Navigate the Cyber and Fraud Risk Landscape

Association of General Contractors
January 10, 2017

Jason Witty
EVP, Chief Information Security Officer
Legal Disclaimer

This information represents the opinion of U.S. Bank and is not intended to serve as a recommendation or solicitation for the purchase or sale of any particular product or service. It does not constitute advice and is issued without regard to any particular objective or the financial situation of any particular individual or firm. These views are subject to change at any time based upon market or other conditions and are current as of the date indicated on these materials. Products and services offered may be subject to credit approval. Eligibility requirements, other conditions, and fees may apply. Deposit products offered by U.S. Bank National Association. Member FDIC.
My Disclaimer
This presentation is meant to educate you – not to scare you.
U.S. Bank is an industry leader.

- ~500 people dedicated to information security
- Strong corporate culture of risk management
  - Direct integration with Line of Business Chief Risk Officers
  - Board charter with quarterly updates
- 20-30% year-over-year investment in program growth past 3 years
- 2016 ISE Central Project of the Year – Enterprise Tokenization Integration Project
- Big data analysis - 3.8 billion events per day

Most Trusted Companies for Retail Banking*  
— Ponemon Institute, 2015 (9 years at #1)

A 2016 World’s Most Ethical Company®**  
— Ethisphere Institute, 2016 & 2015

* U.S. Bank is only bank to rank in the top five for all 11 years since the first privacy trust study was conducted in 2004.
** U.S. Bank is once again the largest U.S.-based bank to ever make this list!

U.S. Bank National Association. Member FDIC. ©2016 All trademarks are the property of their respective owners.
Context in my field is important.
My Favorite “Cyber” Analogy
CISOs as Weather Predictors
The internet is way cool.
Society Has Become Highly Digital

- Hyper-Connectivity
- Hyper-Mobility
- Hyper-Sociability
- Cyber-Physical “Things”
What happens in an Internet minute?

Netflix: 23,148 hours of video watched\(^1\)

YouTube: 138,889 hours of video watched\(^5\)

Google: 4.1 million searches\(^9\)

Twitter: 347,222 tweets\(^6\)

Pinterest: 57,870 page views\(^10\)

Pandora: 31,773 hours of music played\(^11\)

IM: 34.7 million instant messages (MIM) sent\(^12\)

Facebook: 3.3 million pieces of content shared\(^2\)

Instagram: 38,194 photos uploaded\(^7\)

App: 194,064 app downloads\(^8\)

Amazon: $133,436 in sales\(^4\)

Ads: 10 million ads displayed\(^3\)

Amazon Quarterly Income Statement, Year Ending Sept. 30, 2013


Google Official History, Comscore, Jan. 1, 2014


Compute Capacity to Get to the Moon

Apollo Guidance Computer
- 2 MHz processor
- 4 kB RAM
- 75 kB Storage
- Weight: 70 lbs

IBM System/360 Model 75
- 6 MB (6,000 kB) program

Source: https://en.m.wikipedia.org/wiki/Apollo_Guidance_Computer
The Modern iPhone

- 2.23 GHz (2,230 MHz) A10 CPU/RAM/GPU
- 256 GB (256,000,000 kB) Storage

(42,139 x more capacity than it took to put humans on the moon... roughly)
There are more “things” interconnected than ever before.

Gartner estimates that \textbf{6.4 billion} ‘things’ in use at end of 2016.

**Lighting systems** can be controlled using a smartphone app or via the web, as can fans, hot tubs, water pumps, thermostats, even door openers.

**Smart fridge** can track what it stores, alerting when products expire, & even add items to smartphone shopping list.

**Smart TVs** connect to the Internet for web browsing, image sharing, gaming, or watching streaming video.

**Personal medical devices** can be implantable or external & allow remote monitoring / treatment.

**Security cameras & systems** can be remotely armed & checked, get alerts or review your security feeds from any location.

**Today’s cars** are computer-guided and wirelessly connected via Bluetooth, GPS, radio protocols.

**F-35 fighter jet** has a highly advanced computerized logistics system designed to minimize repair and re-equipping turnaround times by monitoring the plane’s status and pre-emptively making service decisions so that ground crews are ready to go before the plane even lands.

**Sources:** Gartner, Forbes, Vice, Cisco IBSG, University of Michigan, ABC News, Qmed, Network World
Augmented reality is bringing together the physical and online worlds.

Pokemon Go! exploded in 2016 and brought augmented reality (AR) to the masses. Leading technology firms, like Facebook, Microsoft, Samsung, are heavily investing in AR.

Sources: CNET, Mashable
Technology is expanding the artist’s palette.

- **Google Tilt Brush** is revolutionizing the definition of painting
- With the swipe of a digital brush, users wearing a connected virtual reality HTC Vive headset can paint life-sized, three dimensional strokes
- Users have created sculptures and calligraphy and used the app for fabric and fashion design
- Google just revealed that the strokes can now be linked with audio tracks, so they form a visual representation of a “beat”

*Source: Tilt Brush*
...BUT...

Cyber threats are at an UNPRECEDENTED level.
Cyberthreats are evolving at an unprecedented pace.

“...the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat.”

– President Obama, April 1, 2015
Business email compromise continues to be a booming exploit for cyber criminals.

Law enforcement globally has received complaints from victims in every U.S. state and 95 countries.

1 Social Engineering
Scammers use social engineering to gain company information to compromise.

2 Masquerading
Once they have the data, they can masquerade or spoof an internal email to request transfer.

3 Email Compromised
An employee within the targeted organization receives the spoof email and authorizes transfer.

4 Money Transfer
Money is transferred from the victim’s account to the fraudulent account.

Example of a Spoofed Email

From: Sally.Smith@anycompany.com
To: Jeff Anderson
Subject: FWD: Payment to ABC Client
Jeff,
Need this processed immediately. Thanks.
Sally
---Begin Forwarded Message
From: Bob.Jones@anycompany.com
Sent: Wednesday, April 16, 2015 3:40 PM
To: Sally.Smith@anycompany.com
Subject: Payment to ABC Client
Sally,
ABC Client called me personally this morning and is fairly upset at us. Need your team to complete the wire they asked for multiple times. Please transfer $151,023 from my admin to 12345678 acct 78910100 as soon as possible.
Bob
Sent from my iPhone.
The Bad Guys are Exceedingly Well Funded.

- 270% increase since Jan. 2015
- Most transfers → China or Hong Kong
- Complaints from U.S. & 79 countries
- 17,642 victims from 2013 to 2016
- Average loss = $25-$75K

Total Exposed Loss
>$2.3 billion since 2013
(as of April 2016)

Sources: http://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/
Crypto ransomware has also become a huge problem for business.

Cyber-criminals collected $209 million in the first three months of 2016 by extorting businesses to unlock computer servers.

**The Lure**

This is the bait used to launch the attack: phishing emails with infected attachments or links, or a hacked website or malicious ad. When the user takes the bait, this triggers the next step.

**Malware Installation**

The malware is installed on the user’s device. The user may not know the malware is being installed and that their device is being taken over with infected software.

**Call Home & Key Exchange**

After the malware is installed, it needs to “call home” to get the unique encryption key from the server so the files can be decrypted after the ransom is paid.

**Encryption**

The ransomware then encrypts files or systems on the device, to restrict access. This effectively locks data from the user or renders the entire device inoperative.

**Ransom/Extortion**

In order to gain access to the system or data, the threat actors request payment (or ransom) from the victim to unlock the device.
An Example Closer to Home….

Construction project owners scammed

1. Project start – ACH payment accounts agreed.

2. After start, project owner receives fraudulent email eg. “crosslandconstructions.com” rather than “crosslandconstruction.com”

3. Project owner changes ACH instructions to send to Fraudsters

4. Weeks later (too late) it is uncovered

5. Project Owner takes the loss.
Fraudulent E-mail caused Sedgwick County to Lose $566,000

Fraudulent vendor requested ACH destination change

1. Ongoing project with Cornejo & Sons

2. Fraudulent email sent to Sedgwick County requesting ACH account change for payments to Cornejo & Sons

3. County changed ACH destination

4. Loss: $566,088.90

The FBI is offering $4.2 million in rewards for The Top 5 “cyber’s most wanted” criminals.

1. Evgeniy Mikhailovich Bogachev | Reward - $3 Million
   - Mastermind behind the GameOver Zeus botnet, which was allegedly used by criminals to infect more than 1 million computers, resulting in up to $100 million in losses since 2009.

2. Nicolae Popescu | Reward - $1 Million
   - Romanian accused of fooling innocent Americans with fake auction posts on several websites, including eBay, Cars.com, and AutoTrader.com, claiming to sell cars that just didn’t exist.

3. Alexsey Belan | Reward - $100,000
   - Russian national wanted for allegedly stealing consumer data by compromising the cyber security systems of three unnamed major US-based e-commerce sites in Nevada and California. After stealing and exporting user databases with passwords to his server, Belan allegedly negotiated the sales of the databases.

4. Peteris Sahurovs | Reward - $50,000
   - Accused of developing and selling a computer virus through advertisements on news website pages. Fake ads forced users to purchase fraudulent antivirus software by flooding victim’s desktops with pop-ups and fake security alerts. Sahurovs, a native of Latvia, made more than $2 Million by selling his “antivirus” software.

5. Shailesh Kumar Jain | Reward - $50,000
   - The only American citizen on the FBI’s Most Wanted Hackers list, made $100 Million by using a flood of pop-up ads and email scamming to convince users that their computers were infected with a virus and then selling them the bogus AV software packages for between $30 and $70.
We work hard to protect ourselves and our customers from these threats.
Information Security Programs must be comprehensive.

Eight information security ecosystem components

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

**NETWORKS**: Are monitored 24x7

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

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

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

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

**INDUSTRY & PARTNERSHIPS**: Provide actionable cost-effective threat and risk intelligence

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

**EMPLOYEES**: First line of defense, key to success

**ANTICIPATE**
emerging threats & risks

**ENABLE**
business growth while protecting existing revenue

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

Regulators
Expect we provide evidence of a STRONG information security program

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

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

Regulators
Expect we provide evidence of a STRONG information security program

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
Velocities require machine-speed decision support.

At U.S. Bank:

• **3.8 Billion** events / day
  – ~6.7 low impact incidents / day

• **$10 Billion** money movement / day

• **1.3 Petabytes** of information security data

• **40 Cyber-threat feeds** / day

• Full time people for:
  – SOC 1/2/3
  – Data Science
  – Hunting
  – Malware reverse engineering
  – Threat Automation
There are several best practices that businesses can use to protect themselves.
Defense in Layers

- Technology Security Controls
- Anti-Fraud Controls
- User Education

Image credit: WikiHow
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
- Contains 4 maturity tier ratings

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management</td>
<td>Access Control</td>
<td>Anomalies and Events</td>
<td>Communications</td>
<td></td>
</tr>
<tr>
<td>Business Environment</td>
<td>Awareness and Training</td>
<td>Security Continuous Monitoring</td>
<td>Analysis</td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td>Data Security</td>
<td>Response Planning</td>
<td>Mitigation</td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Information Protection Processes</td>
<td>Detection Processes</td>
<td>Improvements</td>
<td></td>
</tr>
<tr>
<td>Risk Management Strategy</td>
<td>Maintenance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Communications</td>
<td></td>
</tr>
</tbody>
</table>
There are general cybersecurity best practices that all businesses can implement.

Assign someone to be accountable for information security. Active executive management is essential. Without that involvement and commitment, a firm is unlikely to achieve its information security goals.

Pick a framework and implement it. A sound governance framework is a foundational aspect of an information security program. There are many to choose from, and they can be modified to fit your needs:

- **Maintain security patches.** When cyber-criminals are constantly inventing new techniques and looking for new vulnerabilities, an optimized security network is only optimized for so long. Keep your software and hardware security up to date.

- **Create specific access controls.** Once your IT network is secure, you need to be very careful about who you decide to give access.

- **Educate and train your users.** Users will always be your weakest link when it comes to information security. Regularly educate your users on cybersecurity best practices.

- **Detect and mitigate malware.** Use a layered defense strategy and enclave data that is particularly sensitive.

- **Backup your data.** Make sure your firm is backing up its data. Having the ability to restore your data is critically important as criminals become more sophisticated and technological issues occur.

**Sources:** FINRA, Observe IT, United State Computer Emergency Response Team
Check Fraud

“If you make it easy for people to steal from you, they will.”

Frank Abagnale
Consultant to the FBI and U.S. Bank
Central figure in movie “Catch Me If You Can”
Paper Fraud Prevention Services

- **Positive Pay**
  - A “checks issued” file is sent to the bank. A two point match is conducted against the dollar amount and check number. Any mismatched items are sent to an exception queue for company review.

- **Payee Positive Pay**
  - Additional add on service to positive pay allowing a third point match to payee name.

- **Reverse Positive Pay**
  - Eliminates the need to notify the bank of issued checks. All items are sent to an exception queue for company review.

- **Check Filter**
  - Blocks checks in excess of a specified dollar amount. (zero if checks are not disbursed from the account)

ACH Fraud Prevention Services

- **ACH Positive Pay**
  - Online ability to adjust and determine companies with ACH debit access to your account as unregistered ACH transactions are processed.

- **ACH Block**
  - Blocks all companies from ACH debit access to your account

- **ACH Filter**
  - Only allows preset/pre-registered companies with ACH debit access to your account
Education is Also Key

- Treasury personnel need to understand these threats
- Do not accept wire or ACH instructions over email
- If you think the CEO just requested an urgent wire transfer, walk into her/his office, or call them
- Report anything suspicious to you bank as soon as possible
Key Take-Aways & Recommendations

- Technology and threat landscape are ever changing
- Be aware of scams
- Appoint someone to be responsible for security
- Perform a cybersecurity assessment
- Watch your accounts – see something say something
QUESTIONS?

This information represents the opinion of U.S. Bank and is not intended to serve as a recommendation or solicitation for the purchase or sale of any particular product or service. It does not constitute advice and is issued without regard to any particular objective or the financial situation of any particular individual. These views are subject to change at any time based upon market or other conditions and are current as of the date indicated on