Minutes (PV)

Meeting:	**Information Security Council – Meeting # 5**
Date & Time:	**Tuesday, April 30, 2019 (2:00 – 4:00 p.m.)**
Location:	**The Faculty of Applied Science & Engineering, Michael E Charles Council Chamber, GB202, 2nd Floor, 35 St. George Street**

CHAIR

Ron Deibert

ATTENDEES:

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

REGRETS:

Deepa Kundur, Michael Stumm

BY INVITATION:

Sue McGlashan, Marden Paul, Patrick Hopewell, Mike Wiseman

NOTE TAKER:

Andrea Eccleston

Item

Welcome - Ron D

The meeting convened at 2:00 p.m. with Committee Chair Ron Deibert presiding. The Chair welcomed everyone and introductions were made around the table.

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) 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.

The approval of the public and full versions of the Minutes of Thursday, January 17, 2019, deferred for minor grammatical correction.

What are your concerns about Nation-State threats to the University? - Isaac S (FOR DISCUSSION)

The following are discussion highlights:
Divisional IT departments do not have a clear sense of the specific details related to the impact of nation-state cyber security threats to researchers.

- Research is highly decentralized and not part of the Divisional IT departments.
- Divisional IT departments do not have control or authority over labs in terms of how they set up their IT infrastructure. However, I&ITS provide network services.
- It was also noted that some labs are involved in very complex issues, so the concern is related to property; data sets and regenerating data and there is a need to determine what controls should be in place in order to mitigate the risks for divisions and the university at large.
- Beyond scope and capacity have seen no directive from either central IT or Governance.

The Council also discussed if ISC should take the lead or wait for direction to generate this discussion. The following suggestions were made:

- To seek a directive from the office of the VP Research and Innovation regarding controls, they would like to recommend.
- A member suggested that ISC make a recommendation that Governing Council or senior leadership have a conversation on this issue so that Divisional IT departments feel empowered to have these discussions. The highest level at the University needs to be engaged with the policy response.

Council also held discussion on the kind of nation-states concerns facing the University. Isaac S suggested that a high level tactical discussion on this issue would be worthwhile.

ACTION ITEM:
Isaac S to schedule an information session with the ISC to understand where we are currently situated.

CISO Update - Isaac S (FOR INFORMATION)

Isaac S updated the Council on the following initiatives:

- Currently engaged in ongoing work to build a culture and trust through community engagement to determine needs, as well as, what is working or not working.
- Also, assessment of the overall ISEA portfolio currently underway.
- Regarding the ISC, working on effective measurements in identifying our risks, as well as the effectiveness of our programs.
- Also focused on response and prevention as it relates to compromised accounts and phising.

The Council held a brief discussion on compromised accounts and alternative communication channels.

Isaac S also updated that he is working on benchmarking our cyber-security processes and performance which would allow for more effective decision making. Bo W added that the value is that over time this will allow us to see how we have progressed and it would also allow us to have access to comparative statistics from other peer institutions.

In terms of outreach activities, Isaac S updated on a number of tri-campus engagements which include:

- A guest lecture session at the iSchool.
- Also, currently working on vulnerability management with UTM to pilot an Enterprise tool.
- Have also published a Travel Tip sheet which was presented to a number of divisions and several advisory groups
- In addition, work also underway to implement a “burner” travel device program.

He added that he is also looking for other creative opportunities to get out into the community as there is a high level of interest at all levels in information security and people are very excited to talk about cybersecurity.

Isaac S also updated the Council on a number of top priorities. He said that he is also working with the ISC Work Groups to focus on how to effectively engage as community representatives to do tactical, functional and meaningful work to change security posture in the University.

ISC Working Groups Decision Making Process & the role of the ISC’s - Ron D (FOR DISCISSION)

The Chair introduced the topic of the decision-making process of the ISC and how members envision the authority of this body. Ron D said there is a need to establish some clarity regarding the procedures as it relates how the Council decides collectively whether to proceed with the recommendations of the Working Groups.

Council held a discussion on the following questions:

- Does decision ultimately resides with the ISC or to another group?
- If it is an ISC decision, what is the approach to arrive at a decision? Is it by consensus, a majority vote or something else?
- Are ISC members prepared in advance with the proper information to form decisions?
- How to make timely decisions to not delay significant implementation?

Council also discussed what constitutes quorum for the ISC and other procedural matters. It was noted that there is a need to define quorum and create some rules as there will be issues in the future which will be contentious that require debate. Council to determine implementation timeline.

Council also requested that meeting materials for the ISC should be pre-circulated 1 week in advance of meetings.

ISC Working Group Asks:(FOR APPROVAL)
Incident Response Planning Ask: High-risk phishing response

Patrick H provided the following update on the IR Working group highlighting a number of key activities which include ongoing work to define categories for an incident response as well update to the incident intake webpage which is expected to be completed shortly. He also updated that the IRP-WG have also undertaken table-top exercise, which explored different scenarios. These will be made available to groups across the University in a “train the trainer” format so that other groups can go through the same process. A full incident playbook is also being developed.

Patrick H also submitted a proposal for the Council’s approval to have a process in place to pull phishing emails from mailboxes. The Council held discussion on the tools, approval process and the timeline.

DECISION:
After discussion, the Council moved to approve the proposal to have a process in place to pull phishing emails from mailboxes. All in favour.

ISC Working Group Asks:(FOR APPROVAL)
Procedures, Standards and Guidelines Ask: Data Classification

Mike W reviewed the proposed Data Classification definitions noting that this is a revised version from the document presented at the October 24, 2018, ISC meeting. He said that the current document includes input from the ISC and other stakeholder groups. It was highlighted that most of the community will not have to make decisions based on which category to use and over time there will be maturity on how these data classifications are applied.

Mike W also submitted a proposal for the Council’s approval of The Procedures, Standards and Guidelines working group for a five-tier data classification schema. The following are the discussion highlights and comment:

- A member asked how this would impact faculty, especially for research data. A suggestion was made that a significant educational campaign was necessary.
- Council also suggested some textual improvements and the need to clarify the wording in the explanation section of “Category 2” regarding the kind of data.

DECISION:
After discussion, the Council moved to approve the proposal for The Procedures, Standards, and Guidelines working group five-tier data classification schema. All in favour.

Procedures, Standards and Guidelines Ask: Multi-Factor Authentication for high risk data

Mike W also reviewed the proposed data classification levels and controls with Council noting that approval of the MFA is required for category 4 data and recommended for category 3 data. He submitted a proposal for approval of The Procedures, Standards, and Guidelines Working Group requests approval for the following controls:

- Multi-factor authentication is required to be used when accessing data classified in Data Classification category 4
  and
- Multi-factor authentication is recommended for use when accessing data classified in Data Classification category 3.

Isaac S noted that this approval will enable the PS&G working group to have a technical plan. Group will report back and provide progress report. It was also noted that the actual technology is still to be determined.

DECISION:

After discussion, the Council moved to approve the proposal for the following controls: Multi-factor authentication is required to be used when accessing data classified in Data Classification category 4 and Multi-factor authentication is recommended for use when accessing data classified in category 3. All in favour.

ISC Working Group Asks:(FOR APPROVAL)

Education and Awareness:

Input: Goal to have information security awareness included in training for faculty and staff. Ask: Phishing awareness for staff

Mike W submitted the following proposal of The Education and Awareness Working group that the following statement be approved by the Council. “The Information Security Education and Awareness working group recommends that information security awareness is included in training for staff and faculty. Learning opportunities in information security awareness should also be offered to students”

The following are the discussion highlights and comments:
The Chair noted that wording should be adjusted to “The Education and Awareness working group strongly recommends that……”   It was also noted that there is a need to get specific as it helps with accountability and a good directional statement would make it more effective. The Council also suggested that the Education and Awareness Chair have the group determine what aspirational goal they want to achieve for the current and future years.

A suggestion was made that there is a need to publicize these decisions and to get them written up into different forums.

ACTION ITEM:

Bo W to take the recommendation to HR&E as well as to the group that handles faculty training to have this embedded in their onboarding activities. It should also be noted that this is what the ISC would like to see as the mandate moving forward.

Mike W/Carrie S to amend the document to read “strongly recommend including all ongoing training and orientation for staff and faulty”. If this is not happening, ISC can call it out.

DECISION:

After discussion, the Council moved to approve the proposal for The Education and Awareness Working group statement:
“The Information Security Education and Awareness working group strongly recommends that information security awareness is included in training for staff and faculty. Learning opportunities in information security awareness should also be offered to students.” All in favour.

Committee Term - Ron D (FOR DISCUSSION)

This agenda item has been deferred.

ACTION ITEM:

To be added to the Agenda for the next meeting.

Any other business - Ron D

None

Adjournment- Ron D

There being no further business to come before the Council, the meeting was adjourned at 3:57p.m.