

Cybercrime Risks and Controls

Devon Marsh

Senior Vice President

Treasury Management Risk & Compliance

Hampton Roads
Association for Financial Professionals
April 20, 2010

Together we'll go far



Topics

- Current Environment
- Mitigants
- Thinking about Risks & Controls
- Summary
- Resources
- 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.

Current Environment

Current Environment

Data

Anti-Phishing Working Group (APWG)

Phishing Activity Trends Report – 4th Quarter 2009

- Unique phishing reports submitted to APWG in Q4, 2009 decreased nearly 29 percent from the all-time high of 40,621 in August, dropping to 28,897 reports in December.
- **Member reports to APWG and research reviews reveal a substantial increase in phishing focused on high-value targets such as personnel with treasury authority.**
- October's high of 46,522 unique phishing websites detected by the APWG was down 18 percent from the August, 2009 record high of 56,362.
- The number of unique brand-domain pairs rose to a quarter high of 23,380 in October, still down 4 percent from the all-time high of 24,438 in August, 2009.
- **As in Q3, Financial Services remained the most targeted industry sector in Q4.**
- The United States continued its position as the top country hosting phishing sites in Q4.
- The total number of infected computers dropped to 10,305,805 in Q4, representing more than 47.8% percent of the total sample of scanned computers, the lowest infection rate recorded in 2009.

Source: APWG Phishing Activity Trends Report, 4th Quarter 2009

http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf

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

Legal Climate

August 2009, in *Shames-Yeakel v. Citizens Financial Bank*, the Northern District of Illinois found that the use of single-factor password identification to secure online accounts may create negligence liability.

November 2009, Experi-Metal Inc. (EMI) in Sterling Heights, MI filed suit alleging Dallas-based Comerica created a climate that opened its customers to phishing attacks by sending emails asking customers to click on a link to update the bank's security software. EMI says even though the bank had two-factor authentication using digital certificates for its online banking portal, the phishing scam was able to circumvent these measures.

December 2009, following partial recovery of fraudulent wires, PlainsCapital Bank filed lawsuit against Hillary Machinery requesting that the court certify that PlainsCapital's security was reasonable, and that it processed the wire transfers in good faith. Hillary filed a countersuit in February, saying it would not be bullied. It has since moved its accounts to another bank, citing security as a factor.

Source: <http://www.bankinfosecurity.com/>

Current Environment

Regulatory Climate

In the wake of lawsuits over fraud and "reasonable security," business and bank advocates are at odds over whether federal regulations should be amended to enhance commercial protection.

Jim Woodhill, founder and chairman of Authentify, met with congressional staffers and is scheduling meetings to ask to top lawmakers to amend Regulation E to limit the amount of fraud losses a business could bear from fraudulent ACH or wire transfers.

The American Bankers Association (ABA) opposes any such Reg E amendment. "Security is a shared responsibility," says senior policy analyst Doug Johnson. "Responsibility for secure transactions resides at both the business and consumer, as well as at the financial institution."

Source: <http://www.bankinfosecurity.com/>

Current Environment

Risk Summary

- High level of cybercrime activity
- Increased attention at the national defense level
- Changing legal climate
 - opposing lawsuits by banks and customers over security
 - contention over whether federal regs should enhance commercial protection
- 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

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 for an employee to act alone to commit fraud, and for a single employee's identity to be exploited for 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.

Mitigants

Bench Strength

- Single-incumbent positions increase the opportunity for an employee to act alone or be targeted for exploitation.
- 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.

Mitigants

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.

Mitigants

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.

Mitigants

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.

Mitigants

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.

Mitigants

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.

Mitigants

Active Counter-Cybercrime Measures

- Never click on a link in an e-mail from an unknown source
- Never click on a link in an e-mail from a financial institution in order to enter information
- Maintain current anti-virus, anti-malware protection from reputable sources
- Scan systems
- Scan removable media

Mitigants

Reactive Counter-Cybercrime Measures

Report all incidents

- Financial Institution(s)
- Industry Associations
- Law Enforcement
 - FBI Field Office duty agent
 - FD-71 Complaint Form
 - Low-dollar events will not generate unique cases
 - They *can* contribute to creation of a profile

Mitigants

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

Mitigants

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

Thinking about...

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.

Thinking about...

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.

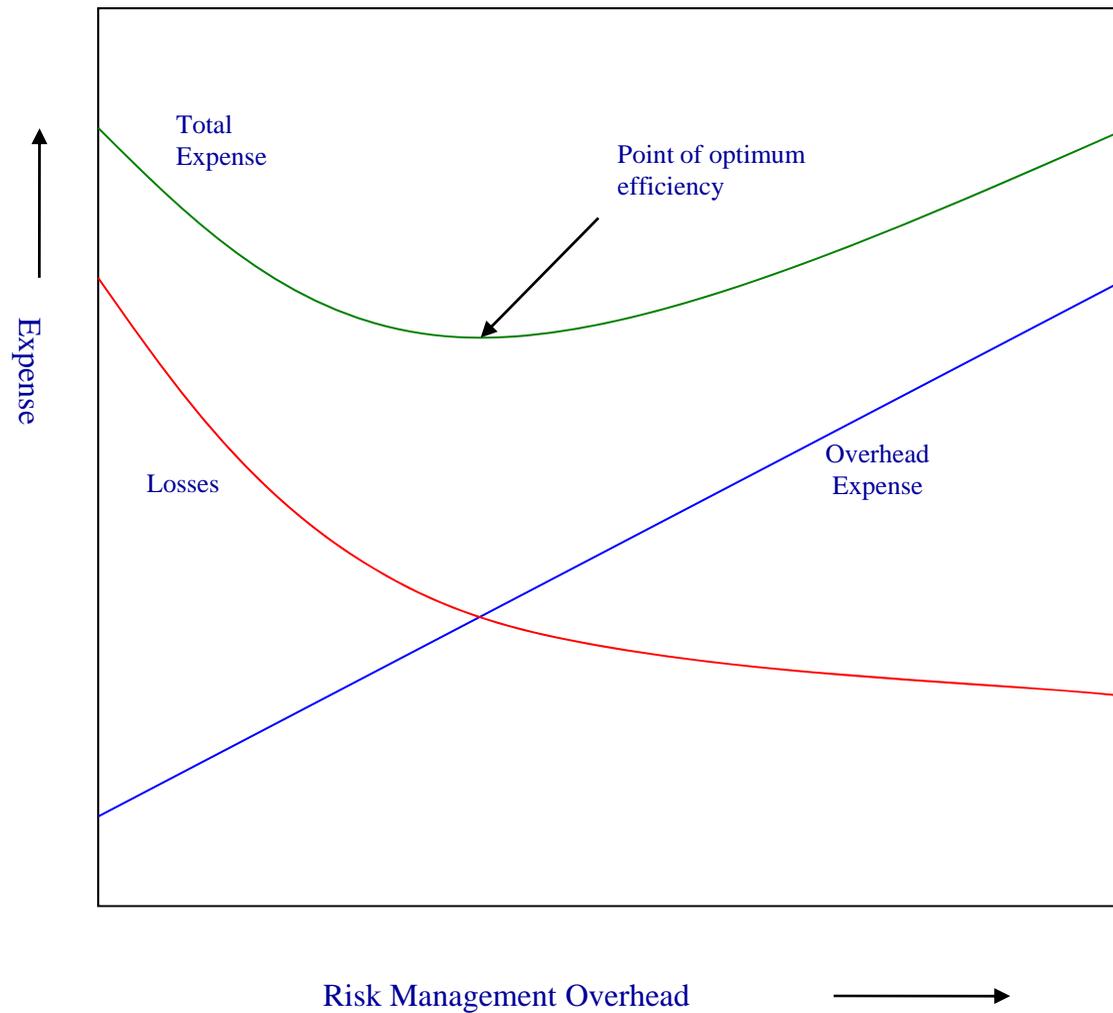
Thinking about...

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.

Thinking about...

Risk Management Optimization



Thinking about...

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">• Don't be a mule• Don't be a phish• Report all incidents
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
- www.staysafeonline.org/
- www.msisac.org/
- www.fsisac.com/
- <http://www.antiphishing.org/>
- <http://www.bankinfosecurity.com/>

Discussion

Contact Information

Devon.Marsh@wellsfargo.com