Minutes

Meeting:	**Information Security Council – Meeting # 2**
Date & Time	**Friday, June 29, 2018 (10::00 – 12:00 noon)**
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, Leslie Shade, Michael Stumm, Bo Wandschneider, CJ Woodford

BY INVITATION

Frank Boshoff, Sue McGlashan(regrets), Marden Paul, Carrie Schmidt, Alex Tichine Mike Wiseman

Notetaker: Andrea Eccleston

Item

WELCOME AND INTRODUCTIONS:

Ron Deibert, Chair, opened the meeting and welcomed all participants. This was followed by a round introduction.

Approval of Agenda:

The Chair invited comments from the Council regarding the meeting agenda. The Agenda was approved as presented.

Approval of Minutes (Public and Full):

The Chair requested Council to review and approve the Public and Full versions of the meeting Minutes of Monday, February 5, 2018. It was clarified that there are two versions of the Minutes, a full version, which will be available on the Team's site and a public version, which contains the fullness of the discussion but not necessarily the details and will be posted on the public website along with the final version of the Terms of Reference.

The Minutes of the February 5, 2018 meeting were approved as corrected.

ACTION:

Carrie S to publish the approved public Minutes of Monday, February 5, 2018 on the ISC website.

Gathering Community Input (For Information)

Item deferred

Working Groups (Drafts – For Approval)

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

Incidence Response Planning:

Alex T provided an update of the threat landscape and incident occurrences by highlighting a number of critical and suspicious machine activities from the last 7-days period. He provided an overview of suspicious UTORID account activities by user category (faculty, students, staff, et cetera.

Council discussed protection and the frequency of changing passwords. A Microsoft survey and recent NIST guidance was cited, which states that "frequency of changing password is not an indicator of how secure you are; instead, the best indicator of protection is based on where password is stored and its length".

The issues around incident culture was raised, it was noted that incidences are viewed as sensitive conversation and not always reported. A key point raised by the IRPWG was that they were not able to quantify what is happening across UofT. While they have some idea of what is happening at the central level, this is not evident at divisional, faculty and smaller units level because information is not visible.

During Council discussion, it was also noted that there is a sustainability problem due to a lack of long-term planning in terms of upkeep and decommissioning.

In regards to ongoing initiatives for the next 12 – 24 months, the WG on IRP would continue work on the collection and aggregation of existing resources across the University on incidence response. It was noted that a significant amount of work have already been done by all three campuses. A proposal to develop a baseline incidence response was presented to Council. It was noted that this will be easy to understand with the goal to guide and help IT teams in the response process. In terms of benefits, it is expected this will unify UofT in the sense of a common framework, common language and definitions.

During Council discussion, there was a question on what process is in place if an incident should occur tomorrow or next week before the structure is in place. In response, it was noted that the current response is to contact ISEA, they would engage all required resources and provide the assistance and guidance that is required. The Chair suggested that IRPWG conduct a mock-up exercise on a data breach, to determine response.

ACTION:
Alex T to present the initial draft Incidence Response Plan at the next ISC meeting.

In term of resources, the IRPWG submitted request for creation of a 1-year internship position to assist with aggregating, compiling, analyzing information and compile into a report. It was also noted that the WG experience some challenges with the frequency and length of meetings and suggested that it would be more efficient for the group to have 1-day retreat every 3 months.

Education Awareness Group:
Carrie S reviewed the Terms of Reference for the Education Awareness Working Group. It was suggested that the 3rd point be taken out of the ToR as that would be part of the operational business, as opposed to the Working Group, which may take on specific phishing programs or specific initiatives.

ACTION:
Carrie S to make amendment to 3rd bullet of the ToR.
[Post-meeting notes:] Upon further review post-meeting, Carrie decided not to make the amendment. In fact, both the education and awareness team and the education and awareness working group are involved in education and awareness efforts.

Carrie S also reviewed upcoming activities for Cyber Security Month in October noting that there will be one marquee event/contest/panel discussion per week. In addition, work is currently underway on an anti-phishing exercise which would involve the Faculties of Law and Engineering and some divisions within ITS. Plan is to conduct a phishing exercise every month and repeat campaigns every three months with the objective to see number goes down, the campaign is to be adjusted accordingly.

ACTION:
Carrie S to follow-up with ISEA to delve more into the incidence occurrence numbers. [Post-meeting notes:] Carrie followed up post-meeting and Mike W stated he would work to provide statistics.

Council was encouraged to review the Security Planner tool developed by Citizen Lab noting that it will be going through refresh by peer review. The Chair extended an invitation for volunteers to get involved.

Research Data Working Group:
Marden P reported that RDWG held three meetings and have completed a few lab and faculty visits. It was noted that work is currently underway to identify the following: needs of faculty regarding research data security, where data security requirements are captured, and volume of specific data security compliance requirements. With respect to current state, there are no available metrics to measure, or consistent, pan-University vehicles to gather and collate data. He added that research data lifecycle is handled locally which is highly dependent on capability of local IT and the research groups themselves. It was also noted that data are being put in places like Dropbox or other convenient locations, perhaps due to lack of knowing else where else to go.

RDWG requested advice from ISC regarding plan to send out survey to either Chairs/Deans or individual PI in order to determine a baseline of what currently exist. The goal of the survey is to identify volume and location of data repositories, variety of data sets and types of regulatory/stewardship/protection requirements for identified data sets.

During the discussion, the following points were raised:

- RDWG need to be mindful that we do not boil the ocean; need to separate data management and information security.
- Would like to see group focus on low hanging fruits, such as, encryption and asking where the servers are located, what is the security in the room and so on.
- Suggestion made for RDWG to engage REB. In the shorter term, we should try and insert into the REB process, so people are thinking about it.
- It was also noted that RDWG need to get feedback on data access requirements in the survey.

Council also discussed the potential for Education Awareness program for researchers' onboarding purposes or online to spread awareness by getting involved in new faculty workshop et cetera.

Action:
Marden to distribute a sample of survey to ISC

Risk, Compliance, Metric and Reporting:

Frank B provided an update on behalf of Sue M re the RCMR Working Group.
The update included:

- A list of the members of the Working Group
- The Terms of Reference of the Working group.
- A summary of progress to date and plans for the future.
    - The focus of current and future work is to create a self-assessment risk framework so that units are able to self-measure their risk in major risk areas, based on survey questions and measuring results based on a Capability Maturity Model.
    - The work is based on investigation undertaken in the Higher Ed space.
    - The group hopes to pilot the process with one or two units to refine the concepts.
    - Input from stakeholders is an essential part of the process, and consultation will take place.

Notes from discussions:

- The purpose is to identify where the weak areas are and where to focus resources and attention.
- It was noted that it is helpful that it comes with a self-assessment process that is very lightweight and this would involve less worry about how people are responding to it. Frank B added that it would enable collection of information that would identify the issues, so this is an interesting model.
- Also noted that the resulting report-unit scorecard will be done on an annual basic to see what the trends are going forward.
- Working Groups have close tie-ins and they communicate with each other in order to address overlap.
- In response to a question raised around whether access would be centralized or localized, it was noted that this will be available via an online application and local units can enter the system and complete the information.
- It was also noted that no faculty is represented in the WG membership.

Action:

Sue M to review faculty representation on the RCMR Working Group

Procedures, Standards and Guidelines Working Group - FRANK WG:

Frank B updated Council that PSGWG agreed that the first few standards should be non-confrontational with a high degree of integrity. In terms of the security standards, procedures and guidelines, they are based on architectural principles for a solution because this format imposes a certain degree of conciseness. Noted that the PCI-DSS compliance was selected as the University currently runs about 300 merchant accounts.

The issue of data classification was also discussed, it was noted that 5-security levels have been identified but still working on their definition. During the discussion, it was noted that in terms of articulation, less classification is better. Council urged PSGWG to keep as simple as possible at the administrator level and for those dealing with desk and student data.

Some Stats (For Information)

Mike W gave a presentation on the following topics with respect to Information Security Operations at U of T:

- Event and Incident Detection/Analysis/Response encompassing networks and services

- Identity and Access Management: UTORid account lifecycle, authentication and authorization services
- Information Security Technical, Privacy and Business Process Risk Assessment
- High Impact Incident Response
- Architecture for enterprise services, web content management, Active Directory and data sharing methods.

Event and Incident Detection/Analysis/Response statistics:

- Detection of 'suspicious devices' (exhibiting possible indication of compromise) by analyzing network traffic from U of T devices owned by faculty/staff/students. Rate of 20-100 per day. Primary events detected: access to known phishing or malicious sites. Majority of events detected from wireless devices which indicates vulnerability due to user-owned rather than University-owned equipment. Current mitigation: notification of departmental IT staff for device response.
- Detection of 'suspicious UTORid accounts' (exhibiting user account compromise due to unauthorized or multi-geographic logins). Rate of 10-50 per day and categorized by role: students exhibit half of compromised account incidents. Suspected causes: password compromise due to phishing, multi-use, sharing.
- Automated response methods which consist of quarantining or blocking external access attempts due to high confidence detections of unauthorized network access (scanning or accessing security devices) and multiple attempted access. Rate of 10K-50K quarantines per day.

Vulnerability Detection via internal device scans:

- These monthly scans measure device and software responses to detect unsupported or unpatched software, a key risk for exploit. Status reports are generated for University units to respond to by mitigating the vulnerabilities (patching, installing firewall protections, and decommissioning old services).

High Impact Incident Response Enumeration:

- A number of information security-related incidents were briefly described including those resulting in financial loss, procurement fraud, complex computing environment compromise, and foreign country phishing attempts

CISO update: (For Inforamtion)

Bo W reported that the search for the CISO has been relaunched and decision made to retain a search firm. Interviews are set for late July 2018.

Shared SOC: (For Informtion)

Bo W provided an update on the Shared SOC initiative noting the Institutional Partners held Face-2-Face meetings at UofT and UBC. Invitation also extended to McMaster and Ryerson to join the table with the four original partner institutions. It was noted that partners also met with The Big Ten in the US (their project is called OMNI SOC) to explore what collaboration between the SOCs might look like. Bo W noted that this is a 1-year proof of concept, to be housed initially at the UofT.

Any other business (For Information)

The Chair thanked the Working Group Chairs for their work, noting that it is exciting to see the level of progress made.

The Chair invited members to forward any suggestions for Agenda item(s) to his attention.

Any other business (For Information)
There was no other business.

Next Meeting (For Information)
The next meeting scheduled for Thursday, October 18, 2018.

[Post-meeting notes:] The next meeting is re-scheduled for Wednesday, October 24, 2018 at 2:00 pm at Simcoe Hall, GOVCN Boardroom # 209, 2nd Floor

Adjournment
There being no further business to come before Council, the meeting was adjourned at 4:05 p.m.