Social Networking and Social Engineering

Emerging Threats Every Auditor Needs to Know About

© InterVeritas Int’l Ltd. 2014 all rights reserved
Power of Association

• Freedom of Association is enshrined in the United Nations Declaration of Human Rights

• Categorizing people by their associations has been a tool used for centuries by oppressive regimes

• Social Media has become the single most powerful tool by which people associate today

• How does this shake out in terms of big data?
People were asked

Pie Chart 2: Did you ever share your sensitive personal information with an organization you do not know or trust?

- Yes: 25%
- No: 12%
- Can't recall: 63%

Source: Ponemon Inst. 2012
Loss of Trust

Pie Chart 5: Did data breach notification cause you to lose trust in the privacy practices of the organization reporting the incident?

- Yes: 70%
- No: 21%
- Unsure: 9%

Source: Ponemon Institute, 2012
We have chosen technology to monitor ourselves both professionally and personally.
We are now in a state of constant exposure

- Hyper connected world
- Lives transformed by computers and people
- Virtual crowds can form within hours
  - So let’s form one  @civilgrits  #IIA
- Drowning in information
Who are we online?

• Anonymous

• Connect with friends only?

• Business Profile?

• A mix of all?
Living in a state of constant distraction

- It is impossible to stay disconnected
- For some it is an addiction – I just CAN’T shut it off.
Social Media is here to stay

• If I post it, you can bet that someone somewhere may be interested in it.

• Many people say “I’m really nobody of interest so who cares?”

• Everyone now has a voice and a level of engagement.
Facebook

Engagement
• We’ve got to have a corporate presence on Facebook!
• What’s in a like?
• Became the new metric….click through ads are a thing of the past.

Responsibilities
• Why are we on Facebook?
• Do we actively engage our followers?
• Who represents our brand?
• Are we effective?
LinkedIn

Engagement
• Corporate Profile
• Increase corporate exposure
• Attract employees
• Retain employees

Responsibilities
• Ensure relationships are managed with stakeholders
• Do employees maintain the reputational risks of the organization
Twitter

Engagement
• Create brand awareness
• Instant connect with market and consumer
• Real time communication
• Service & support
• Press release/news management

Responsibilities
• Must respond to tweets in timely fashion
• Maintain consistent corporate message
• Readiness to deal with negative messaging
SOCIAL ENGINEERING
Greatest Emerging Threat

What is Social Engineering?

Using deception & manipulation to obtain confidential information.
Why Use Social Engineering?

• If the easiest way to penetrate the security of an organization is through its people, Social Engineering becomes the most efficient tool by which to achieve this goal.
Gathering information on Facebook

• Birthday
• Place of Employment
• Friends & Associates
  – Names & photos of co-workers
• Contact information
• Interests
Impact of LinkedIn

• As of January 2013, LinkedIn reports more than 200 million registered users in more than 200 countries and territories.

• How many people post their entire detailed resume online?

• How important is it for people to be truthful in their resumes or profiles? Historically people have embellished things just a bit?
LinkedIn is one of the most popular vehicles used by hackers to attempt to send phishing emails to users.
Top Threats from Linked In

• Employees disclose too much information

• Linked In vehicle whereby most sophisticated phishing emails are sent
Twitter

- The service rapidly gained worldwide popularity, with over 500 million registered users as of 2012, generating over 340 million tweets daily and handling over 1.6 billion search queries per day.

- Unregistered users can read tweets, while registered users can post tweets through the website interface, SMS, or a range of apps for mobile devices.
Top threats from Twitter

• Lack of response to customer complaints

• Tweets can go viral & are hard to undo once picked up

#hasjustinelandedyet

InterActiveCorp PR director fired over insensitive tweet
Going to Africa. Hope I don't get AIDS. Just kidding. I'm white!

12/20/13, 9:19 AM

4,175 RETWEETS  2,118 FAVORITES
Disclaimers

• How many of you have this type of disclaimer on your twitter profile?

• “Tweets here are my own and are in no way attached to my employer”

• If your online activity is deemed harmful to your company’s brand or reputation, they have the right to terminate employment
Top Data Breaches

Adobe

- Nearly 3 million records, more than 150 million username/password combos, and source code from Adobe Acrobat, ColdFusion, ColdFusion Builder and other unspecified products were stolen.

September, 2013
More unravelling

• Originally just though a compromise of 3 million PII records, it's now clear that Adobe is contending with the loss of a vast trove of login credentials, and, more startingly, its source code

www.haveibeenpwned.com
Top Breaches

Target

• Payment systems were hacked, compromising 40 million customers’ payment information

• Sources say it was due in part to a clicked phishing link that caused the system breach.
Add Social Media

Social Media =

- Dec 18-19, more than 587,000 tweets relevant to breach were sent, a rate of about 12,000 tweets per hour.

- During that time, Target’s Twitter handle was mentioned more than 48,000 times.

- Hashtag #target had more than 31,000 mentions December 18-19 and #databreach had more than 5,200 mentions.
Heartbleed

- **Heartbleed** is a security vulnerability in OpenSSL software that lets a hacker access the memory of data servers.

- **500,000** Web sites could be affected. That means a user’s sensitive personal data -- including usernames, passwords, and credit card information -- is potentially at risk of being intercepted.

- **How does the bug work?** The vulnerability lets a hacker access up to 64 kilobytes of server memory, but perform the attack over and over again to get lots of information. That means an attacker could get not just usernames and passwords, but also "cookie" data that Web servers and browsers use to track individuals and ease log-in.
Some sites affected by Heartbleed

- Facebook
- Instagram
- Pinterest
- Tumblr
- Twitter
- Google
- Yahoo
- YouTube
- Dropbox
- Gmail
- Amazon Web Services
- Go Daddy
- Etsy
- Flikr
- Minecraft
- Netflix
- Soundcloud
- Box
- Wikipedia
OPPORTUNITIES FOR INTERNAL AUDIT

- Training
- Policy
- Implementation
- Regulatory
- Metrics
- Risk
- AUDIT
Integrating levels of engagement

Policy development audit review
  – Social Media Policy
  – Code of Conduct
  – IT Policy

Integration of policies for greater understanding of risk and compliance

Does your social media policy advise staff on how much information they should post on LinkedIn for example?
Education is the key

- Social Media Policies can’t replace good judgement and oversight.
- Some companies don’t have them
- Some have been deemed overbroad
- Some merely serve as guidelines
- Better to understand the implications of certain behaviors
Policy development & review

• Clear instructions that provide guidelines for employee behavior for safeguarding information.

• Must be a fundamental building block in developing controls to counter potential reputation, data leakage & security threats.
What stage is your social media policy at?

• Does it only outline what the parameters of organizational usage are?
• Does it define what is and isn’t acceptable usage of social media by staff?
• Does it clearly outline what can be posted and what cannot?
  – Some corporations do not allow staff to post where they work on their personal social networking sites.
• What are the consequences of non-compliance?
Role of internal audit

- Social Media Policy
  internal & external
- Social Media Strategy
- Social Media Governance
- Metrics
- Monitoring
- Plan Execution
- Regulatory & Compliance
- Training
Why Should We Care?

• If we don’t know the types of tactics being used to gain access to our information, then we can’t protect our assets.

• Is data leakage important to the auditor?

• Is is part of your portfolio to monitor controls?

• Do we think that computer breaches are for the security or IT department only?
Social Media Threat Landscape

Technology
- Unauthorized Disclosure
- Intellectual Property Leakage

Data
- Vulnerabilities
- Trojans, Viruses, Worms

People
- Identity Theft
- Social Engineering
- HR Violations
- Loss of Productivity

Organization
- Reputation Loss
- Privacy Risk
- Trademark Infringement
- Loss of Content Control

Public
- Unsatisfied Customers
- Negative Publicity
- False Impressions

Risk Categories:
- Organization Reputation
- Loss of Content Control
- Loss of Productivity
- Privacy Risk
- Trademark Infringement
- HR Violations
- Social Engineering
- Identity Theft
- Unauthorized Disclosure
- Intellectual Property Leakage
- Trojans, Viruses, Worms
- Unsatisfied Customers
- Negative Publicity
- False Impressions