Minutes (PV)

Meeting:	**Information Security Council – Meeting # 4**
Date & Time:	**Thursday, January 17, 2019 (10:00 – 12:00 p.m.)**
Location:	**The President's Boardroom # 132** **1st 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, Isaac Straley (**Co-Chair**), Michael Stumm, Bo Wandschneider, C.J. Woodford

BY INVITATION:

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

REGRETS:

Leslie Shade

NOTE TAKER:

Andrea Eccleston

Item:

Welcome - Ron D

Ron Deibert, Chair, opened the meeting and welcomed all participants. This was followed by a round-table introduction of all participants in attendance.

Approval of Agenda - Ron D – All (FOR APPROVAL)

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

Approval of Minutes of October 24, 2018 (Public and Full) Ron D (FOR APPROVAL)

The Chair requested Council to review and approve the public and full versions of the meeting Minutes of Thursday, October 24, 2018.

The public and full versions of the Minutes of Thursday, October 24, 2018 meeting were approved as a correct record, subject to the following amendments:
Page 1, Line 16 - ACTION ITEM should be amended to read "Carrie S to publish the approved Public Minutes of June 29, 2018 on the ITS website, on the ISC page".
Page 4, Line 3 under Procedures, Standards and Guidelines Working Group should read", it was noted that the proposed data classifications would be comprised of 5 categories".

ACTION:
Carrie S to publish the approved Public Minutes on the ITS website, on the ISC page.

Introduction, initial thoughts and questions – Isaac S (FOR INFORMATION)

The Chair extended a warm welcome to Isaac Straley recently appointed Chief Information Security Officer and Co-Chair of the ISC.

Isaac S provided Council with details of his background and his initial thoughts on the inaugural role of CISO at UofT. In terms of personal goals, these include:

- Enabling the mission of the University
- Protecting the rights and dignity of all members of our community (i.e. faculty/students/staff/research subjects etc.)
- Empowering people and units to make effective decisions to effectively run security programs

He also emphasized some of his areas of concerns which have a significant impact on the Higher Ed space, these include:

- Account compromise, such as phishing and stolen password as areas where most data breaches start and should be of significant concern especially for the University because it has so many accounts and systems.
- Vulnerable devices and the ability to attack a computer device.
- In terms of research and data, these are significant issues and the University need to be proactive in developing comprehensive programs and strategy to address risks, as well as, educate people about consequences.
- In terms of research espionage and infrastructure by the nation states, universities are a real target and there is the need to find ways to socialize and educate on this issue.

Isaac S also updated Council on a number of priorities areas as ISEA continue to build culture and work on trust with the community, these include:

- Consultation with leadership, faculty, and students while continuing to build upon the programs and initiatives already in place by the Education and Awareness team.
- In addition, plan also underway for review of the ISEA team, its projects and initiatives, as well as, a review of its branding and communication initiatives. He highlighted that one of the areas for enhancing communication is sharing metrics on the state of security at UofT. By way of example, he noted that it would be useful to communicate about how many devices and accounts are compromised. These meaningful metrics along with some education programs would give the community a sense of what we are doing, as well as, provide useful information to help drive decisions.

In terms of his areas of focus, Isaac S informed Council that these would include:

- Focus on efficient measures such as MFA as this is very tangible and important if rolled out effectively.
- Implementation of phishing awareness campaigns while leveraging the security features in O365.
- Also, plan to raise awareness and create protocol around on how to reduce risk in the area of international travel and digital security.
- Another area of focus is building a culture around security. To achieve this aim, he plans to provide support to units and departments on how to implement their cybersecurity and risk assessment programs. This would involve looking at technical requirements and resources available in order to provide the tools to assess their specific programs. He added that security is not all about technology but the need to build a culture that is very effective.

- In terms of incident response, plan underway to improve and enhance the process. He added that the Incidence Response Working Group chaired by Alex T is doing some great work by looking at how we can help units better identify and triage incidents. He highlighted short term initiatives such as tabletops ops designed to stimulate discussion on incidence response at the University.
- In the area of procurement and vendor suppliers, also plan to work on how to standardize processes.

During Council discussion about the role of the ISC, the following points were noted:

- ISC's role is to be a champion in the community and/or build consensus with various audiences for decision making to move things forward.
- In terms of its decision making power, it was noted that ISC's decisions are important as they set the norm at a high level. While it does not have the force of authority, it is not to be underestimated because it sets the tone to run against the grain. While the ultimate decision making power is vested in Governing Council, historically at UofT it is Committees and Boards where expertise develop and Governing Council draw on the those bodies to make decisions. Thus, ISC decisions while not legislative authority are important to influence Governance.

Council also discussed the role of the CISO, it was noted that this is an opportunity to position the role from an institution-wide perspective as opposed to being viewed as just a resource for Central IT. To this end, it was suggested that CISO need to be present in the community by creating horizontal linkages with units/divisions. It was also noted that it is important to get message out that security risks cannot be resolved by technology only but also need to implement processes. There was also discussion on strategy for CISO engagement with the Community. Council agreed that getting concise message out was important to start the engagement process.

Issac S concluded his presentation noting that he would be meeting with ISC members individually in the near future.

<u>Update on Integrated Information Risk Framework – Sue M (FOR INFORMATION</u>)

Sue M provided the Council with the following update:

- an overview of the integrated information risk framework;
- reviewed the proof of concept (POC) and results
- as well as, put forward a submission of funding request

In terms of process, it was noted that:

- Units would score themselves against those risks, per question.
- They would then provide a strategy for that particular risk and then plan for that strategy if it fits and the reason why they are accepting that strategy. This then gives us an Information Risk Management Program.
- With regards to the ISC, all those results are reported into a dashboard for the ISC to review.

During Council discussion, the following points were clarified or raised:

- Comparing scores across individual units will not initially be meaningful.
- Comparing averages across many units will provide useful data.

A suggestion was made to have some analysis to pull out themes and that is something that needs to be discussed as part of the maturity of the program piece. It was also noted that in terms of scores and reasons; need to get the data out in a useful way that will support decision-making. To this end, it may require analyst personnel resource to identify the meaningful information and should be part of the funding request to add additional staff to help pull out issues of concern.

In terms of what is new from the last update to Council, it was noted that work now completed with one small IT-centric research unit and plan underway to complete up to 5 other units by April 2019 as well as work with Zoran P (UTSC) and Sotira C (A &S) in the near future

Sue M also updated Council on time commitment and methodology. She said that current work involved doing the proof of concept for the units that are willing to be part of the pilot. In terms of time commitment, it was noted that a minimum of 4 hours was required, not including the research-related question. It was also clarified that at this stage only working with IT people but plan to include administrative leaders and these assessments would likely take more time.

With respect to the next cohort, Sue M noted that she would like to provide results that are more meaningful for the next 5 units. In terms of time commitment on ITS side, it would be 2–3 hours and on the units' side realistically 6 hours. A suggestion was made to look at ways to incorporate questionnaire via APP so that people could do a bit at a time, something that does not necessarily require a chunk of time that they can fit into their day. In response it was noted that work on an APP is currently underway.

Sue M also provided an overview of the result of a PoC for an IT-centric research unit noting that this was the first group to complete the entire program which include both the self-assessment and a plan. In terms of observations, this will require a lot of scaffolding and workshops. She also highlighted the requirement for a UofT standard policies and guidelines as it would be much more productive in completing the risk assessment and applying the standard controls. It was noted that ISEA is working on standards and guidelines, and if other units have good practices in place it would be useful to publish them.

Council also discussed some of the key aspects of the pilot data. A member asked if there was a way to code cases in instances where nothing is being done. In response, it was noted that there is a non-applicable option on every question. Bo W added that it is a different value than not applicable.

ACTION:
Sue M to amend response collection to include the option for recording cases where nothing is done.

In terms of funding objectives, it was noted that there is a need to provide aid to the units in understanding their information security risk. Sue M outlined the 3 phases of activities in her funding proposal noting that in term of funding objective there is the intention to provide aid to units in understanding their information security risk and to meet the requirements of the Policy on Information Security and the Protection of Digital Assets that units develop an Information Risk Management Program (IRMP).

Advanced Threat Protection and Azure Information Protection (FOR INFORMATION)

Marden P updated Council that plans are underway to implement a group of the extra security features on O365 - Multi-Factor Authentication (MFA), Azure Information Protection

(AIP), and, Advanced Threat Protection (ATP). He noted that the team has been working with an external firm to develop a reference model configuration inside our quality assurance (Office 365 QA) environment. Currently, the services are configured and the system administrators are trained on moving into the production environment. He also provided demos on the Azure Information Protection (AIP) and the Multi-Factor Authentication with Conditional Access.

The Security Council held a discussion regarding Marden P's request for direction on implementation sequence, it was suggested that this should start with Finance, Vice President and at the Chair levels. There was also discussion about the need to ensure that we socialize this well to the community that these tools are going to be turned on. In terms of roll-out, it was noted that we have the skills to move from QA into production.

Any other business (FOR INFORMATION)

Carrie S updated Council on a number of upcoming events:

- A Workshop offered by the Provost's Office and led by ITS - information security and education and awareness teams - on Managing Your Digital Footprint is scheduled for January 19, 2019. The goal is to provide faculty with practical tips on how to safeguard personal and professional information online; in public and the workplace. The event will also introduce the CISO and it is anticipated that about 50 people will be participating.

- Staff, students, and faculty have also been invited to participate in UofT's Data Privacy Day event on January 28, 2019. In terms of activities, will include interactive pop-up booth; meet and greet the CISO; the Director, Information and Protection of Privacy Office, and the Education and Awareness Team.

Next meeting - Ron D (FOR INFORMATION)

The Chair noted that the next meeting of the ISC will be held on Tuesday, April 30, 2019 at 2:00. p.m. in the President's Boardroom # 132 at Simcoe Hall.
{POST-MEETING NOTE: Meeting has been relocated to: **The Faculty of Applied Science & Engineering, Michael E. Charles Council Chamber (GB202), 2nd Floor, 35 St. George Street}**

Adjournment - Ron D

There being no further business to come before Council, the meeting was adjourned at 11:55 a.m.