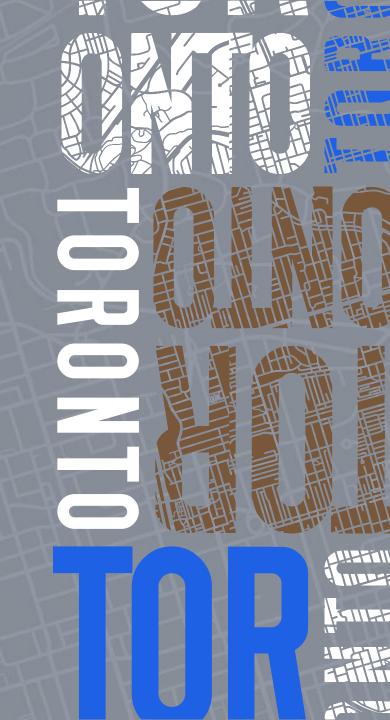


Risk and Cybersecurity Committee Update

Rob Seastrom, Chair





Look at this Agenda!!!

What / Why
How
Risk Register
What Then?
Other Activities

What/Why

- The Risk and Cyber Security Committee (RCSC) is a standing committee of the Board of Trustees (created 28 February 2022).
- Exists to assist the whole Board in performing its fiduciary duty of risk identification and assessment (charter on arin.net along with other standing committee charters).
- Risk is anything that imperils successful execution of our mission.
- Many kinds of risk: Compliance, Legal, Strategic, Reputational, Operational, Security, Human, Financial, Physical... and more!
- Not limited to cyber risk infosec C/I/A risk just a subset of operational and security risk.



How do we track and prioritize risks?

- We are worse multitaskers than we think
- UOregon study circa 2008 concluded "humans can only focus on 4 things at once"
- Any organization has more than four identified risks!
- We prioritize and track risks the same way we do other project management write stuff down.



What is a Risk Register

- Document a risk, write it down
- Assign a score to likelihood, impact (1-5, unspecified units)
- Classic risk calculation: risk = likelihood x impact
- Super sloppy numbers, very subjective
- Yet it gives us a tool to prioritize what matters, not be Eeyore walking in circles mumbling "oh dear"
- Preserve the collection of written down risks as a living document



What do we do with it?

- Curated by RCSC, CEO, CISO, assistance from other staff including General Counsel
- Sort by computed risk = we can focus our minds
- Review with entire Board of Trustees to inform fiduciary duty choices
- Develop remediation plans as prioritized



I don't see the risk register contents in the BoT minutes...

Like all sensitive matters, risk register items are handled in Executive Session in camera (we are meeting in Canada, so will use the approved local term).

Minutes are public, contents of the risk register are not; indeed discussing how we are mitigating risks could have an adverse effect on our risk exposure.



Why is this important to me as a member?

- One of the duties of the BoT is to manage (not eliminate) risk to the organization. There is inherent risk in everything we do; from a governance perspective the Board's responsibility to the organization and the membership is to drive risk exposure to acceptable (non-zero) levels.
- But you, our members, may see things we don't.
- The risk register ensures that concerns you bring to us don't go into a black hole.
- If you see something, say something.





Other Activities

- Collaboratively set goals for things like:
 - Tabletop exercises (IR and other)
 - Security certifications
 - Data governance and privacy policies
 - Other tests and documentation of our adherence to best practices and readiness
- Results and status updates are our CISO's story to tell, you'll hear from him later.



RCSC Members 2024

Rob Seastrom (chair)

Hank Kilmer

Chris Tacit



Thank you

Questions and Comments?



