Anatomy of a Social Engineering Attack
Exploiting Human Behaviors
Introductions

Wendy Frank  
PwC, Principal  
(818) 397-3040  
wendy.l.frank@pwc.com

Brian Lee  
PwC, Manager  
(213) 663-0337  
blee@pwc.com

David Miles  
PwC, Director  
(602) 327-3049  
david.miles@pwc.com
Overview

What is It?
- Introduction to Social Engineering
- Notable Social Engineering Attacks
- Impact of Social Media

Why Should You Care?
- Statistics
- Risks & Impact

How They Do It
- Methodologies & Approach
- Demo
- USB Drop Impact

How to Protect
- Risk Mitigation Strategies
- Where to begin?
- Key Take-Aways
What is It?
What is Social Engineering?
Hacking the Human Weakness

Social-Engineering;
/ˈsəʊʃəl-ˌɛnɪdʒəˈnɪrɪŋ/
1. The act of psychological manipulation which influences a person to perform an action or divulge sensitive information.

• Email
• Email addresses can be spoofed to look like they are coming from a legitimate sender. Be cautious about clicking on links in emails—even from trusted sources.

• Phone Calls
• Individuals can gain your information by claiming to be with Information Security, the Help Desk, etc. Never provide your account information, password, or other sensitive data over the phone to unknown individuals.

• Imitating an individual
• Intruders can follow staff into restricted buildings and areas. Never let someone follow you through a door unless you know them.

• Information provided by internet resources
• Users can access information you provided online. Be careful what you post and store in your online accounts. Assume anything you post will be never be deleted (even if you delete it).

• Redirection of internet traffic to malicious look-a-likes
• Malware can infect any computer and antivirus software is not perfect. Be careful about what you download and open from the internet. Avoid using public computers or kiosks to access your email or any accounts. Assume those computers have keystroke loggers installed.

**Phishing**

**Vishing**

**Impersonation**

**Social Networking Reconnaissance**

**Pharming**

Types of Social Engineering Attacks
What makes social engineering so scary?

Social engineering is one of the most overlooked yet most effective ways for a malicious user to extract information or gain access into an organization's internal network.

There is no science or appliance that can fully protect against social engineering attacks.

Social engineering attacks greatly increases the need for strong internal network security controls.
# Notable Social Engineering Attacks

## Real Life Attacks

### Phishing Against Government Entities

With tax season in full swing in the US and UK, there is a 400% spike in phishing emails targeting taxpayers. Email from IRS and HMRC delivers attachment that steals credentials, including SSN and account numbers.

Another variant scams users into paying taxes through an IRS look-alike site.

### Free SSL Certificate Abuse

Hackers are taking advantage of a certificate authority offering free SSL-certificates in order to mask malicious intentions.

This has resulted in numerous banking malware campaigns allowing malicious users to obtain private data.

### Compromised Supervisory Control And Data Acquisition (SCADA) Systems

700,000 people lost power in Ukraine after phishing attacks shut down servers and prevented them from rebooting.

### Global Financial Institution Hack

After falling victim to cyber theft, a large financial institution sent fake phishing emails to employees to test their awareness.

20% of users clicked on the link.

### Security Company Breach

What started as a phishing email with an attachment capable of installing a backdoor ultimately led to a compromise of their security tokens.

### Major Bank Heist

In Belgium, an unknown man walked out with 120,000 carats of diamonds worth about €21 million Euros (or $28 million in 2007), using only his charm and no technology.

### 4-1-9 “Nigerian Prince” Scams

Advance Fee Fraud (AFF) aka "4-1-9" fraud, where victims are promised a portion of a large amount of money in return for paying the upfront costs of retrieving it. These scams cost victims $12.7 billion worldwide in 2013 alone.

### Ransomware

A hacker group was able to place malware onto multiple Los Angeles based hospitals resulting in multiple cases of network downtime. The attackers demanded a large sum of money in exchange of regaining control over the network.
The Curse of Social Media
How the Information Can Be Used

Social media and our tendency to overshare, provides a wealth of information about individuals and their contacts completely free of charge.

Your publically available profiles such as Amazon wish lists, eBay bidding history, Facebook, Instagram are examples of ways attackers can:

• Define cyber attack targets by where they work or what groups they are apart of.
• Learn routines, patterns of behavior, interests, contacts, location and their weaknesses.
• Find answers to security questions used to authenticate or reset passwords.
• Formulate precisely targeted attacks.
Why Should You Care?
Global Stats
The alarming figures

Phishing
- Over 110 trillion emails are sent annually.
- On average, 205 billion emails are sent daily.
- 90% spam & marketing.
- 23% of phishing attacks are successful due to recipients opening the messages. 11% clicked on attachments.

Smishing
- Over 5 Million customers targeted for attacks.
- 60% click a link.
- 26% call back.
- 14% reply to texts.

Impersonation
- Medical identity theft has nearly doubled in 5 years, from 1.4 million adult victims to over 2.3 million in 2014.
- 88% of reported stolen assets were personal data.

Fact!
Average time to get the first victim – 82 seconds!!
Why Should You Care?  
Vectors Used in Successful Security System Breaches

Note:
- Hackers will target the weakest link of a security system – most often the employees of an organization.
- As a whole, individuals tend to share too much information on social media. This is becoming a larger issue as the number of social media platforms increase.

Source: Verizon’s “2012 Data Breach Investigation Report”
Why Should You Care?
Employees Targeted By Hackers

Note: Business impact of social engineering attacks to organizations:
- Legal
- Financial
- Operational
- Reputational

Source: Verizon’s “2012 Data Breach Investigation Report”
Risks & Impact

Social Engineering

- Financial Loss
- Reputational Impact
- Compliance Risk
- Cyber Espionage and Loss of Intellectual Property
- Legal Repercussions
How They Do It
**Attacker Methodologies & Approach**

**The Art of Intrusion**

- **Identify**
  - Identify a target (or targets) to determine a path of least resistance or least complicated way to gain a foothold into an organization's network.

- **Preparation**
  - Prepare the strategy and materials needed to exploit the gaps identified in organizations' social engineering awareness.

- **Execute**
  - Launch social engineering exploit and gain access into the organization.

*Remember!*
The largest vulnerability lies within human curiosity and lapse of judgement.
Demo

<table>
<thead>
<tr>
<th>Internal Network</th>
<th>DMZ</th>
<th>External Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Shares</td>
<td></td>
<td>Malicious USB Drive</td>
</tr>
<tr>
<td>Internal Resources</td>
<td></td>
<td>Phishing Email</td>
</tr>
<tr>
<td>Databases</td>
<td></td>
<td>Attacker</td>
</tr>
</tbody>
</table>

Campus Perimeter
Real Life Story: The Impact of a USB Drop Attack
Timeline of a social engineering exercise

1) 6:30 P.M. MT
   • USBs loaded with the malicious spreadsheet

2) 9:15 A.M.
   • USBs dropped at Loc 1

3) 10:40 A.M.
   • Two sessions opened at Loc 1 from a single USB drive
   • CFO opened file

4) 1:20 P.M.
   • USBs dropped at Loc 2

5) 2:05 P.M.
   • Two additional sessions opened (1 Loc 1, 1 Loc 2)

6) 3:14 P.M.
   • Two additional sessions opened (1 Loc 1, 1 Loc 2)

7) 7:29 A.M.
   • One additional session opened (Loc 1)
Ways To Protect
Protecting Your Organization
Risk Mitigation Strategies

Social Engineering Defense Strategy

1. Conduct Social Engineering Campaign
2. Perform Gap Analysis
3. Design Remediation Strategy

Objectives

User Awareness
Secure Policies, Procedures & Plans
Stronger Internal Network Controls
Social Engineering Campaign
Conduct multiple social engineering exercises using varied techniques on diverse audiences to assess how members in your organization would react to true-to-life social engineering attacks. Weigh their role and privileges into your planning and analysis.

Gap Analysis
With the data gathered from the social engineering campaign, assess where your organization currently is and where it should be based on industry leading practices, emerging threats, and your organization’s history.

Remediation Strategy
Develop a detailed remediation plan that will address strategic weaknesses found in the gap analysis. The plan should focus on the education of staff based on roles, identification and detection of potential attacks, and the appropriate response.
Where do you begin?

**Organizational**
- Identify the organization’s most **valuable assets** and ensure the proper controls are in place to protect them.
- Conduct periodic social engineering assessments to **test the effectiveness** of your security training and awareness program.
- Ensure software and systems are **patched regularly** and up-to-date.
- **Educate employees** on common social engineering techniques.

**Individuals**
- Use **good sense and caution** when using and sharing information with people you don’t know.
- Review your current social networking **privacy settings** to limit disclosure of personal info.
- Do not click on **suspicious links** from people you don’t know (or those you do!)
- **Change passwords** periodically.
- Enable password, PIN or fingerprint lock on mobile devices and lock your device whenever it is left unattended.

**Risk Mitigation**
Key Takeaways

---

**Step 1**
Survey the cybersecurity threat landscape and identify potential threats that have a possibility of affecting the integrity of your organization’s technical infrastructure.

**Step 2**
Conduct a risk based threat assessment that will prioritize threats based on level of impact and likelihood of the threat compromising your organization’s technical infrastructure.

**Step 3**
Based on the assessment develop or modify existing controls framework to address priority threats. Examples include: Incident Response Plan, TTX, etc.

---

*Remember!*
Information security responsibility and accountability starts with the individual.
Cyber Risk Management
Cyber Risks

1. Global Instability
   Cyber as a Top Strategic Priority

   - Cyber-attacks have become a key trend affecting global businesses and economies, and are expected to accelerate over the coming years.
   - Given the potential for significant business and economic impact, organizations should treat cyber as a strategic business risk issue and strive to become cyber resilient.
   - Cyber has become a fundamental part of managing enterprise value. Furthermore, poor cyber risk management will likely cost a number of senior management teams their roles.
   - Expect significant cyber regulatory requirements and heightened scrutiny.

2. Rise of State-Directed Activities
   New Threats and Actors

   - There will be a continuous rise in the number of state sponsored actors with extensive resources, time and budget at their disposal.
   - Governments will continue to militarize their cyber capabilities, targeting public and private sector organizations across the globe.
   - There will also be a sustained threat from criminal organizations, hacktivists and terrorist groups targeting financial services institutions.
   - Lastly, the likelihood of a successful cyber-attack involving critical infrastructure is increasing and the potential impact could be staggering.
Cyber Risks

3. Heightened Connectivity

- Financial services organizations continue to look for innovative ways to digitize their business processes, products, channels and services. Increasing reliance on Cloud technology and other third party services will dramatically change the risk environment and how exposures are managed.
- Technology advances have lowered the barriers of entry for cyber threats that are outstripping the industry’s ability to keep pace.
- Other technologies, such as those that combine big data analytics with Cloud solutions will improve detection capabilities, allowing for near real time routing of threats to segregated environments.

4. Shortage of Resources

- Demands for top cyber talent are growing significantly and the market place will become more competitive over time.
- Need to anticipate a steady increase in the cyber workforce as well as the expenditure required to attract, develop and retain key resources. This will likely cause significant strain on an organization’s expenses.
- Every organization will need a Chief Digital Risk Officer or “Cyber Czar” who possesses business knowledge, risk management experience, technology and security expertise. These individuals will be very difficult to find.
- Expect the role of the CISO to be on par with that of the CRO and CIO, but with enhanced skills and capabilities.
Top Priorities for Cyber

1. Proactively manage cyber risk and regulation: Organizations should treat cyber risk as a strategic business issue and focus on becoming cyber resilient. They should develop specific cyber risk appetite - both corporate-wide and by lines of business. They should also incorporate baseline regulatory requirements into the current environment and include cyber as a key priority in the organization's overall regulatory program.

2. Build and execute a cybersecurity strategy: Organizations should understand the evolution of cyber threats and threat actors on an ongoing basis, leveraging cyber threat intelligence from a number of internal and external sources. They should then develop and execute a plan to mitigate exposure to these threats, making adjustments to their risk control posture as the threat landscape changes.
Top Priorities for Cyber

1. Proactively manage cyber risk and regulation
2. Build and execute a cybersecurity strategy
3. Establish a commercially reasonable cyber capability:
   Cyber programs should be tailored to the risk profile of the organization as well as the expectations of clients, shareholders and regulators. Organizations should also understand how they compare to their peers and industry standards, adjusting where necessary based on inherent business risk and impact. Leading organizations will go beyond “commercially reasonable” to differentiate themselves.

4. Develop a world class cyber response:
   Organizations should adopt an enterprise risk management approach, focusing on incident response and crisis management as a key priority. Scenario planning should take place with the executive management team and attack simulations should be conducted on an ongoing basis.

5. Acquire, develop and retain key talent

6. Align cyber team in line with business risks
Top Priorities for Cyber

1. Proactively manage cyber risk and regulation

2. Build and execute a cybersecurity strategy

3. Establish a commercially reasonable cyber capability

4. Develop a world class cyber response

5. Acquire, develop and retain key talent: The organizational model for cyber should be adjusted to focus more on enterprise and business risk management. Organizations should then determine the required skills, capabilities and resource requirements before hiring the necessary talent to fill any gaps.

6. Align cyber team in line with business risks: Establish governance and reporting lines for cyber. Make the executive team accountable for risk decisioning. Segregate broader budgeting and funding from the technology budget. Develop appropriate linkages to both the risk and technology functions.
Questions?

Wendy Frank  
Principal  
(818) 397-3040  
wendy.l.frank@pwc.com

Brian Lee  
Manager  
(213) 663-0337  
blee@pwc.com

David Miles  
PwC, Director  
(602) 327-3049  
david.miles@pwc.com

© 2016 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC US refers to the US member firm, and PwC may refer to either the PwC network of firms or the US member firm. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

PricewaterhouseCoopers has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. PricewaterhouseCoopers gives no express or implied warranties, including but not limited to any warranties of merchantability or fitness for a particular purpose or use and shall not be liable to any entity or person using this document, or have any liability with respect to this document. This report is intended for internal use only by the recipient and should not be provided in writing or otherwise to any other third party without PricewaterhouseCoopers express written consent.