Clark Nuber: How Cybersecurity programs are effecting fraud.

Anthony Hargreaves
How Cybersecurity programs are effecting fraud
Agenda

• Introduction
• Todays audience
• What’s happening out there?
• Data & Cybersecurity impact on fraud
• Tips on scams, phishing, spoofing, and scrapping
• Tips on how to combat Cyber & Fraud threats
• Summary
• Q & A
Anthony Hargreaves

• Originally from Australia
• 15 Years Experience:
  – National Australia Bank – Credit Card Fraud and phishing scams
  – Protiviti IT Auditor – Focus on SOX & IT Consulting
  – Safeway – Focus on PCI and Database re-engineering
  – EY – Focus on IT and Cloud compliance
  – Clark Nuber focus on IT Security Programs
Introduction - Relationships

• Family, friends, partners, community
• Smart phone
• Bank
• Employer
• Tax preparer
• Healthcare provider
• As a consumer
• Giving back and preparing for retirement
Todays Audiences

• Interactive – Show of Hands
Today’s Audience

• No individual, organization, or industry is immune
What’s Happening Out There?

- Email (contacts, sensitive info)
- Banking apps
- Expense apps
- Payment Apps
- Social media (all about you)
What’s Happening Out There?

Special Announcement

DOWNLOAD OUR APP TODAY!

Just scan the QR code or search “United Way Norman” in your app store! You’ll get exclusive access to events, news via push notifications and much more!

Clark Nuber
Cybersecurity Program

Make-up

• An Effective Frame-work
• End-to-End Scope
• Comprehensive Risk Assessment and Threat Modelling
• Proactive Incident Response Plan combined with training
• Dedicated Cybersecurity resources
Anti-Fraud Program

Make-up
• Risk Assessment
• Code of Ethics and Anti-Fraud Policies
• Tone from the top
• Training
• Vehicles for reporting non-compliance
• Centralized Data Repository
• Standardized case investigation, management and disposition
• Data analytics
• Evaluation and validation (Monitoring or Internal Controls)
• Available Fraud or Loss Prevention resources
What’s Happening Out There?

• Increase in technology, software and devices

• Availability of the data these devices produce, consume and store.

• Increase in data breaches

• Cybersecurity laws and regulations remain behind or in a state of flux
Technology + Devices = Data

- Increase in devices

<table>
<thead>
<tr>
<th>World Population</th>
<th>6.3 Billion</th>
<th>6.8 Billion</th>
<th>7.2 Billion</th>
<th>7.6 Billion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Devices</td>
<td>500 Million</td>
<td>12.5 Billion</td>
<td>25 Billion</td>
<td>50 Billion</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connected Devices Per Person</th>
<th>2003</th>
<th>2010</th>
<th>2015</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>More connected devices than people</td>
<td>0.08</td>
<td>1.84</td>
<td>3.47</td>
<td>6.58</td>
</tr>
</tbody>
</table>

Source: Cisco IBSG, April 2011
What’s happening out there

• Increase in devices
What’s happening out there

- Increase in availability of information
What’s happening out there

Top 5 most cyber-attacked industries in 2016

- Healthcare
- Manufacturing
- Financial Services
- Government
- Transportation

Source: 2016 IBM X-Force Cybersecurity Intelligence Index
What’s happening out there

- Top 12 Health Care data breaches by people impacted

<table>
<thead>
<tr>
<th>Nbr</th>
<th>Who</th>
<th>Individuals affected</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Anthem</td>
<td>80 Million</td>
<td>Jan, 2015</td>
</tr>
<tr>
<td>2</td>
<td>Premera Blue Cross</td>
<td>11 Million</td>
<td>Jan, 2015</td>
</tr>
<tr>
<td>3</td>
<td>TRICARE Management Activity</td>
<td>4.9 Million</td>
<td>Sep, 2011</td>
</tr>
<tr>
<td>4</td>
<td>Community Health Systems</td>
<td>4.5 Million</td>
<td>Apr, 2013</td>
</tr>
<tr>
<td>5</td>
<td>Advocate Health Care</td>
<td>4.03 Million</td>
<td>Jul, 2013</td>
</tr>
<tr>
<td>6</td>
<td>Health Net Inc.</td>
<td>1.9 Million</td>
<td>Jan, 2011</td>
</tr>
<tr>
<td>7</td>
<td>New York City Health &amp; Hospitals</td>
<td>1.7 Million</td>
<td>Dec, 2010</td>
</tr>
<tr>
<td>8</td>
<td>Montana Department of Public Health and</td>
<td>1.3 Million</td>
<td>Jul, 2013</td>
</tr>
<tr>
<td>9</td>
<td>AvMed Inc</td>
<td>1.22 Million</td>
<td>Dec, 2009</td>
</tr>
<tr>
<td>10</td>
<td>The Nemours Foundation</td>
<td>1.06 Million</td>
<td>Aug, 2011</td>
</tr>
<tr>
<td>11</td>
<td>Blue Cross Shield of Tennessee</td>
<td>1.02 Million</td>
<td>Oct, 2009</td>
</tr>
<tr>
<td>12</td>
<td>Sutter Medical Foundation</td>
<td>943,434</td>
<td>Oct, 2011</td>
</tr>
</tbody>
</table>

114,413,434
What’s happening out there

- Top 12 Health Care data breaches by people impacted

<table>
<thead>
<tr>
<th>Nbr</th>
<th>Who</th>
<th>Individuals affected</th>
<th>When</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Anthem</td>
<td>80 Million</td>
<td>Jan, 2015</td>
<td>Sophisticated attack</td>
</tr>
<tr>
<td>2</td>
<td>Premera Blue Cross</td>
<td>11 Million</td>
<td>Jan, 2015</td>
<td>Sophisticated attack</td>
</tr>
<tr>
<td>3</td>
<td>TRICARE Management Activity</td>
<td>4.9 Million</td>
<td>Sep, 2011</td>
<td>Lost or theft of backup tapes</td>
</tr>
<tr>
<td>4</td>
<td>Community Health Systems</td>
<td>4.5 Million</td>
<td>Apr, 2013</td>
<td>Sophisticated attack</td>
</tr>
<tr>
<td>5</td>
<td>Advocate Health Care</td>
<td>4.03 Million</td>
<td>Jul, 2013</td>
<td>Theft of 4 unencrypted PC's</td>
</tr>
<tr>
<td>6</td>
<td>Health Net Inc.</td>
<td>1.9 Million</td>
<td>Jan, 2011</td>
<td>Theft of 9 server drives</td>
</tr>
<tr>
<td>7</td>
<td>New York City Health &amp; Hospitals</td>
<td>1.7 Million</td>
<td>Dec, 2010</td>
<td>Theft of backup tapes</td>
</tr>
<tr>
<td>8</td>
<td>Montana Department of Public Health and</td>
<td>1.3 Million</td>
<td>Jul, 2013</td>
<td>Hacked a server</td>
</tr>
<tr>
<td>9</td>
<td>AvMed Inc</td>
<td>1.22 Million</td>
<td>Dec, 2009</td>
<td>Theft of 2 unencrypted PC's</td>
</tr>
<tr>
<td>10</td>
<td>The Nemours Foundation</td>
<td>1.06 Million</td>
<td>Aug, 2011</td>
<td>Alleged theft of 3 unencrypted backup tapes</td>
</tr>
<tr>
<td>11</td>
<td>Blue Cross Shield of Tennessee</td>
<td>1.02 Million</td>
<td>Oct, 2009</td>
<td>Theft of 57 encrypted computers hard drives</td>
</tr>
<tr>
<td>12</td>
<td>Sutter Medical Foundation</td>
<td>943,434</td>
<td>Oct, 2011</td>
<td>Theft of a Desktop computer</td>
</tr>
</tbody>
</table>

114,413,434
Data and Cybersecurity impact on fraud
Data Classification

• Data Classification model
Data Classification

• In the U.S. you need to be aware of:
  • The Federal Trade Commission (FTC) Act
  • The Financial Services Modernization Act (Gramm-Leach-Bliley Act)
  • Health Insurance Portability and Accountability Act (HIPAA)
  • The Fair Credit Reporting Act

• EU will enact General Data Protection Regulation (GDPR).
  • Is a very vast and complicated act – it will impact the U.S.
  • Goes into force May 25, 2018

• The directive affects all companies that hold or use European personal data, whether that company is located in Europe or not.
How best to prevent limit fraud

Whistleblower

Internal Controls

Security Training

- Separation of duties
- Clear description of responsibilities
- Non-concentration of power and confidence
- Job rotation
- Mechanisation of work
- Auto checking system
- Prescribed format
- Physical, mechanical and electronic control

Clark Nuber
What does Data and Fraud Look Like?
Some Common Attacks

• Online Spoofing
  • Phishing
  • Ransomware
  • Scrapping
• Documentation Fraud
• Wire Fraud
• Vendor Management
• Data theft
Some Common Attacks

**Why Phishing Scams Keep Working**

Enter your bank account number. SCAM.

**Wait for It**

Enter your bank account number. SCAM.

**There It Is**

Enter your bank account number. Okey-dokey.
Some Common Attacks - Phishing

1. Fake sender domain. (not service@paypal.com.au)
2. Suspicious Subject and content.
3. Bad grammar
4. Hovering over link reveals suspicious URL.
Some Common Attacks - Ransomware

---

Sun 4/12/2013 11:55 AM
Internal Revenue Service <office@irs.gov>

[1]Spam KSE Payment confirmation for tax refund request # 75991792

To: [Redacted]

Attachments: confirmation_75991792.doc (58 KB); ATT00001.txt (236 B)

Dear taxpayer,

You are receiving this notification because your tax refund request has been processed. Please find attached a copy of the approved 1040A form you have submitted, containing your personal information and signature. On the last page, you can also find the wire transfer confirmation from the bank.

Transaction type: Tax Refund
Payment method: Wire transfer
Amount: $7592
Status: Processed
Form: 1040A

Additional information regarding tax refunds can be found on our website: [http://www.irs.gov/Refunds](http://www.irs.gov/Refunds). Please note that IRS will never ask you to disclose personal or payment information in an email.

Regards,
Internal Revenue Service
Address: 1111 Constitution Avenue, NW
Washington, DC 20224
Phone: 1-800-829-1040
Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.
Some Common Attacks - Hoax
Some Common Attacks – Web Scraping

This is the authentic listing from the MLS. Note the descriptive copy, brokerage, MLS# and correct price and street.

This is the fake. Notice the street name and price are different.
Some Common Attacks – Documentation Fraud

• On the rise again
• Scammer fabricates documents – Name your Industry!
• Scammer takes out a new overdraft/mortgage/credit card
• The criminal takes the cash – leaves owner debt
Wire Fraud

• Obtain the email address format of the company
• Identify persons in positions of authority to wire funds
• Send an email with fraudulent wire transfer instructions
• The victim follows the instructions, and the money is sent to the scammer
• The scammer acquires the funds.
Importance of Vendor Management

- Know your Third Party Vendors
- Understand Service Level Agreements
- Review key access roles
- Align data policy with yours
- Understand documentation handling procedures
- Perform regular document destruction
- Know your data breach protocols
Attacked from Within
What does Data and Fraud Look Like?

• So what does this mean?
• Financial Information
• Transactional Data
• Personally Identifiable information
  • Info which can assist with ID fraud/social engineering
  • The past, present, or future records.
• Intellectual Property
• Trade Secrets
• Digital media that can be converted to currency
Combating Fraud & Cyber Threats
The Relationship of Cybersecurity and Fraud

• 5 Tips for Cybersecurity
• 5 Tips for Data Security
• 4 Best Technical Tips
• 3 of Anthony’s recommended baby steps
5 Tips Cybersecurity

1. Verify the front lines
   – Maintaining a detailed and integrated network diagram.

2. Identify Cyber threats
   – Perform an annual risk assessment.
## 5 Tips Cybersecurity

<table>
<thead>
<tr>
<th>Threat (What could happen?)</th>
<th>Threat Agent (Who could do it?)</th>
<th>Vulnerability (Is it possible?)</th>
<th>Existing Safeguards (What is in place to prevent it?)</th>
<th>Consequence (What is the worst thing that could happen?)</th>
<th>Severity</th>
<th>Likelihood</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stored data (e.g. history, programs) is intentionally modified or corrupted by unauthorized individual through local access</td>
<td>1. Malicious Insider</td>
<td>1. Disgruntled employee/contractor</td>
<td>1. Personnel screening 2. Access control logs 3. Offsite storage of backups</td>
<td>1. Economic Loss 2. Product Safety 3. Corp Image</td>
<td>Med</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
5 Tips Cybersecurity

1. Verify the front lines
   – Maintaining a detailed and integrated network diagram.

2. Identify Cyber threats
   – Perform an annual risk assessment.

3. Network scanning and Security Assessments
   – They walk among us! Know your IT environments limitations and scan and test it frequently.

4. Data Classification
   – Define what is your organizations data assets.

5. Know your incident response plan:
   – Rehearse your incident response plan.
5 Tips on Data Security

Create a Data Management Policy
   Encompass Data Classification and Document retention and destruction

1. Take stock – Network Diagram/Data Flow
2. Scale down – Keep only the information you need
3. Lock it – Apply appropriate safety measures
4. Pitch it – Destroy it once you don’t need it
5. Plan Ahead – Be prepared for a data breach

Note: Many states have different PII laws
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (1) Application whitelisting of permitted/untrusted programs, to prevent execution of malicious or unapproved programs including DLL files, scripts and installers.</td>
<td>Essential</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>2 (2) Patch applications, e.g., Java, PDF viewers, Flash, web browsers and Microsoft Office. Patch or mitigate systems with extreme risk vulnerabilities within two days. Use the latest version of applications.</td>
<td>Essential</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>No</td>
<td>Yes</td>
<td>Possible</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3 (3) Patch operating system vulnerabilities. Patch or mitigate systems with extreme risk vulnerabilities within two days. Use the latest suitable operating system. Avoid Windows XP.</td>
<td>Essential</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>No</td>
<td>Yes</td>
<td>Possible</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>4 (4) Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.</td>
<td>Essential</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>No</td>
<td>Possible</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Passwords are like Underwear

• Change them regularly
• Keep them long

• Don’t leave on your desk
• Don’t loan them to anyone
Know and map your controller

The greatest controller for the greatest games lineup in Xbox history

Xbox Elite Wireless Controller

- Thruster Pack
- Smart Link
- Molotov / Sprint & Zoom
- Issue Orders
- Switch Grenade
- Switch Grenade
- Tracking
- Frizzle Weapon
- Throw Grenade
- Pause
- Switch Weapon
- Crouch
- Jump
- Action & Reload
- Look / Make

Logic Access

Change Management

Operations

Clark Nuber
Know and map your controls

Entity Level Controls
- Mission / Purpose
- Strategies and Plans
- Policies & Procedures
- Risk Assessments
- Training & Education
- Internal Audit
- Quality Assurance
- Board Communication

Manual Controls
Involves **NO** reliance on a system or application and are performed by people:
- Fixed asset acquisitions in excess of $10,000 are approved by the Capital Asset Committee and the CFO via physical signature on a capital expenditure form.

IT Dependent Manual Controls
(ITDM) controls have both a manual and a system component (typically with reports)
- The A/P sub-ledge is reconciled to the general ledger on a quarterly basis; the reconciliation is reviewed by the CFO

IT General Controls
- Logical Access (Security)
- Change Management
- Operations

Application Controls
Application controls are completely automated, and are either programmed or configured within the application itself:
- Embedded Control: System is programmed (hard coded) to perform the control
- Configurable Control: System is configured via settings within the application to perform the control
## Know and map your controls

<table>
<thead>
<tr>
<th>Entity Level Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL1 Does the entity have key policy and procedures documented and reviewed annually</td>
</tr>
<tr>
<td>EL2 Is an annual Risk Assessment performed</td>
</tr>
<tr>
<td>EL3 Does security training and education take place</td>
</tr>
<tr>
<td>EL4 Does board communication involve updates on IT operations, Cybersecurity and business</td>
</tr>
<tr>
<td>EL5 Does strategic planning take place and is communicated annually</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logical Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>LA1 General IT security procedure settings are documented and approved</td>
</tr>
<tr>
<td>LA2 Password settings are enabled and appropriate for access to network and applications</td>
</tr>
<tr>
<td>LA3 Access to privileged IT functions is limited to appropriate individuals</td>
</tr>
<tr>
<td>LA4 Access to privileged financial system resources is limited to appropriate individuals</td>
</tr>
<tr>
<td>LA5 User provisioning processes require appropriate approval and are established</td>
</tr>
<tr>
<td>LA6 Physical access to system hardware is restricted to appropriate individuals</td>
</tr>
<tr>
<td>LA7 Logical access and system perimeter is monitored</td>
</tr>
<tr>
<td>LA8 Segregation of Duties exists within the logical access environment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Change Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM1 Changes are authorized</td>
</tr>
<tr>
<td>CM2 Changes are tested</td>
</tr>
<tr>
<td>CM3 Changes are approved before deployment</td>
</tr>
<tr>
<td>CM4 Changes are monitored</td>
</tr>
<tr>
<td>CM5 Segregation of Duties exist within the change management environment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IT Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPS1 Financial data is backed up and recoverable</td>
</tr>
<tr>
<td>OPS2 System Backups are monitored for errors and resolved</td>
</tr>
<tr>
<td>OPS3 IT Operations has incident management procedures to resolve issues in a timely manner</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP1 Embedded system controls have been identified and annually tested</td>
</tr>
<tr>
<td>APP2 Configurable system controls have been identified and annually tested</td>
</tr>
</tbody>
</table>
# Know and map your controls

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Risk</th>
<th>[Client Name] Control</th>
<th>Control Owner</th>
<th>Effective Date</th>
<th>Frequency</th>
<th>Control Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LOGICAL ACCESS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LA1 - General IT security settings are documented, reviewed and approved.</td>
<td>Security standards are not documented and impacts the organizations ability to promote security awareness and training. Network perimeter and security configurations are not documented or optimized to prevent unauthorized access.</td>
<td>LA1a) Documented IT Security Policy and Procedures exist at [Client Name] and are reviewed and approved on an annual basis.</td>
<td>IT Director</td>
<td>06/30/13</td>
<td>N/A</td>
<td>Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LA1b) [Client Name] IT department document and maintain an IT network diagram which is updated as needed and reviewed and approved on an annual basis.</td>
<td>IT Director</td>
<td>06/30/13</td>
<td>Annually</td>
<td>Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LA1c) A “Technology Summary” document listing all relevant (in scope) applications is updated as needed and reviewed and approved on an annual basis.</td>
<td>IT Director Finance Director</td>
<td>06/30/13</td>
<td>Weekly</td>
<td>Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LA1d) Security awareness training is mandatory for all new hires and provided on an annual basis for all employees.</td>
<td>IT Director Human Resource Manager Finance Director</td>
<td>06/30/13</td>
<td>Annually</td>
<td>Key</td>
</tr>
</tbody>
</table>
Anti-Fraud Program

Make-up
• Risk Assessment
• Code of Ethics and Anti-Fraud Policies
• Tone from the top
• Training
• Vehicles for reporting non-compliance
• Centralized Data Repository
• Standardized case investigation, management and disposition
• Data analytics
• Evaluation and validation (Monitoring or Internal Controls)
• Available Fraud or Loss Prevention resources
What can YOU do Right Now?

• Are you confident with the accuracy of your data classification, Anti-Fraud policy – is it effectively enforced?
• Do you currently have a whistle-blower hotline?
• Are your IT security policy and procedures current?
• Do you receive annual security awareness training?
• Are you aware or involved in your annual Risk Assessment or Cybersecurity program?
• Are your IT General Controls formalized?
• Has an IT Security or network penetration test been performed in the last 36 months (Yes/No)
Summary
Thank you for your attention

Please contact

Anthony Hargreaves
425.635.4558
info@clarknuber.com
“Anthony Hargreaves” in the Subject Line