The aftermath of a crypto-ransomware attack at a large academic institution

Leah Zhang-Kennedy[1], Hala Assal[2], Jessica Rocheleau[3], Reham Mohamed[4], Khadija Baig[5], and Sonia Chiasson[6]

[1]*University of Waterloo, Stratford Campus, Canada*
[2-6]*Carleton University, Ottawa, Canada*

Abstract

In 2016, a large North American university was subject to a significant crypto-ransomware attack and did not pay the ransom. We conducted a survey with 150 respondents and interviews with 30 affected students, staff, and faculty in the immediate aftermath to understand their experiences during the attack and the recovery process. We provide analysis of the technological, productivity, and personal and social impact of ransomware attacks, including previously unaccounted secondary costs. We suggest strategies for comprehensive cyber-response plans that include human factors, and highlight the importance of communication. We conclude with a *Ransomware Process for Organizations* diagram summarizing the additional contributing factors beyond those relevant to individual infections.

1 Introduction

In the Fall of 2016, a large North American university was subject to a crypto-ransomware attack. The attack occurred just before the start of the exam period and coincided with major national scholarship application deadlines. The malware compromised Windows computers accessible from the university's main network during off-hours, infecting computers that were powered on and propagated through the network overnight.

Exact details of the attack were never made public (and cannot be disclosed here), but the attack impacted many computers belonging to research groups, academic departments, and all levels of university services.

Initially described by the university as a "network interruption", most of the university's computer systems were temporarily shutdown or taken offline to contain damage. The university did not pay the demanded ransom of 39 bitcoins (approximately $38,000 at the time) to release the encrypted files.

Immediate recovery efforts took several days, with the productivity impact being felt by users for weeks post-attack.

Most current ransomware falls under one of two general categories: *lockers/blockers*, which focuses on disabling resources such as denying access to the device, and *crypto*, which encrypts data files on the infected device and withholds access to the decryption key. In both cases, the attackers request ransom to regain access [19, 38]. In this paper, we primarily concentrate on crypto-ransomware, as was used in this incident.

There is a significant rise in ransomware infections within organizations [18, 29]. Given the prevalence of this threat, it is critical that we understand its impact on organizations. The technical tasks in the aftermath of such an attack such as containing the threat and returning the systems to a functional state are clearly of vital importance, but an attack of this scale also has significant impact on the individuals within the organization. Our aim was to understand the immediate and longer-term impact of this incident on end-users in hopes of learning how organizations can better prepare and respond. As researchers, we were not involved in the recovery efforts; our intention was to learn from the incident as third-party observers, not to assign blame or criticize. Rarely do we have the opportunity to conduct research studies with a large number of victims of cybercrime in the immediate aftermath of the incident; we believe that the time-sensitive data collected here offers valuable insight.

We conducted a survey with 150 respondents and interviews with 30 affected students, staff, and faculty to understand their experiences during the attack and the recovery process. Our main contributions are: (1) analysis of the technological, productivity, and personal and social impact of ransomware attacks, including previously unaccounted secondary costs, (2) strategies for the development of a comprehensive cyber-response that include human factors and highlights the importance of communication, and (3) a refined *Ransomware Process for Organizations* diagram summarizing the additional contributing factors beyond individual infections.

2 Background and Related Work

Although the first instances of ransomware can be traced back approximately 30 years, the surge in modern ransomware began in 2005 [19, 33], with a dramatic increase in prevalence [27] and research attention since 2015. A 2018 literature survey and taxonomy by Al-Rimy, Maarof, and Shaid [2] offers a recent overview of the research landscape, while Scaife, Traynor, and Butler [35] present a great introduction to the subject.

Technical Efforts: Most of the research has focused on the technical aspects of ransomware. Several proactive or preventative techniques have recently been been proposed, such as UNVEIL [20], ShieldFS [8], CryptoDrop [34], and PayBreak [22] which operate at the operating system and filesystem levels to detect and correct suspicious activity, or FlashGuard [16], which uses the firmware-level recovery properties of solid state drives (SSD) to recover without explicit backups. Among others, some have worked on improving detection by devising new techniques for identifying obfuscated binaries [26] and for automated behavioral analysis to extract footprints [7] to identify ransomware and other malware.

Organizational Considerations: If the malware is *correctly* implemented, recovery once systems have been infected is largely a matter of re-imaging and restoring from backups [35] since decryption is infeasible. Even if successful, this process is usually slow and painstaking [40, 41], and is only as reliable as the latest backups. It can leave organizations with significant downtime, productivity loss, and revenue losses [24, 29]. According to Sophos, the median cost to organizations for recovering from a ransomware attack in 2017 was US$133,000 [38]. Kaspersky Labs [18] report that 47% of medium-sized business spend several days to restore access to encrypted data and 25% spend several weeks.

In the absence of backups or if the backup files are also encrypted, the victim may have little choice but to pay the ransom in hope to that decryption key will restore the affected files. The decision of whether to pay the ransom is contentious [9,24]. Statistics relating to how much and how often victims pay the ransom are unreliable given that there is no onus to report such actions. Estimates range from 25% to 65% [10, 15, 29]. Organizations are increasingly targeted, particularly by malware designed to quickly spread across networks, and are proportionally being demanded to pay larger ransoms [29]. The most common expert advice to organizations is to not pay the ransom [9, 10, 17, 24, 31], but others suggest that paying the attacker may be worth the risk since, without the decryption key, organization could further suffer from lost productivity and expenses spent on recovery [41].

Human Involvement: Other work highlights that ransomware prevention, mitigation, and recovery require a socio-technical approach including active involvement of users through appropriate security practices [37]. Luo and Liao [23] recommend that prevention of ransomware threats in organizations should focus on awareness education for both upper management and employees.

In a personal account of dealing with ransomware [3], Ali defined a "ransomware process" that starts with infection and the victim recognizing the problem through the loss of functionality/data. The victim decides whether to pay the ransom, leading to functionality/data being returned or possibly lost for good. In some cases, the attackers offer an extension or increase the ransom, returning to the payment decision process. Although this is a good general illustration of the ransomware response process, this simplified decision tree does not take into account ransom decisions made by business and organization and how end-users fit within this process.

While there are clear human consequences to ransomware attacks, research including users is limited. Redemption [21], a recent OS protective mechanism requiring user input on whether to terminate suspicious processes was found to have acceptable usability. Forget et al. [12] describe the circumstances surrounding a ransomware infection observed during a longitudinal study, but this was not the focus of their work.

Shinde et al. [36] conducted a survey with 23 Dutch end-users and interviews with 2 ransomware victims. Their results suggest that payment by victims to attackers is very low due to the victims' distrust of the attackers. Furthermore, poor technical knowledge of the payment methods may create barriers for victims intending to pay the ransom. Additionally, the survey suggests low awareness of ransomware in corporate settings and that users rely on IT departments for malware prevention and attack response. In reality, however, interviewed victims relied on colleagues for help and continued to be unaware of possible mitigation strategies after the attack. The study offered an interesting preliminary look into end-users' experiences and perceptions of ransomware, but a larger sample size is needed to confirm the results.

Given the limited research involving users, we seized this opportunity to collect time-sensitive data in the immediate aftermath of a 2016 ransomware attack.

3 Our Approach

We conducted two studies to understand the impact of this attack on end-users: an online survey with 150 participants ("respondents" hereafter) and interviews with 30 participants ("interviewees" hereafter) who were personally affected by the attack. Participation was open to all university students, staff, and faculty members.

Participants were recruited through posters, emails, and social media. The purpose of the study was dis-

closed as "to understand the effects of the campus-wide 'network interruption' on the university community". To ensure accurate recollection of the events, we collected data within six weeks of the initial attack. Both studies were cleared by our institution's Research Ethics Board.

4 Survey Methodology

We conducted an anonymous online survey, hosted by Qualtrics^{TM} with 90 females and 60 males ($n = 150$), having an average age of 35.6 years. Respondents consisted of students (38%), university staff (31%), and faculty members (13%) from a wide range of academic backgrounds; 25% of respondents have a technical background. Most respondents (77%) used devices with a Windows operating system on campus; some used Mac (13%), Linux (8%), or other types (2%) of systems.

We iterated the survey questions and pilot tested them with colleagues. The survey (see Appendix B) consisted of multiple choice, 5-point Likert-type questions, and open-ended questions. It reconstructed and retroactively assessed participants' thoughts, emotions and behaviours during the attack; their post- and pre-attack security practices; and their impressions on how the university managed the situation and how its emergency protocols for cyber-attacks can be improved. The survey was done on a volunteer basis and took approximately 30 minutes—they were not compensated for their participation.

The researchers summarized quantitative responses using descriptive statistics. We verified that the skewness and kurtosis was within ± 2, which are acceptable values for normal univariate distributions [11]. Additionally, we tested whether there are differences in the data collected from respondents with and without technical backgrounds. Responses to open-ended questions were analyzed using Inductive Qualitative Analysis [6]. During the round-1 of coding, one author open-coded qualitative survey data. Codes were identified based on an inductive approach where the meaning of the codes are strongly linked to the data [30]. For example, one respondent described how he felt after finding out about the attack: "I was pretty upset that [the university] had not communicated the issues through email or a website update". The response was initially coded as *Upset*. During round-2 of coding, two authors worked together to review and refine the codes, merging codes with similar meaning. For example, Round-1 of coding of a question about prominent feelings during the attack generated 19 codes, which were later reduced to 15 after Round-2. For instance, the code *Upset* was merged with *Angry* to create the concatenated code *Upset/Angry*. After assigning the codes, they were treated like other nominal or categorical data. Where appropriate, the frequencies of different responses were counted and reported.

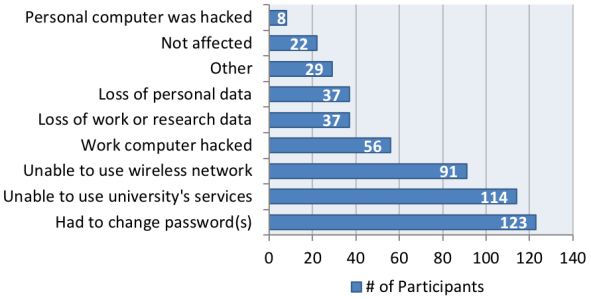

Figure 1: Technological impact on individuals.

5 Survey Results

When reporting the survey results, Likert-scale data is presented with means and standard deviations, where 5 = most positive and 1 = most negative.

5.1 Impact

We inquired about the direct impacts of the incident to gain a sense of the magnitude of the event. We note that this was a voluntary survey and users who had been directly infected were probably more likely to respond.

Technological impact: Figure 1 summarizes the reported effects of the attack on users. Most severely, 43% of respondents reported that their work ($n = 56$) and personal computers ($n = 8$) had been infected, and the majority reported disruptions of varying severity; only 15% ($n = 22$) were reportedly unaffected by the incident. In total, 31% ($n = 47$) of respondents said they experienced some type of data loss during the attack, which 25% ($n = 37$) are personal or work related: 16% ($n = 24$) were able to recover it through backups and 15% ($n = 23$) experienced permanent data loss. Restoring access to essential services/computers reportedly took more than three days for the majority 64% ($n = 96$) of respondents; however, 25% ($n = 37$) had services/computers restored within a day and 12% ($n = 18$) did not lose access at all or did not use the affected resources and services. We also asked respondents to estimate the magnitude of the attack. Responses highlight some of the confusion surrounding what was really happening on campus. Estimates ranged from 5 to 50,000 infected computers, with a median response of 500.

Personal and social impact: Other impacts on respondents included the loss of productivity and time for restoring files and resources, and emotional effects, such as stress. Figure 2 captures the emotional impact of the attack on respondents as summarized from an

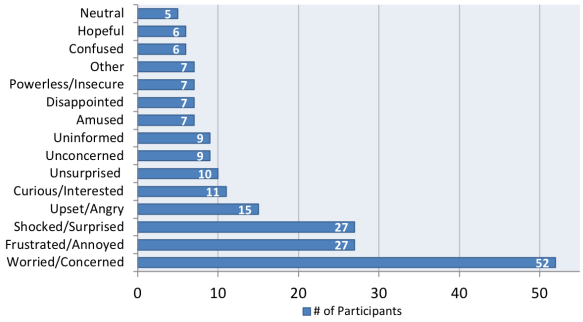

Figure 2: Prominent emotional impact on individuals.

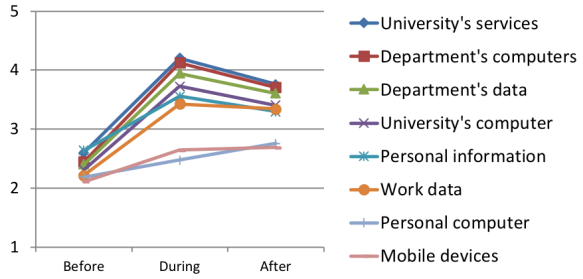

Figure 3: Mean perceived likelihood of compromise for resources at three time points. (5 = most likely)

open-ended question. Prominent feelings evoked by the cyber-attack were "worried" and "concerned" about personal and work data, "frustrated" and "annoyed" about the loss of productivity and poor communication, and "shocked" and "surprised" that a large university could be breached. Respondents said data loss was their greatest fear during the attack ($n = 51$). This is followed by the fear of unauthorized access or theft of personal and financial information ($n = 38$). Some were concerned about negative consequences of lost productivity ($n = 27$), such as missing deadlines, and others worried about infected/encrypted computers ($n = 17$).

5.2 Risk Perception

One side-effect of such incidents is individuals' shaken confidence in the organization and increased risk perception. When asked, 57% of respondents ($n = 86$) believed the university could have prevented the attack. Most respondents said they were not worried about cybersecurity attacks before the incident ($M = 2.5$, $SD = 1.2$), but their worry increased after the attack ($M = 3.5$, $SD = 1.1$).

We now report on a series of questions relating to respondents' risk perception before, during, and after the attack. Respondents felt least vulnerable before the attack, followed by a sharp spike in concern during the attack. In the weeks following the attack, the level of concern dropped but respondents remained wary or unsure, pointing to the lingering effects of such incidents.

Likelihood of compromise: We first asked about the likelihood of compromise for various services, data, and computers, on a scale of 1 = very unlikely to 5 = very likely. Results are summarized in Figure 3. Before the attack, all services, data, and resources were perceived as unlikely to be compromised ($M = 2.1$ to 2.6). Naturally, the perceived likelihood of compromise was highest during the attack ($M = 2.5$ to 4.2), with all university resources perceived as vulnerable. The perceived risk reduced somewhat after the attack ($M = 2.7$ to 3.8) but remained above neutral for all university resources. The two resources not managed by the university, mobile devices and personal computers, were considered least vulnerable, suggesting that respondents attributed the increased risk directly to the organization's resources as opposed to generally increasing their wariness.

Prior work on users' computer security behaviour in an organizational context suggests that users' behaviour relating to secure choices is based on users' perception of the risk [4, 28]. In this incident, respondents viewed the attack and associated risks as directed at the university rather than individual users. The implication of the perceived negligible risk to individual users suggests that large-scale cyber-attacks on organizations may not significantly change end-users' security behaviour in the long term. We elaborate on the effect of the attack on end-users' security behaviour in Section 5.3.

Confidence in security measures: Respondents' confidence in the university's ability to protect their data on the university network was somewhat confident before the attack ($M = 3.8$, $SD = 1.1$), doubtful during the attack ($M = 2.5$, $SD = 1.2$), and nearly neutral ($M = 2.8$, $SD = 1.3$) post-attack. Following a similar pattern, respondents felt secure connecting to the university's wireless network before the attack ($M = 4.0$, $SD = 1.1$), insecure during the attack ($M = 2.1$, $SD = 1.1$), and neutral post-attack ($M = 3.0$, $SD = 1.2$).

To mitigate risks, respondents said they were likely to follow the security advice from the university's computing services; and this remained largely constant before ($M = 3.9$, $SD = 1.1$), during ($M = 4.2$, $SD = 1.1$), and after the attack ($M = 4.1$, $SD = 1.1$).

5.3 Security Practices

We asked respondents about their security practices before, during, and in the weeks following the attack to determine whether the attack influenced their practices.

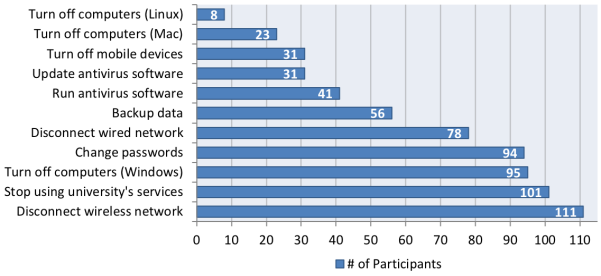

Figure 4: Security measures taken within 24hrs.

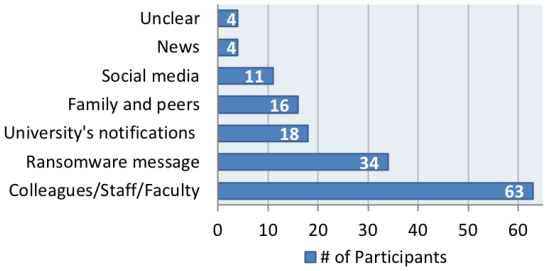

Figure 5: Source of "network interruption" notification.

Respondents' primary security practices prior to the attack were backing-up files ($n = 56$) manually or automatically (e.g., saving on a network drive backed up by the university daily), avoiding clicking on suspicious links or files ($n = 36$), using security software such as an antivirus ($n = 34$), using strong passwords ($n = 26$), and periodically changing passwords ($n = 23$). Twenty-one percent ($n = 32$) said they had no personal security practices and relied entirely on the university's computing services for securing their computers. For context, we note that all university-managed computers run antivirus software, but some groups opt to manage their own systems, and individuals may also use their own computers on campus. Among other security measures, the university also had a relatively stringent password policy.

Respondents reported a clear increase in "emergency" measures to protect resources in the 24 hours after the attack, often at the cost of productivity. Figure 4 shows the most common actions were disconnecting from the wireless network ($n = 111$), avoiding university services ($n = 101$), turning off Windows computers ($n = 95$), changing passwords ($n = 94$), disconnecting from the wired network ($n = 78$), and backing-up data ($n = 56$). Some engaged in running ($n = 41$) and updating ($n = 31$) antivirus software, and turning-off mobile devices ($n = 31$). A few respondents using Mac ($n = 23$) and Linux ($n = 8$) operating systems also turned off their computers.

In the longer term, security practices of 42% ($n = 63$) of respondents were unchanged by the attack. Others backed up data more frequently ($n = 24$), avoided saving on local drives ($n = 16$), changed their passwords ($n = 15$), and made other small changes ($n = 32$). There was a slight increase in respondents' rate of data backup, with 73% ($n = 109$) backing-up at least once a month after the attack compared to 66% ($n = 99$) prior.

We asked whether the incident had encouraged respondents to learn more about cybersecurity; most were indifferent ($M = 3.3$, $SD = 1.0$). Respondents felt that this rather significant incident was 'something that happened' which was out of their control and saw little need to increase their cybersecurity knowledge in response.

5.4 Communication

We asked respondents when and how they learned about the attack. Sixty-nine percent of participants said they first learned about the "network interruption" (as it was initially called) before noon on the day of the attack ($n = 104$). The rest found out later that day ($n = 27$), or could not precisely recall ($n = 19$). Figure 5 shows how users first discovered the "network interruption". The majority were informed through word-of-mouth or through the news and social media. Only 12% ($n = 18$) said they were first notified officially by the university.

Many respondents were somewhat dissatisfied with the official university communications during the attack ($M = 2.6$, $SD = 1.3$). In particular, they felt the information provided did not address their specific concerns ($M = 2.4$, $SD = 1.3$), and reassured them only a little ($M = 2.1$, $SD = 1.2$). They found the communication somewhat confusing ($M = 2.4$, $SD = 1.3$), and felt it neither decreased ($M = 2.2$, $SD = 1.2$) nor increased their worry ($M = 2.4$, $SD = 1.2$). The information did not help respondents understand what they should do ($M = 2.6$, $SD = 1.3$), or inform them of preventive steps they should take in the future ($M = 2.3$, $SD = 1.2$).

During and after the attack, half of respondents attempted direct communication with the university's IT staff for information. Respondents reported in-person communication ($n = 35$), email ($n = 27$), phone calls ($n = 41$), and leaving voice messages ($n = 19$). The remaining 49% ($n = 73$) of respondents had no direct communications with the IT staff. Respondents tried a variety of methods to stay informed, primarily relying on word-of-mouth. Sixty-seven percent ($n = 97$) said they acquired information from friends, fellow students, faculty, or other colleagues. Social media ($n = 87$) and mainstream news ($n = 59$) were also frequent sources. To access official details, respondents checked the university's website ($n = 81$), read emails from computing services ($n = 70$), received updates from their departments ($n = 67$), and checked internal IT websites ($n = 16$).

Only 10% of respondents ($n = 15$) believed the university managed the situation surrounding the attack well

and their most frequent concerns surrounded communications. Forty-eight percent of respondents ($n = 72$) believed that communication during and after the attack could be improved, and that there is a need for a clear cyber-attack emergency response and communication plan. Respondents offered specific suggestions, but generally, they simply needed more information, more frequently. Fifty-nine percent ($n = 89$) believed the situation should have been made public immediately or as soon as possible, instead of masquerading as a "network interruption". Within internal communication, respondents wanted clear details about the problem ($n = 31$), specific and consistent instructions about what to do ($n = 21$), more frequent updates ($n = 15$), and overall improvements to the emergency notification system ($n = 15$). Respondents expected a median of 5 status updates per day during the first 24 hours after an attack, twice per day for the next few days, and once a week during the following weeks.

5.5 Paying the ransom

When asked about the maximum ransom the university should pay, 55% percent ($n = 83$) of respondents said that the university should pay $0. Of those who felt a paying might be appropriate, maximum values ranged from $100 to $1,000,000. In related Likert-scale questions, most reiterated that the university should not pay the ransom, neither for unlocking all of the infected computers ($M = 1.8$, $SD = 1.2$), nor for unlocking only computers that contained important files ($M = 2.0$, $SD = 1.4$). Respondents were against paying the ransom because they were unsure whether the attackers would unlock the files ($M = 3.1$, $SD = 1.3$). However, if the university did not pay, many were also uncertain whether the university could recover lost data ($M = 2.8$, $SD = 1.3$).

5.6 Technical vs. non-technical users

Using Welch's t-tests, we did not find a significant effect in most cases between the respondents with and without technical backgrounds, except on 5 survey questions: non-technical respondents felt significantly more secure connecting to the university's wireless network before the attack ($t(56) = -2.62, p < 0.05$). Non-technical respondents were significantly more likely to follow recommended protective advice before ($t(52) = -2.52, p < 0.05$), during ($t(52) = -2.6, p < 0.05$), and after the attack ($t(51) = -2.95, p < 0.005$). Lastly, the information received from the the university was significantly more confusing to non-technical users than those with technical backgrounds ($t(70) = -2.56, p < 0.05$).

5.7 Survey summary

Our survey results revealed two main dimensions of the attack's impact on respondents from the affected organization. First, the majority of the university community suffered technological disruptions that ranged from temporary loss of access to permanent data loss. The majority of respondents who lost access to essential services/computers lost more than three days of productivity. This is an indirect cost that is difficult to quantify, particularly when also considering the impact on students. Second, we identified that a crypto-ransomware attack on an organization has a great personal and social impact on its end-users. The strong negative feelings described by our respondents suggest that the personal and social implications of such incidents are as significant and noteworthy as technological ones.

Our respondents' risk perception before, during, and after the attack suggests that an attack on an organization increases users' perceptions of risk relating to the organization during the attack, yet it has marginal effects on the perceived risk of personal resources/computers. Our survey results confirm prior research [28]; perceived susceptibility to risk is a likely determinant for users' computer security behaviour. Most security behaviour changes we observed were "reactive" rather than "proactive" and occurred within 24 hours of the attack. Our results suggest that most users are unlikely to change their computer security behaviour in the long-term because they believe cyber-security attacks on organizations are out of individual users' control.

In the event of a cyber-attack, our respondents identified that communication is paramount to an effective cyber-attack response. The quality, frequency, and promptness of information disseminated affected respondents' perceived competency of the organization and overall satisfaction as a university community member. Without an effective communication plan, information may propagate informally through word-of-mouth, which could lead to miscommunication and confusion.

6 Interview Methodology

We audio-recorded semi-structured interviews with 14 students, 13 staff, and 3 faculty members ($n = 30$). We recruited as widely as possible, making sure to reach faculty, staff, and students across the entire campus through appropriate mailing lists, social media posts, and posters. From all who came forward, we interviewed all faculty, staff, and students who were directly affected. We also interviewed several users who were indirectly affected until we were repeatedly hearing very similar responses. Seven respondents had a technical background. Interviews were conducted in-person in a private area on cam-

pus. Interviewees were asked to reconstruct their attitudes and experiences with the attack, and changes in their security practices following the incident. The interview guide is available in Appendix A. Interviews lasted approximately one hour each and interviewees were compensated $20. The research team transcribed the audio recordings. We omitted all identifying information (e.g., names, department) from the transcriptions, and assigned anonymous usernames. Interviewee usernames contain a letter identifying the interviewee's role within the university (**F** = faculty, **S** = staff, **G** = graduate student, **U** = undergraduate student) followed by a randomly allocated sequential number (e.g., F2, S11).

We used inductive thematic analysis [6] to analyze the interview data, similar to prior qualitative studies in this area [13, 39, 42, 43]. The first author conducted opening coding of the transcripts using ATLAS.ti, generating on average 40 noteworthy excerpts per transcript and an initial list of 146 codes. To facilitate analysis, codes were organized into 25 categories describing commonalities between codes. For example, 5 codes that described interviewees' worries, such as missing deadlines, infecting computers, deleting data, stealing information, and safety were categorized as 'fears'. Two researchers worked to refine and merge codes, resulting in a final list of 137 codes. To increase the reliability of the analysis, the second researcher conducted open coding independently for 30% of the transcripts (i.e., 10 participants, distributed across different demographics) using the established code list. A Cohen's Kappa (k) test found good agreement between the two researchers' analysis, $k = 0.82$ (95% CI, 0.80 to 0.85), $p < 0.005$. The two researchers met to resolve any disagreements, coming up with a mutually agreeable set of codes for the excerpts. Following this process, the first researcher independently verified the remaining excerpts following the collaboratively established codebook. From these, main themes were extracted along with representative quotes.

7 Interview Results

The interviews offered opportunity for more in-depth exploration of the issues mentioned in the surveys. We present the results organized by general theme, aligning with the survey where appropriate for easier comparison.

7.1 Impact

Our interviewees' accounts of the impact of the ransomware attack on individuals were both technological (e.g., blocking access to email) and emotional (e.g., causing stress). We identify the loss of access to resources (technological), productivity, and morale (personal and social) as the three overarching effects of the attack.

7.1.1 Technological Impact

Individuals with infected computers obviously felt the largest impact and describe the helplessness experienced at the inability to access any of their data. According to one graduate student, all 14 computers in their research lab were infected. Attempts to access files on the infected computers led to the infuriating ransom message "we can help" (G1). A faculty member describes his reaction at seeing years of work become inaccessible:

> ***F3:*** [I had] all my work [on Dropbox], about fifteen years of work, and I was trying to get on with grading and stuff and I couldn't because they were all encrypted. It slowly started turning all the files into encrypted files at home as well. Then I realized this thing was not going to stop [...].

Interestingly, the impact for many people resulted as much from the emergency measures necessary contain the infection as the actual attack. "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", explained an IT staff (S14). Interviewees identified that inability to access files, WI-FI, and the university's online resources such as the student learning and management systems and email servers were the worse consequences. Many lost their primary means of communication both internally and with the outside world (who were unaware that their email messages were not received); others could not find alternate contact information for university members because it was posted on inaccessible services (e.g., university website).

The incident was "really messy for students [because] it was the final week before exams, and everyone was trying to submit their final assignments" (S6). A student added, "first, I needed the Internet to enter the database of the library to work on my paper. Second, we needed to submit online. Both of them were a problem" (U6). A staff from student services believed that "students were deeply affected." Scholarship applications were due, and "they weren't able to get transcripts [...]. We were trying to get all of these files together for students, and we couldn't get anything" (S2). Similarly for other staff, "all the files that were regularly used... were inaccessible" (S14). A faculty recounted, "I couldn't get into any of my work files; I couldn't work on my lecture; I couldn't do my Powerpoint; I couldn't get into email. I couldn't do anything at the university" (F2).

Interviewees said they lost access to both online and offline resources, such as physical workspaces normally reserved online. They saw "a mass exodus" on the day of the attack due to a lack of access to necessary resources (S11). University staff were eventually sent home and many students left campus to work.

7.1.2 Productivity Impact

Interviewees with infected computers spent significant time recovering data from backups or other sources. As a faculty described, data "had to be rescued from any source we could find" (F1). Interviewees retrieved data from network backups, external backups, cloud services, email attachments, and copies from other people. However, data recovery was neither easy nor up-to-date. For example, infected computers were re-imaged and restored from the university's network backups, but "the stuff stored on the network... was about a month old...", said a graduate student. Additionally, "any files that were open at the time of the backup wasn't backed up" (G1). Interviewees also told cautionary tales about automatic file syncing across devices; several (G1, S11, S7, S10, F3) described that auto-syncing/backups "turned into a nightmare" as the infected files quickly "polluted" other devices. In one account, a staff described a colleague's ordeal: "his files were corrupt on his system and that was feeding to Dropbox and all these other people linked to his Dropbox were getting corrupted files" (S11). Eventually, the colleague was able to recover through Dropbox.

Participants also described losses of valuable productivity tools and resources, including "all desktop shortcuts" (S1), "400 bookmarks" (S11), and carefully drafted email templates: "I've been working on [my email templates] for two years", a staff said, "I had a reply for almost everything a student could ask. I had these beautiful long emails with everything that a student could possibly need and I lost all of it" (S2). Affected participants were "frustrated" and "annoyed" that "there's nothing [computing services] could do" (S2) because these items were not saved on the network backups. Weeks after the incident, many were still feeling the aftermath of the attack:

> ***S1:*** Even now I still run into issues... just when I need things, all of sudden it is not working properly. So I am still constantly calling [computing services] and saying "Ok, I had this folder, it isn't there now". There are tons of little things like that... your work days are interrupted and you are not working at the same pace or being able to accomplish as much as you'd like because you're on the phone for an hour with [computing services].

Several interviewees believed that the significant loss in productively is an under-estimated impact of ransomware infections. A staff argued, the attack "cost the university in lost productivity far more than they could have paid out for ransom" (S3). Productivity costs "may be invisible in a university", said a faculty, but they are nevertheless big costs (F1) which included delays in research outcomes. As another example, a second faculty (F2) describes losing all teaching materials for the upcoming semester and having to spend weeks redeveloping these rather than working on an upcoming book and research.

Even those without infected computers suffered loss of productivity. Many interviewees said they lost at least several days to a week of productivity during "one of the busiest months of the year" (S2). The attack "delayed every due date", and it was "really tough to catch up (S2). A direct impact was the inability "to do our jobs without having connectivity to the Internet and all the applications that [the university] uses and subscribes to" (S9). With no instructions of what to do, staff "kept their front lines open" (S8), but others describe idle time since they could not accomplish any of their regular tasks (S2, S4, S8); we were basically "paralyzed", said another (S9). Students similarly described an inability to complete homework, collaborate, and study in the days prior to exams (e.g., "One of my classes was online, so I wasn't able to watch the lectures" (U4)).

7.1.3 Personal and Social Impact

Interviewees described the personal and social effects of the experience that led to poor morale within the community. Words such as "stressed", "frustrated", "anxious", "scared", and "panicked" ran repeatedly throughout interviewees' accounts of their experiences. "A lot of people were stressed and frustrated", said a student, "people were fuming a little bit, especially people who were relying on the [school] computers and weren't able to access those resources" (U8). Similarly, a staff felt "frustrated" because "everything is broken" (S7). Another interviewee described how it left them shaken:

> ***S2:*** I would say it was an eye-opener, [...], knowing that we are really not safe, you know. All of the information that we have online, and this is my first experience ever being hacked or having anything sort of personally taken from me by hackers [...] it was just an awakening of sorts [...] And I never felt that before, I never had any concern before, [...] and now I'm nervous, honestly. To be honest, I'm nervous. It's made me more cautions and more nervous.

Emotional toll: Many interviewees reported strong negative feelings about the experience, but also noticed a discrepancy between their emotional response and the actual impact of the attack on their data. In our sample, severe data loss (i.e., significant amounts of work/research data permanently lost) was less common than recoverable data loss or no data loss. A student reported, "my feelings were more than severe, but in reality, I didn't see something severe," and "I didn't lose anything" (U6). In other words, many interviewees re-

called their emotional response as "severe in feelings"', but that the attack was "not severe in reality" because it did not affect their personal data or computers (U6).

Other than fears of direct data loss, participants feared that the malware might damage personal computers, cause missed deadlines, and compromise personal or financial information. For example, a staff who is also a parent asked her child to avoid logging on to university systems because "I don't want to be in a situation where I have to replace a five thousand dollar MacBook or something. I'm like, "I don't want you to get some contamination and bring it home."(S4)

Some said that they felt unsafe on campus: "I was afraid to come to the university...", said a student, "so I decided to leave the university and escaped to Starbucks" (U6). Others coped by staying off the school network and WI-FI, and incurred financial costs by using their mobile data to access the Internet instead. International students were particularly impacted by the loss of connectivity because they were unable to talk to their families back home. One student explained,

> ***U5:*** I have a lot of international friends and most of them were actually very very homesick. Especially since exams are coming they were very stressed out and I know a lot of them are constantly talking to their parents 24/7. And because they were unable to talk, they were very desperate and it made them turn on [mobile] data. Like they don't really have it, then they would still start using it and that is when they are indirectly losing money... and they're getting stressed out.

This account highlights some personal and social impacts of cyber-attacks. Users faced emotional costs at being isolated from their social support network and were additionally stressed by indirect financial costs.

Another emotional impact was the fear of being penalized for missing deadlines. This clearly impacted students: "We had a paper due and everyone couldn't access their papers, so everyone was freaking out in my program" (U10). Even though most students received extensions, the process was stressful. One undergraduate student explained, "it impacted everyone, like 'panicking', especially being in first-year. You just see people frustrated. [Students] want to get in touch with the professors but having no way, and did not know how else to contact them. People were just losing their minds" (U9).

Interviewees also worried, "do they have any of my personal information? Are they going to get employee information?" (S6). The uneasiness caused them to avoid their financial accounts because they were unsure of the extent of the attack. For example, a student said, "my dad sent me money at that time, but I was not able to check my bank because I was really too scared to check it. I didn't even check it like after a week or so" (U2).

Our assessment was that most interviewees recovered from the attack, and that the personal and social impact was significant but mostly temporary. A staff sums up:

> ***S4:*** Looking back, at the end of the day, all the stuff was really just anxiety based. 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].

In these data excerpts, interviewees recounting their experiences by voicing anxieties, frustrations, and fears. Interviewees shifted between talking about technological effects, to describing incidental effects like loss of productivity, then to talking about the emotional toll. Our data suggests that effects of cyber-attacks on users are complex, multifaceted, and difficult to measure.

A sense of belonging to a community: The attack caused resentment and damaged users' relationship with the university. Interviewees saw themselves as "belonging to" and "a part of" a larger community (U9). However, with respect to this incident, participants felt that they "didn't have a role in the situation" (G1), and that their opinions did not matter. "We weren't asked about how we felt about the situation", a staff said (S6). It appears that most resentment came from a perceived lack of transparency and clear communication about what had happened. Many interviewees were dissatisfied that they found out about the ransomware attack through rumours and news reports instead of from the university directly. A staff member argued,

> ***S6:*** There's nothing wrong with saying we've been hijacked. Hearing it on [the news] before you hear it from the campus higher-ups, it's like "why is there such a secrecy?"

Instead of feeling that the university community was working together to solve the problem, interviewees felt sidelined and kept in the dark. "It was kind of like we didn't have a role in this situation. We were just kind of the people that were affected and [we should] stay out of the way" (G1). Some believed that "each person should be allowed to make the decision" about paying the ransom to recover his or her data (S7). A graduate student resented how infected computers were handled.

> ***G1:*** The IT guy from our department came in after we had all left for the night, came in and wiped every [infected] computer in the lab. To our knowledge, there hadn't been a resolution [at

the time] about whether [the university] was going pay or not, and they just made the executive decision to delete everything. We were upset because that made it final, like we are never getting these files back. They never gave us the choice. They never gave us the option.

Clearly, affected interviewees were upset at being excluded from the decision-making process, and this damaged their sense of belonging to the university community. Data lost may have been inevitable, but this highlights how an organization's handling of an incident can impact its strong sense of community.

7.2 Security Practices

We noted many common misconceptions about security best practices, suggesting a need for more proactive cybersecurity training geared towards the university community and customized to the needs of different users.

As an example, we highlight discussion about backing up data, which was particularly relevant to this incident. One faculty detailed intentionally avoiding the university's network drives to save important files, believing that their workstation's local hard drive was safer, and gave an interesting analogy to explain their reasoning:

> ***F2:*** I had about sixty five reports [...], and the safest place for me to keep them was on that drive, on my own computer, because it's supposed to be password protected and have all the security [...] So I kept it on there and it's all gone. [...] If somebody broke in [to the office] and stole the files in the old days, then the stuff was gone and nobody would scream at them because they didn't make photocopies of them and take them home!

Several interviewees were rethinking their backup and storage strategies. Some who were previously using cloud services and automatic syncing were reconsidering, while others decided that they would now be "vigilant in getting various copies of everything that you need, in different areas. Backing up everything like crazy." (S2). Others had lost confidence in the university infrastructure and vowed to store data off-campus instead.

7.3 Communication

Many believed that the main cause of dissatisfaction and frustration among faculty, staff, and students was not the cyber-attack itself, but how the situation was communicated. A staff explained, "everybody understands that stuff happens, but communication is key. if you're not telling people what is going on, that is creating a whole other level of panic" (S11). A large part of interviewees' retelling of their experiences revolved around communication, highlighting it as a critical.

7.3.1 Communicating during an incident

In the event of a cyber-attack, interviewees believed that it is extremely important to notify the university community about the situation promptly and as accurately as possible. Instead of being forthcoming, interviewees felt the university "hid behind this terminology of 'network interruption', which is not really accurate" (S8). Users were instructed to "disconnect everything" and "shut everything down" (S3), but no details were provided about why. A student recounted:

> ***U4:*** On the first day when I walked into the library and there was a sign saying, "Don't use the WI-FI – Don't use the computers"; it didn't say why. I heard some people in front of me say "Oh whatever, I'm still going to use the computer, I don't care". I think if they had known it was because of malware they definitely wouldn't have wanted to use it... Maybe they didn't want people to panic or to worry, but if people are going to listen I think it's important to give them that knowledge so they understand why they don't want you to use it.

These accounts highlight the necessity of informing people about the risks and vulnerabilities when instructing people what to do. Furthermore, providing users with vague or inaccurate information may cause them to undermine the seriousness of the problem. Others felt the notification came too late: "we're working in the library and then we're told that we can't go on to the WI-FI. I had already been on the WI-FI... so I started to panic" (U8). Another student recalled, "they told me not to log in on the lab computers or log in to [the university] services [...], but at that point, it was already too late because I already did" (U3).

Interviewees thought that the little information provided by the university was "vague", "cryptic", and "unhelpful". The update "didn't really tell a lot of useful information," that enabled people "to make decisions" (S7). Employees wanted answers to questions such as "can I turn my computer on?" or "can we work?" (S1). Not having the information made people "very cautious", and they kept their computers shut-off longer than required (S10), adding to the loss of productivity.

While informing users about cyber-attacks, interviewees identified that users should be provided with "a standard set of procedures" (S12) to follow, and actionable instructions about what they should do. For example, a tutorial leader said, "I didn't know if I should actually tell my students not to open their laptops... It was a

blur, like I didn't know what should I do and what should I not do" (U1). A staff said, "we all received the very bizarre coded messages from the central university that never really explained what to do" (S10). Similarly, a faculty recalled"getting directions at some point to not to turn [her] computer on, but then was 'told to go ahead and go home and everything will be fine' ... "All I knew was it wasn't working" she continued, and "it took a few days before anybody told me if you do come in don't try to sign on. And again, that was pretty much word-of-mouth" (F2). Interviewees expected useful updates at set intervals from the university. The updates should keep the users "in the loop" (S8) about progress, how and when the university will resolve the issue, what resources are open, and what users should do. They also wanted to know when life could return to normal:

> ***G1:*** 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. 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.

7.3.2 Planning ahead

Interviewees voiced a need for a detailed cyber-response plan that mapped out the flow of communication from the top administration to the school departments, and to the members of the university community, including full-time and part-time faculty, staff, and students. It is critical that the plan covers scenarios when all online and network services are down. Some believed that a cyber-response plan could be coordinated between computing services and campus security to ensure immediate alternative lines of communication. The broader university community should be aware of this plan so that they know what to expect when an incident occurs.

7.4 Paying the ransom

The interviewees recognized that paying or not paying the ransom is a moral, ethical, and pragmatic dilemma. They showed deep sympathy for those who lost data. A staff empathized, "I'm not a researcher and I don't have anything important on my desktop, but I would hate to think that all of my lifelong work was lost and there wouldn't be some sort of accountability to the university on doing whatever they can to provide it" (S9).

On a pragmatic level, some believed that the decision to pay the ransom would be a matter of weighing the costs, such as the cost of data, the cost of downtime, and the cost of rebuilding. A staff explained:

> ***S7:*** if you had a high reliability that if you paid you would get your stuff back, then it becomes simply a cost: the cost of paying to get it back directly versus the cost of the money and energy that has been spent in the interim trying to bring things back and to fix things. I figure I've probably effectively lost about three weeks of work in terms of time spent either recovering stuff and not being able to do my real job.

A graduate student further explained this rationale:

> ***G1:*** When you look at the sum of money [the attackers] were looking for, it doesn't sound like a lot to an organization. Yes, you are paying domestic terrorists; yes, you are giving in to it, but when you look at the amount of money that you spent on getting this research done — the amount of money you put into the research, the amount of money in grants that the university has worked hard to get, and that they've lost all that data and all of that research. It seems counterproductive to just not pay off the ransom.

Through explanations like this, some interviewees argued that the decision on whether to pay the ransom could be based on a calculation of productivity costs weighed against the ransom amount. Although this line of thinking seemed practical, these participants also recognized that the decision to pay a ransom is much more complex than a simple monetary transaction.

In the end, however, most interviewees agreed with the university's decision to not pay the ransom. Many interviewees, particularly those who were not affected by data loss, appeared to be convinced that the ethical principles outweigh the pragmatic considerations. Many believed it is ethically wrong to pay criminals, and that paying would encourage more criminal activity because it is a demonstration of weakness and sets precedence for other attacks. Some described paying the ransom as a "band-aid" solution because "giving in to these types of demands doesn't actually solve the problem" in the long run (S13). Several compared their rationale to why governments will not pay ransoms for hostages. Additionally, most believed that criminals cannot be trusted, and there is no guarantee that the data will be returned, unaltered, and not copied for malicious use. The university could also risk the attacker asking for a higher ransom.

7.5 Interview Summary

The attack significantly hindered students, faculty, and administrative staff's ability to do work for several days and the remnant of impact was felt for weeks after the attack. However, the personal and social impact was possibly more severe than the technological impact. Interestingly, the emotional toll on users was only par-

tially caused by the direct effects of the ransomware attack. Other variables, such as lack of communication and transparency led to decreased morale, trust, and a feeling of disconnectedness by the members of the university.

Interviewees recognized that the response to a ransomware attack is difficult because it includes ethical, moral, and pragmatic considerations. In the end, however, interviewees displayed distrusted the attackers and supported the university's decision not to pay the ransom.

8 Discussion

8.1 The unaccounted costs of attacks

Estimates of the financial and productivity costs to organizations as a result of ransomware are available in the literature (e.g., [18, 38]). Beyond these, we identified other costs that may not receive as much attention but that can be equally damaging.

Emotional toll: Users experience stress and anxiety, and this may extend well beyond the immediate aftermath of an attack since it may take weeks (or longer) for users to catch up, recreate lost data, or deal with the consequences of the attack (e.g., delays in graduating due to lost research data, missed publication deadlines impacting promotion/tenure dossiers, increased workload as a result of lost templates).

Disconnect from social supports: When incidents result in inaccessible communication channels, users may feel isolated and disconnected from their social support network (thus increasing the emotional toll) exactly when such support might be needed. This was particularly apparent with students who rely on the university infrastructure as their primary internet access point, but also among staff unable to reach colleagues.

Indirect financial costs: End-users may incur indirect financial costs, such as additional mobile data, costs relating to working off-campus (e.g., overage charges on home internet accounts), or purchasing additional resources (e.g., a new backup drive). While relatively minor costs, they may impose hardship on those with fixed incomes such as students. There may also be financial consequences to missed opportunities (e.g., inability to apply for a scholarship).

Increased security burden: End-users may be subject to new, tighter security measures. These measures may impose additional longer-term productivity losses beyond those directly associated with the incident if certain tasks become more complicated.

We highlight that many of these costs are a result of the (necessary) security response to an attack. And while some may be inevitable, they should be considered as part of a comprehensive cyber-response plan, and minimizing them is desirable.

8.2 Suggested User-Centric Strategies

Several lessons emerged from our research suggesting how organizations should handle such incidents. There are obviously other factors at play when determining a cybersecurity response, and not all of these were lacking in this particular incident, but we believe that these insights could help devise a comprehensive plan.

Share the plan: An explicit cyber-response plan should be shared with the broader community *before* an incident happens. This should, at minimum, explain what is expected of users during an incident, how information will be conveyed and by whom, and a communication schedule. The communication channel should not put users at increased risk. For example, users may connect to the organization's WI-FI if updates are coming through organizational email accounts. We also suggest having an explicit policy for what will happen in response to an attack, along with explanations. For example, 'our organization will never pay ransoms because doing so increases the likelihood that the organization is targeted for further attacks.' or 'we will erase and reimage infected devices because we cannot guarantee that they are not otherwise compromised.' This information should be conveyed simply and clearly ahead of time so that everyone understands what to expect.

Communication is key: This was by far the most requested component. Communication during and after an incident needs to be frequent, straightforward, and upfront. Our end-users wanted regular updates five times daily during an incident, twice per day for the next few days, and once per week for the following weeks. They also needed explicit closure to an event; they wanted to hear from an official source that everything had been resolved. (i.e., similar to how weather forecasts broadcast that 'the weather warning has been lifted'). The on-going communication should include specific advice for end-users and describe any adjustments made as a result of the incident (e.g., Can they access specific resources? What should they do with their workstations or personal computers/devices? Are certain deadlines extended? How do they contact individuals if regular communication is disrupted?). The communication may need to be customized for different user groups. Decades of literature on warnings and crisis communication for other types of emergencies, such as natural disasters, offer comprehensive strategies and assessments of best practices (e.g., [25]; much of their approaches may be transferable to cyber-attacks.

Give victims a voice: End-users most affected by the incident wanted a voice in the recovery process. It will likely be infeasible to meet every request, but organizations should recognize that individuals were impacted well beyond the impersonal lost of organizational data.

By-passing their involvement in the recovery process further compounds the negative, long-lasting impact. As we witnessed in our study, many victims simply wanted an opportunity for a debrief. They wanted to discuss their experience, be heard, and have their insight and suggestions taken into account.

Practice user-centric security: A common response to attacks is to tighten the security policy, increasing the burden on end-users. We argue, however, that security policies must be realistic and not place an undue burden on users. Security policies that are too restrictive (e.g., disabling access to commonly used services), cumbersome (e.g., making it more difficult to accomplish tasks), or that make unrealistic demands on users (e.g., frequent password changes) will be bypassed by users, either intentionally so that they can accomplish their primary tasks [14,44] or accidentally by making errors. Re-examining policies is reasonable but changes should be carefully weighted against their human cost.

Offer user-centric training: Cybersecurity training should be an on-going service. In a large organization, training will need to be tailored to meet various needs. Given our interviews, we suggest that one-on-one consultations may even be advisable to address individual concerns and help end-users set up their system in a way that is both secure and meets their needs. In general, training material needs to explain the threats and how security strategies address these threats. Users are more likely to comply if they understand how their actions contribute to protecting their and the organization's resources [1]. Here also, the broader risk communication literature may offer useful insight (e.g., [5,32]).

Provide user-centric data storage: Storage and backup must be straightforward, usable, and offer the needed functionality (e.g., file sharing and remote access). Many users did not store (or infrequently stored) data on the organization's network drives where it could have been restored relatively easily. It may be tempting to dismiss this as 'the user's fault'; however, in many cases users had legitimate reasons for their decisions: the official storage options did not provide the functionality they needed, the functionality was awkward/difficult to use, or users misinterpreted the 'safest' options.

8.3 Refined Ransomware Process

Inspired by Ali's *Ransomware Process* [3] for individuals, we extend description to organizations. Our refined *Organizational Ransomware Process* diagram is available in Figure 6. One important differentiating factor is the potential loss of autonomy for individual end-users who must rely on the organization to respond to the attack. From our analysis, this may cause additional emotional and productivity strain, as well as incur additional

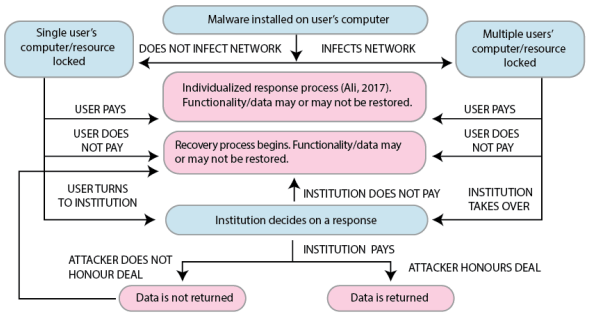

Figure 6: The ransomware process.

'unaccounted costs' (see Section 8.1), regardless of the eventual outcome of the incident.

8.4 Limitations and Future Work

The studies may have a self-selection bias since end-users who were most impacted may have had the most interest in participating. For this reason, generalizations about the entire community should be made with caution. We also relied on self-reporting; participants may have misremembered, left out details, or selectively shared with us. There were sufficient commonalities across reported experiences, however, that we believe that these are reasonable accounts. While we do not wish that other organizations fall victim to attack, it would be interesting to explore whether our findings hold for other organizations, in similar or different domains.

9 Conclusion

We had the (un)fortunate opportunity to be present in the immediate aftermath of a crypto-ransomware attack at a large academic institution. We collected data from end-users through surveys and interviews to understand the impact and their experiences throughout the incident. We identified the technological, productivity, and personal and social impacts on users, including some typically unaccounted costs that should be considered when developing cyber-response plans. Most participants recognized that attacks happen, but they expressed an important need for clear and timely communication within the organization about the incident, and a need for a voice in the recovery process. We additionally propose strategies to help organizations better prepare for similar attacks. Given the statistics about ransomware attacks on organizations, it is prudent to assume that an attack is likely and prepare accordingly. Our work demonstrates that both advance planning and recovery efforts must address human factors because the effects may last well beyond the technical recovery of resources and data.

10 Acknowledgments

R. Mohamed acknowledges graduate funding from an Ontario Trillium Scholarship. S. Chiasson acknowledges funding from NSERC for her Canada Research Chair and Discovery Grants.

References

[1] ADAMS, A., AND SASSE, M. A. Users are not the enemy. *Communications of the ACM 42*, 12 (1999), 40–46.

[2] AL-RIMY, B. A. S., MAAROF, M. A., AND SHAID, S. Z. M. Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. *Computers & Security* (2018).

[3] ALI, A., MURTHY, R., AND KOHUN, F. Recovering from the nightmare of ransomware - how savvy users get hit with viruses and malware: A personal case study. *Issues in Information Systems 17*, 4 (2016).

[4] AYTES, K., AND CONOLLY, T. A research model for investigating human behavior related to computer security. *AMCIS* (2003), 260.

[5] BEAN, H., SUTTON, J., LIU, B. F., MADDEN, S., WOOD, M. M., AND MILETI, D. S. The study of mobile public warning messages: A research review and agenda. *Review of Communication 15*, 1 (2015), 60–80.

[6] BRAUN, V., AND CLARKE, V. Using thematic analysis in psychology. *Qualitative research in psychology 3*, 2 (2006), 77–101.

[7] CHEN, Q., AND BRIDGES, R. A. Automated behavioral analysis of malware: A case study of wannacry ransomware. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)* (Dec 2017), pp. 454–460.

[8] CONTINELLA, A., GUAGNELLI, A., ZINGARO, G., DE PASQUALE, G., BARENGHI, A., ZANERO, S., AND MAGGI, F. Shieldfs: A self-healing, ransomware-aware filesystem. In *Proceedings of the 32nd Annual Conference on Computer Security Applications* (New York, NY, USA, 2016), ACSAC '16, ACM, pp. 336–347.

[9] DEMURO, P. R. Keeping internet pirates at bay: Ransomware negotiation in the healthcare industry. *Nova L. Rev. 41* (2016), 349.

[10] EVERETT, C. Ransomware: to pay or not to pay? *Computer Fraud & Security 2016*, 4 (2016), 8 – 12.

[11] FIELD, A. *Discovering statistics using SPSS*. Sage publications, 2009.

[12] FORGET, A., PEARMAN, S., THOMAS, J., ACQUISTI, A., CHRISTIN, N., CRANOR, L. F., EGELMAN, S., HARBACH, M., AND TELANG, R. Do or do not, there is no try: user engagement may not improve security outcomes. In *Symposium on Usable Privacy and Security (SOUPS)* (2016), pp. 97–111.

[13] FORGET, A., PEARMAN, S., THOMAS, J., ACQUISTI, A., CHRISTIN, N., CRANOR, L. F., EGELMAN, S., HARBACH, M., AND TELANG, R. Do or do not, there is no try: user engagement may not improve security outcomes. In *Symposium on Usable Privacy and Security (SOUPS)* (2016), pp. 97–111.

[14] HERLEY, C. So long, and no thanks for the externalities. In *New Security Paradigms Workshop (NSPW)* (2009).

[15] HERNANDEZ-CASTRO, J., BOITEN, E., AND BARNOUX, M. Second online survey. Tech. rep., University of Kent in Canterbury, Press Release, 2014.

[16] HUANG, J., XU, J., XING, X., LIU, P., AND QURESHI, M. K. Flashguard: Leveraging intrinsic flash properties to defend against encryption ransomware. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, 2017), CCS, ACM, pp. 2231–2244.

[17] KASPERSKY LAB. Kaspersky security bulletin 2016, 2016.

[18] KASPERSKY LAB. The Cost of Cryptomalware: SMBs at Gunpoint, Accessed August 2017. `https://www.kaspersky.com/blog/cryptomalware-report-2016/5971/`.

[19] KEVIN SAVAGE, PETER COOGAN, H. L. The evolution of ransomware. Tech. rep., Symantec Corporation Security Response, 2015.

[20] KHARRAZ, A., ARSHAD, S., MULLINER, C., ROBERTSON, W. K., AND KIRDA, E. Unveil: A large-scale, automated approach to detecting ransomware. In *USENIX Security Symposium* (2016), pp. 757–772.

[21] KHARRAZ, A., AND KIRDA, E. Redemption: Real-time protection against ransomware at end-hosts. In *International Symposium on Research in Attacks, Intrusions, and Defenses* (2017), Springer, pp. 98–119.

[22] KOLODENKER, E., KOCH, W., STRINGHINI, G., AND EGELE, M. Paybreak: Defense against cryptographic ransomware. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (New York, NY, USA, 2017), ASIA CCS, ACM, pp. 599–611.

[23] LUO, X., AND LIAO, Q. Awareness education as the key to ransomware prevention. *Information Systems Security 16*, 4 (2007), 195–202.

[24] MANSFIELD-DEVINE, S. Ransomware: taking businesses hostage. *Network Security 2016*, 10 (2016), 8 – 17.

[25] MILETI, D. S., AND SORENSEN, J. H. Communication of emergency public warnings: A social science perspective and state-of-the-art assessment. Tech. rep., Oak Ridge National Lab., TN (USA), 1990.

[26] MING, J., XU, D., JIANG, Y., AND WU, D. Binsim: Trace-based semantic binary diffing via system call sliced segment equivalence checking. In *Proceedings of the 26th USENIX Security Symposium. USENIX Association* (2017), pp. 253–270.

[27] MINIHANE, N., MORENO, F., PETERSON, E., SAMANI, R., SCHMUGAR, C., SOMMER, D., AND SUN, B. Mcafee labs threat report, December 2017.

[28] NG, B.-Y., KANKANHALLI, A., AND XU, Y. C. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems 46*, 4 (2009), 815–825.

[29] O'BRIEN, D. Ransomware 2017. *Internet Security Threat Report* (July 2017).

[30] PATTON, M. Q. *Qualitative evaluation and research methods*. SAGE Publications, 1990.

[31] PUBLIC SAFETY CANADA. Ransomware: WannaCry, Accessed August 2017. `https://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2017/al17-006-en.aspx`.

[32] REYNOLDS, B., AND SEEGER, M. W. Crisis and emergency risk communication as an integrative model. *Journal of Health Communication 10*, 1 (2005), 43–55.

[33] RICHARDSON, R., AND NORTH, M. Ransomware: Evolution, mitigation and prevention. *International Management Review 13*, 1 (2017), 10 – 21.

[34] SCAIFE, N., CARTER, H., TRAYNOR, P., AND BUTLER, K. Cryptolock (and drop it): stopping ransomware attacks on user data. In *36th International Conference on Distributed Computing Systems (ICDCS)* (2016), IEEE, pp. 303–312.

[35] SCAIFE, N., TRAYNOR, P., AND BUTLER, K. Making sense of the ransomware mess (and planning a sensible path forward). *IEEE Potentials 36*, 6 (Nov 2017), 28–31.

[36] SHINDE, R., VAN DER VEEKEN, P., VAN SCHOOTEN, S., AND VAN DEN BERG, J. Ransomware: Studying transfer and mitigation. In *Computing, Analytics, and Security Trends (CAST)* (2016), IEEE, pp. 90–95.

[37] SITTIG, D. F., AND SINGH, H. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied Clinical Informatics 7*, 2 (2016), 624.

[38] SOPHOS. The state of endpoint security today, 2018.

[39] STOBERT, E., AND BIDDLE, R. The password life cycle: user behaviour in managing passwords. In *Symposium on Usable Privacy and Security (SOUPS)* (2014).

[40] US-CERT. Alert (TA14-295A) Crypto Ransomware, Accessed August 2017. `https://www.us-cert.gov/ncas/alerts/TA14-295A`.

[41] VALACH, A. P. What to do after a ransomware attack. *Risk Management 63*, 5 (2016), 12.

[42] VANIEA, K., AND RASHIDI, Y. Tales of software updates: The process of updating software. In *SIGCHI Conference on Human Factors in Computing Systems* (2016), ACM, pp. 3215–3226.

[43] VANIEA, K. E., RADER, E., AND WASH, R. Betrayed by updates: how negative experiences affect future security. In *SIGCHI Conference on Human Factors in Computing Systems* (2014), ACM, pp. 2671–2674.

[44] WHITTEN, A., AND TYGAR, J. D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium* (1999).

A Interview Guide

These questions were a guide only. Interviews may have deviated if participants mentioned other relevant issues.

1. How did you find out about the network interruption? What did you do in response? Did you discuss with others? How did you feel?
2. How did you stay updated on the incident?
3. How did the incident affect you directly? How did it affect your work? your ability to communicate? your plans? Did you lose any data? Was your computer compromised? What impact has it had on you? What impact did it have on those around you?
4. Before this attack, what did you know about ransomware? Have you learned more about it? How did you get info?
5. Before this attack, what kind of security measures did you take? How often did you backup your data?
6. And now, after the attack, how have your security practices changed? How often do you back up your data now? How likely are you to follow the recommended security practices by [computing services]?
7. What was your overall impression of the severity of this attack? How many computers do you think were infected? Was any important data lost or compromised?
8. Should [university] pay the ransom in these situations? How much should they pay? Should they reveal what steps have been taken to recover data? If [university] paid, how likely is it that they would recover the data? If [university] did not pay, how likely is that they would recover the data?
9. What did you learn from this incident?
10. What could [university] have done differently once the attack occurred?
11. Do you have any other stories about your experiences with this attack that you would like to share? Or do you have any other thoughts youd like to share?