Presenters

**Stephen McCarney**  
Global Director of Security and Cloud Portfolio Marketing  
Stephen.McCarney@unisys.com

**Bob Olson**  
Vice President  
Global Financial Services  
Robert.Olson@unisys.com
Agenda

Security Trends in the Financial Services Industry

Unisys Security Portfolio

Mobility Security

Concluding Remarks

Q & A
Impact and Challenges for the CIO
Enterprise CIOs are facing the most disruptive period in the history of IT

**Convenient** for the End User

- Infrastructural shift to Cloud Computing
- Shift to mobility as the “new desktop”
- Collaborative shift to social computing
- Informational shift to unstructured data and real-time analytics
- Cybersecurity shift towards “zero trust” security models

**Complex** for the CIO

- **Multiple deployment models** for data centers – public and private clouds
- **Multiple device types** for end users – smartphones, tablets, and laptops
- **Increased risk** associated with the loss of sensitive corporate information
- **Rising storage costs**; requires significant new analytics infrastructure
- **Porous perimeter** calls for innovative approach to tackle emerging threats
Cybersecurity Implications for CISOs
Current “perimeter-based” security models are inadequate and costly

CISO Challenges

- **Increasing Cybercrime** sophistication, frequency, and scale
- **Accelerated shifts** to cloud-, mobile- and social-enabled infrastructures and applications
- **Preventing leakage** of sensitive data across the borderless enterprise
- **Complying with regulatory requirements** during a time when a Big Data trend accelerates data volume, velocity, and variety
- **Any misstep can lead to costly loss of productivity, customers, and reputation**

Costly Data Breaches

Remediating successful data breaches costs companies an average of **$8.9M per year**
- Ponemon Institute, October 2012

Source: Ponemon Institute IT Security Tracking Study

© 2013 Unisys Corporation. All rights reserved.
Security Investment
A compliance and risk management IT investment priority

Survey: 2013 IT Spending Plans

Please indicate your IT spending plans for each of the following areas for 2013
Select one of the following for each area - increase, maintain, decrease

<table>
<thead>
<tr>
<th>Area</th>
<th>2012</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product development</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile banking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marketing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance / risk management functions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call centers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Back office support functions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Branches</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product/ account administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: OVUM - Business Trends: North American Retail Banking Technology Investment Strategies (January 2013) North American Retail Banking primary research study based on interviews with 75 senior retail banking IT executives. Institutions represented were from Canada (13.3%) and the US (86.7%)

Banks need to invest in compliance and risk management solutions to comply with increasing regulatory requirements
Security Threats for Financial Services
High velocity and rapidly evolving threat landscape

Top 10 Security Challenges*

1. State-sponsored espionage
2. DDoS attacks
3. Cloud migration
4. Password management
5. Sabotage
6. Botnets
7. Insider threats
8. Mobility
9. Internet
10. Privacy laws

* AT&T Top 10 Security Challenges for 2013
Security Failures are Bad for Business

“50%...” of bank customers are more likely to consider robust identity verification methods to be very compelling or extremely compelling factors in choosing a new bank. *

Lose faith in Bank
“56% of respondents lost faith in their bank after just one fraudulent attack**

Move to Competitor
“40% of businesses move some or all of their banking business to a competitor after a security breach***

Fear of Mobile Banking
“68% of customers cite security risks as the main cause for not adopting mobile banking***

* Javelin Strategy & Research: “Banking Authentication and the FFIEC”  ** 2012 Metaforic Survey  *** © 2013 Unisys Corporation. All rights reserved.
### Priority Areas of Focus

<table>
<thead>
<tr>
<th>Securing New Points of Vulnerability</th>
<th>Opportunity</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-level targeting, money mules, vendors and supply chain are avenues into the financial enterprise</td>
<td><strong>Secure all areas</strong> – not just cloud, social and mobile – but now software defined networks (SDN) and “Internet of Things”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cloud Security across all Deployment Models</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizations are facing increasing cloud security needs as they progress towards utilizing more than one cloud provider infrastructure</td>
<td><strong>Put in place a consistent security model</strong> across all these disparate cloud environments</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Increasing shift to Authentication as a Service and Bring Your Own ID (BYOID)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizations investigating more secure, flexible models for authentication and entitlements</td>
<td><strong>Balance decentralized ownership with centralized control</strong> while elevating overall authentication levels</td>
</tr>
</tbody>
</table>
Unisys Security Portfolio
We help you adapt, thrive and grow while protecting what matters most

Cybersecurity
- Stealth
- Security Advisory Services
- Security Operations Center
- Managed Security Services

People Identity Solutions
- Identification and Credentialing
- Identity and Access Management

Mobility Solutions
- Mobility Assessment Service
- Mobility Application Services
- Mobile Device Management
- End User Experience Monitoring

Location, Perimeter and Surveillance Security
- Risk Compliance and Governance
- Location Perimeter and Surveillance Security Solution
- Border and Facility Security
- Systems Video Surveillance Consolidation
Services and Features

- **Cloak servers and PC entry points** running sensitive applications or storing private information, making servers undetectable to unauthorized users.

- **Segregate data and transactions inside the network** so that only those with access know transaction is occurring, making it **undetectable** to everyone else.

Benefits

- Provides only authorized access to corporate intranet.
- Protects regional assets from rogue endpoints.
- Segregates corporate and regional assets based on “need to know.”
- Fosters availability while ensuring confidentiality and data integrity.
- Enhances application security by enforcing “Least Privilege.”
- Uses existing infrastructure – no rip and replace.
- Facilitates regulatory compliance.
- Easily scales to changing business requirements.
Stealth Under Extreme Scrutiny

Crypto-Module

Network Risk Assessment
CWD 05
AF Comm Agency

IV&V
National Center for Counter-terrorism and Cybercrime SOCOM

Export License
Dept of Commerce

FIPS 140-2 Certification
NIST

Stealth

DIACAP MAC-1 Certification
JFCOM

DIACAP MAC-1 Certification
CWD 10

NSA EAL4+ Certification
NIAP

2005
CWD 05
USAF

2006
Combined Endeavour
EUCOM

2007
CWD 08
DISA

2008
CWD 09
DISA

2009
JUICE 09
CECOM

2010
CWD 10
SOCOM

2011
GTRI
DJC2 PMO
SPAWAR

“Large Integrator”
Tests and fails to break Stealth

2012
Private Lab
SSVT Validation:
Failed to compromise

Emerald Warrior ‘12
SPRNet IATT

DIACAP: DoD Information Assurance Certification and Accreditation Process
MAC: Mission Assurance Category (Level 1 is Highest)
DISA: Defence Systems Information Agency
EUCOM: European Command
SOCOM: Special Operations Command
JFCOM: JOINT Forces Command
JIL: Joint Intelligence Laboratory

CWD: Coalition Warrior Interoperability Demonstration (4 wks)
JUICE: Joint User Interoperability Communications Exercise
CECOM: Communications Electronics Command (US Army)
GTRI: Georgia Tech Research Institute
DJC2: Deployable Joint Command and Control
NIST: National Institute of Standards and Technology
NIAP: National Information Assurance Partnership
Unisys Stealth Solution Suite

Enterprise wide – Consistent Security Approach

Stealth Secure Remote Access
Protects data communication for teleworkers across the Internet superior to traditional VPN, using the Stealth driver loaded to a laptop or SSVT.

Stealth Regional Isolation
Designed to secure information exchanged over public or private networks from many geographic locations.

Stealth Solution for Cloud
In a cloud, Stealth hides virtual workloads from unauthorized access in single or multi-tenant environments.

Stealth Data Center Segmentation
Cloaks servers running sensitive applications or storing private information; these servers are obscured to anyone without the required Stealth crypto keys.

Cloud Data Center
- A Virtual Web Server
- B Virtual Web Server
- A Virtual App Server
- B Virtual App Server
- A Virtual DB Server
- B Virtual DB Server
Security Advisory Services
Optimize performance and mitigate risk

Services and Features

- **Governance and Compliance**: security program integration, roadmaps, framework and compliance audits
- **Technology**: security assessments, deployments, emerging technology and infrastructure enhancements
- **Services**: penetration testing, process improvements and staff augmentation

Design and Implementation

- **Governance and Compliance**: security program integration, roadmaps, framework and compliance audits
- **Technology**: security evaluations, integration, deployments and program gap analysis
- **Services**: system based compliance audits, vulnerability assessments, and solutions management
Unisys Secure Operations
24/7 peace of mind with enhanced security benefits

Services and Features

• Remote Managed Security Services: tailored security services for security monitoring, security management, security information and event management, threat and risk intelligence, content filtering, security consultancy and security-as-a-service from the cloud

• End Point Security Services: comprehensive protection from threats targeting laptops

Benefits

• Cyber Threat Protection: maintain, advance and mature security capabilities

• Regulatory Compliance: facilitate compliance with regulatory requirements

• Enterprise Visibility: provides advanced cyber situational awareness and intelligence analysis capabilities
Unisys Identity Management Solutions
Improving efficiency/risk mitigation in employment-related processes

- Banks and its regulators are looking for improvements in employee security with added participation in background checks
- Consolidated capture of fingerprints and improved investigation workflow are under consideration
- Using the LEIDA framework to provide a proven platform for integration and workflow management between the bank and service providers
Unisys Mobile Security

Greater security, lower risk
A more holistic security approach for the enterprise and consumers. Four key dimensions of security: user, device, apps and data.

Key Capabilities
• Multi-Factor Authentication
• User, Device, Data and App Security

Benefits
• Integrated security from user to data
• Multi-factor authentication capabilities
• Peace of mind
Unisys Mobile Security--- Mobile Enterprise
Secure Mobile Eco-System

User
- Segment User
- Biometric solution for secure user authentication
- PIN
- GPS
- Facial Recognition
- Voice Recognition
- Iris Recognition

Device
- Encrypted enterprise data
- Application password enforcement
- Remote erase

Application
- SSO
- No firewall holes
- Authorized device check
- Role-based admin
- Policy groups

Data
- Segment Data
- Guaranteed delivery
- AES-192 encryption
- FIPS 140-2 certificate
- Data Loss Prevention (DLP) solution in place.

Multi-Factor Authentication

Stealth
- Confidential / Critical
- Non-Critical

MDM

Secure App Wrap

VPN \ Encrypted

Auth. Server

Firewall
Multi-factor Mobile User Authentication

Facial Image
Speech Pattern
GPS Location
PIN
Other Identity Data

A Ubiquitous Collection Device

Securely Transmitted to an Identity Verification Server

Business Rules
Authentication Services

Decision
Unisys Stealth Solution
Secure remote access; teleworking

**Problem:** Bank executives and customers want to securely access and share sensitive data while they are mobile.
Financial services executives and employees need secure remote access to the enterprise to ensure secure financial transactions.

**Solution:** Unisys SSVT or Stealth for Mobile

**Before Stealth:**
- Ordinary Secure USB

**After Stealth:**
- SSV1 Stealth USB

**Results:**
- Travelling executives can avoid carrying corporate laptops and instead use their tablet or use SSVT to securely login from any available PC or laptop -- from home, a cyber-café, a hotel, an airport, etc.
- Connecting to their virtual desktop reduces the risk of compromise of the VDI infrastructure.
Unisys Converged Security Solutions
Integrating location and identity to protect your critical business infrastructure

End-to-end physical access control integrates identity controls with location monitoring devices to provide command and control of policy compliance and risk management.
Closing Thoughts: Maximizing Security

With Unisys Security Solutions pave the way for
The next generation Financial Services Organization
Concluding Remarks

• For more information, please contact:
  – Your Unisys Account Team
  – Bob Olson, VP Global Financial Services, Robert.Olson@unisys.com
  – Stephen McCarney, Marketing Director, Stealth Solutions, Stephen.McCarney@unisys.com
Thank You