WELCOME

Cybersecurity and Social Media: Protect Your Organization and Reap the Benefits

Presented by:
Eric M. Wright, Shareholder, Technology Advisory Services
Daniel J. Desko, Senior Manager, IT Audit and Risk Advisory Services

Cyber Security for Non-Profit Organizations

Eric M. Wright, Shareholder
Technology Advisory Services

Agenda
• What has been happening?
• Non-profit breaches
• Some fun facts
• The crooks are getting smarter
• The hidden ramifications of a breach
• How can I protect myself?
• What should I do next?
What has been happening?

I am a non-profit, why should I worry?

Data Breaches and Non-Profits

- In 2005, 92 breaches affecting 3 million records
- In 2014, 138 breaches affecting 7.7 million records
- Since 2005, Not for profit organizations have been the target of 2,753 breaches, affecting 201 million records
What are they after?

- Donor details
- Credit cards data
- Personally identifiable information
- Financial information
- Health information

The world we live in

Fun Facts

- 1 in 10 US citizens are subject to identity theft
- If you make more than 70K, you are 2x more likely to be targeted
- In 2013, 13.1 million consumers were victims of identity theft
- 52% of all fraud involved on-line transactions
- Average time incurred to re-establish your identity - 330 hours
More Fun Facts

• 2011 - 20% of the people who received notice of a possible breach became victims
• 2012 - 25% of the people who received notice of a possible breach became victims
• 2013 - 33% of the people who received notice of a possible breach became victims

Verizon Data Breach Report - Takeaways

• 92% of breaches came from outside the organization
  – 55% from organized crime
  – 19% affiliated with other state agencies
• 75% of breaches driven by financial motives
• 76% exploited weak or stolen credentials
• 69% discovered by external parties
• 66% took months or more to discover

Verizon Data Breach Report – Other Takeaways

• 19% of attacks combined multiple techniques (phishing, malware, hacking, etc.)
• 75% of attacks were opportunistic (companies not targeted directly)
• 78% of intrusions took little or no specialist skills/resources
• US accounted for 66.5% of all compromised records in 2013
Verizon Data Breach Report – Malware Sources

Attackers Time to Exploit Vulnerability versus Organization’s Ability to Defend
2009 Breaches by Type

2013 Breaches by Type

Financial Cost of a Data Breach

- Legal Fees
- Credit Monitoring
- Forensic Consultants
- Public Relations/Crisis Management
- Fines
Reputational Damage

- Front page news
- Notifying donors, employees, consumers, government agencies
- Public outcry
- Loss of donor trust and support
- Reluctance of volunteers to serve

So what do we have to look forward to?

This is one solution to cyber security

"I keep our secure files in a coffee can buried behind the office. You can’t hack into that with a computer!"
Layered Approach to Defense

Defense in Depth Layers

- Date
- Application
- Host
- Internal Network
- Perimeter
- Physical
- Policies, Proceded, Awareness

Policies and Procedures

- Serve multiple purposes
  - Serves as your commitment to your constituents on how you intend to protect the information they share with you
  - They convey your expectations to your employees. Limits arbitrary and capricious action, and counters the “I did not know” defense to such claims.
- Update your risk assessment as your environment changes

Physical Security

- Controls should include
  - Servers should only be assessable by IT personnel
  - Contractors should be escorted while working on site
Perimeter

- Firewalls are installed that are currently patched and ports are appropriately configured
- Vulnerability scans and Penetration testing is conducted at least annually
- Firewall rules are examined and evaluated for conflicts annually
- Installation and monitoring of intrusion detection systems

Perimeter (continued)

- Replace old firewalls with advanced solutions that include advance malware detection, website filtering and Identity awareness tools
- Implementing web filtering to restrict access to vulnerable sites

Internal Network/Hosts

- Implement a centralized anti-virus and malware solution that updates servers and workstations automatically
- Implement a strong password policy for all users
- Limit access to highly privileged accounts to appropriate personnel
- Implement a multi-layered email spam solution
**Internal Network/Hosts (continued)**

- Remove or disable terminated users accounts upon separation
- Proactively patch servers, browsers and workstations
- Conduct internal vulnerability scan annually
- Segment your network as needed. Flat networks significantly increase data breach risk

**Internal Network/Hosts (continued)**

- Educate users on the importance of complying with security policy with a heavy emphasis on social engineering

**Internal Network/Hosts (continued)**

- Consider implementing new virus and malware tools. Older tools are signature based - Investigate profile based solutions
- Remote users should connect to the network using some form of 2 factor authentication
- Provide access to users on a least privileged basis
Applications

• Grant users access on a least privileged basis
• Implement a strong password policy
• Perform code scans before changes are loaded into production for custom developed web applications
• Remove or disable terminated users accounts upon separation

Data

• Encrypt sensitive data, if possible
• Encrypt mobile devices that are used to store data (Jump drives, backup tapes, laptops)
• Data being transferred should be encrypted or use a secure method of transmission
• Wipe the storage devices of retired equipment

What Actions should I be taking?

• Accept that this is an enterprise-wide risk, not just an IT issue.
  – Stakeholders include, but are not limited to, the Boardroom, HR, Audit, IT and Legal
• Establish awareness that controls and processes have been specifically designed to prevent attacks
  – New hire orientation
  – Ongoing awareness and communication
  – Visible to the organization
Address the Weakest Link

What Actions should I be taking?

• Integrate cyber risk strategy into the organization’s strategic plan
• Have a team dedicated to managing cyber threats and your incident response plan
• Identify your organization’s most critical data assets
  – Where do these assets reside?
  – Who has access to these assets?

What Actions should I be taking?

• Implement a layered defense
• Identify vendors used for business functions involving critical data assets.
  – Make sure you understand their security policies and procedures
Managing Social Media Risk

Daniel J. Desko, Senior Manager
IT Audit and Risk Advisory Services

Learning Objectives

A. Understand the purpose of social media use in organizations
B. Impact and risks associated with having a corporate social media presence
C. Controls and best practices to mitigate social media risk

Agenda

• Survey results
• What is social media
• Benefits of social media
• Threats/Risks/Controls
• Social media disasters
On which social networking website(s) does your company maintain a corporate presence?

- Facebook
- Twitter
- LinkedIn
- Own Platform
- YouTube
- None

Does your organization block any social media websites from employee usage while they are on company time?

- Yes 47%
- No 53%
Top Reasons For Blocking

1. Productivity issues, time waster, etc.
   – Overwhelmingly the #1 reason for those who block
2. Information security (distant 2nd place)
3. Bandwidth (distant 3rd place)

Why Don’t You Block?

• “We are not dictators.”
• “Social media is representing a critical means to reach-out, interact with our customers and nurture our relationship with them. Which is at the very core of how we have been doing business for more than 100 years.”
• “Lack of management perception of risk.”
• “Because we use it as part of marketing.”

Does your organization use social networking and blogs for any of the following purposes?

[Chart showing usage of social networking and blogs for various purposes]
Does your organization allow its employees to identify the organization by name on their profiles on social network platforms or blogs?

- No
- Yes, Must Follow Policy/Guidelines
- Yes, No Policy/Guidelines

Which employees openly represent your organization on social media sites?

- Chief Marketing Officer
- Corporate Communications
- Social Media Coordinators
- Director of Investor Relations
- CFO

Is social media a part of your organization’s governance structure or processes?

- No
- No, but we plan to
- Yes
Social media is ______________?

Thoughts on video

- Social media must be embraced, however, it should be done so carefully and strategically.
- What was the most shocking point made in that video to you?
- After watching that video it seems as if social media is the way the world is communicating and there is no stopping it.
- Social media is an advanced and real time means of communication.

Top 5 Benefits of Social Media

- Communications platform
- Donor growth
- Brand recognition
- Referral source
- Recruiting conduit
Communications Platform

- Direct donor engagement
  - New campaigns
  - Convey messages instantly and low cost
- Donor surveys
  - Receive feedback real-time

Communications Platform Continued

WATERisLIFE - #FirstWorldProblems hashtag overtaking

Donor Growth

- Direct donor engagement tool
- Demographic information
- Capture email addresses and other info
- Potentially expansive reach
Donor Growth Continued

- Online ad spending officially surpassed print ad spending as of 2012.

Brand recognition

- Generate “buzz” around the office water cooler
- Get people sharing your video, pictures, content on their personal pages
- Using social media as a branding tool successfully takes creativity
Brand Recognition Continued

Social media outlets are valuable sources of business referrals – LinkedIn – YouTube – Blogs – Forums – Etc...

All of these outlets point back to your business

Referral Source Continued
Recruiting Conduit

- Social media outlets are great tools for recruitment
  - Potential employees learn about your organization
  - Sites such as LinkedIn allow you to search for potential employees
  - Save on recruiting costs and get to know potentials hires better

Risks of A Corporate Social Media Presence

...let's understand them.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Risks</th>
<th>Risk Mitigation / Control Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exposure to customers and the enterprise</td>
<td>Customer backlash/adverse legal actions</td>
<td>- Develop brand protection guidelines and assign staff or hire a firm</td>
</tr>
<tr>
<td>through a fraudulent or hijacked corporate</td>
<td>Exposure of customer information</td>
<td>that can scan the Internet and search out misuse of the enterprise</td>
</tr>
<tr>
<td>presence.</td>
<td>Reputational damage</td>
<td>brand</td>
</tr>
<tr>
<td></td>
<td>Targeted phishing attacks on customers or</td>
<td>Give periodic informational updates to customers to maintain awareness</td>
</tr>
<tr>
<td></td>
<td>employees</td>
<td>of potential fraud</td>
</tr>
</tbody>
</table>

4/22/2015
## Risks of A Corporate Social Media Presence

<table>
<thead>
<tr>
<th>Threat</th>
<th>Risks</th>
<th>Risk Mitigation / Control Strategy</th>
</tr>
</thead>
</table>
| Mismanagement of electronic communications and/or inappropriate content posted on official corporate social media outlets. | • Reputational risk (self inflicted)  
• Customer backlash  
• Brand tarnishing | • Strictly control who can post content  
• Strictly control how users access corporate social media outlets  
• Policy for approval of any content posts  
• Social media crisis response plan  
• Consider what can go wrong before posting  
• Do not link corporate pages to personal accounts |

<table>
<thead>
<tr>
<th>Threat</th>
<th>Risks</th>
<th>Risk Mitigation / Control Strategy</th>
</tr>
</thead>
</table>
| Unclear or undefined content rights to information posted to social media sites. | • Enterprise’s loss of control/legal rights of information posted to the social media sites  
• Media (images, videos, content, etc.) that are a product of the organization can be easily copied, re-used without consent | • Ensure that legal and communications teams carefully review user agreements for social media sites that are being considered  
• Policies that dictate to employees what info should be posted as part of the enterprise social media presence  
• Log all communications requests and validate approval |

<table>
<thead>
<tr>
<th>Threat</th>
<th>Risks</th>
<th>Risk Mitigation / Control Strategy</th>
</tr>
</thead>
</table>
| The move to a digital business model may increase customer service expectations. | • Customer dissatisfaction with the responsiveness received on social media sites, leading to potential reputational damage for the enterprise  
• Customer retention issues | • Ensure that staffing is adequate to handle the amount of traffic that could be created from a social media presence  
• Create notices that provide clear windows for customer response  
• Content to establish expectations |
Risks of A Corporate Social Media Presence

<table>
<thead>
<tr>
<th>Threat</th>
<th>Risks</th>
<th>Risk Mitigation / Control Strategy</th>
</tr>
</thead>
</table>
| Introduction of viruses and malware to the organizational network through the allowed use of social media sites. | • Data leakage/theft  
• “Owned” systems (zombies)  
• System downtime  
• Additional unplanned resources required to clean systems | • Anti-virus/malware installed on systems & updated daily  
• Content filtering technology to restrict or limit access to social media sites to appropriate users only  
• Establish or update policies and standards  
• Inform employees of the risks involved with using social media sites |

Excessive employee use of social media in the workplace. | • Network utilization issues  
• Productivity loss  
• Increased risk of exposure to viruses and malware due to longer duration of sessions | • Manage accessibility to social media sites through content filtering or by limiting network throughput to social media sites |

Use of personal accounts to communicate work-related information. | • Privacy violations  
• Reputational damage  
• Loss of competitive advantage  
• Trade secret exposure  
• Transmission of sensitive data | • Work with the HR department to establish new policies or ensure that existing policies address employee posting of work-related information  
• Work with the HR department to develop awareness training and campaigns that reinforce these policies |
**Risks of A Corporate Social Media Presence**

<table>
<thead>
<tr>
<th>Threat</th>
<th>Risks</th>
<th>Risk Mitigation / Control Strategy</th>
</tr>
</thead>
</table>
| Employee posting of pictures or information that link them to the enterprise. | • Brand damage  
• Reputational damage  
• Trade secret exposure  
• Customer loss | • Work with the HR department to develop a policy that specifies how employees may use enterprise-related images, assets, and intellectual property (IP) in their personal online presence  
• Self-policing or monitor each other as best you can |

**Common Themes Among Mitigation Strategy**

- Policies and procedures
  - Making sure employees read and understand them
  - Training on the policy and procedures
- Assess risk on a continual basis
- Limit, control and monitor access to the corporate social media presence
- Monitor the corporate page and for fake pages

**Control Implementation Strategy: Assess Risk**

- Determine which risks are most applicable to your organization
  - Determine impact of the risks
  - Determine likelihood of occurrence
  - Even attempt to assign a rough estimate dollar value to the potential loss associated with each risk
- Revisit the assessment at least on an annual basis
Control Implementation Strategy:
Control Implementation strategy:
Policies, Procedures & Training

- Involve the key stakeholders
  - Communications
  - Sales & Marketing
  - Technology
- Define what social media will be officially used for and in what capacity
- Develop a right sized training approach based on risk
  - Face to face, webinar, online document, etc.
- Ensure your organization possess the right capabilities and fill in the missing links

Control Implementation strategy:
Control & Monitor

- Restrict user access to official pages
- Determine chain of approval for various levels of content (text, media, sales messages, etc.)
- Set frequency of monitoring activities
- Determine which tools to use:
  - Google alerts (free tool)
  - Google trends (free tool)
  - Socialmention.com (free tool)
  - Tweetscan.com (free tool)
  - Lithium (paid service)
  - Radian6 (paid service)
  - Market Sentinel (paid service)
Risks Of Too Many Controls

- Stifle business/marketing efforts
- Legal risks
  - If policies are too stringent they may be unlawful under the National Labor Relations Act
- Disenchanted employees if the company blocks social media sites
  - In reference to the Millennial generation, a recent Cisco report noted, “The ability to use social media, mobile devices, and the Internet more freely in the workplace is strong enough to influence job choice, sometimes more than salary.”
- While many social media sites are free the cost of FTEs to monitor and control the corporate social media presence can be staggering

Social Media Disasters

- McDonald’s tried to promote the quality of their ingredients and have fans share positive experiences via a Twitter campaign
- Instead, the tag became a way for animal activists and less-than-satisfied diners to air their grievances
- The #McFail hash tag was born

Social Media Disasters

- A drunk Red Cross employee accidentally tweeted from the official account on his phone
  - Ryan found two more 4 bottle packs of Dogfish Head’s Midas Touch beer.... when we drink we do it right #getngalizzare
  - He thought it was his personal account
Social Media Disasters

- A hacking group gained access to Fox's Twitter accounts and started tweeting that President Obama had been assassinated and that ground zero had been attacked.
- They promptly removed the false reports and worked with Twitter to prevent future compromise.

Social Media Disasters

- After watching the first presidential debate, a KitchenAid employee mistakenly sent a tweet through the KitchenAid corporate account rather than her personal account.
- The message was quickly deleted and replaced by a more "brand appropriate" message, which apologized for the Obama remark.
- Outrage was almost immediate, with angry Twitter users threatening to boycott the company.

Social Media Disasters

The risk of linking personal and corporate accounts is one of the most easily avoidable risks, however the impact of this risk continues to be the most harmful and negatively impactful.
Thank you for coming!

Upcoming Events:

EACUBO Local Pittsburgh Workshop: June 1, 2015
Schneider Downs Bi-annual Not-for-Profit Symposium: July 30, 2015