Nonprofit Risk Management 101

Presented by: Nyk McKissic

Holland & Knight

What is Risk?

- Risk is:
    - The possibility of suffering harm or loss;
    - A thing or course of action involving uncertain danger.

But in a business or nonprofit context?

- Risk is:
    - The possible downside of any business decision.

How do we deal with Risk?

In every business decision, we consciously or unconsciously take one of the following paths (or a mixture of them):

AVOID the risk – don't proceed

MITIGATE the risk – implement procedures to reduce the possibility

ACCEPT the risk – take the chance

EXPLOIT the risk – capitalize on the risk

Today's Topics

- Financial Risk
- Cyber Risk
- Volunteer Risk
- Insurance

Financial Risk

Financial Risk

Fraud can only occur when opportunity, pressure, and rationalization are all present.

The Fraud Triangle

Where
Opportunity

Pressure
When

Rationalization
Why

Opportunities for Fraud

- **Opportunities** stem from inadequate or no:
  - segregation of duties
  - supervision and review
  - internal controls

Opportunities for Fraud

- Duties of authorization, custodianship, and recordkeeping not segregated
- Unrestricted/unmonitored access to assets or data
- Transactions not recorded resulting in a lack of accountability

Opportunities for Fraud

- Assets not reconciled with the appropriate records
- Unauthorized transactions or overriding controls
- Unimplemented controls due to lack of personnel or expertise
- Employees or volunteers over whom there is little or no supervision

Pressures

- **Pressures** can be imposed due to:
  - personal financial problems
  - personal vices
  - unrealistic deadlines and performance goals

Pressures

- The current economic environment continues to provide additional pressures on staff and volunteers
  - Job loss
  - Healthcare costs and/or lack of insurance
  - Adult children without jobs
  - Pension and other retirement income losses
  - Personal vices
  - Unrealistic expectations

"Rationalization"

- **Rationa*lies*** occur when the individual develops a justification for their fraudulent activities
- Intent to replace the funds
- Feel the organization owes it to them
- "Everyone else is doing it"

Embezzlement Facts

- Avg. time as employee – 8 years
- 33% in finance or accounting role
- Median loss: $357,650
- 79% involved more than one person
- 24% involved theft of cash
- 38% involved manipulating accounting systems
- 65% of cases, someone noticed something
- 45% filed criminal charges

Source: Hiscox Inc., The 2018 Hiscox Embezzlement Report.

Fraud Prevention

- Both the ability to rationalize and many of the pressures are dependent on the individual; therefore, fraud risk and prevention efforts **focus on removing opportunities.**

- “It can never happen here.”

Fraud Prevention

- Design controls to make it difficult for fraud to be committed and remain undetected
- Security controls for systems and data
- Monitoring controls over bank accounts, financial records and transactions

Fraud Prevention

- Education and training
- Prosecute staff and volunteers found committing fraud; Deterrence
- Conduct internal audits

Poll Question #1

In terms of financial risk, does an organization have control over any of the elements of fraud? If so, which element(s) can be affected?

A. Opportunity

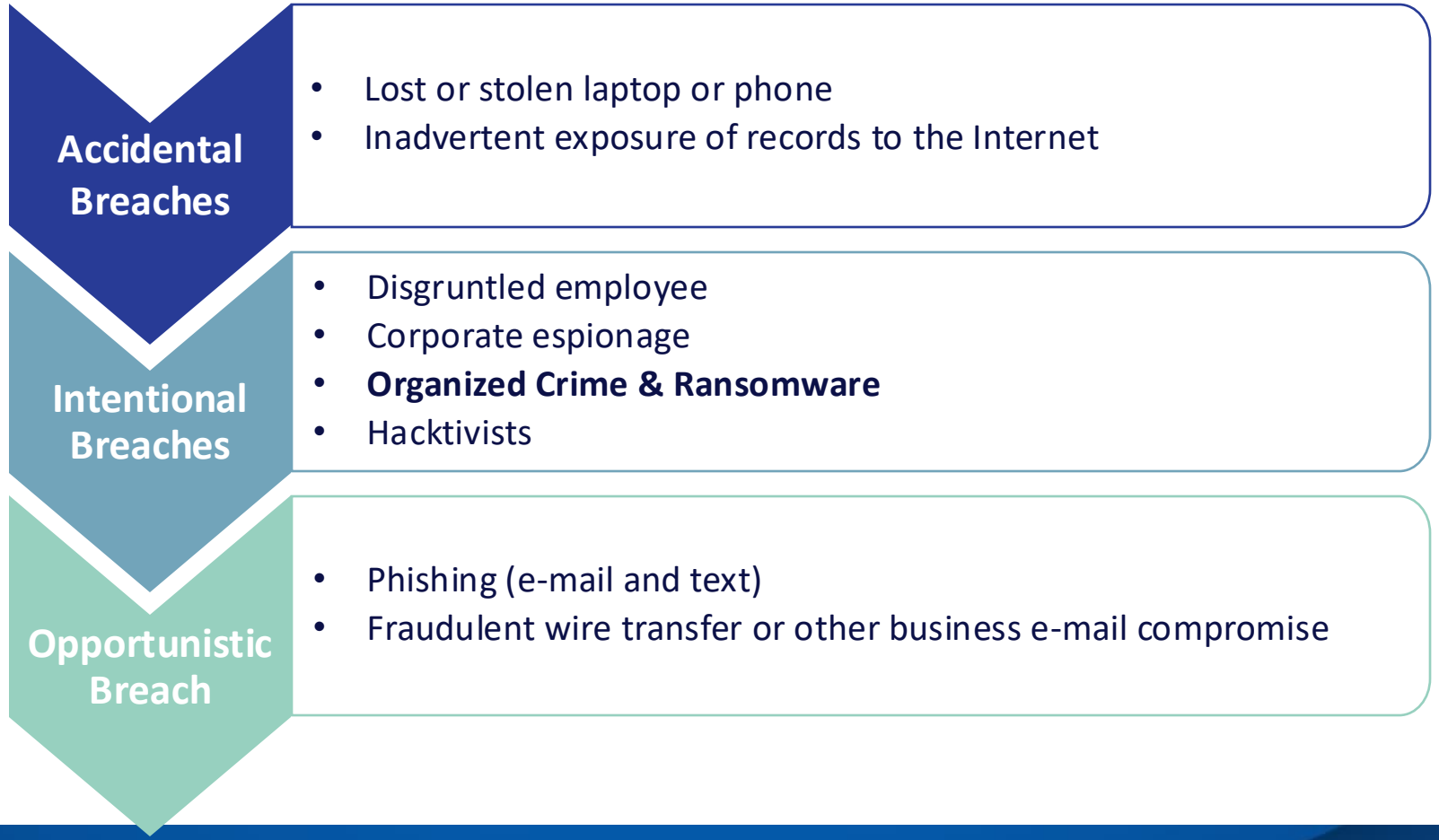
B. Pressure

C. Risk

D. We just have to take it as it comes…

Cyber Risk

Breach Types



Multiple Risks of Data Breach

- Intellectual property and other proprietary data
- Personal information (credit card, SSN, DOB, credit card numbers, medical records, etc.)
- E-mail correspondence and other internal documents
- Business disruption
- Reputational harm and loss of donor confidence

Understand Your Risks

- Audit - What data do you have? Is there data you no longer need? Privacy policy?
  - Prioritize - Which data are most valuable?
  - Where are the data stored?
  - Who has access?
- Assess vulnerabilities and security measures (firewalls, internal segmentation, logs and intrusion reports, etc.)
- Assess people
- Assess physical security
- Review disaster recovery plan

Internal Policies

- Network Access, Encryption, Passwords
- BYOD and Social Media; Ability to wipe devices
- Privacy Policy and Website Terms of Use
- Essential elements of effective security
  - Policies should apply to everyone with access to data (no exceptions for top management)
  - Training and monitoring employees and contractors (one study found that 91% of attacks start with phishing attacks)
  - Regular practice and review of policies and audit of systems

Risk Mitigation Strategies

- Cyber Insurance – Risk Transfer
- Effective contracts – Risk Allocation
- Training and Effective Policies – Risk Mitigation
  - Testing
  - Planning
  - Assessments
  - Drills
- Understand Breach Notification Laws and requirements
- Build relationships in advance

Relationships

- Identify, select and negotiate an **incident response retainer agreement** with a technical provider
- Select a law firm partner
- Establish a relationship with a PR firm
- Get to know law enforcement

Poll Question #2

Church A learns it has been the victim of a cyberattack. In addition, Church A learns that its computer systems have been subject to a data breach. However, six months before the breach, Church A obtained cyber insurance to protect the organization from any financial losses that could occur from a cyber attach.

What risk management tool has Church A implemented?

A. Risk Mitigation

B. Risk Allocation/Shifting

C. Risk Transfer

D. All of the Above

Volunteer and Employee Risk

Volunteers vs. Employees

- Are volunteers different from employees?
- How can volunteers ***and*** employees put the organization at risk?

What harm can volunteers and employees do?

Where do we begin…? (from bad to worse)

- Bad PR
- Accidents; property damage
- Breach confidential information
- Lawsuits
- Risk your tax exempt status
- Violate laws

Volunteers and Employees

- Screening
- Training
- Management/Supervision
- Avoid bad things/bad acts
- Age Appropriate
- Evaluate what translates to a remote volunteer
- Continue to inform about important issues like confidentiality
- Review existing volunteer agreements – are they sufficient?

Insurance

Types of Insurance

- General Liability
- Property
- Auto
- Workers' Compensation
- Umbrella
- Director & Officer
- Crime
- Cyber
- Others

Insurance

- Limits of Liability
  - Individual
  - Aggregate
- Specific Endorsements
  - Volunteers
  - Participants
  - Watercraft
  - Others

Insurance Certificates

- Proof of Insurance – Understand what it all means
  - Types of insurance/limits
  - Certificate holder
- Being Named “Additional Insured”
- Waiver of Subrogation

Poll Question #3

Church B, which is located in East Texas, wants to conduct a boat racing event as a fundraising event. Church B already maintains general liability insurance.

Should Church B obtain any additional insurance for the event? If so, what kind?

A. None – Church B is fine with its general liability coverage

B. Auto

C. Director and Officer

D. “Well, it depends…”

Questions?

Nyk McKissic
Associate
Holland & Knight LLP
Nykolas.mckissic@hklaw.com
214.969.2131
One Arts Plaza
722 Routh Street, Suite 1500
Dallas, Texas 75201
www.hklaw.com