The Aftermath of a Crypto-Ransomware Attack at a Large Academic Institution

Leah Zhang-Kennedy
University of Waterloo, Stratford Campus

Hala Assal, Jessica Rocheleau, Reham Mohamed, Khadija Baig, **Sonia Chiasson**
Carleton University

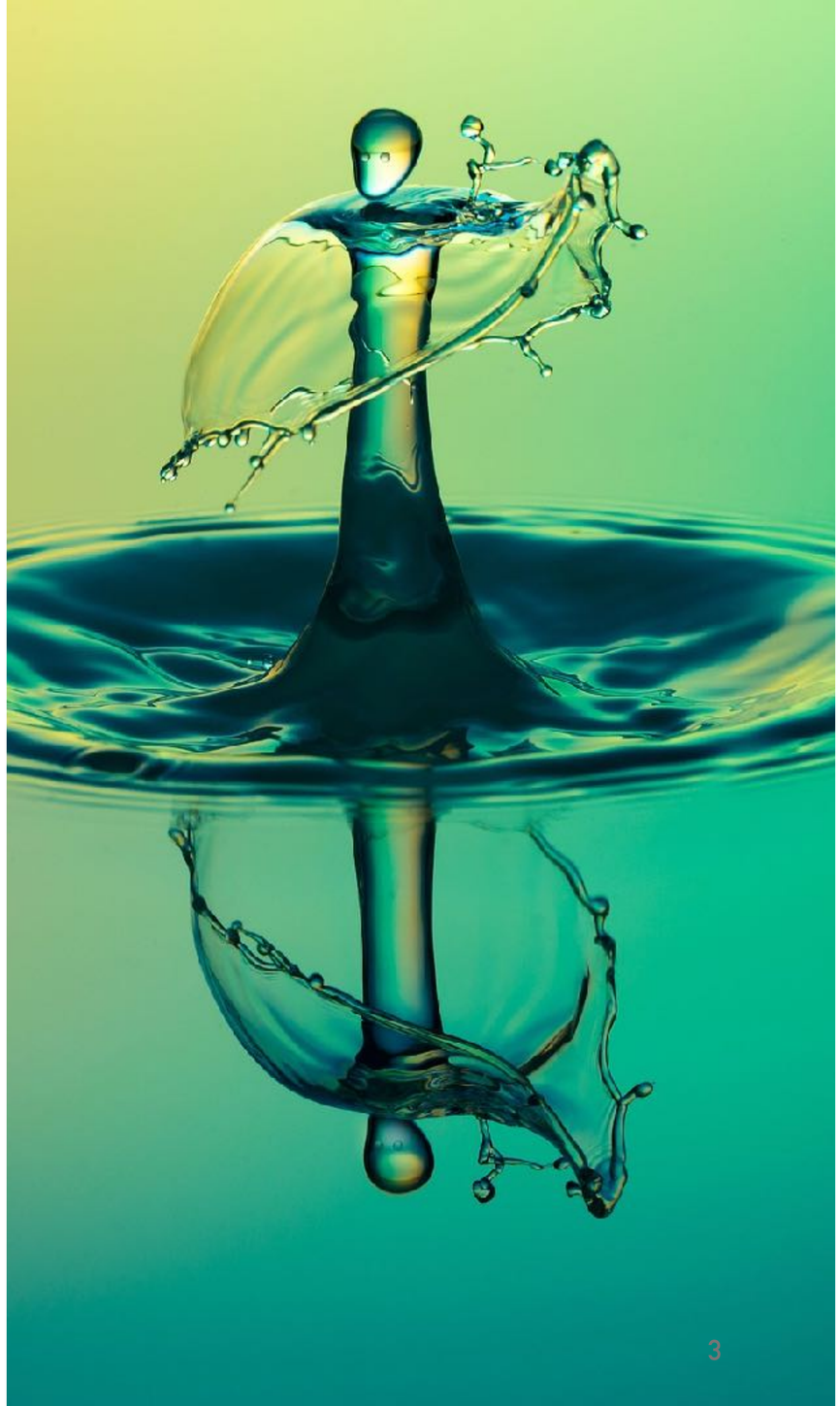
We had the (un)fortunate opportunity to witness the immediate aftermath of a significant ransomware attack at a large university...

here's what happened...

“

We are experiencing...

'a network interruption'



Our aim was to **understand** the immediate and longer-term impact of this incident on end-users to **learn** how organizations can better prepare and respond

UNDERSTAND WHAT HAPPENED

SURVEY METHODOLOGY

- 150 participants
  - faculty (13%), staff (31%), students (38%), undisclosed (18%)
- Collected within 6 weeks, ~30 min per survey

- Questions
  - pre/post attack security practices
  - behaviours, thoughts, emotions during the attack
  - impressions of how the situation was managed
  - areas for improvement of emergency protocols

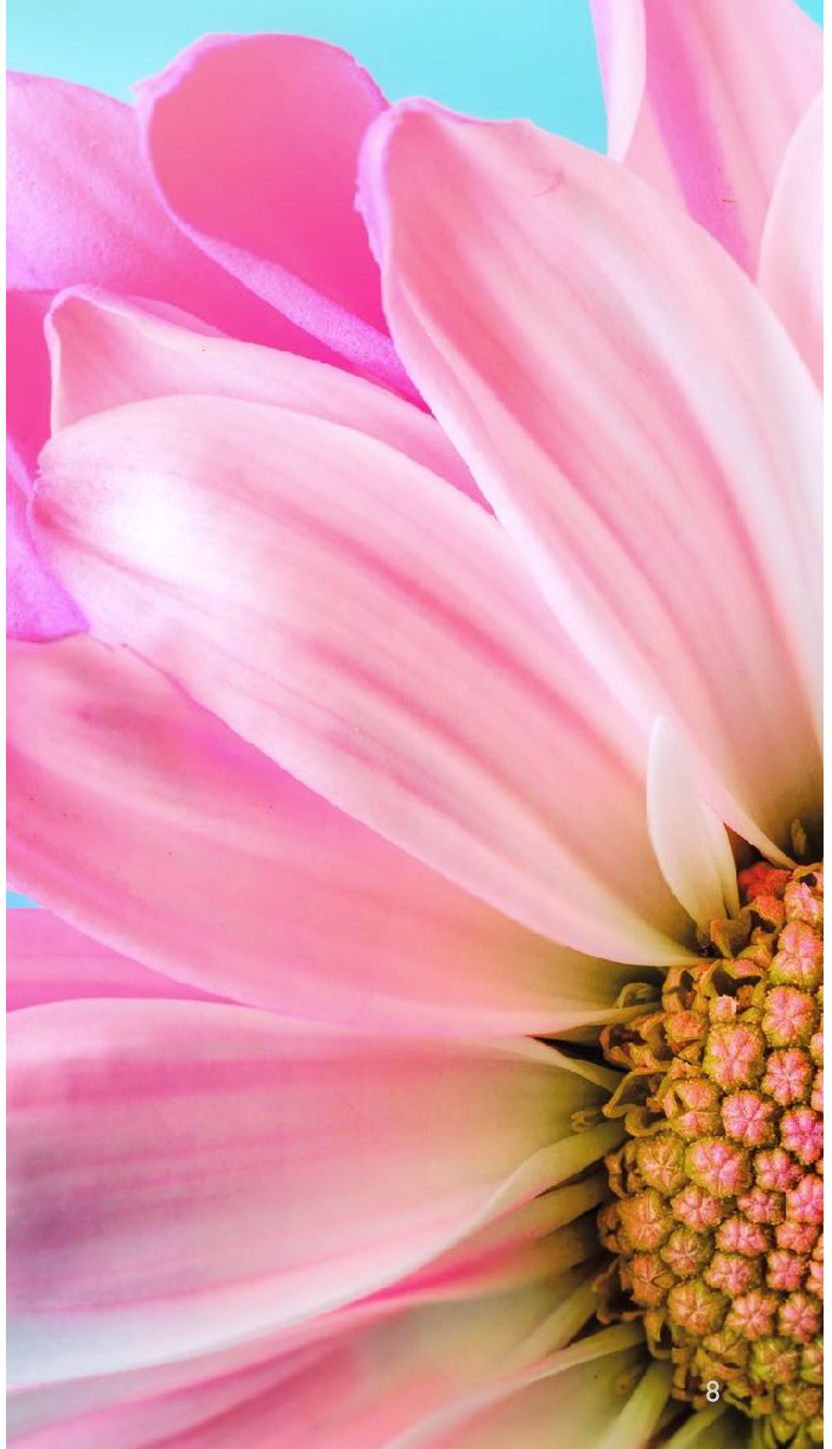
INTERVIEW METHODOLOGY

- 30 participants
  - faculty (3), staff (13), students (14)

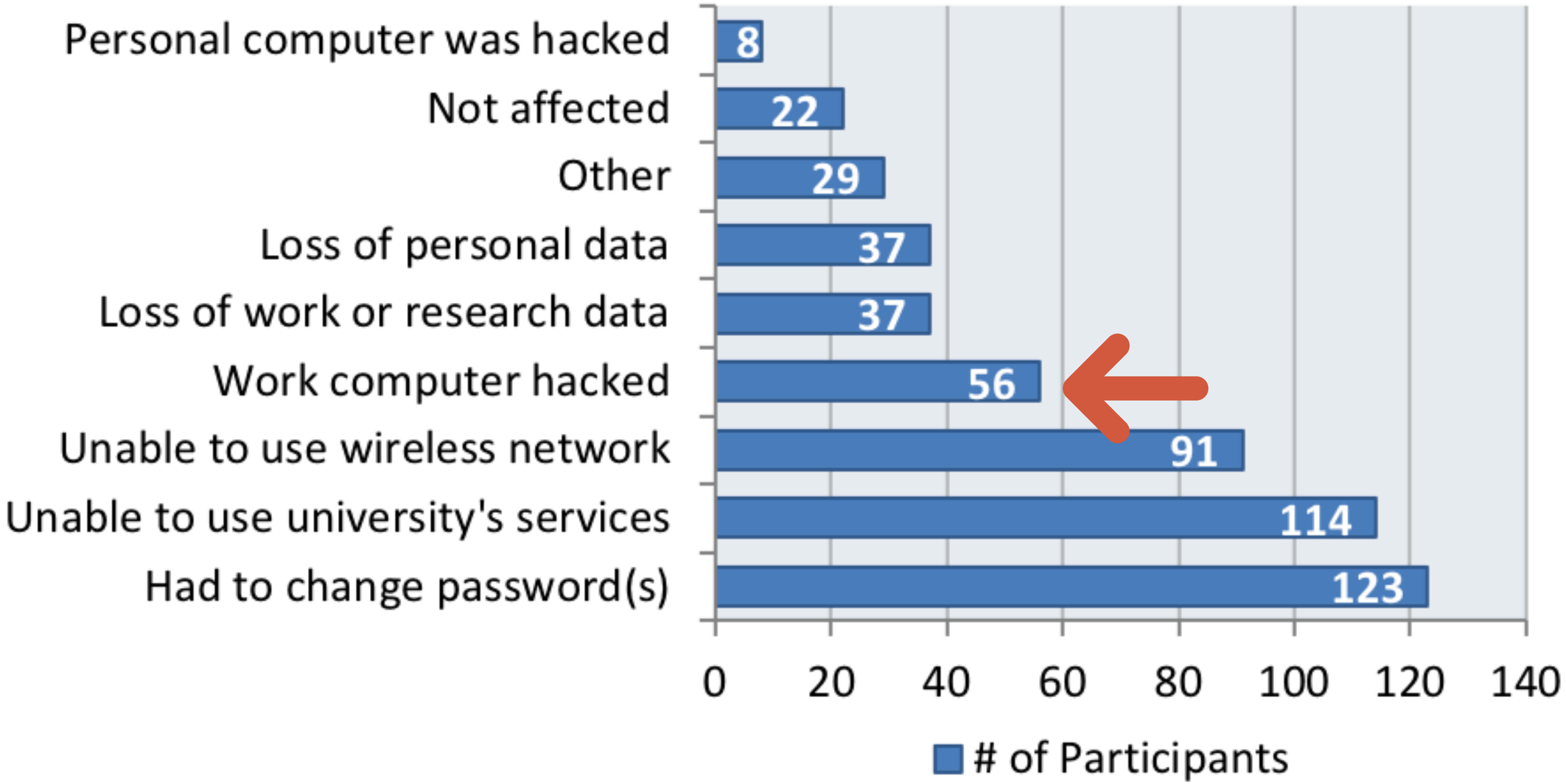
- Collected within 6 weeks, ~60 min interviews

- Questions
  - pre/post attack security practices
  - attitudes and experiences with the attack and emergency protocols
- Inductive thematic analysis

RESULTS



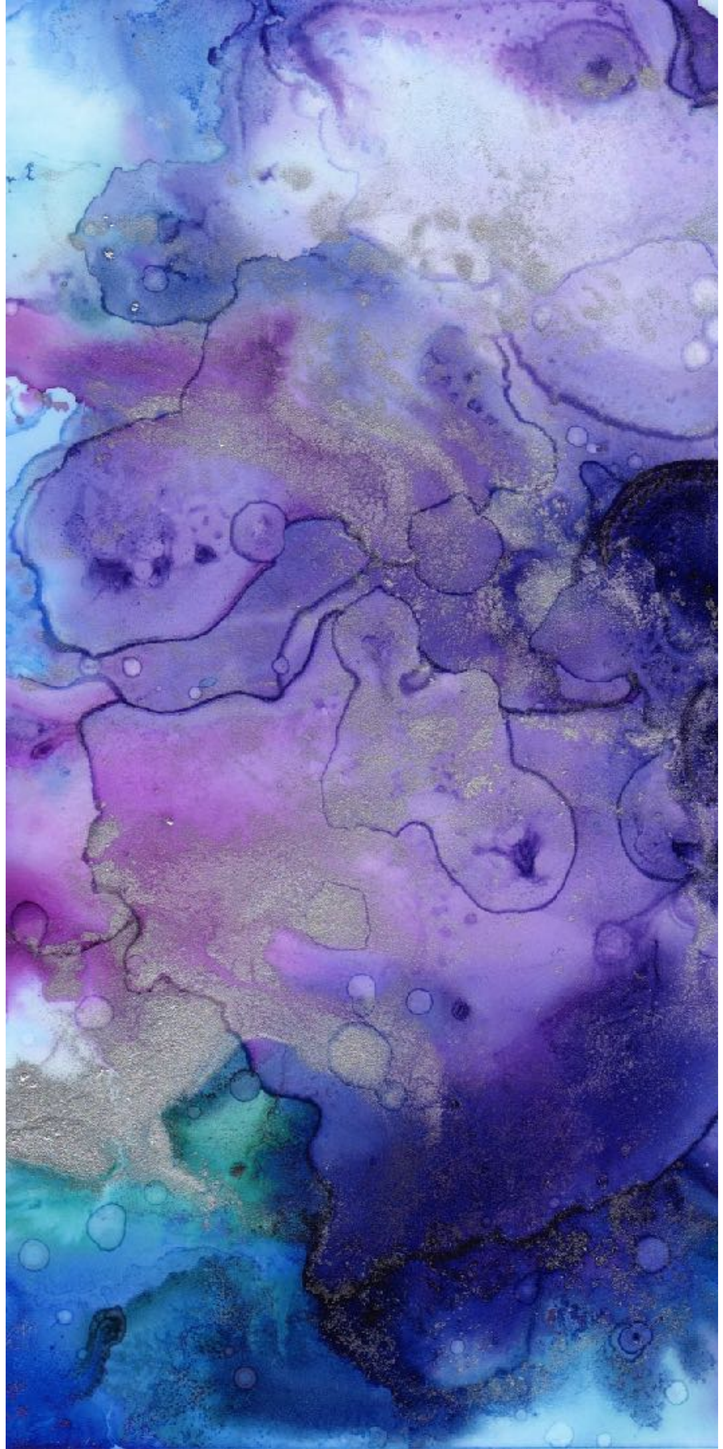
1. TECHNOLOGICAL & PRODUCTIVITY IMPACT



“

Pretty much everyone was impacted in some way [...] whether it’s being not able to use a computer or not being able to use some service

- Staff



“

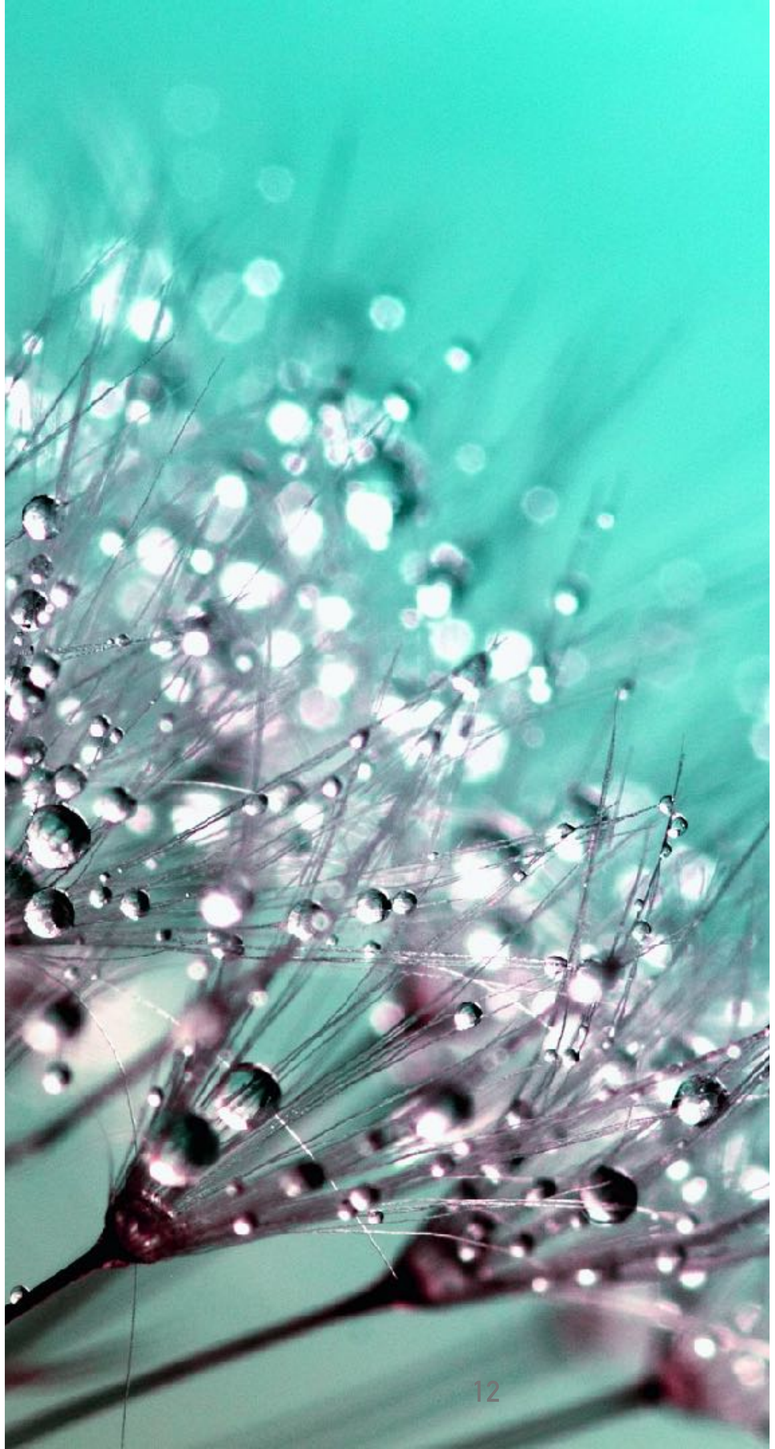
That’s all my work there, about fifteen years of work [...] But then it slowly started turning all the files into encrypted files at home as well, and then I realized this thing was not going to stop until it had done them all.

- Faculty member

“

Even now I still run into issues... just when I need things, all of sudden it is not working properly [...] Your work days are interrupted and you are not working at the same pace or being able to accomplish as much.

- Staff



2. PERSONAL AND SOCIAL IMPACT

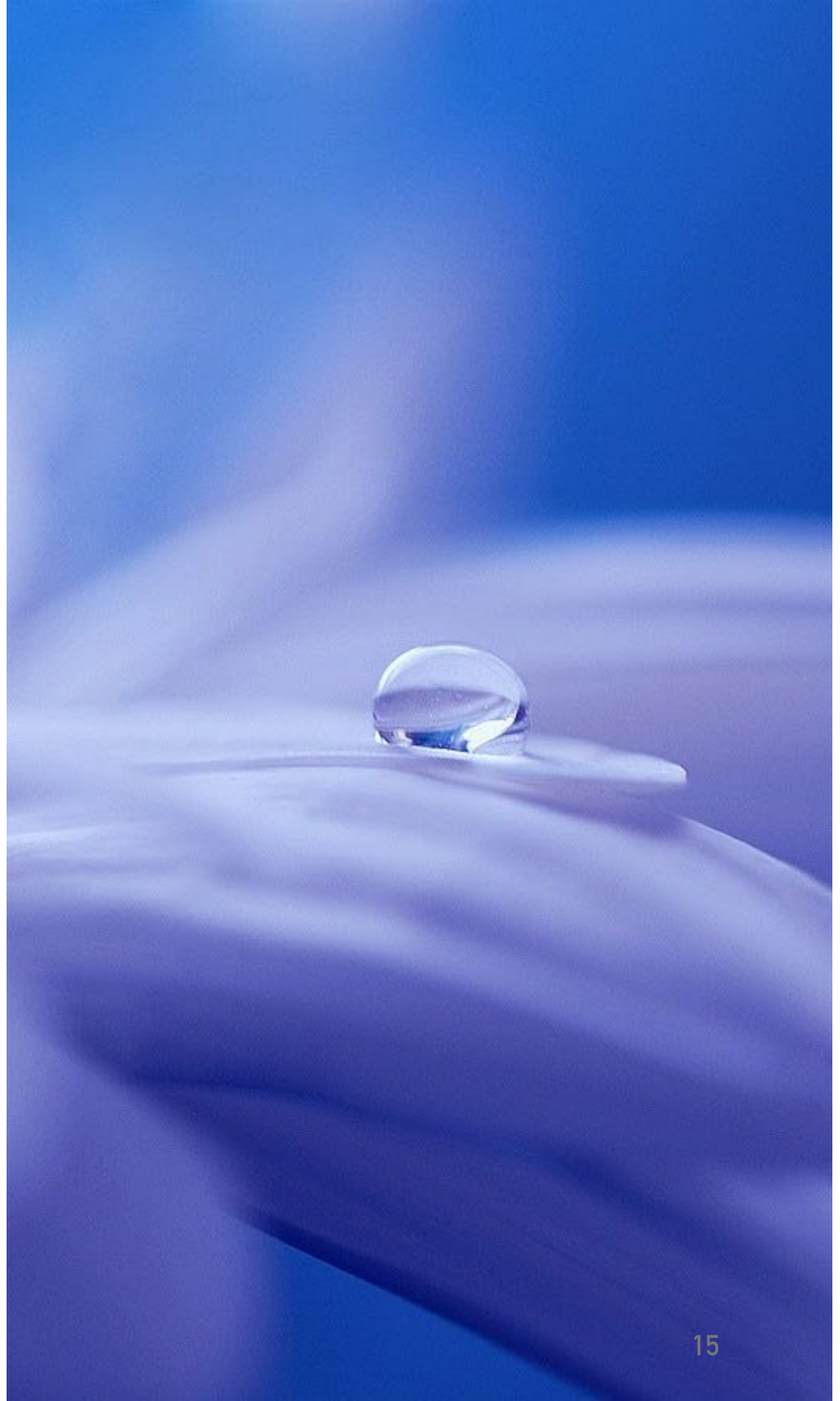
- Worried/concerned (n=52)
- Upset/angry/disappointed/insecure (29)
- Frustrated/annoyed (27)
- Shocked/surprised (27)
- Feared
  - data loss (51)
  - loss/theft of personal & financial data (38)
  - lost productivity (27)
  - further infection (17)

> I coincidently had a doctor's appointment around that time and my blood pressure was really high. . . I was anxious about the fact that I lost work and people weren't able to email me, then there was a whole rush of people that needed to talk to me, and I was anxious about [catching up].
>
> - Staff

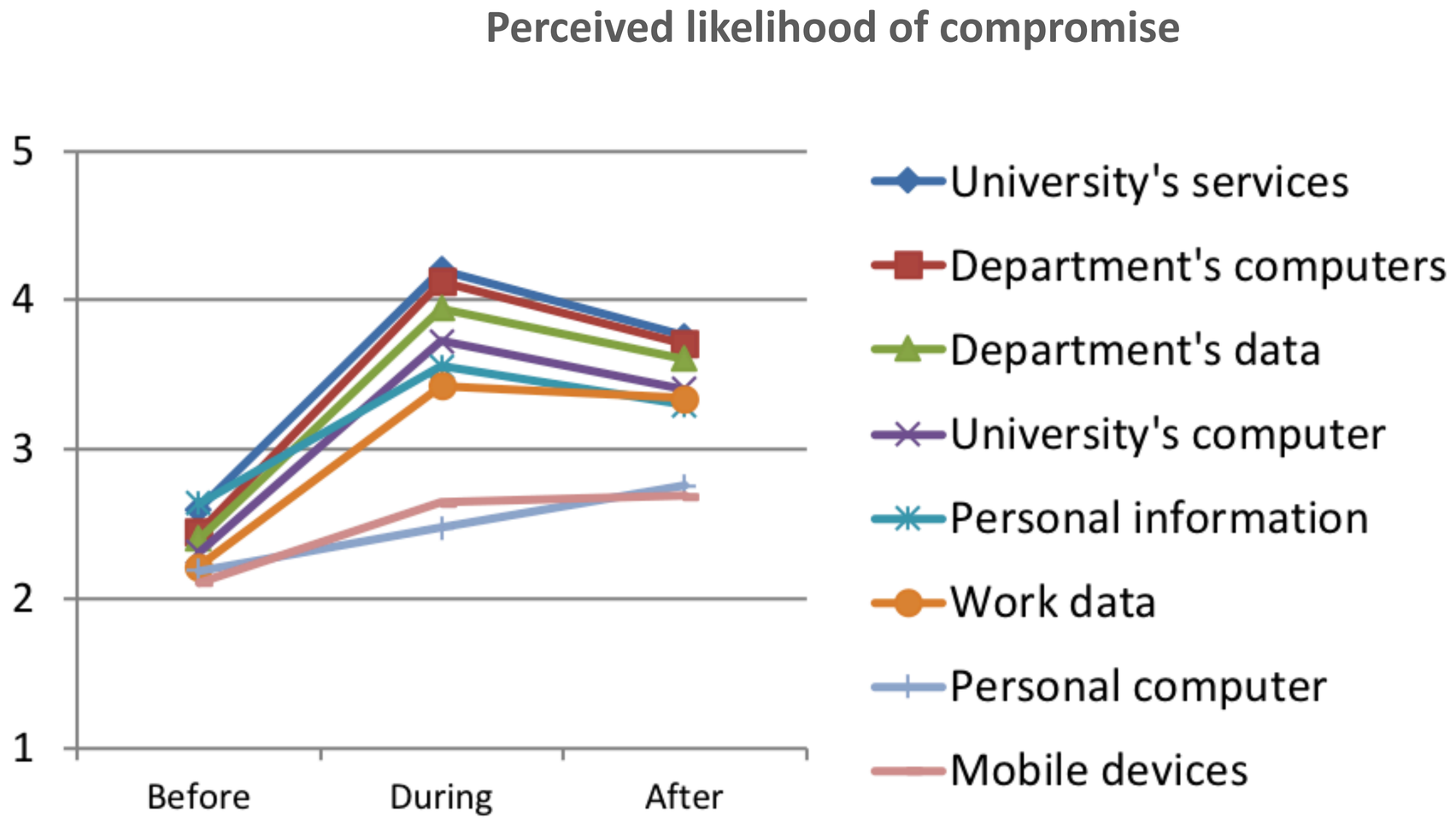
“

It was kind of like we didn’t have a role in this situation. We were just the people that were affected and [we should] stay out of the way

- Grad student



3. RISK PERCEPTION AND SECURITY PRACTICES



4. COMMUNICATION

- Only 12% were first notified through official channels.
- Relied on word-of-mouth, social media, news
- Only 10% thought the university handled the incident well.

- Wants:
  - clear details about the problem
  - consistent instructions
  - frequent updates

“

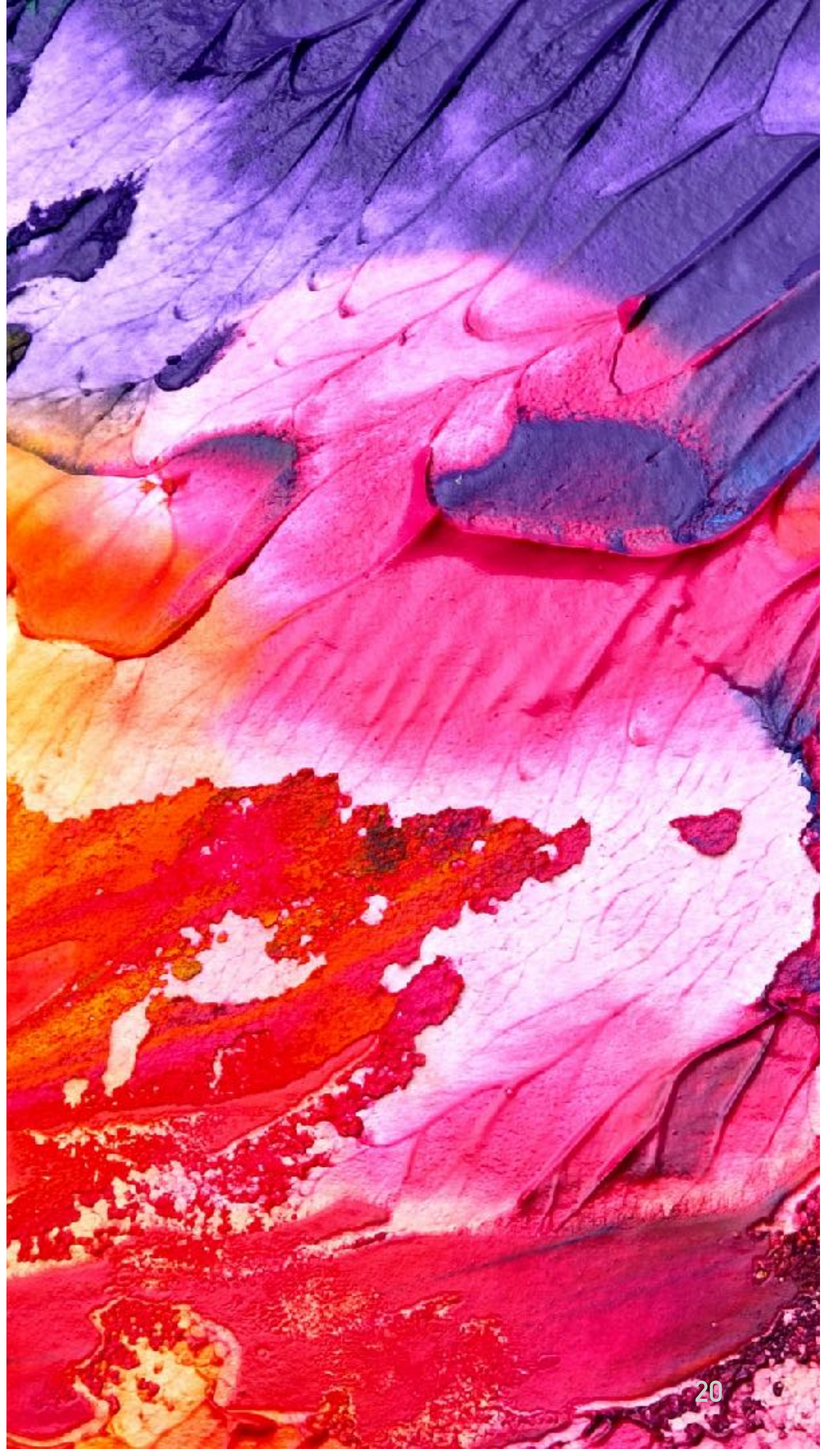
Communication is key. If you’re not telling people what is going on, that is creating a whole other level of panic

- Staff

“Still to this day to be honest, I don’t feel like there was ever an end. There was [notifications] like ‘we are working on the situation [...] Ok you can connect again’. It was never like ‘It’s over.’ So it’s all very much like it’s never really ended”

- Grad Student

WHAT DID WE LEARN?



1. Share the plan

2. Communication is key

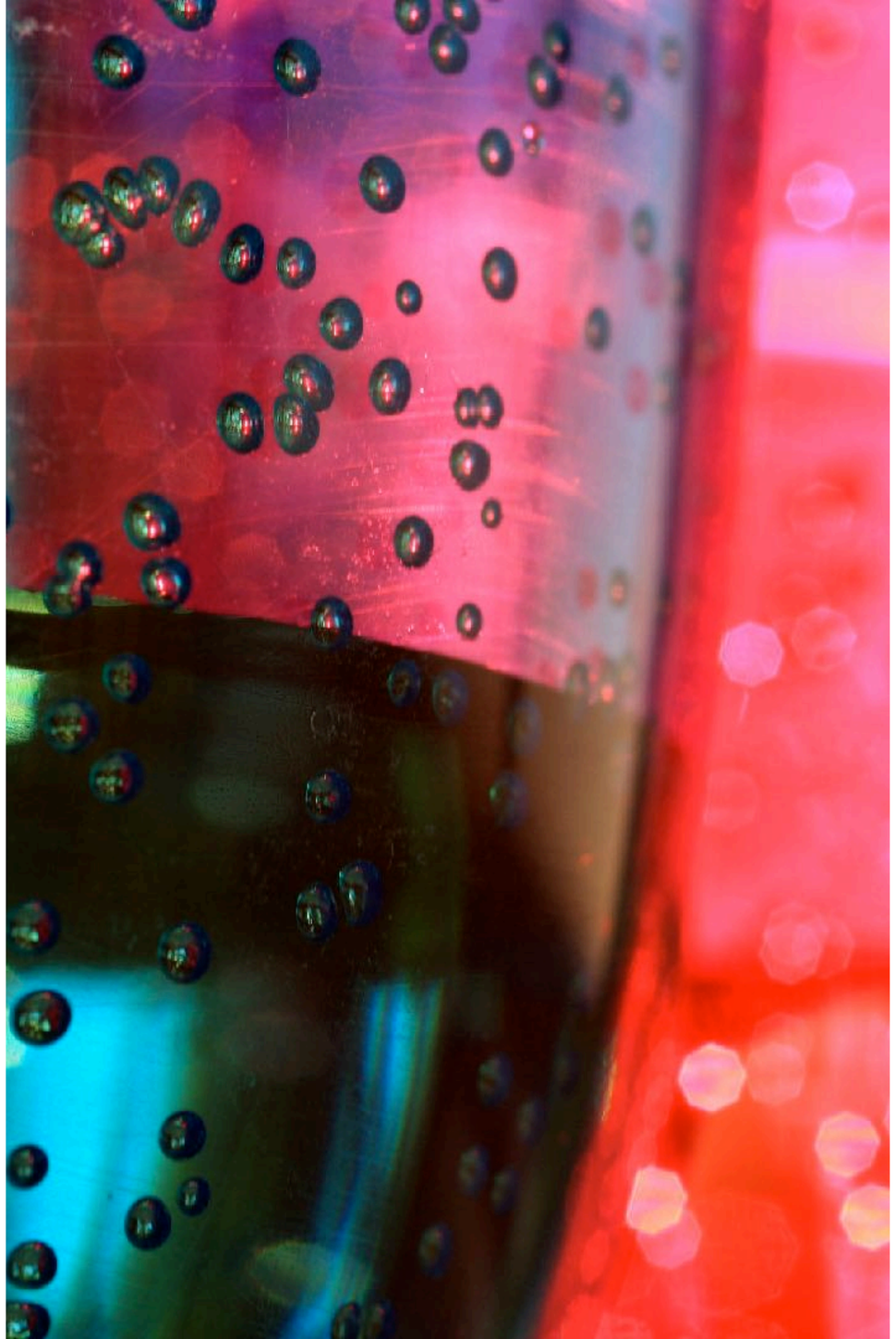
3. Give victims a voice

4. Practice user-centric security

5. Offer user-centric training

6. Provide user-centric data storage

CONCLUSION



QUESTIONS?

Sonia Chiasson

chiasson@scs.carleton.ca

Our lab:

http://chorus.scs.carleton.ca