Draft Minutes PV

Meeting:	**Information Security Council – Meeting # 6**
Date & Time:	**Monday, September 9, 2019 (2:00 – 4:00 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, Sian Meikle, Zoran Piljevic, Leslie Shade, Bo Wandschneider, C.J. Woodford

BY INVITATION:

Sue McGlashan, Marden Paul, Alex Tichine, Mike Wiseman, Carrie Schmidt, Kelly Carmichael-FIPPA

NOTE TAKER:

Andrea Eccleston

Item

Welcome - Ron D

The meeting convened at 2:00 p.m. with Committee Chair Ron Deibert presiding. Rafael Eskenazi, introduced Kelly Carmichael, Freedom of Information and Protection of Privacy (FIPP) Coordinator to the Council. The Chair welcomed everyone. This was followed by around the table introductions.

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 pre-circulated.

Approval of Minutes of January 17, 2019 (Public and Full) & April 30, 2019 (Public and Full) Ron D (FOR APPROVAL)

The Chair requested the Council to review and approve the public and full versions of the meeting minutes of Thursday, January 17, 2019 and Tuesday, April 30, 2019.

No changes were made to the minutes of January 17, 2019 and April 30, 2019 meetings. The minutes were approved as presented.

ACTION ITEM:

Carrie S to publish the approved Public Minutes of January 17, 2019 and April 30, 2019 on the ITS website, on the ISC page.

Start of meeting discussion - Isaac S (FOR DISCUSSION)

Recent Incidents – Incident Workgroup

Alex T provided the Council with an updated membership list. He noted that this represents a cross section of faculties and divisions. In terms of incidence, it was reported that compared to the previous year, the number of UTORid compromises with respect to account resets is about the same. He also noted that additional protection measures are currently in place as a result of O365 deployment. Alex T also reported that results from suspicious internal devices are about the same pattern as the previous year. In terms of visibility, he added that there is work still to be done on that front.

In referencing the incident dashboard, it was noted that the common goal is to ensure there is a trend of increased visibility. In addition, the main objective is to provide the numbers that we see within the WG and ITS outwards to faculties and division so that they can respond and can see what is happening in real time. Alex T also noted that the ideal goal is the integration of an incidence response with the service desk so that in the event of a compromise there is a workflow process that take place for issues resolution.

During the discussion, the Council was asked to provide feedback on the following:

- What type of information were they interested in seeing given the range of data that can be generated?
- Is there an interest in having information on cost implications with respect to:
    a) Major incidence, including visibility to major incidences where data has been compromised
    b) Impact on business operation
    c) Fraud in general related to information security?

In response, it was noted that it would be useful to see the following:

- Those trends over time as well as the correlation between suspicious internal devices versus devices that are confirmed to be compromised.
- With respect to phishing and devices, would like to see a breakdown by category and type.
- The Council also requested to see the global perspective trend lines and also what are we measuring against.

It was noted that having the ability to drill down would add an education component to how we communicate this to faculty and staff as they would be able to see a snapshot of the major thing issues at play.

The Council also held a discussion on the ISC's role in responding to incidence response and IT governance. It was noted that the objective is for the ISC to have governance over the program and not on the incidence response itself as there is an operational plan in place. It was also noted that that the goal of the table is to ensure that resources are being advocated for and allocated most effectively to address security issues especially to sectors that incidents are rising.

Alex T also updated that in terms of initiatives a key emphasis of the WG at this point is to identify and formalize investigation process especially for high risk incidence.

<u>CISO Update - Isaac S (FOR INFORMATION)</u>

Isaac S updated the Council on the following initiatives:

- He noted that a lot of work has been done to figure out the current state and work currently underway to track some key substantive risk issues.
- It was noted that one of the most challenging issues is with respect to data repositories. He added that some work being rolled out on data classification and training to address this issue, and this is a big area of focus for the Risk Management team.

In terms of changes to the IS security team and the security landscape across campus it was noted that:

- IT security staffing recruitment was successfully completed for a number of positions and have also started to see positions in the divisions get filled as well.
- Currently looking to build a unified security presence while maintaining the distributed nature of the university. To this end, the three IS Security positions at UTM/UTSC/KPE now have a dotted line reporting to the CISO. They are now actively part of IS team meetings.

Bo W added that he is excited about this and it is consistent with the ITS Strat Plan, IT @ UofT adding that security is a new area for some of these divisions, so building in this way is going to strengthen as we shore up the weakest links.

- Isaac S also noted that a number of students have been added to the team, and this is part of his education mission to start a program to grow talents.

The Council held a discussion on the nation states' threat attribution. It was noted that there is a need to focus on research, as this is a space where it is a big issue. The Chair noted that this is an area of research interest in his Lab. He asked if there is an opportunity for research leading to publication or if this was just internal research to better understand the threat environment. In response it was noted that the focus was on research enterprise and will be done through an operation lens, but from CISO's perspective he is open to any opportunity that will highlights the issues.

The Council also discussed other threat landscapes. It was suggested the Council sponsor a larger conversation on campus. The stated goal would be to lead to a policy which is consistent with the mission and purpose that would give guidance to the University as well as elevate the level of awareness. It was the consensus that the notion of getting academia to talk about this is an excellent idea. The Chair also tabled a number of topics for future discussion at the ISC.

Isaac S also reviewed the CISO's priorities for 2019-2020.

- Noted that procurement activity currently underway for firewall parameter around our network. Expectation is to have this finalized towards the end of the year and have the system installed by the beginning of the year. He added that that this will then be deploy to programs and divisions.
- He also reported on an initiative around the MFA noting that ISEA is currently in the middle of working on three PoCs.
- It was also noted that an external security assessment will be undertaken in November 2019. Plan is to bring in three Higher Ed CISOs to participate in the assessment, one Canadian and two from the US. A report will be produced.

2019-2020 Security Budget (FOR ENDORSEMENT)

Issac S also reviewed the draft budget with the Council noting that request is being made for endorsement of the approach not specifics and that the document is a work in progress.

The Council held discussion how the ISC can support and provide guidance for the process.

NIST CSF- INTRODUCTION:(FOR INFORMATION)

Isaac S provided an overview of the NIST CSG process, noting that the value of this exercise is to try to set the blue line and fugure out the pain-points. He walked the Council through the process.

NIST CSG – Implementation Tier Targets:

Isaac S provided the Council with an overview of Cyber Security Framework. It was noted that he would be using the Self-Assessment program and the Risk Assessment Program to map this to get measurements to determine how we set these targets. He said he wanted:

- To use the ISC to determine how to set these targets as to where we want the university to be as well as to capture different points of view in the input process
- Goal is to take threats and concerns and turn into a profile that can be measured across three areas – risk management process, integrated risk program and external participation. He said it is about how the process is informed by the risk and business needs.
- He added that the proposal for assessment should use broad measures. What makes sense to look at for the institution and then if we like same we see can mature into breaking apart the categories into specific targets. Big division versus single faculties.
- He added that this is to give the Risk Assessment program some directive.

ACTION ITEMS:

- **Isaac to provide a copy of the spreadsheet to the Council**
- **Members of ISC to complete survey and return to Sue M by end of September 27th**

ISC Research Workgroup Terms of Reference and Approach(FOR APPROVAL)

Marden P provided the following status update on the Research WG noting that:

- The WG is still awaiting insights and input from the Granting Council with respect to the university research data management plan.

- It was also noted that a new program, the Centre for Research and Innovation Support, came into being with the mandate to focus on research data, research support and research computing.
- He added that the WG has also taken a step back and reviewed its first principles to ensure that the group's focus is in the right direction. The review also reset the guiding principles.
- The WG met with the CISO and FAS Research to ensure that the group's work fits within the CISO's framework and defined more clearly what they aim to accomplish.

He also updated the Council on the following revised principles:

- To acknowledge the different research requirements and applications across the data classification schema types;
- To recognize the multi-faceted elements of data protection -- the need to protect data themselves, as in preservation/ quality-assurance/ consistency, and also to recognize the specific requirements of research sponsors, funding agencies, and the University;
- The objective is to create a clearinghouse with CRIS and other partners in order to disseminate research data security guidance and practices.

In response to Marden P's question, the Council concurred that the WG was going in the right direction. They requested that the following be added to the guiding principles:

- The requirement to identify data that whose loss may bring reputational risk to the University
- In addition to the legal requirements.

The Council also held a discussion on the type of space for secure data storage, for example, cloud-based, public research data repositories, archival storage, discipline-specific repositories, internal storage facilities. It was noted that the challenge of spreading awareness across the University and the need to add education and awareness capacity for dissemination.

The Council advised that the group focus on two elements of the goals initially and then #5 (these numbers are aligned to the presentation slide presented at the meeting):

1. Work with the research and IT communities to formalize research data management procedures, standards and guidelines;
2. Develop a catalogue of available secure data storage facilities at the University;
5. Working collaboratively with Divisions, Libraries, Centre for Research & Innovation Support, SciNet to deliver research data management and security training to faculty members and support staff.

<u>Committee Term:(FOR DISCUSSION)</u>

This item was deferred to next meeting.

<u>ACTION ITEM:</u>

Deferred to the next meeting.

<u>Any other business - Ron D</u>

Carrie S provided the following update:

- On Wednesday, September 11th Information Security and Education and Awareness will be hosting a booth at the UTSU orientation street fair. This is also open to faculty and staff.
- Cyber Security Awareness Month launches on October 1st . The Information Security team will be hosting events on the three campuses. Activities include panel discussion and lots of event to help university employees learn how to better protect their data and privacy.
- More details to follow.

<u>Adjournment- Ron D</u>

There being no further business to come before the Council, the meeting was adjourned at 4:02 p.m.