David Tompkins
Partner
Performance Solutions International

Aaron McPherson
Practice Leader, Payments and Security
Financial Insights, an IDC company

Information Security within the Financial Services Industry

Webcast March 5, 2008

Webcast Logistics

- **Audio lines are muted until Q&A session**
- **Submit your questions via the Live Meeting Chat window at any time (or audio at end)**
- **Slides available within 24 hours for all attendees**
- **Technical Problems**
  - Email **dstark@idc.com**
- **All other requests:**
  - Email **sales@financial-insights.com**
  - Email **info@goto-psi.com**

Our Partnership Provides You With...

- Blended solution that leverages data driven research and training with years of experience in the financial services industry
  - A logical and proven method for learning the industry fundamentals
  - Business drivers and challenges at the CXO and LOB levels
  - Highly customizable training
  - Continuous knowledge transfer with ongoing subscription
  - An ongoing dialogue with:
    - Financial Insights' expert analysts to support key investment decisions and go-to-market strategies
    - PSI Instructors to discuss the application of the training

Financial Insights™ An IDC Company

PSi

Agenda for Today's Session

- Business and regulatory drivers
- Information security threats
- Tools and strategies used by financial institutions
- Information security IT ecosystem
- Top 10 security concerns
- Essential guidance and summary
- Questions and answers
  - Live meeting chat or audio

Financial Insights™ An IDC Company

PSi

Introducing Our Speakers

- **Aaron McPherson, Research Director, Payments and Security**
  - Specializes in the strategic implications of new technology for the payments industry
  - Provides analysis on the strengths and weaknesses of payment industry competitors
  - Previously with IDC American Management Systems (AMS), and as a financial analyst in the Executive Office of the Commonwealth of Massachusetts

- **David Tompkins, Partner, Performance Solutions International**
  - Co-founding Partner of PSI
  - 20 years of experience in financial services industry, working with financial institutions, regulators, consulting firms and solution providers
  - Currently responsible for PSI's financial services industry training curriculum, including client deliveries and new course development

Financial Insights™ An IDC Company

PSi

And now David Tompkins..

PSI's Financial Services Industry Curriculum

Source: Information Security in Financial Services training program, PSI

Today's Threat to Information Security

- Greater reliance on IT to store and process information
- Attacks are becoming more sophisticated
  - Organized crime, terrorists
  - Increasing value of stolen information
- Increasing costs of data breaches
  - Investigation and auditing
  - Customer communication
  - Litigation (increasing public awareness)

Source: Information Security in Financial Services training program, PSI

Business and Regulatory Drivers
Do Financial Institutions Care?

- Financial services is the most targeted industry
- Reputational risk is high
- Regulatory burden is increasing
  - Consumer privacy and protection
  - Exposure to third parties
  - Conflicting regulations
- Internet is critical to long-term strategic plans
- Third-party breaches impact financial institutions
- Direct financial losses can be significant

> "The biggest risk isn't the loss itself but the bank's reputation."
>
> - Karl Landert, CIO Private Banking and EMEA, Credit Suisse *Bank Systems & Technology, May 24, 2007*

Source: Information Security in Financial Services training program, PSI

Protecting Physical Assets

- High profile incidences of stolen/lost laptops and data tapes

- How are financial institutions responding?
  - Staff education
  - Data encryption
  - Hard-disk-lock passwords
  - Extending to other portable devices *(mobile devices, USB drives)*
  - "Remote kill"

Source: Information Security in Financial Services training program, PSI

Information Security Threats in Financial Services
Internal Threats

- 75% of measured security losses are internal
- Internal threats include
  - Staff carelessness
  - Internal fraud and theft
- How are financial institutions responding?
  - Internal policies and processes
  - Staff education and background checks
  - Physical security measures in data centers
  - User authentication and authorization

"The things that keep me awake at night are all around staff fraud. It is a massive problem. We're not good at spotting and stopping it."

- Derek Wylde,
  Group Head of Fraud, HSBC
  The Banker, November 6, 2006

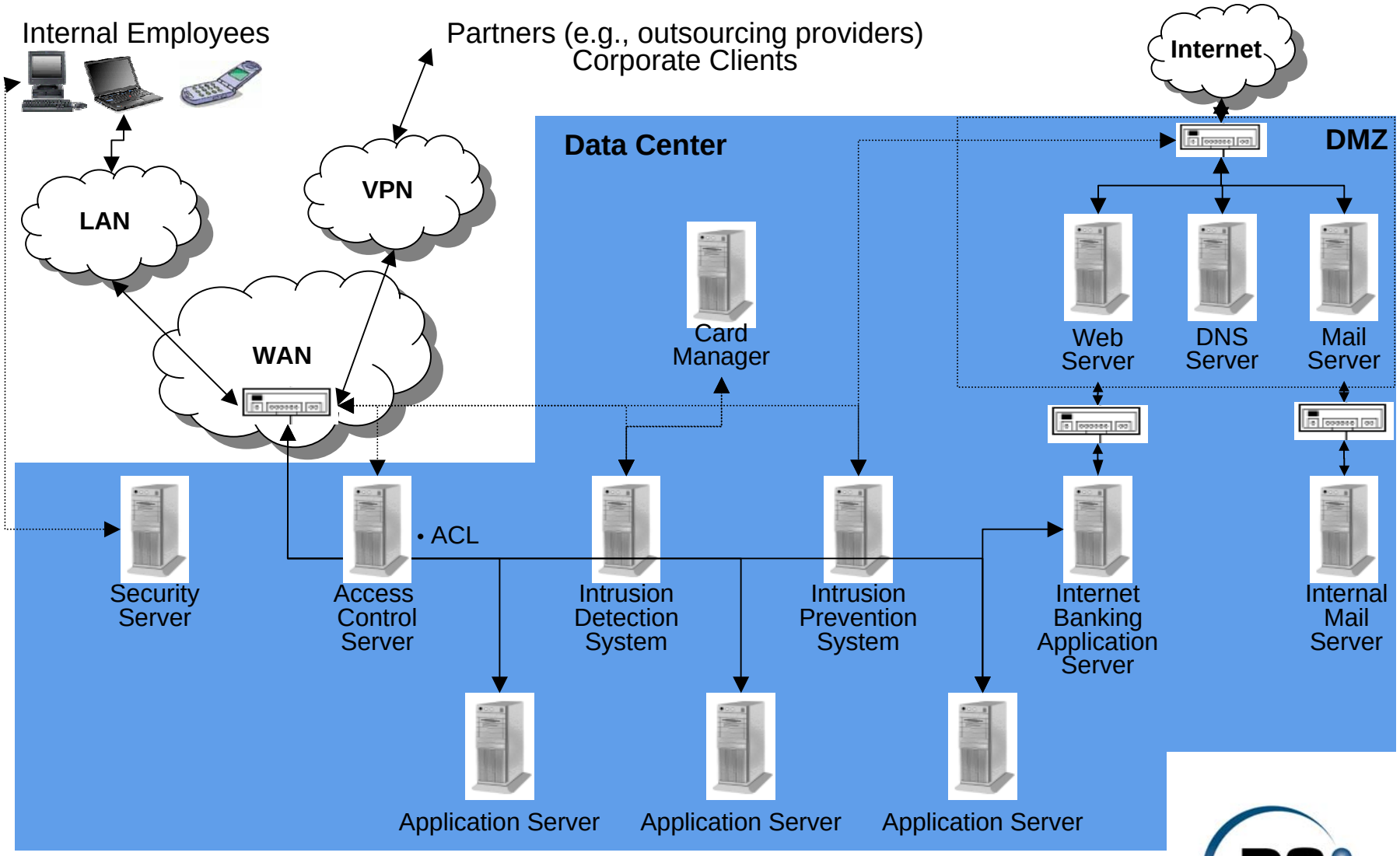
Source: Information Security in Financial Services training program, PSI

Information Security Threats in Financial Services
External Threats

- External threats include
  - Hacking
  - Attacks on customers
  - Emerging threats

- How are financial institutions responding?
  - Perimeter security
  - User authentication and authorization
  - Patch management
  - Customer education
  - New customer services
  - Working with third parties to improve controls
  - Multifactor authentication

Information Security
IT Ecosystem



Source: Information Security in Financial Services training program, PSI

Information Security Management

- Security is becoming a “C-level” issue
- Great focus IS governance
  - Management structures
  - Strategies, policies, procedures and standards
  - Reporting *(internal, regulatory)*
  - Controls assessments, testing and audit
- Adhering to industry standards *(ISO/IEC 27002: 2005)*
- Centralizing IS management

Source: Information Security in Financial Services training program, PSI

Why Aren't Financial Institutions Doing More?

- Information security is less than 3% of IT budgets
  - Considered a cost, not an investment
- View of information security applications as
  - Complex and burdensome
  - A strain on network and system resources
  - Difficult to deploy and maintain
- Need to balance cost of information security with
  - Actual losses
  - Reputational and regulatory risks

Source: Information Security in Financial Services training program, PSI

Financial Insights™
An IDC Company

And now Aaron McPherson..

Top 10 Security Concerns of Financial Institution CIOs and CTOs

Protecting the Customer Connection

1. Securing Consumer PCs
2. Improving Account Opening
3. Credentialing – Verifying Identity of Both Customer and Institution Online

Compliance Issues

4. Inconsistent State-Level Data Breach Laws
5. Inconsistencies Between Security Standards, Risk Models, and Maturity Models
6. PCI Compliance

Managing and Understanding the Problem

7. Creation of a Fraud Taxonomy to Facilitate Comparisons of Technology and Exchange of Data
8. Quantifying the Effectiveness of Security Measures and Processes
9. Resiliency and Disaster Recovery
10. Records Management

Protecting the Customer Connection

- **Phishing continues to be an issue**
  - One bank found itself shutting down over 1,000 fake sites
  - Customers were being tricked into giving over challenge questions as well as answers
  - Use of challenge questions may actually make consumers less secure by encouraging them to reveal more personal information
- **As consumers become more aware of phishing, fraudsters are switching tactics**
  - "Vishing," or spoofed interactive voice response (IVR) lines, are beginning to appear
- **Most CIOs and CTOs we spoke with expressed uncertainty about what the proper solution would be**
  - Sending a password via mobile phone text message?
  - Password generation via hardware token?
  - Biometric scan on the keyboard or attached device?

Compliance Issues: Inconsistent State-Level Data Breach Laws

- In response to widely publicized data breaches like the TJX incident (more than 40 million cards compromised), dozens of states have enacted separate data breach laws
  - Consumer activism is strongest at the state level
- Many laws do not distinguish clearly between theft of a card number (transactional fraud) and identity theft, criminalizing both
  - This creates legal risks for banks, particularly those that service merchants who accept cards
- Inconsistent laws require additional resources at the bank level to ensure compliance for those institutions that operate nationally
- Obvious solution is a pre-emptive federal law… but what form should it take?
  - General nervousness about pushing for additional regulation.
  - Upcoming elections make it difficult to get action through Congress

Inconsistencies Between Security Standards, Risk Models, and Maturity Models

- Between August and December 2007, a group of financial industry, insurance, consulting and vendor executives met under the sponsorship of the International Committee for Information Technology Standards (INCITS), the main US organization for IT standards.
- The group delivered a report, available at http://www.incits.org/tc_home/sbp/sbp070049.pdf, which found that:
  - There are three distinct types of standards that financial institutions employ in the information security space:
    - compliance frameworks,
    - risk management models, and
    - maturity models.
  - The users must devote resources to integrate these standards, since the reference documents themselves are developed independently.
  - Users are usually not involved in the development of the standards, seeing it as a non-revenue generating activity.

Inconsistencies Between Security Standards, Risk Models, and Maturity Models

- The study group recommended that a taxonomy be developed to establish a common frame of reference for all standards to follow, making it easier to map them onto each other
  - The Financial Services Technology Consortium is currently working on a similar taxonomy, although for fraud rather than information security in general
- In addition, the study group urged an awareness campaign be mounted to ensure that financial institutions were aware of the standards that existed to guide them in securing their systems.
- Risk models should be modified to handle low likelihood, high impact events with greater sensitivity, assigning different levels of control to different levels of risk.
- Finally, the study group urged standards bodies, regulators, and financial institutions to find ways to work together more effectively with each other as well as with other stakeholders such as third-party processors and customers.

Payment Card Industry (PCI) Security Standard Overview

- **Establishes a minimum benchmark for secure processing of card payments**

- **Focuses on six main areas:**
  - Build and Maintain a Secure Network
  - Protect Cardholder Data
  - Maintain a Vulnerability Management Program
  - Implement Strong Access Control Measures
  - Regularly Monitor and Test Networks
  - Maintain an Information Security Policy

Financial Insights™ An IDC Company

PCI Compliance Efforts

- **Current enforcement efforts are focused on "Level 1 and 2" merchants**
  - Level 1: more than 6 million transactions/year
  - Level 2: 1-6 million transactions/year
  - Annual on-site audits and quarterly reviews
  - Main issue is storage of "full track" magnetic stripe data and PINs
  - Acquirers (merchant banks) face escalating monthly fines of $5,000-$25,000/merchant for non-compliance

- **Deadlines:**
  - September 30, 2006: All acquirers had to submit a PCI compliance plan for their Level 1 merchants
  - September 30, 2007: All Level 1 merchants must have validated compliance
  - December 31, 2007: All Level 2 merchants must have validated compliance

Source: RSA Security Survey, March 2007

PCI Compliance – a Mixed Bag

- Visa announced incentive payments in December for compliance by March 31, 2007
- Lower interchange rates will be offered
- As of January 22, 2008, according to Visa:
  - More than 75% of Level 1 merchants were compliant;
  - Nearly 66% of Level 2 merchants were compliant.
- This still leaves a lot of merchants out of compliance!
  - Most of the level 3's and 4's
  - Merchant processing banks increasingly worried they may be held liable because they have the "deep pockets."
  - Congress considering legislation to hold merchants liable for the costs of security breaches.
  - Courts have so far upheld the right of issuers to hold merchants liable.
  - Even without liability, fines can be expensive – Fifth Third has already paid Visa over $0.8 million in fines over the TJX breach

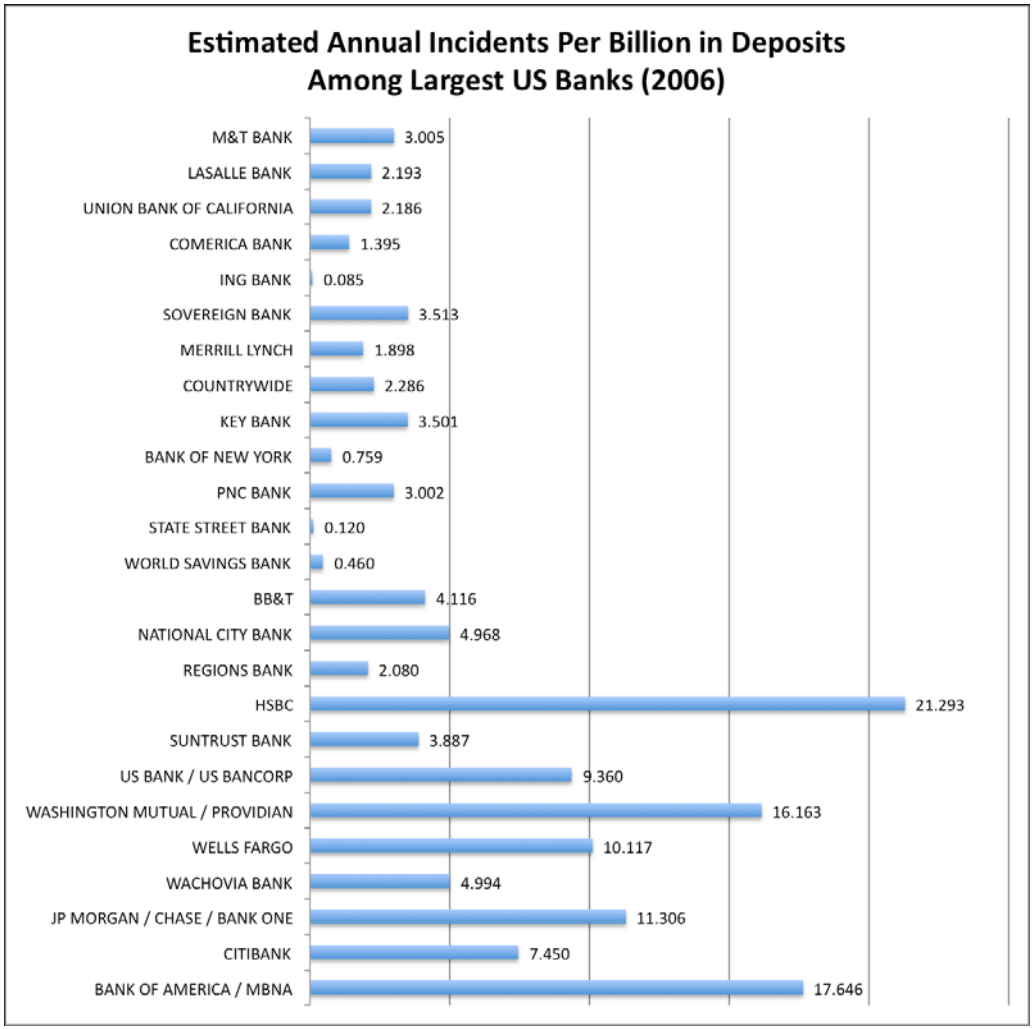
Managing and Understanding the Problem

- **No consistent, universally accepted measure of fraud:**
  - **2007 AFP Payments Fraud Survey:**
    - Only surveyed corporates
    - Limited to check and ACH fraud
    - 42% of those reporting fraud suffered no actual losses
    - No attempt to estimate total losses to the US economy
  - **CyberSource 8th Annual Online Fraud Report**
    - Only surveyed online merchants (n=351)
    - Limited to cards and ACH
  - **FTC Internet-Related Fraud Complaints**
    - Consumers, self reported (n=204,881)
    - Limited to wire, credit card and check

Financial Insights™ An IDC Company

How Well is Bank of America Doing on Security?

- Bank of America received many press mentions in 2006 for its SiteKey security system, which used a customer-selected picture and challenge questions to prevent phishing and increase security. This system was adopted by many US banks.
- However, according to recent report based on FTC complaints gained through Freedom of Information Act requests, BofA was 2nd worst in the US 2006 with 17.6 incidents of ID theft per $1B in deposits.
- Bottom line: we need a consistent way to compare performance and measure progress



Source: "Measuring Identity Theft at Top Banks," Hoofnagle, Chris, 2008. Available at http://www.finextra.com/finextra-downloads/newsdocs/hoofnagle.pdf

Financial Insights An IDC Company

Efforts to Manage and Understand the Problem

- **Financial Services Technology Consortium:**
  - "Better Collaboration Tools for Fighting Fraud - Real-time Sharing of information for Fighting Fraud" Project
    - Goal is to determine what sorts of information can be shared, and through what means
    - Fraud taxonomy has been developed to guide discussion
  - "Resiliency Model Initiative: Phase 3"
    - FSTC has been working with Carnegie Mellon's Software Engineering Institute to develop a resiliency model.
    - Resiliency has come to encompass not only natural disasters, but also physical and cyber attacks.
    - Phase 3 is aimed at piloting the model that has been worked out to field test it
    - Ultimate goal is a model that can be used for benchmarking as well as establishing an initial plan.
- **Records Management**
  - Many CIOs interested in the issue of e-mail retention

Essential Guidance and Summary

- Regulations, sophisticated criminals and high levels of reputational risk continue to make information security a top IT strategic initiative for financial institutions
- Successful information security management requires a coordinated strategy involving security governance, applications, systems and services
- Financial institutions need to find a way to make the benefits of information security investments show up in business cases
  - Too often, they lose out to “revenue producing” initiatives, even though they prevent revenue losing events
  - See “Innovation Killers”, Harvard Business Review, January 2008
- There is an urgent need for greater collaboration:
  - Between financial institutions and government
  - Between financial institutions and their customers
  - Between the financial institutions themselves
- Technology is only part of the solution: social and organizational factors are at least as important

Financial Insights™ An IDC Company

PSi

Questions? Live Meeting Chat or Audio

David Tompkins, Partner
Performance Solutions International
dtompkins@goto-psi.com

Aaron McPherson, Practice Director
Payments and Security
Financial Insights, an IDC company
amcpherson@financial-insights.com

Slides will be posted and an email will be sent.

Thank you for attending!

Information Security within the Financial Services Industry

Webcast March 5, 2008