BYOD: Managing the Risk of Personal Devices at Work

Wednesday Webinar – July 10, 2013

Erin Gloeckner & Alex Ricketts, Project Managers
Nonprofit Risk Management Center
www.nonprofitrisk.org
Erin@nonprofitrisk.org & Alex@nonprofitrisk.org
202-785-3891

Managing the Risk of Personal Devices at Work

Why BYOD?

Easy to manage
Appeals to employees
May cut costs

Who Brings their Own?

Broward Center for Performing Arts
Pioneer Resources
Compassion Australia

Device Management Options

Employee owned devices

- Devices with Work & Home features

Nonprofit-owned / No BYOD Policy
Depends on the employee

What's the Biggest BYOD Risk?

Employers have less control of devices and data
Employees can control the nonprofit's assets

Top 5 BYOD Risks

1. Security
2. Employee Rights & Privacy
3. HR & Employment Laws
4. IT Department Control
5. Cost

Risk #1: Security

Lost phones and tablets:

- Ex. Losing a tablet with entire donor database

No use of Passcodes for devices:

- 90% of U.S. employees use personal devices, 39% of the devices were not passcode protected

No encryption for work emails
Access to unsecured Wi-Fi hotspots
Uploading data to non-owned servers
International travel:

- Data protection
- Border searches
- Espionage

Sharing trade secrets:

- "About half of employees admit to keeping confidential data and 40% plan to use that data at their new job." - Ponemon Institute, 2013

eDiscovery challenges:

- Misappropriation may be harder to prove

- Access to the devices will be a challenge

Employees do not disclose data breaches:

- 11% of U.S. employees would not tell employers that their device was compromised even if confidential info was leaked – Aruba Networks, 2013

What are We Required to Do?

Encryption

Breach notification

Secure data retention & destruction

Contractual obligations

Legal Implications

Violation of regulatory requirements to secure personal information: HIPAA, & GLBA

Security breach notification laws in almost every state

- Encryption safe harbor

Average cost of a breach is $3.94/lost record or $3.7M (average of over 1M records lost)

- Added reputational cost!

Data Security Statistics

Loss or theft of devices

- Lost and stolen equipment accounts for 31% of breaches
- Lookout helped 9 million people locate their devices; one locate request every 3.5 seconds

Data breaches

- In 2012, 5% of breaches were committed by internal employees which decreased from 18% in 2011 – Verizon Risk Team
- 96% of breach victims had not achieved compliance regulations

Friends and family

- 27.5% of FINCEN suspicious activity reports involving identity theft involved friends, family, employee in home

Legal Language

- Almost 50% of breach notification laws provide no clear definition of 'encryption' – RSA Conference 2012

***Risk #2:* Employee Rights & Privacy**

BYOD Pros:

- Employees know how to use devices
- Don't have to juggle a cell, a pager, a Blackberry…
- Productivity + happiness rise

BYOD Cons:

- Security strategies infringe upon employee rights & privacy
- Nonprofit has legal & contractual obligations to retain and/or destroy work data on employee devices

Employee Privacy Issues

Remote wipe:

- Employees have a reasonable expectation of privacy

- Computer Fraud & Abuse Act if unauthorized access causes damages > $5,000

SCA: Stored Communications Act

- *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp*

***Risk #3:* HR & Employment Laws**

Performance management

- Work or Facebook?

Discrimination, hostile work environment

- Different BYOD rights or surveillance of one employee over another

Labor Laws

- Unlawful surveillance

GINA: Genetic Information Nondiscrimination Act

Inappropriate employment decisions based on access to personal devices

Workplace Safety

- Driving and talking or texting
- The injured person is more likely to sue the employer rather than the employee-driver

Wage & Hour

- Off-the-clock work by non-exempt employees
  - Emails themselves are evidence of time spent and notice to employer
- Work by non-exempt *or exempt* employees during weeks off or leaves of absence
- Time spent dealing with IT issues related to devices

***Risk #4:* IT Department Control**

Operational:

- IT has responsibility… also has reduced ability to fulfill it
- IT has to deal with various devices

Cultural:

- Internal disputes, possible silos from IT access to coworkers' devices

***Risk #5:* Cost**

Pros: Employees may cover some costs

Cons: Study by Xigo found that 67% saw no difference and only 9% saw savings

Smart Savings or Money Pit? Musings from Cecil Lynn – eDiscovery Counsel @ Littler Law Firm

Organizations spend 33% more on BYOD because they:

- Lose bulk purchasing power
- Provide more tech support
- Can't budget security risks… often cost more than imagined

To BYOD or Not to BYOD?

How much risk can YOU take?

- Option1: Don't allow any devices on internal network that the IT department doesn't control
- Option 2: For specific employees, allow access from personal devices
- Option 3: Well-managed BYOD program for all employees

Biggest BYOD Mistake NPs Make:
Switching to BYOD without updating technical controls, policies, and employee training.

Setting Up Your BYOD Program

1. Technical Controls
2. Policies
3. Education & Training

1. Technical Controls

Restrict access for departing employees
Establish a protocol for wiping devices
Partner with mobile service provider for a security agreement – policing work info on personal devices
Link personal devices to the nonprofit's network while controlling malware/viruses

A Data Breach can Still Happen
Cyber liability insurance
IT Department must be ready to respond to a breach

2. BYOD Policies

In Employee Handbook:

- Acceptable use policy
- Disciplinary code
- BYOD Agreement: Waive rights so IT department can access

Acceptable Use Policy
List both acceptable and unacceptable uses
Unacceptable:

- Transferring organizational funds on a device owned by the employee
- Permitting or obtaining access to systems or networks unless authorized
- Disclosing private facts about an employee or client
- Using device or data on the device for personal financial gain, in a manner creating a potential conflict of interest for the employee or for the organization
- Any use violating law or government violation

Information security rules & implications

- What you must protect & why
- Reporting data and security breaches

IT Department's authority & responsibilities

- Who will purchase/maintain device & software?

Driving & Devices:

- Prohibit use of cell phones while driving
- Address hands-free technology
    - You should issue hands-free equipment if you require employees to use while driving

Employee Privacy Rights:

- No use of identity information in hiring decisions
- Nonprofit claims surveillance rights if employees show signs of inappropriate behavior

Disciplinary Code

- Hold employees accountable to Acceptable Use Policy
- Point scale

BYOD Agreement

Employee authorizes:

- IT department access
- Wipe if phone is lost or the employee departs the organization

Employee agrees to:

- Follow BYOD policies
- Protect the nonprofit's data
- Notify IT department when devices have been breached

3. Education & Training

Data security training

- Which data must be protected?
- Where is data safe or unsafe?
    - When to encrypt emails
    - Cloud apps & server safety
- No transferring funds
- Accessing networks securely – CITRIX codes, etc.
- Reporting security breaches & lost devices

Wage & Hour training

- Non-exempt may not access work email or make work calls outside work hours

Safety while driving

- How to use hands-free devices safely

Resources for managing device: AT&T Toggle

Remember…

- Data breaches and other risks can still occur at a nonprofit that owns every device!
- Human error exists in both environments!
- Plan ahead no matter which path you choose…

Additional Resources:

- **Nonprofit Risk Management Center**
  My Risk Management Policies: www.myriskmanagementpolicies.org
  Insurance for Cyber Risks article:
  http://www.nonprofitrisk.org/library/articles/Insurance_for_Cyber_Risks.shtml
- **White House Digital Government**
  Bring Your Own Device Toolkit:
  http://www.whitehouse.gov/digitalgov/bring-your-own-device
- **Computerworld**
  Nonprofit Cuts Costs with BYOD article:
  http://www.computerworld.com.au/article/451636/non-profit_cuts_costs_byod/

- **NOLO**
  Cell Phone Policies for Employees Who Drive:
  http://www.nolo.com/legal-encyclopedia/cell-phone-policies-employee-drivers-30171.html
- **Weil**
  Privacy Challenges in Drafting "BYOD" Policies:
  http://www.weil.com/news/pubdetail.aspx?pub=11307

Sign Up for Risk eNews!

www.nonprofitrisk.org

When One Door Closes

By Melanie Lockwood Herman

There are only sixteen days left to receive a $175 discount on registration for the 2013 Risk SUMMIT. Don't let the discount door shut on you! Register by May 31st to enjoy the lowest registration rates for this year's conference, August 25-27 in Boston.

I've been thinking a lot lately about the expression, "When one door closes, another door opens..." The statement is attributed to Alexander Graham Bell, whose full thought was: "When one door closes, another opens; but we often look so long and so regretfully upon the closed door that we do not see the one which has opened for us."

Change is the only constant in the risky world in which nonprofit organizations live and serve. In some cases, changes come about when one door closes: a long-time relationship with a partner nonprofit ends, a donor stops giving to pursue new interests, or a valued employee retires or leaves to pursue a new career or higher education.

Crossing Thresholds Safely

After many years as a nonprofit leader and more transitions than I care to count, I've collected a handful of tips that help me close

GREAT AMERICAN
INSURANCE GROUP
Specialty Human Services Division
SpecialtyHumanServices.com
Exclusively for 501(c)(3)s
Click to Learn How
STOP Paying State Unemployment Taxes

Risk Webinars

The 2013 program continues on May 1st with **HR Risk: Take the High Road without Getting Lost**. This webinar offers

Thank You!

Erin Gloeckner & Alex Ricketts, Project Managers
Nonprofit Risk Management Center
www.nonprofitrisk.org
Erin@nonprofitrisk.org & Alex@nonprofitrisk.org
202-785-3891

Nonprofit Risk Management Center