




**Risk Management and
Information Technology**

Board Leadership Calgary
October 21, 2017
Linda Dalgetty, Vice-President (Finance and Services), U of C
Allen Amyotte, Director Internal Audit, U of C



Outline for Session

- 1.** Discuss ERM concepts: IT Risk is Institutional
- 2.** Review components of IT risk
 1. Governance
 2. Backup and Recovery and Business Continuity Planning
 3. Security (GCCs)
 4. Payment Card Industry (PCI) compliance
- 3.** Summarize Approach for small to medium NPO
- 4.** Case Study

10/21/2017 Board Leadership Calgary 2017



1. Enterprise Risk Management Approach

- Think of what the institution is trying to achieve
- Think about what could not be tolerated by the NPO that would highly affect operations (independent of IT)
 - Business continuity?
 - Privacy breach?
 - Website down?
 - Funding hit?
- Think about categories of risk
 - Reputational
 - Financial
 - Compliance
 - Operational
- Think about where IT underpins these areas

10/21/2017

Board Leadership Calgary 2017



1. U of C Enterprise Risk Management

- 10 Institutional Risks defined for the university.
 - Including IT Risk.
- Risk appetite set by management and approved by the Board of Governors.
- Risk outcome measured by:
 - Operational Impacts
 - Financial Impacts
 - Reputational Impacts
- Decision-making guided by operational, financial and reputational impacts.

10/21/2017

Board Leadership Calgary 2017



1. U of C Example: Ransom Payment- The Decision

- 7 Day Window
- Risk-Based Decision Making
 - Executive Leadership Team
 - Board of Governors
- Key Questions
 - What didn't we know?
 - What data could/would be lost with no chance of recovery?
 - Would we actually get the keys?
 - Would the keys introduce additional risks?
 - Would the University be a greater target?
 - Would this mitigate any potential litigation due to lost info?



10/21/2017

Board Leadership Calgary 2017



2.1 IT Governance

Governance (IIA Definition):

Structures and processes for decision making, direction, accountability, control and behaviours in an organization

Key areas of focus:

- *Decision rights (day to day, investment, direction)*
- *Policies and procedures*
- *Accountability structures*
- *Risk Management*

10/21/2017

Board Leadership Calgary 2017



2.2 IT Backup and Recovery and Business Continuity

- Organizations are dependent on technology: full stop
- Backup and recovery in an event is first
 - *Where is the data backed up to?*
 - *Can it be recovered (has anyone ever tried)?*
 - *Hardware and software availability?*
- Maintaining operations post-event is beyond emergency response
 - *Key assets still secure?*
 - *Operations able to continue uninterrupted?*
 - *Is the plan written and available? ie/hardcopy!*

10/21/2017

Board Leadership Calgary 2017



2.3 IT Security and General Computer Controls (GCCs)

- Information Security (NIST definition): The protection of information systems from unauthorized access, use, disclosure, disruption, modification or destruction *in order to* provide confidentiality, integrity and availability
- Types of systems:
 - *Stand-alone systems with software, internet and email*
 - *Networked systems as above*
 - *Cloud-based software accessed through a browser*

10/21/2017

Board Leadership Calgary 2017



2.3 IT Security and General Computer Controls (GCCs)

- Types of organizations:
 - *NPO has its own staff and own IT assets*
 - *NPO has only volunteers using their own IT assets*
- Threat vectors
 - *External hacking*
 - *Internal fraud*
 - *Social engineering including phishing*
- Common controls (GCC)
 - *Access management (segregation of duties)*
 - *Change management (changes to software and systems)*
 - *Firewalls, anti-virus and patching*

10/21/2017

Board Leadership Calgary 2017




2.4 Payment Card Industry (PCI)

- Significant for anyone who accepts credit cards.
- Requires significant controls over credit card information (think CVV #s)
- Provider can shut you down
- A leak can kill your reputation

10/21/2017


Board Leadership Calgary 2017



3. Approach

- Understand the NPO
- Determine keys for delivering on mandate and the broad areas of “enterprise” risks
- Understand where IT affects these risks
- Determine your “crown jewels” (data assets)
- Cyber risks viewed through same lens as physical security of people and assets at the strategic level, not just an IT issue
- Ask the question of mgmt.: what keeps *you* up at night? Answer will be very disclosive

10/21/2017 Board Leadership Calgary 2017



3. Approach

- Consider:
 - Significant regulation or compliance requirements
 - Privacy
 - PCI
 - Third party providers and SOC 1 and 2 report provision
 - Web services including Dropbox
 - Knowledge of Social Engineering, Phishing
 - Knowledge of basic control concepts like SOD
 - Remember the nimbleness of small and medium NPOs

10/21/2017 Board Leadership Calgary 2017



4. Case Study

- Review case individually
- Discuss with group the primary risks
- Identify key factors that influence the NPO's IT risks by priority (H, M,L)
- Present and discuss

10/21/2017

Board Leadership Calgary 2017



10/21/2017

Board Leadership Calgary 2017