Ivey | Publishing

UNIVERSITY OF CALGARY
HASKAYNE SCHOOL OF BUSINESS

W21012

CYBER ATTACK AT THE UNIVERSITY OF CALGARY

Naor Cohen and Catherine Heggerud wrote this case solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

It was about 1:00 a.m. on May 28, 2016, when Kevan Austen's phone rang. The number on the screen was familiar. "Kevan, I'm sorry to be calling at this time," the caller said. "We've been experiencing severe security issues in the last few hours. You'd better come here as soon as you can. We have pop-up screens with ransom notes for bitcoins and it looks like we've been hit with a cyber breach!"

Austen was the associate director, infrastructure operation and sustainment at the University of Calgary (U of C), and his portfolio included the operations centre, which, as the nerve centre of the university's information technology (IT) infrastructure, monitored all information systems on campus around the clock. Austen thought he had seen it all during his tenure on campus—until the security breach that May. His experience and intuition told him that this was a money grab. He was not looking forward to the next few hours, which he expected would involve heated discussions about whether to pay the ransom, along with also trying to restore network services.

Austen jumped into his truck and barrelled down the highway toward the city. Living on an acreage west of Calgary, he had done this drive daily for years. As he drove, he called the server technicians, asking them to come to campus immediately.

THE UNIVERSITY OF CALGARY

A young, public research institution in Calgary, Alberta, the U of C had over 30,000 undergraduate and graduate students and employed over 5,000 academic and non-academic staff.[1] It had originally been part of the University of Alberta but became a separate, autonomous public university in 1966. The U of C had grown rapidly between 1966 and 2016 and now had five campuses, including one in Doha, Qatar. Its 14 faculties offered more than 250 academic programs. In 2011, the U of C embarked on an ambitious plan to be a top-five research institution in Canada. This plan, known as the Eyes High strategy, required the U of C to expand its research capacity and capabilities. It involved recruiting additional top-tier researchers and launching an extensive philanthropic campaign, which increased the university's media presence, highlighting the many achievements scholars were accomplishing in Calgary. By 2016, the Center for World University Rankings had ranked the U of C eighth in Canada.

[1] "Enrolment by University," Universities Canada (blog), accessed January 20, 2020, www.univcan.ca/universities/facts-and-stats/enrolment-by-university/.

There were six types of post-secondary institutions in Canada: comprehensive academic and research universities, comprehensive community colleges, independent academic institutions, polytechnic institutions, specialized arts and cultural institutions, and undergraduate universities. The U of C was one of four comprehensive academic and research universities in Alberta and one of 15 large research universities with medical schools in Canada, known as the U15 Group of Canadian Research Universities. As such, it received substantial public funds from the provincial government to support its priorities.

The university's main governing body was the board of governors. In Alberta, university boards of governors operated in accordance with the *Post-Secondary Learning Act* and the *Alberta Public Agencies Governance Act*. The main responsibility of the board was to oversee the management and operation of the university's business and affairs as legislated by the provincial government. The board's duties were discharged through the president and senior officers of the university.[2]

Spring 2016 was an unusually busy time for the U of C. The campus was celebrating its golden anniversary.[3] From May 28 to June 3, it also hosted the 2016 Congress of the Humanities and Social Sciences, with the theme of Energizing Communities.[4] During the conference, 12,000 visiting scholars from around the world descended on campus, participating in research symposia and colloquia. The U of C had also opened its residences to 1,200 displaced victims of the Fort McMurray wildfire—an enormous blaze that had forced the largest community evacuation in Alberta's history.[5] Spring session classes were cancelled to accommodate the visitors, yet the campus was bustling with people from around the globe.

EMERGENCY RESPONSE TEAM RESPONSE TO INFRASTRUCTURE FAILURES

Austen had started his career on campus in 1989, running the microcomputer store. His technical expertise had allowed him to continue to grow his career, and he had taken various roles on IT services and infrastructure teams on campus. Austen, who was passionate about emergency IT operations, headed the emergency response team (ERT), which was responsible for ensuring the integrity of university data assets and quickly restoring service to the campus community in the event of an emergency. He understood the importance of IT services to research and teaching activities and took great pride in the ERT's responsibilities to protect these vital functions (see Exhibit 1).

In the early morning of May 28, questions raced through Austen's mind: Where was the problem? Was it a cascading network failure, or was the problem at the server level? And what was it: a propagating virus, a corrupted disk? He knew that many of the network's servers were not local disks. Theoretically, the storage servers could have just gone offline; it had happened before. Initially, the teams thought the network infrastructure might be failing and causing the alarm, but as the night unfolded, it became evident that this was not a standard network failure.

By the time Austen arrived on campus, IT operations had discovered a pop-up ransom note on a server (see Exhibit 2). The U of C's system had been breached by ransomware. Austen called in the rest of the IT leadership and activated the ERT. Catherine Heggerud, the director of customer engagement and experience,

[2] University of Calgary, "The Governors of the University of Calgary: Mandate and Roles Document," University of Calgary Secretariat, 2014, accessed January 20, 2020, www.ucalgary.ca/secretariat/board-governors.
[3] Eva Ferguson, "University of Calgary to Celebrate 50th Anniversary at Alumni Event," *Calgary Herald*, April 28, 2016, accessed January 20, 2020, https://calgaryherald.com/news/local- news/university-of-calgary-to-celebrate-50th-anniversary-at-alumni-event.
[4] "Congress 2016," Federation for the Humanities and Social Sciences, accessed January 28, 2020, www.ideas-idees.ca/events/congress/2016.
[5] Scott Strasser, "Fort McMurray Evacuees Find Refuge in University of Calgary Residences," *Gauntlet*, May 10, 2016, accessed January 20, 2020, https://thegauntlet.ca/?s=Fort+McMurray+Evacuees+Find+Refuge+in+University+of+Calgary+Residences.

was called around 4:30 a.m. As the duty director for the ERT, Heggerud's role was to take responsibility for the IT staff during any emergency and to safeguard the incident commander, Austen, freeing him from routine tasks in order to allow him to focus on the primary task: isolating the root cause of any problem. The duty director's responsibilities also included ensuring good morale among the extended team.

At 5:00 a.m., calls were also made to Linda Dalgetty, vice-president, finance and services; Janet Stein, director of risk management and insurance; and Rae Ann Aldridge, associate vice-president of risk. By 8:00 a.m., Austen and Heggerud had the ERT and supporting IT team assembled. As ERT members and support staff arrived on campus, Austen went over the night's events in his head. There were many moving parts, and explaining what had transpired would take patience.

IT operations had noticed unusual alarms on Friday evening, May 27, 2016. Austen was called in on Saturday at 1:00 a.m. At 2:00 a.m., IT operations called campus security after discovering a ransom note on a server: "All your files are encrypted with RSA-2048 encryption. RSA is an asymmetric cryptographic algorithm. You will need a private key to recover your files. It is not possible to recover your files without a private key."

The ransom note demanded a payment of 27 bitcoin for the recovery key and stipulated a payment deadline in seven days, after which the private key would be permanently deleted.

Coincidentally, Stein had signed a cyber-liability insurance policy just a few days before the breach happened. The policy included access to an independent breach coach. The coach was notified of the situation and was providing ongoing advice to the campus team. As they heard what had transpired in the middle of the night, everyone knew they were mired in an emerging crisis.

As incident commander, Austen was at a fork in the road. The ransom request made it clear that the team had to stop the malware from propagating. Austen did not have time to think about the ransom. His priority was containment only, not remediation; his focus was to preserve data and contain the malware, stopping it from propagating from server to server. One option for doing this was to disconnect the network, but that would affect the university's entire operation. Austen felt uncomfortable shutting down key services like active directory servers, which powered the campus email system.

Since the propagation method was unknown, Austen risked his professional reputation and recommended disconnecting the network to prevent further spreading of the virus. As Austen gave the ERT the green light, the scenario looked like a scene from a movie: IT people physically pulled cables off the backs of machines in the data centre, bringing university operations to a grinding halt. Was he making the right decision? Had he missed anything?

CRISIS MANAGEMENT TEAM EVALUATION AND HANDLING OF THE BREACH

Dalgetty was the leader of the IT crisis team. She had joined the university in July 2014, transitioning from industry, where she had served in a variety of senior leadership positions, including as chief information officer and chief financial officer. Dalgetty preferred to be well informed; she did not like surprises. She highly valued open, honest, transparent communication.

Dalgetty had a team of resourceful people who were supported by the breach coach and D'Arcy Moynaugh, a consultant from a major consulting firm. The breach coach and the cybersecurity team from the consulting firm brought valuable skills and knowledge, including knowledge about accessing the dark web—a part of the Internet whose access required specific software and that allowed its users to conduct business through anonymous peer-to-peer networks. The malware, however, was highly sophisticated. Servers were down, files

were encrypted, and email had come to a grinding halt. More than 9,000 email addresses had been lost, which made communication on campus a true challenge. The immediate solution was to use posters on all entrance doors asking faculty and staff not to turn on their computers due to a network failure (see Exhibit 3).

As the day wore on, more decision makers were brought into the loop. By noon, the executive leadership crisis management team (CMT) held its first meeting. At the request of U of C's president, Dr. Elizabeth Cannon, Dalgetty called Bonnie DuPont, chair of the board of governors, to provide her with a briefing on the emerging crisis. Ensuring the appropriate management of institutional risk was a board duty. Dalgetty informed DuPont that years of university research had been hijacked—the U of C was being held hostage.

Dalgetty's previous crisis experience in industry had leveraged a command-and-control structure to rapidly address crises. However, running a large university was complex, and the governing structure of the university did not allow for the top-down directives prevalent in private industry. Dalgetty was now the bridge between the IT crisis team and the CMT. The IT crisis team made its recommendations to the CMT, and the CMT took its decisions to the board of governors. While IT recommended shutting down the entire campus network, Dalgetty knew these decisions could not be made strictly at the technical level because the university's reputed ability to protect its researchers' intellectual property was at stake. The golden anniversary celebrations and all the visitors on campus meant the world was watching.

When the posters went on the doors, a wave of enquiries was prompted about how the university was managing the issue. Staff had no access to services like the active directory, and scholars had more than just research data on their computers: personal files such as photos, videos, financial statements, and other elements of their personal lives were out of reach. Compounding this issue was the lack of proper communication channels. With the rumour mill turning faster than ever, the story leaked to the public. Every crisis meeting included communications professionals, who were focused on crafting the message and controlling the story.

Luckily, the U of C website landing page was still operational, and the university had a Twitter account, allowing for some information sharing.

As the days went by, specific communication channels were set up through the UC Emergency Mobile app to allow the emergency operations groups to communicate directly with the leadership team. One of the CMT's early decisions was to not go public with the breach. The word *ransom* was not mentioned outside of the CMT. But how could the CMT ensure information was still being shared with the community—and still control the story—without proper communication channels? This role became the domain of the senior leadership team (SLT).

The SLT was composed of about 56 campus leaders, including associate vice-presidents, vice-provosts, deans of faculties, and associate deans. The SLT met on Tuesday May 31, where its members were asked to be key communicators within their faculties. This meant explaining what was happening within IT and preparing people to migrate their email boxes to Office 365, a cloud-based email solution. Paper-based instructions were required since digital communication was unavailable. However, the CMT had decided not to disclose the root cause of the issue with the SLT. Instead, Dalgetty's team talked in general terms about malware issues and network failure—and this was the consistent message, internally and externally.

The discussion regarding a ransom payment did not officially start before Tuesday, May 31. The ransom note had a seven-day deadline, and the first 72 hours had been spent getting all the right people in the geographically dispersed organization onto the same page. This had meant ensuring that IT people were on rotational duty 24/7. It had also meant engaging with the cyber-liability insurer and setting contracts in

place for specialized services such as the team from the consulting firm, the breach coach, and a public relations agency. This had been challenging because the university had no robust business continuity plan to deal with a cybersecurity breach of this size. Funding for IT security in 2016 was approximately 4 per cent of the IT capital budget (see Exhibit 4). Regardless, the university continued to engage with its technical teams and other consultants. Teams worked around the clock, allowing Dalgetty and her team to engage in dialogue about the ransom.

On Wednesday, June 1, the board's executive committee met. Logistically, it was not easy to bring 21 leaders from various committees together with the chair and vice-chair of the board. The meeting provided a formal sounding board and "stress test" for the decisions being made, and weighed these against the university's enterprise risk management framework. The enterprise risk management framework evaluated the institutional risks of operational impact, financial impact, and reputational impact. If the university paid the ransom, the financial impact would not be significant, as 27 bitcoin would cost approximately CA$21,000.

MALWARE, RANSOMWARE, AND CYBERCRIME

While the U of C was near ground zero for this virus, it was not the only one under attack. Collaboration with other organizations gave the university insight into the ransomware. The strain used to attack the U of C in May 2016 was known as SamSam, which was known to attack organizations in the health care, government, and education sectors.[6] However, it was estimated that public organizations were more likely to disclose these incidents than private organizations, and that more than half of SamSam's victims were from the private sector (see Exhibit 5). SamSam targeted more than users' documents. It also encrypted the configuration and data files required to run applications like Microsoft Office and to email clients. This meant huge complications in terms of system recovery. It was believed that SamSam and similar kinds of malware were designed and launched for financial gain.[7] Therefore, they primarily targeted critical infrastructure systems, since victims would be willing to pay to recover these.

Notoriously sophisticated, SamSam used operating system features to compromise its victims' networks. This malware exploited vulnerabilities in the systems to penetrate networks using a remote desktop protocol that allowed its hackers to gain access to domain user accounts. Once a domain administrator logged into a system, the hackers stole the administrator's credentials. With these stolen credentials, the hackers took control of a server and used it as a command centre to map out the network. At this point, the hackers used scanning tools to choose their target computers and access the file systems. The attack was usually launched late at night, when the targeted organization was least prepared to deal with it. A deployment tool was released to copy files across the network and encrypt as much information as possible before presenting the organization with the ransom demand.

Ransom payments were transacted in bitcoin, a digital cryptographic currency without a central bank. In the second quarter of 2016, the market capitalization of bitcoin was almost US$10 billion.[8] The anonymity that came with cryptocurrency made bitcoin a popular choice among criminals, who used it to fund and facilitate their illegal activities. Approximately 49 per cent of the total value of bitcoin transactions was associated with illegal activities such as the trade in illegal drugs, pornography, terrorism, money laundering, and avoidance of capital controls.[9]

---

[6] Sophos Ltd., *SamSam: The (Almost) $6 Million Ransomware*, Sophos, 2018, accessed January 20, 2020, www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf?cmp=26061.

[7] "Ransomware: Your Money or Your Data," *The Economist*, January 17, 2015, 414(8921), 57(US), https://link.gale.com/apps/doc/A397490892/WHIC?u=ucalgary&sid=WHIC&xid=02a11fd1.

[8] M. Szmigiera, "Bitcoin Market Capitalization Quarterly 2013–2019," Statista, October 2, 2019, accessed January 20, 2020, www.statista.com/statistics/377382/Bitcoin-market-capitalization/.

[9] Sean Foley, Jonathan R. Karlsen, and Tālis J. Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?," *Review of Financial Studies* 32, no. 5 (2019): 1798–1853.

The attackers provided instructions on how and where to buy bitcoin in their ransom notes. Victims could confirm payments and receive decryption instructions via a payment site hosted on the dark web, where a timer indicated the "time played." The hackers provided their victims with three payment options: In the first option, victims could pay a small fee in bitcoin and receive the private key to decrypt one computer. The second option was more cost-effective; victims could pay the full ransom amount in one payment and receive the keys needed to decrypt all affected computers. The last option involved paying half the ransom and getting the keys to decrypt half of the affected computers (randomly selected by the hackers). Each option meant something different for the victim in terms of remediation. There was very little evidence to suggest that the SamSam attacker ever negotiated on the price. In fact, the value of the ransom demands had increased over time. With the average monthly take around US$300,000, SamSam had brought its hackers more than US$5.9 million since late 2015 (see Exhibit 6).[10]

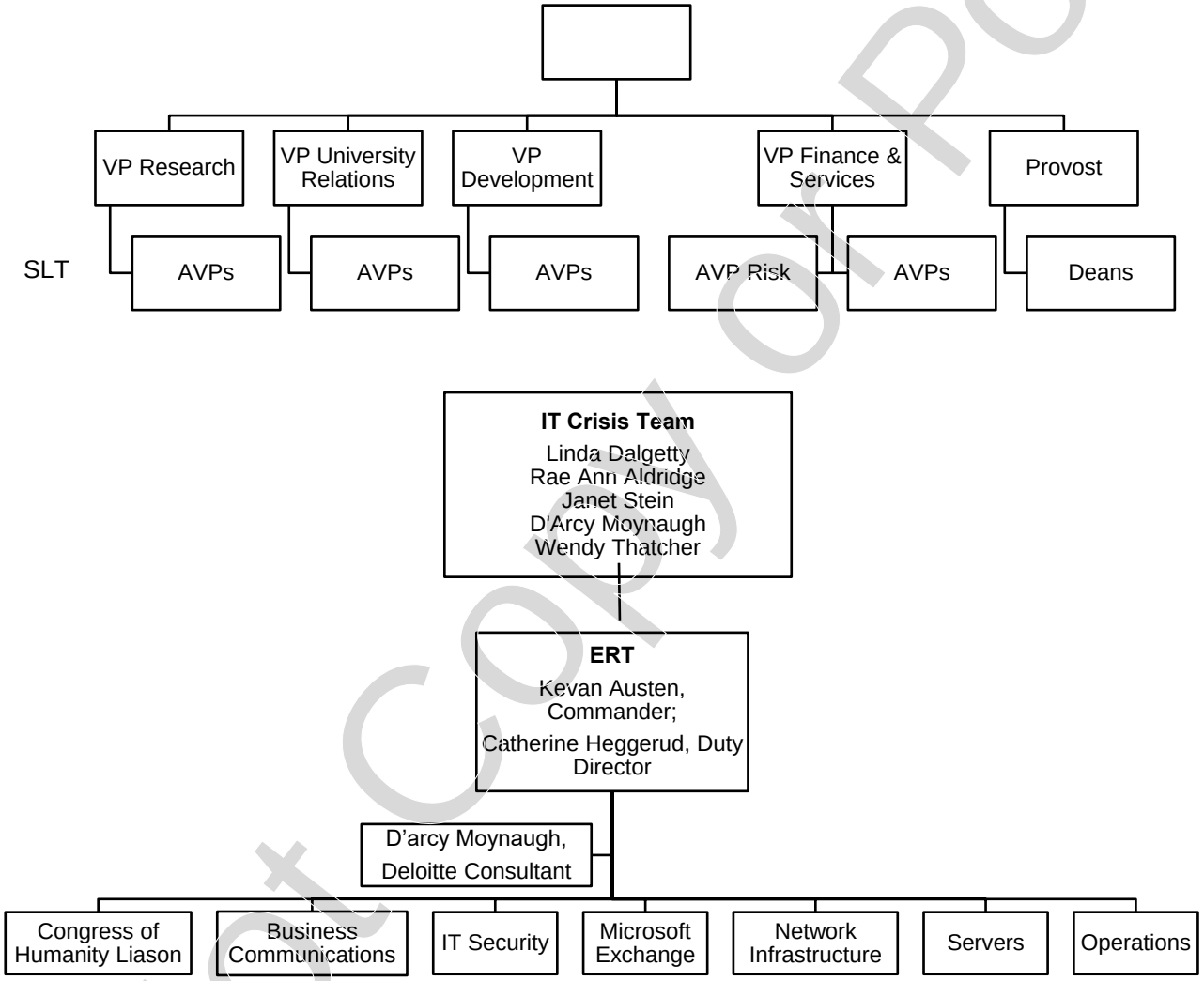
NEXT STEPS

As the clock ticked on the ransom note, the U of C faced considerable challenges. Austen and the ERT had not found patient zero—the source of the infection—which meant the university was still vulnerable to further attacks. Dalgetty faced pressure from the board and faculty, who wanted open, transparent internal communication and hoped to recover years of research. The morale among the IT team reached new lows as members continued to work around the clock on containment and remediation. To complicate matters, sleep deprivation was impairing their decision-making skills.

Should the university pay the ransom? The cyber-insurance policy would not cover ransom payments. If the university paid the ransom, how would the public react, assuming taxpayer money would go to criminals? The CMT had decided to shield both the SLT and the public from the fact that the situation was a ransom attack. Was this decision prudent? File recovery meant that researchers' files had to be scanned, risking their privacy. The order in which files were recovered also meant there would be quick access for some and delays for others. How should privacy and prioritization be managed?

[10] Sophos Ltd., op. cit.

EXHIBIT 1: UNIVERSITY OF CALGARY ORGANIZATIONAL CHARTS



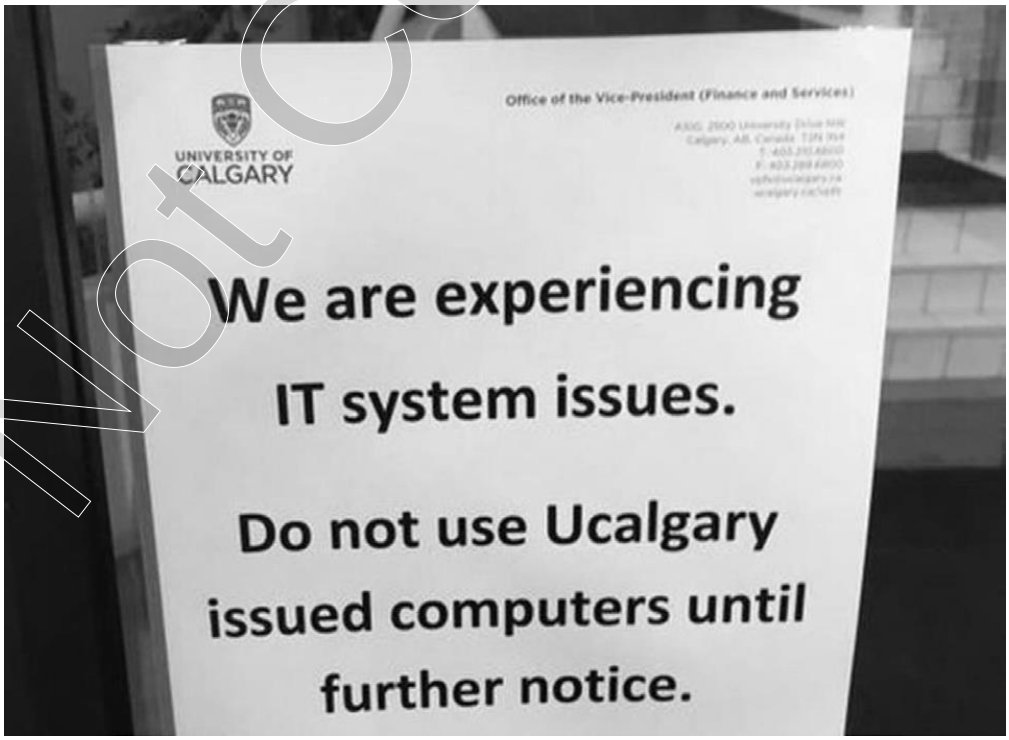
Notes: SLT = senior leadership team; VP = vice-president; AVP= associate vice-president; IT = information technology; ERT = emergency response team.
Source: Created by case authors using institutional information.

EXHIBIT 2: UNIVERSITY OF CALGARY RANSOMWARE ATTACK TIMELINE

Friday May 27, 2016	IT operations noticed suspicious activity on university servers.
Saturday May 28, 2016 (Day 1)	1:00 a.m.: Kevan Austen was called. 2:00 a.m.: The first ransom note was discovered by IT operations. 3:00 a.m.: Austen arrived on campus and activated the emergency response team. 4:30 a.m.: Catherine Heggerud was called. 5:00 a.m.: The IT crisis team was called. 8:00 a.m.: The entire IT crisis team met. 12:00 a.m.: The executive leadership crisis management team met, and Bonnie DuPont, chair of the board of governors, was notified.
Sunday May 29, 2016 (Day 2)	Key contracts were put in place, and specialized teams arrived on campus. Alternative communication channels were established, and cybersecurity teams worked to identify patient zero, the source of the ransomware.
Monday May 30, 2016 (Day 3)	
Tuesday May 31, 2016 (Day 4)	The senior leadership team met.
Wednesday June 1, 2016 (Day 5)	The executive committee of the board met and discussed the ransom payment.

Note: IT = information technology.
Source: Created by the case authors using institutional information.

EXHIBIT 3: DOOR POSTERS



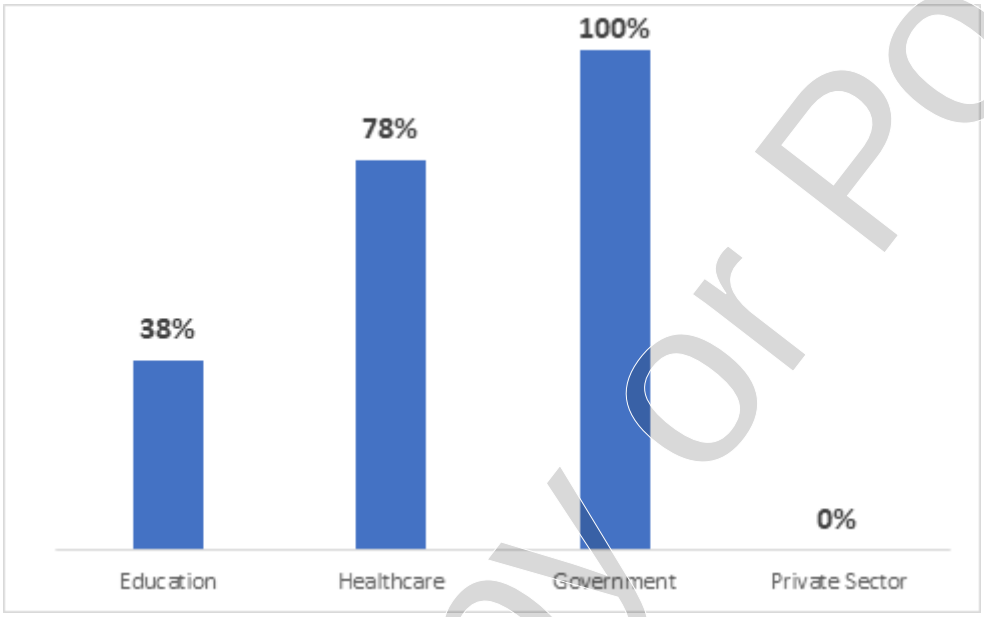
Source: Organization files.

EXHIBIT 4: UNIVERSITY OF CALGARY—IT CAPITAL BUDGET FOR 2016–2017

Information Technology Focus Areas	Description	Funding Request (CA$ millions)	Areas of Focus
Security	• significant investments required to secure the university's IT environment and ensure the security and privacy of sensitive information	1.5	Teaching and Learning, Research, and Administration
Integration	• greater integration to address increased demand for a higher level of data integrity, data availability, and data mining	4.5	Teaching and Learning, Research, and Administration
Servers, Storage, and Systems	• to employ more efficient technology and system solutions with greater functionality to address the growing requirements of research analytics, academic outreach, and student services	15.5	Teaching and Learning, Research, and Administration
Ongoing Maintenance and Support Agreements	• evergreen funds, required to support and maintain current systems affected by foreign exchange and continuous maintenance cost increases	7.0	Teaching and Learning, Research, and Administration
Data Centres	• increased demand for additional computing and storage capacity requires further investment into data centre co-location solutions, cloud platform provider solutions, and server hosting options solutions	7.5	Teaching and Learning, Research, and Administration
Total		36.0	

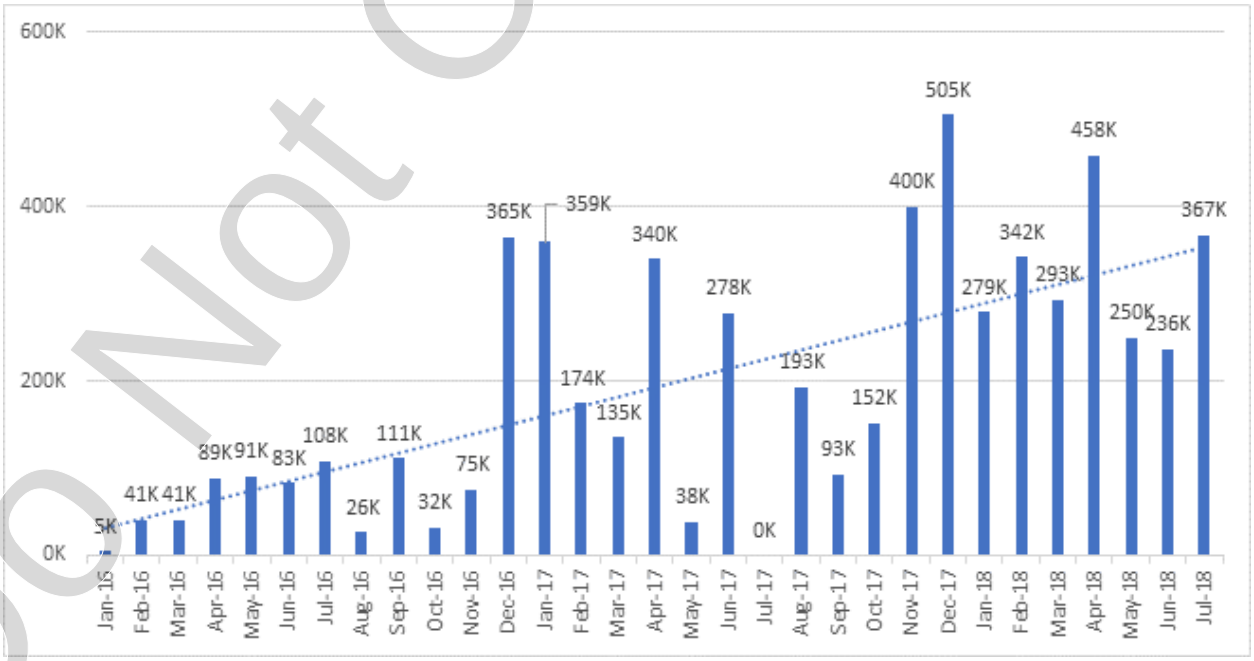
Note: IT = information technology.
Source: Create by authors using institutional information.

EXHIBIT 5: PERCENTAGE OF SAMSAM VICTIMS GOING PUBLIC, BY SECTOR



Source: Adapted by the authors from Sophos Ltd., *SamSam: The (Almost) $6 Million Ransomware*, July 31, 2018, accessed January 20, 2020, www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf?cmp=26061.

EXHIBIT 6: SAMSAM RANSOM PAYMENTS (IN US$; TOTAL: US$$5.9 MILLION), JANUARY 12, 2016–JULY 21, 2018



Source: Adapted by the authors from Sophos Ltd., *SamSam: The (Almost) $6 Million Ransomware*, July 31, 2018, accessed January 20, 2020, www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf?cmp=26061.