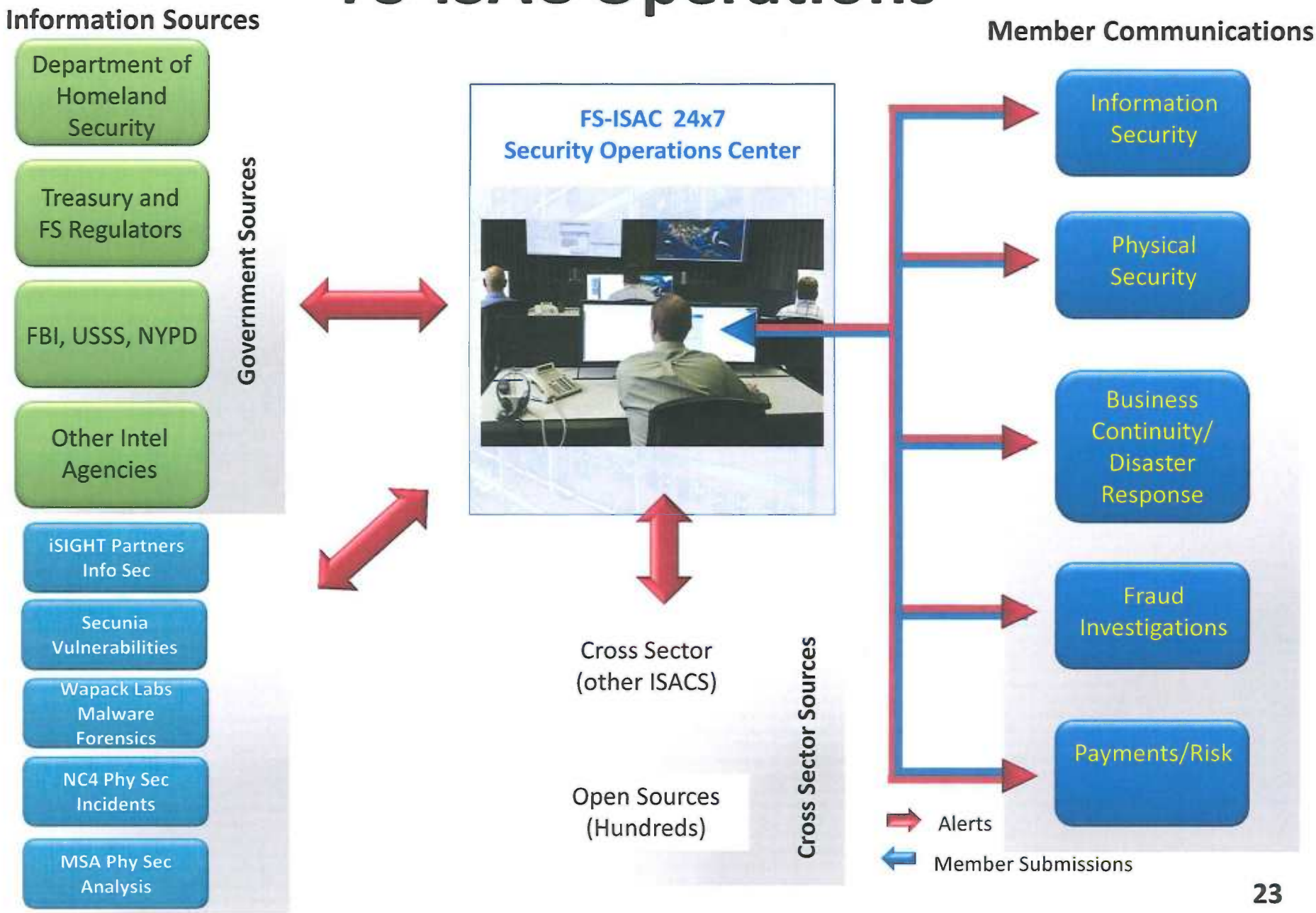
Information Sharing and Analysis Tools

- **Threat Data, Information Sharing**
  - **Anonymous submissions**
  - CyberIntel listserv
  - Relevant/actionable cyber and physical alerts (Portal)
  - **Special interest group email listservs**
  - Document repository
  - Member contact directory
  - Member surveys
  - Risk mitigation toolkit
  - Threat viewpoints

- **Ongoing Engagement**
  - Biweekly threat calls
  - Emergency member calls
  - Semiannual member meetings and conferences
  - Regional outreach program
  - Biweekly educational webinars

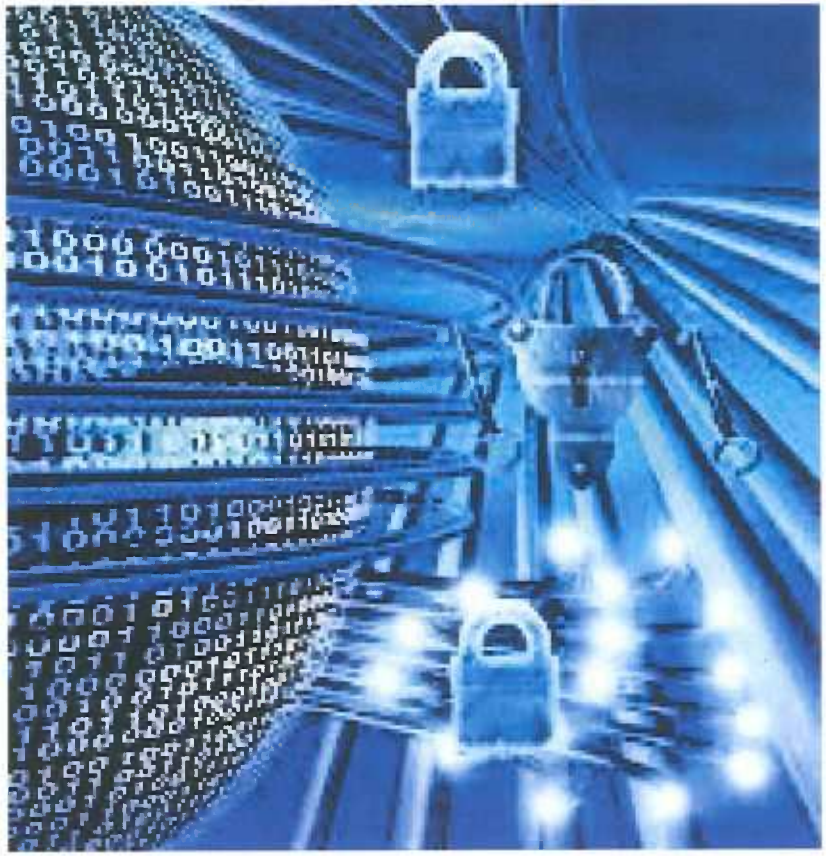
- **Readiness Exercises**
  - U.S. and EU government-sponsored exercises
  - CAPP exercise
  - Advanced threat/DDoS exercise
  - Industry exercises-QD2/pandemic

FS-ISAC Operations



Case Study: Retailer Breach

- Advisory: January 16, 2014
  - Malware analysis
  - Exploit of system vulnerability
  - Techniques/Tactics/Procedures of the attack
- FS-ISAC contribution: Recommended risk mitigation steps
  - Network security
  - Cash register and point of sale security
  - Administrative access



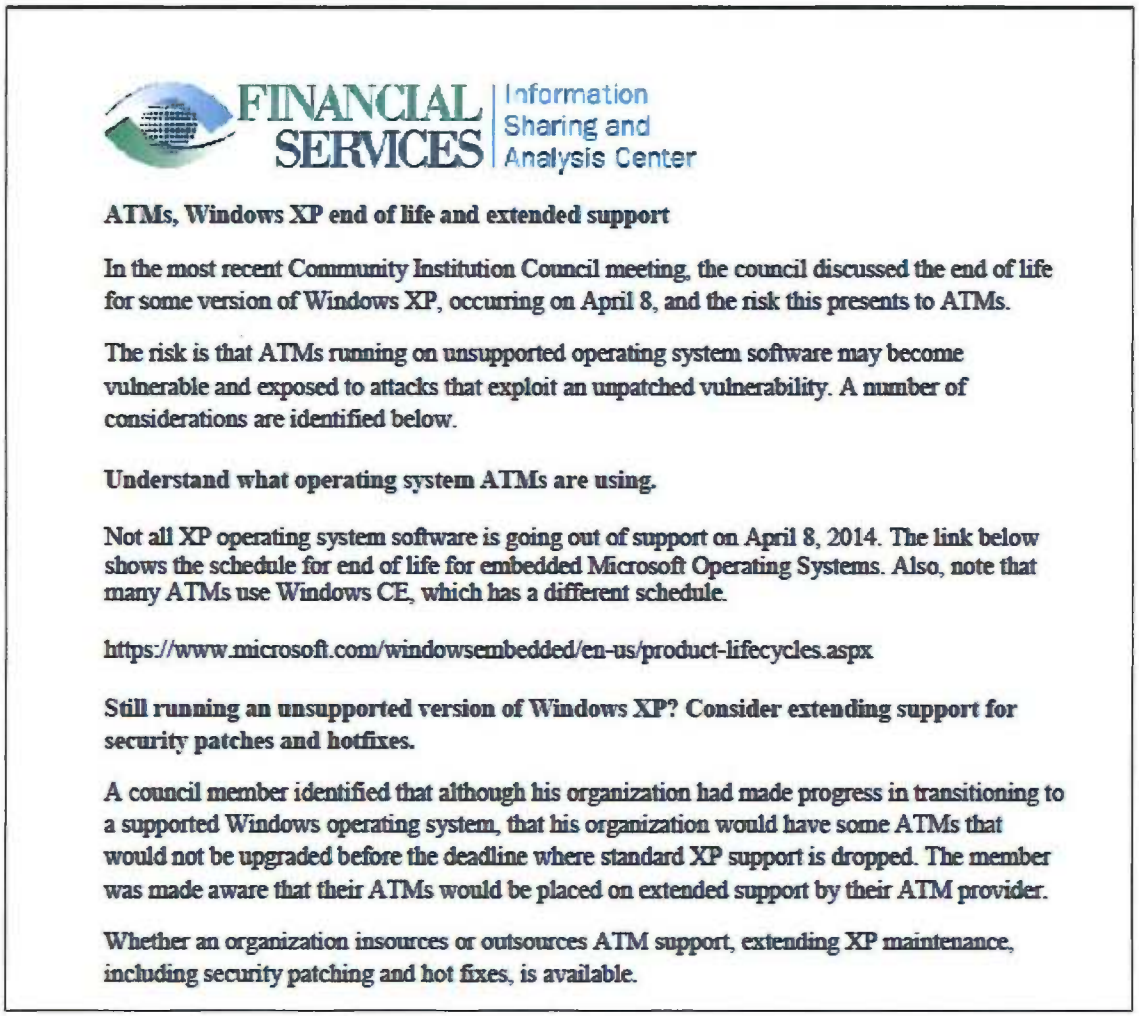
Efforts for Community Institutions

- Community Institution Council with bimonthly calls
- Security toolkit under development on "How to Build a Security Strategy"
- Developing mentorship program linking small institutions to large institutions

Community Institution Case Study: ATM Risk from Windows XP end of life

- FS-ISAC Community Institution Council reviewed impact on ATMs from Windows XP end of life
  - Microsoft ends support of Windows XP April 8, 2014
  - 95 percent of ATMs run on XP
  - Community Institution Council members shared strategies on
    - Extending maintenance
    - Determining ATM Operating System
    - Extended XP support
    - Network isolation options

Advisory with Summary Recommendations for Handling Windows XP End of Life



FINANCIAL SERVICES | Information Sharing and Analysis Center

ATMs, Windows XP end of life and extended support

In the most recent Community Institution Council meeting, the council discussed the end of life for some version of Windows XP, occurring on April 8, and the risk this presents to ATMs.

The risk is that ATMs running on unsupported operating system software may become vulnerable and exposed to attacks that exploit an unpatched vulnerability. A number of considerations are identified below.

Understand what operating system ATMs are using.

Not all XP operating system software is going out of support on April 8, 2014. The link below shows the schedule for end of life for embedded Microsoft Operating Systems. Also, note that many ATMs use Windows CE, which has a different schedule.

https://www.microsoft.com/windowsembedded/en-us/product-lifecycles.aspx

Still running an unsupported version of Windows XP? Consider extending support for security patches and hotfixes.

A council member identified that although his organization had made progress in transitioning to a supported Windows operating system, that his organization would have some ATMs that would not be upgraded before the deadline where standard XP support is dropped. The member was made aware that their ATMs would be placed on extended support by their ATM provider.

Whether an organization insources or outsources ATM support, extending XP maintenance, including security patching and hot fixes, is available.

Information Sharing Benefits

- Early warning
- Technical insights into types of attacks and success/failure of attacks based on defensive measures used by others
- Collective expertise of vendors, government and FI subject matter experts
- No attribution
- A sense of community and real-time sharing of what is working
- **Contacts:**
  - Bill Nelson, President and CEO
    bnelson@fsisac.us
  - Beth Hubbard, Director of Member Services
    bhubbard@fsisac.us

Closing Remarks

Doreen Eberley

FFIEC Task Force on Supervision Chair

FDIC, Director

Division of Risk Management Supervision

Questions?