

# Cybercrime Risks and Controls

---

**Devon Marsh**

Senior Vice President

Treasury Management Risk

Commonwealth Association for  
Financial Professionals

October 22, 2009

Together we'll go far



# Topics

- Cybercrime Today
- Risks
- Mitigants
- Thinking about Risks & Controls
- Summary
- Discussion

# Disclaimer

This presentation and the information contained herein is made available as an educational resource. It is not intended to serve as legal advice.

# Cybercrime Today

# Current Environment

## Data

### Anti-Phishing Working Group (APWG)

### Phishing Activity Trends Report - First Half 2009

- Unique phishing reports submitted to APWG recorded a high of 37,165 in May, around 7 per cent higher than last year's high.
- The number of unique phishing websites detected in June rose to 49,084, the highest recorded since April 2007's record of 55,643.
- The number of hijacked brands ascended to a high of 310 at the end of Q1.
- **Payment Services became phishing's most targeted sector, displacing Financial Services in Q1 & Q2.**
- Banking Trojan/password-stealing crimeware infections detected increased more than 186 percent between Q4 2008 and Q2 2009.
- The total number of infected computers rose more than 66 percent between Q4 2008 and the end of the half, 2009 to 11,937,944, representing more than 54 percent of the total sample of scanned computers.
- Sweden moved ahead of the United States as the nation hosting the most phish websites at the half's end.
- China hosted the most websites harboring Trojans and downloaders from March through June.

# Current Environment

## Legal Climate

August 21, 2009, in *Shames-Yeakel v. Citizens Financial Bank*, No. 07 C 5387 (N.D. Ill.), in the Northern District of Illinois, the Court finds that the use of single-factor password identification to secure online accounts may create negligence liability.

# Current Environment

## Magnitude of Threat

October 15, 2009 (Chicago) – “Treasury Strategies Sees Possible Bank Failures Due to Fraud Losses”

- Possibility of a bank failure within next 3 years
- “...good likelihood that both community banks and even regional banks will fail...”
- Fraudsters making decisions with longer investment horizon than banks are attacking:
  - Sleeper accounts
  - Patient malware
  - Moles who acquire information on controls

# Current Environment

## National Security Climate

On September 18, 2009, the Director of National Intelligence Dennis C. Blair unveiled the 2009 National Intelligence Strategy – the blueprint that will drive the priorities for the nation's 16 intelligence agencies over the next 4 years. The National Intelligence Strategy (NIS) is one of the most important documents for the Intelligence Community (IC). It lays out the strategic environment, sets priorities and objectives, and guides current and future decisions on budgets, acquisitions, and operations.

Source: FS-ISAC Collective Intelligence Alert, September 29, 2009

# Current Environment

## National Security Climate

Mission objectives of the National Intelligence Strategy:

- Combat Violent Extremism
- Counter WMD Proliferation
- Provide Strategic Intelligence and Warning
- Integrate Counterintelligence capabilities
- **Enhance Cybersecurity**
- Support Current Operations (ongoing U.S. diplomatic, military, and law enforcement operations).

# Current Environment

## Risk Summary

- Increased Cybercrime activity
- Changing legal climate
- Increased attention at the national defense level emphasizes the threat
- Additionally, new stressors on employees:
  - tight credit
  - decreased home values
  - hollow bonus structures
  - reduced or non-existent salary increase pools
  - a bow wave of consumer debt.

# Current Environment

## Response

- In instances of employee identity theft & corporate account takeover, Cybercrime can mimic internal fraud.
- Fraud is not new, but current distress may increase the risk that it might occur.
- Classic fraud control procedures deserve emphasis to ensure an appropriate control environment.
- Additional measures are necessary to address new components of the threat.

# Mitigants

# Dual Control

- Separates tasks to ensure no single person has absolute control over all phases of a transaction.
- Assignment of responsibility to two people reduces the opportunity—perhaps the temptation—for an employee to act alone to commit fraud.
- Few measures can prevent collusion, but dual control can thwart a lone perpetrator.
- This is a fundamental way to discourage internal fraud and thwart external initiation of transactions.

# Bench Strength

- Single-incumbent positions increase the opportunity for an employee to act alone.
- They are a weak link in the event of absence or disaster.
- Bench strength eliminates a single point of failure, enhances recovery capability, and may increase the chance that someone will notice something unusual.
- Ensure at least two people know how to perform each function related to processing financial transactions.

# Access to Information

- Focus on *Clearance* and *Need to Know*.
- Ensure only authorized parties can request transactions or sensitive information.
- Confirm a customer's identity.
- Authentication is equally important within an organization.
  - Define internal authentication procedures.
  - Define system access criteria.
  - Periodically review system access.

# Documentation

- Retain evidence of requests to change account information.
- Record the method of authentication used to identify the requestor.
- This may not prevent fraudulent transactions, however it might dissuade perpetrators.
- Documentation will enhance the trail of evidence.

# Physical and Information Security

- Lock unattended workstations.
- Eliminate shared PCs with a common password.
- Prohibit password sharing.
- Prohibit access device and token sharing.
- Limit access to workspaces where transactions are created or customer information is openly handled.
- Limit the presence of cell phones with cameras in areas where financial information might be in view.
- Restrict the use of flash drives.
- Prohibit account information in non-secure e-mail.

# Testing

- Test the controls that make up a formal risk management program.
- Control processes from end to end.
- Rely on objective reviewers for testing.
- Rotate reviewers to prevent complacency and to cast a fresh set of eyes on a process.
- Don't overlook outsourced or off-shored processes, which may deserve unique controls beyond those in place for in-house, on-site functions.

# Training

- Remind, Inform, Persuade
- Training can range from formal courses to casual refreshers and reminders.
- Quick reference guides and checklists provide valuable tools.
- Remind employees that controls are in place not just to protect the company, but to protect them as well.

# Active Counter-Cybercrime Measures

- Maintain current anti-virus, anti-malware protection from reputable sources
- Scan systems
- Scan removable media

# Reactive Measures

- Report all incidents
  - FBI Field Office duty agent (in Richmond: 804-261-1044)
  - FD-71 Complaint Form
  - Low-dollar events will not generate unique cases
  - They *can* contribute to creation of a profile

# Consultants' Recommendations

Treasury Strategies recommends four steps that banks can take:

- Ensure sufficient capital
- Upgrade risk management capabilities
- Collaborate as an industry
- Educate clients about schemes

# Nothing New

- The information up to this point should be familiar.
- Ironically, familiarity can weaken the effectiveness of controls, as routine processes are susceptible to boredom, inattention, and decreased diligence.
- In the current economic and Cybercrime environment, traditional risk management controls are more important than ever.

# Thinking about Risks and Controls

# Authentication

- FFIEC Guidance stressed authentication of customers.
- In an age of identity theft, it is not enough to authenticate the customer. Full authentication includes the transaction, as well.
- NACHA's WEB rule anticipated this with its requirement for a fraudulent transaction detection system.

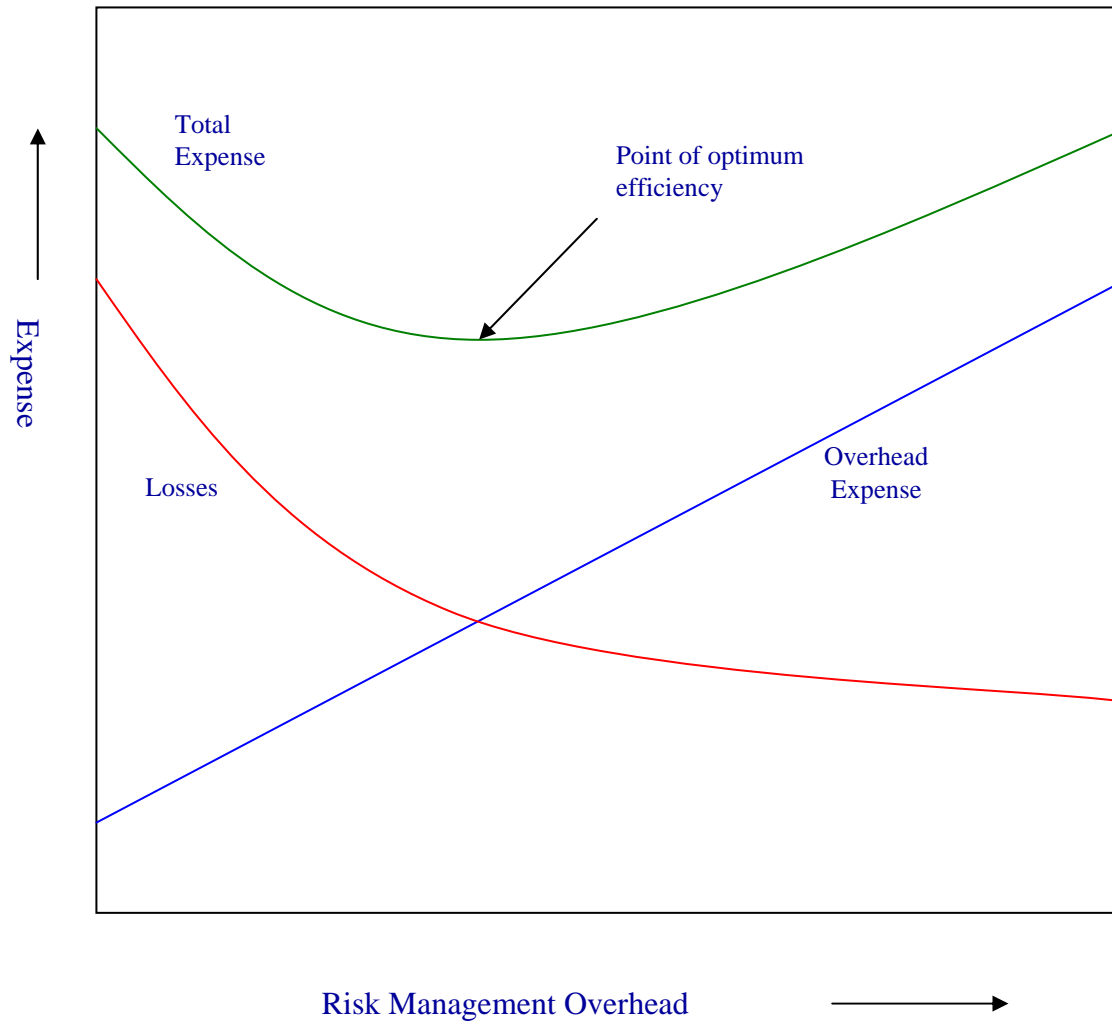
# Hoarding

- Treating best practices as proprietary information can be costly.
- In a business community, failure to share risk management expertise may actually increase risk for all participants. The errors of others can mean non-value-added repair work for the home company.
- Remind people to reflect on factors that help them contain risks, describe those factors without including proprietary or confidential data, and share knowledge with others who operate in the same environment.

# Risk Management

- The risk management determination: the actual cost of risk mitigation versus the possible cost of an uncontrolled environment.
- The actual expense of controlling all possible risks can exceed the likely cost of all probable risks.
- Involve the right decision makers, exercise good judgment in identifying opportunities for adverse outcome, and avoid the temptation to regard an untenable number of conditions as risks.

# Risk Management Optimization



# Cost-Benefit: Perpetrator's Perspective

In the cost-benefit equation that fraud perpetrators calculate, we must increase the cost.

- Criminal charges
- Sentencing guidelines
- Extradition arrangements with other countries
- Enforcement and collaboration in other countries

# Summary

## Complementary Actions To Address the Threat

Role	Action
Initiator of Transactions	Practice traditional transactional controls. Train to promote awareness of the threat. Remain vigilant against malware and phishing. Report all incidents to law enforcement.
Financial Institution	Authenticate the payment, not just the initiator. Provide risk management guidance as part of the value proposition, especially when prescribed measures seem onerous or customer-unfriendly. Report all incidents to law enforcement.
Industry	Promote awareness. Key messages: <ul style="list-style-type: none"><li>• Don't be a mule</li><li>• Don't be a phish</li><li>• Report all incidents</li></ul>
Law Enforcement	Take in all information. Cooperate across agencies to share information. Develop composite pictures.
Legislative and Diplomatic Environment	Increase the cost of the crime. Promote international cooperation.

# Resources

- [www.dhs.gov/cyber](http://www.dhs.gov/cyber)
- <http://richmond.fbi.gov>

# Discussion

# Contact Information

[Devon.Marsh@wellsfargo.com](mailto:Devon.Marsh@wellsfargo.com)