Cyber Security “State of The Union”

Presented by: Jason Witty, Senior Vice President & Chief Information Security Officer
U.S. Bancorp

January 29, 2015

This information represents the opinion of U.S. Bank and is not intended to be a forecast of future events or guarantee of future results. The factual information provided has been obtained from sources believed to be reliable, but is not guaranteed as to accuracy or completeness.
Agenda

- The World Around Us
- Digitization of Money
- Hyper-connectivity
- Threats and Risks
- Corporate Risk Management
- Personal Risk Management
Huge Cyber-Crime Ring Steals $45 Million From Two Banks

The World Around Us
Indicators of our Digital Dependence

U.S. GDP
16 Trillion
~ 20% of global economic activity

U.S. Debt
16 Trillion
Government debt is +100% of GDP

Daily payments via U.S. banking system
16 Trillion*
*Intra-day Liquidity Flows

Sources: CIA World Factbook, IMF, Bureau of Economic Analysis, Federal Reserve Bank of New York
Highly Interconnected Digital Economies

Global GDP (2011): 70 trillion

Width of Lines = total value of cross-border investments between regions as a % of GDP

Annualy...
$101 trillion (2011) global foreign investment assets

Daily...
- $16 trillion routes through the U.S. banking system
- $4-5 trillion turnover through global currency (FX) markets
- >80% of FX trades involve US$

Compare to...
- Brazil’s GDP: $2.3 trillion
- UK GDP: $2.4 trillion
- Japan GDP: $5.9 trillion
- China’s GDP: $8.2 trillion

Source: Exhibit A10 of McKinsey paper: Financial globalization: Retreat or Reset?
Rise of Alternative Currencies

+ 50 other listed currencies (source: coinmarketcap.com)
Technology’s Global Inflection Point

- 7.1 billion population
- 6.8 billion cell service subscriptions – almost one per person
  (UN projected figures for 2013)
- Smartphone sales now surpass cellphones
  (Gartner, Aug 2013)
- 2.7 billion people had Internet access in 2013
  (UN projected figures)
- 1.23 billion Facebook users
  (Dec 2013)

Source: UN Millennium Development Goals Report
“The cybersecurity threat to our Nation is real, evolving and imminent. The recent Intelligence Community’s 2013 Global Threat Assessment now indicates that cyber has surpassed terrorism as the number one U.S. national security threat”, with other top intelligence officials stating that “cyber attacks that destroy networks in the U.S. could come in the next few years.” – U.S. House Homeland Security Committee, Sept 2013
## Prosecution in the USA

### # of prosecutions filed vs. not prosecuted

<table>
<thead>
<tr>
<th>Year</th>
<th>Not Prosecuted</th>
<th>Prosecution Filed</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>286</td>
<td>1861</td>
<td></td>
</tr>
<tr>
<td></td>
<td>135</td>
<td>436</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1327</td>
<td>1363</td>
<td></td>
</tr>
<tr>
<td></td>
<td>481</td>
<td>181</td>
<td></td>
</tr>
</tbody>
</table>

### % of prosecutions not convicted, or convicted without prison sentence, or ending with a prison term

<table>
<thead>
<tr>
<th>Year</th>
<th>Convicted, prison term</th>
<th>Convicted, no prison</th>
<th>Not convicted</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>94.2</td>
<td>3.4</td>
<td>2.3</td>
</tr>
<tr>
<td></td>
<td>82.2</td>
<td>12.4</td>
<td>10.1</td>
</tr>
<tr>
<td></td>
<td>75.9</td>
<td>14.0</td>
<td>5.4</td>
</tr>
<tr>
<td></td>
<td>57.1</td>
<td>25.6</td>
<td>17.2</td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>86.3</td>
<td>8.7</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>83.1</td>
<td>9.2</td>
<td>7.8</td>
</tr>
<tr>
<td></td>
<td>76.5</td>
<td>12.8</td>
<td>10.7</td>
</tr>
<tr>
<td></td>
<td>58.5</td>
<td>25.7</td>
<td>15.8</td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>81.3</td>
<td>10.9</td>
<td>7.8</td>
</tr>
<tr>
<td></td>
<td>84.1</td>
<td>6.9</td>
<td>9.0</td>
</tr>
<tr>
<td></td>
<td>76.8</td>
<td>12.9</td>
<td>10.4</td>
</tr>
<tr>
<td></td>
<td>69.4</td>
<td>21.2</td>
<td>9.4</td>
</tr>
</tbody>
</table>

### Source

TRACFED Database – Syracuse University
Threats: Insider

- Can be accidental or malicious – both can be hard to anticipate unless controls are already in place, and both will lead to data &/or financial loss

- Impact can be minimized through good management / HR, employee education, and effective access management controls

- Some insider threats are sponsored by nation-states and are in search of intellectual property or classified information
Threats: Organized Crime

- Globally, cybercrime costs a minimum of **$300 billion a year**, and may be much higher (McAfee/Center for Strategic and International Studies 2013)
- 80% of malware detections are Trojans (Anti-Phishing Working Group)
- Keeping filters, updates & patches current is a challenge because malware-as-a-service has efficiently automated distribution to keep ahead of countermeasures
One Example: 45MM Pre-Paid Card Heist (Globally)

Threats: Hacktivists

- Ideologically motivated with a wide range of skills and abilities
- Responsible for more data breaches than cybercriminals according to Verizon DBIR
- Some have links to foreign governments
Threats: Nation-states

- Persistent and stealthy
- May target supply chain/vendors first to get access credentials
- Goals vary from espionage and intelligence-gathering to sabotage
- Evidence of direct nation-state involvement is usually circumstantial
Information Security Standards

Wide Financial Services Industry Adoption of:
- **PCI-DSS** - Payment Card Industry Data Security Standard
- **ISO/IEC-27002** - Information technology Security techniques - Code of practice for information security management
- **CoBIT** - Control oBjectives for Information and related Technology
- **COSO** - Committee of Sponsoring Organizations of the Treadway Commission
- **NIST 800-53** - Recommended Security Controls for Federal Information Systems and Organizations (Federal customer data protection)
Obama’s Response

February 12, 2013

Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience

Executive Order 13636 directs the Executive Branch to:
- Collaborate with industry to develop voluntary Cybersecurity Framework – National Institute of Standards and Technology (NIST)
- Promote and incentivize the adoption of cybersecurity practices
- Increase volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore the use of existing regulation to promote cybersecurity

Presidential Policy Directive-21 directs the Executive Branch to:
- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
- Understand the cascading consequences of infrastructure failures
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Protection Plan
- Develop comprehensive research and development plan
# NIST Cybersecurity Framework

## Framework Overview and Design

### Background
- Published February 12, 2014 by the National Institute of Standards and Technology (NIST)
- **Voluntary** federal framework (not a set of standards) for critical infrastructure services
- Provides common language for organizations to assess, communicate and measure improvement security posture

### Controls
- High-level controls provide the framework of **“what”** but not **“how”**
- 5 functions, 22 control categories, 98 key controls derived from industry best practice and standards

### Maturity Tiers
- Includes standardized model for identification of maturity of each cybersecurity activity/control design called “Tiers”

## Framework Categories

<table>
<thead>
<tr>
<th>Identify</th>
<th>Asset Management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>Protect</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
</tr>
<tr>
<td>Detect</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
</tr>
<tr>
<td>Respond</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
</tr>
<tr>
<td>Recover</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
</tr>
</tbody>
</table>
Keeping Pace: Must be Intelligence Driven

**Customers**
Place TRUST in us and demand we are careful stewards of their data and transactions

**Shareholders**
Require we protect revenue to enable GROWTH

**Employees**
Strive for excellence and are interested in how and where they WORK

**Business Lines**
Require AGILITY and fast time to market to meet business goals and customer demand

**Cyber-Threats**
Require us to have MATURE prevention, detection and recovery controls to keep pace

**Regulators**
Expect we provide evidence of a STRONG information security program

Customers
Shareholders
Employees
Business Lines
Cyber-Threats
Regulators
Keeping Pace: Must be Comprehensive

**ANTICIPATE**
Emerging threats & risks

**ENABLE**
Business growth while protecting existing revenue

**SAFEGUARD**
U.S. Bank information & assets

Eight Information Security Ecosystem Components

- **DEVICES**
  - Are secure and patched regularly to keep secure over time

- **APPLICATIONS**
  - Are secure in development and production

- **THIRD PARTIES & VENDORS**
  - Control parity is risk-based and protections are appropriate

- **CUSTOMERS & CLIENTS**
  - Are educated on cyber-risks and their role protecting their devices

- **DATA & INFORMATION**
  - Is secure at rest and in transit

- **NETWORKS**
  - Are monitored 24x7

- **IDENTITY & ACCESS**
  - Is appropriate based on job role

- **INDUSTRY & PARTNERSHIPS**
  - Provide actionable cost-effective threat and risk intelligence
Personal Risk Management
- Social Media
- Mobile
- Phishing
- Computer Hygiene
### What Is Social Media?

#### Social networking
- **Facebook**: Most popular, 1.3bn users
- **Google+**: Integrated apps, 500m users
- **LinkedIn**: Professionals, 175m users
- **Myspace**: Entertainment, 25m users
- **Klout**: Measures influence

#### Content communities
- **YouTube**: Video, 1tr views
- **Flickr**: Image gallery, 80m visitors
- **DeviantArt**: Art portfolios, 36m visitors
- **Instagram**: Photo editing, 100m users
- **Pinterest**: Scrapbooking, 25m visitors

#### Blogs / microblogs
- **Twitter**: Microblog, 500m users
- **Tumblr**: User generated, 77m blogs
- **Huffington Post**: News / political blogging content provider, 54m visitors monthly
- **LiveJournal**: User generated, 1.7m users

#### Virtual / game worlds
- **Steam**: Service, 54m users
- **Xbox Live**: Microsoft, 35m users
- **World of Warcraft**: Gaming, 10m players
- **Habbo**: Virtual chat, 10m users
- **Second Life**: Virtual world, 1m users

#### Collaborative projects
- **Reddit**: Social news, 43m users
- **Wikipedia**: Crowd-sourced Encyclopedia, 1.5bn users
- **Coursera**: Educational, 1m students
- **Kickstarter**: Virtual chat, 73k projects

#### Locational
- **Foursquare**: Mobile / geo, 20m users
- **Smartphones**: Geographic data

#### Key tenet
Information is permanently stored online & can be accessed & freely distributed to any other participant
The Risk of Social Media – Misrepresentation & Trust

This is who they claim to be…

1.5% of all Facebook accounts are estimated to be fake

Facebook’s first earnings report

This is who they are…

Fake accounts and profiles can be used for:
- Cyberbullying
- Extortion / blackmail
- Kidnapping

Journal of Adolescent Health
The risks of Social Media – Information Is Overshared

Bad assumptions:
• What we share will be seen by the intended audience
• Audience always has good intent
• Social media companies change privacy policies or add new features that may violate privacy

Physical risks…
- 78% of burglars use social media to target properties
- 74% use Google Maps & Street View to case houses

Credit Sesame survey

What you can do
- Have a family policy on what is shared
- Get involved in your family’s social networks
- Think carefully before you share
- Keep up-to-date on social media site changes
- Beware of geotagging

Reputation risks…
Tips for Social media

SOCIAL MEDIA AND GEOTAGGING — A RISKY COMBO

• Certain mobile apps & social media sites can track and share your location

• YouTube comedian Jack Vale uses his phone to find oversharing strangers, then startles his target with a ‘mind-reading’ act of their personal info.

BE AWARE OF WHAT YOU’RE SHARING

• Learn how to use privacy settings on devices, also on social media sites & apps
• Manage your friends list carefully
• Be careful when you share:
  • Personal information
  • Workplace information
Criminals send bogus messages designed to trick you into a desired behavior like:
- Clicking on a malware-infected link
- Filling in a form or web page with log-in and other information they can steal
- Installing malware-infected software

Tricks they use include:
- Imitating corporate branding to look legitimate
- Playing to emotions like fear or greed to get you to act
- “Spear-phishing” single individuals to avoid email detection routines

WHAT YOU CAN DO:
- Scrutinize all links before you click in an email
- Be super careful with email attachments
Staying Secure @ Home

• Maintain up-to-date anti-virus software

• If you have Windows XP or Vista, it’s time to upgrade…

• Make sure the following software tools are always up-to-date
  • Your Operating System (Windows, Mac, iOS, etc.)
  • Your web browser
  • Adobe Flash
  • Oracle Java
  • Adobe PDF Reader

• Parents of teenagers should be extra vigilant

• Use a dedicated computer or personal smartphone for online banking instead of a family computer
Personal Risk Management: Key Takeaways

1. Have a family social media policy – include location services
2. Consider using a specific device for eCommerce and nothing else
3. Keep all of your device software up to date
4. Be exceedingly cautious with links or attachments in emails
5. Choose passwords wisely