Minutes

Meeting:	**Information Security Council – Meeting # 3**
Date & Time:	**Wednesday, October 24, 2018 (2:00 – 4:00 p.m.)**
Location:	**GOVCN Boardroom, Room 209** **2nd Floor, Simcoe Hall (SH) 27 King's College Circle**

CHAIR:

Ron Deibert

ATTENDEES:

Heidi Bohaker, Sam Chan, Rafael Eskenazi, Deepa Kundur, Sian Meikle, Zoran Piljevic, Leslie Shade, Michael Stumm, Bo Wandschneider, C.J. Woodford

BY INVITATION

Sue McGlashan, Marden Paul, Carrie Schmidt, Alex Tichine, Mike Wiseman

NOTE-TAKER

Andrea Eccleston

WELCOME:

Ron Deibert, Chair, opened the meeting and welcomed all participants.

Approval of Agenda:

The Chair invited comments from the Council regarding the meeting agenda. No changes were tabled. The Agenda was approved as circulated.

[Post-meeting notes:] There was a re-ordering of the Agenda Items 5 (CISO update) and Item 6 (Example of managing purchase risk – information risk and risk management assessment).

APPROVAL OF MINUTES OF JUNE 29, 2018 (Public and Full):

The Chair requested Council to review and approve the public and full versions of the meeting Minutes of Friday, June 29, 2018.

The public and full versions of the Minutes of Friday, June 29, 2018 meeting were approved with changes as noted:

In response to question raised, it was noted that the Public Minutes are posted at http://main.its.utoronto.ca/about/committees/information-security-council-isc/#6501

ACTION:

Carrie S to publish the approved Public Minutes of Friday, June 29, 2018 on the ITS website.

WORKING GROUPS UPDATES:

Bo W informed ISC that:

- Mike Wiseman has taken over the Chair role of the Procedures, Standards and Guidelines Working Group from Frank Boshoff.
- In addition, WG Chairs will be meeting on a regular basis to consolidate details presented to the Council and Mike W will coordinate this initiative.

The Chairs reported on the progress of their respective Working Groups as follow:

Risk, Compliance, Metric and Reporting:

Sue M reported that the focus of the WG on RCMR is to create an Integrated Information Risk framework that includes a Self-Assessment (IRSA) so that units are able to self-measure their risks in major risk areas. She provided an overview of the framework which involves organizing risks into risk areas, measuring performance in that risk area against a Capability Maturity Model, and managing the risk:

- **Organize:** The risk areas have been narrowed to Information Risk areas
- **Measure**: A Self-Assessment has been piloted with two units
- **Manage:** A scorecard that would be available to each unit was presented. It was highlighted that the scorecard allows unit leadership to easily identify where problems exist
- **Manage:** A dashboard in which all unit results would be displayed was discussed. The dashboard would allow the ISC and senior leadership at the University to identify areas around constraints, such a lack of resources, and other commonalities; this overview is valuable at an institutional level.

The framework using the IRSA does not as yet include a method for units to develop an Information Risk Management Program, as required by the Policy on Information Security and the Protection of Digital Assets; and that WG on RCMR would like to add two additional items to extend the IRSA into an Information Risk Management Program. In addition, each unit would also be asked to:

- Provide a strategy for each response in the risk areas (i.e. Mitigate / Accept / Avoid / Transfer)
- Provide a reason/plan for each strategy chosen.
- **Highlighted that the strategies and plans are governed by each Unit**
- The goal is to provide a standard minimum report for each unit Management Program
- This provides units with simplified way to provide their IRMP

These strategies and plans would form part of the dashboard

During Council discussion, the following points were clarified:

- This process will take time to mature. During Year 1-2, no proof would be requested, thus results depend on people's goodwill. Years 3– 4, the next stage, would ask people to supply some proof, but this may take longer.

The next steps are refining the questions, extending the pilot and rolling out the assessment. To this end WG Chair requested the following resource:

- Require help for proper system of collection of data in stakeholder meetings in order to maximize the use of time. Also, plan to continue working one on one with group who are willing to help refine the questionnaire. Heidi volunteered her unit as one of those who would help.
- Help with designing workshops
- Help in creating survey tool and dashboard
- Help in running workshops

During the discussion, it was agreed that pilot would require two people for this project because of the multiple skill set required.

There being no further questions raised, the Chair asked for a motion to support the resource funding request.

On motion by Heidi Bohaker, seconded by Ron Deibert, and carried unanimously, Council approved and strongly supports the Integrated IR Management Program framework funding request to move forward with the pilot project.

ACTION:
Sue to refine requirements and submit to the IT Initiatives Fund, as well as, bring forward document to the next sitting of the ISC.

Incidence Response Planning:
Alex T updated that incidence reporting at the University is currently located in several on-line locations and in some instances list of contacts are outdated. The WG on IRP's is currently working on revision of the U of T Incidence Response page in order to bring it up to date. Noted that the goal is to pick something that is tangible and realistic to implement in order to provide the most significant impact across the University. WG on IRP presented Council with a draft of the Incident Response Web Page for consideration.

ACTION:
Alex T to submit proposal on how to categorize incident based on severity level and required response at the next sitting of Council.

Alex T also reviewed the Incident Response checklist currently in use by UTM. He suggested that there is a need to socialize this concept as a way to structure response across various U of T Help Desks for a consistently guided response. Alex T requested ISC's approval to move forward and update the IT&S incident response page based on consultation with ISEA and The Education and Awareness Team.

The Chair noted that the overall aim is great and he liked the direction in which this is going.

During discussion, the following suggestions were tabled:

- For future state, it would be nice to work towards something that is less text heavy and more of a triage that involved something of a security planner, where there is a series of cards to direct people to the right path.
- It was also noted that it would be desirable to adopt a single point of intake for Information Security incident reporting, similar to 911..

Council recommended implementing changes, as presented within the draft, to improve the Incident Response process to ensure access and more accessible.
ACTION:
Alex T to present checklist for IT professionals within divisions to ensure consistency on how to respond to incident at the next sitting of Council.

Procedures, Standards and Guidelines Working Group
Mike W reviewed the proposed Data Classifications with the ISC, noting that the terms of reference for the PS & G working group is to produce standard and controls to reduce risk. In reviewing the 1st draft, it was noted that the proposed data classifications would be comprised of 5 categories

whose definitions encompass 99% of data in use at the University. Noted that confidentiality is the main focus in the classifications however integrity is also a requirement.. In providing an overview, it was noted that:

- The WG expects public, internal and confidential will be the three most public facing categories and broad community of users would be concerned with the first three categories.
- The WG is assisting the Office 365 deployment by advising on the configuration of the Advanced Information Protection component which is used to classify and protect email and documents. These classifications will have associated controls, such as, confidential documents can only being seen by those in the confidential group. This will be passed on to implementation team to test on users.
- The WG expects that research data, based on initial evaluation, may fall mainly in one category, 'Internal'.
- Finally, the WG is conscious of the need to apply the classifications in the most user friendly terms as possible.

The WG's next steps are the development of controls and standards to be tied to the data classifications, for example, requirement to use single-factor authentication for Internal data. With respect to guidelines, which are documents that translate standards into how-to guides, these are expected to be another example of easing the use of standards and controls in common services.

Education Awareness Group:

Carrie S reported that Education and Awareness Working Group (WG) has met three times since the council last convened. The focus is on engaging stakeholders (faculty, students & staff). Carrie S to reach out to ISC members to find out what channels they use and how to leverage their channels.

Carrie S presented results to-date on summer and fall activities including Cyber Security Awareness Month. The campaign was in mid-swing, halfway through the campaign.

Also updated on anti-phishing campaign that targeted the following Faculties: Law; Engineering and Chemistry. In terms of results, (low open and click rates of the phishing simulation emails) it could not be determined if users were savvy or the exercise was not sophisticated enough. Campaign will be repeated every three months to gage movement and improvement. In terms of future activities, the Procurement Department and Rotman have volunteered for phishing exercise during the fall and winter period. UTM anti-phising campaign will occur in December/January.

In terms of other outreach activities, have been doing a lot of students focus events to get the word out about information security, anti-phishing, safe online use, and where to go for more information – Security Matters website. Also include high level of media engagement in terms of print, social media and online. Also met with a number (200 plus) of students during orientation week at the Student Union street fair. Carrie S noted that there were a number of volunteers from the WG committee and thanked them.

Carrie S also reported on activities and results around Cyber Security Awareness Month (see posted presentation), noting that tagline is "Security matters every day". Highlighted a number of planned activities including collaboration with Information Security and Enterprise Architecture (ISEA) and the other chairs of the WGs to bring awareness on how we incorporate information security in our every day life at work and home.

Carrie also highlighted some notable results and analytics:

- Positive results show that in mid-October there were 1,752 page views on Security Matters website and 238 page views on the Phish Bowl page
- There were 238 views in the Phish Bowl
- The numbers are doubling the previous highest results

It was also reported that Cyber Security Awareness Month activities include:

- Panel discussion, which was also livestreamed, targeted staff and students on "How to incorporate cyber awareness into your everyday life". A total of 40 people attended.
- A play funded by ITS, titled *Fake Nerd Girl* and followed by a panel about staying safe online, protecting identity etc. (ITS staff, Chloe Payne and Mike Wiseman were both on the panel). It was almost a full house in the theatre – 80 plus people.
- Other activities include contest, articles, blogs, tip sheet, surveys and some promotion materials including posters.

Directed council to the Phish bowl web page on the Security Matters website, where phishing incidents are posted at (https://securitymatters.utoronto.ca/category/phish-bowl/)

Research Data Working Group:

Marden P reported that the group had taken the advice of the ISC to not attempt to boil the ocean in terms of offerings to faculty and staff. As such, the working group focused on immediate deliverables that would being utility to the community which include:

- A checklist of Information Security Good Practices was created. This checklist starts at the macro level -- data centres/machine rooms/server closets, listing good practices for their configuration, down to the micro level, handling of devices containing University data such as smartphones or USB keys. Where specific guidance is provided, reference materials as to how to implement are included.

- In addition, in keeping with the theme of providing assistance to PIs, the Information Security department will replicate its successful Laboratory Information Systems Good Practices workshop under the auspices of the Research Oversight Compliance Office. The workshop or a variant will also be targeted to new faculty or at the New Academic Administrators education program co-ordinated by the Office of the Vice-Provost, FAL.

- Third, the UTL has an index of discipline-specific accredited data repositories. These will be made more visible.

Example of managing purchasing risk - information risk and risk management assessments - Sue M (FOR INFORMATION)

Sue M presented Council with details of the information risk and risk management assessments process undertaken for the vendor chosen the institutional Learning Management system.. The risk recommendations and findings were provided to the Director and the project team.

In terms of recommendations for cloud vendors, the following is usually included in the contract:

- How to deal with a breach in terms of who should be notified; the need to specify in contract that we are provided logs, as if not specified we could be charged a lot.

In our LMS implementation

- Data retention was reviewed.
- The team addressed concerns about linking social media
- what mobile apps have access to

CISO update - Bo W

Bo W reported that CISO search successfully concluded and the official start date is December 3, 2018.

Any other business - Ron D (FOR INFORMATION)

Bo W reviewed an email from UBC regarding their revised privacy and access policy, which stipulates that fundamentals training is now a mandatory requirement for faculty, staff, researchers, student employees and contractors who use UBC Electronic Information and Systems. He asked Council if this is something that should be on UofT's radar.

A member also put forward a suggestion for future discussion at the ISC around the issue of faculty access to student information in the learning management ecosystem. It was noted that this would fall under the purview of Susan McCahan, Vice-Provost, Academic Programs and Vice-Provost, Innovations in Undergraduate Education.

Next meeting - Ron D (FOR INFORMATION)

Chair noted that no date set for the next sitting of the ISC.

Action Item:

Chair instructs Andrea E to poll members for availability via doodle pool and schedule meeting accordingly.

Adjournment - Ron D

There being no further business to come before Council, the meeting was adjourned at 4:00 p.m.