J Info Technol Teach Cases (2018) 8:161–171
https://doi.org/10.1057/s41266-018-0037-7

TEACHING CASE

Cybersecurity: the three-headed Janus

Erica Diffee[1] · **Pratim Datta**[2,3]

Published online: 1 March 2018
© Association for Information Technology Trust 2018

Abstract Multiple entities define the stage: Ayn, an accomplished CIO; James, an idealistic CEO; Kira, an unscrupulous hacker; Randcom, a rail company; and Zuidia, a country reinventing itself. These entities intersect in a tense cybersecurity gameplay. A cyber-attack rages across multiple fronts, targeting Randcom's technology, processes, and people, suddenly delivering a staggering blow to the company. Ayn stands in the eye of the storm, figuring a path forward. This cybersecurity case study offers an active learning and role-playing experience for students. Immersing the student in the anatomy of a cybersecurity attack, this case converges various perspectives: the hacker, the company, and the macro environment (e.g., country culture). In the process, this case highlights conflicting strategic choices and opportunity costs of decisions in an environment that requires a company to be both competitive and yet secure across three cybersecurity facets: technology, processes, and people. This case could be used as a class discussion and exercise as well as a role play with multiple protagonists. Specific roles include the CEO, the CIO, the hacker, and the CFO. This case brings together multiple viewpoints, often conflicting, representative of real-life decisional and ethical dilemmas in the context of a company. This case, further contextualized using a developing country as the backdrop, adds an additional layer of decisional trade-offs. Nonetheless, this case is representative of IS and cybersecurity decision making in a company, regardless of the type of country.

Keywords Cybersecurity · Cyber-attack · Culture · Ethics · Hacking

The Disquiet

Despite receiving one of the top positions in her country, Zuidia,[1] Ayn was restless. She had recently been appointed as the CIO of Randcom,[2] Zuidia's largest railroad company. Ayn was tasked with the job of digitally transforming Randcom's infrastructure and services to compete in a new democracy and a new century. Zuidia's media lauded Ayn's transformational caliber and pedigree.

Ayn sat down, stiffened her back, and looked up at the ceiling. Her restlessness had a single point of origin. Randcom's IT enterprise design and architecture were antiquated but the CEO, James, wanted Ayn to create and add a new IT services platform called Randcom 2.0. Randcom 2.0 was being heavily marketed as a game changer. Randcom 2.0 would create top-notch user experience in ticketing, scheduling, routing via networked

✉ Pratim Datta
pdatta@kent.edu

Erica Diffee
endiffee@gmail.com

[1] 2395 Tyre Drive, Hudson, OH 44236, USA

[2] A408, College of Business, Kent State University, Kent, OH, USA

[3] The University of Johannesburg, Johannesburg, South Africa

[1] Zuidia, although fictionalized in this case, refers to 2014–2015 events that occurred in the Republic of South Africa. The Teaching Case is based on real-life events and the South African context and emerging challenges (Symantec 2016).

[2] Randcom is used as an amalgam of two major South African companies, Gautrain, a public commuter company (https://www.gautrain.co.za/, https://citizen.co.za/news/south-africa/285122/gautrain-hack/), and PostBank (http://www.postbank.co.za/), a financial savings division of South African Postal Service, that were hacked (My Broadband 2014; Vaas 2012).

enterprise systems. In short, Randcom was trying to reinvent itself via technology. Nothing wrong with that, except for the hastiness. A new platform was a splendid idea but hastening its release could put other systems in need of serious upgrades at risk. Randcom could make itself vulnerable to a multitude of cyberthreats. New technology has a tendency to gloss over, rather than fix, old vulnerabilities. But what could she do? Should she carry-on with the Randcom 2.0 release timeline or step on the brakes of James' idea of progress and competitive differentiation?

Ayn sighed. The executive meeting was to begin in 5 min. Although she hadn't even proposed her idea, she already felt defeated. She looked at the clock again. Time to go, she thought.

James Rith, the CEO of the company, began the meeting with his vision for the future. "I want the company to focus on strategic investments for the future. Pollution from cars and trucks plagues our cities. We are an ecological alternative to driving, and our customers should know that. At the end of the day, our efforts should be about helping our customers, making it affordable to travel through our cities. But people perceive rail-travel to be a thing of the past. We have to keep up with the times with a state-of-the-art digital footprint. No more physical tickets, forms, traditional mumbo-jumbo. Time to crawl out of the vestiges of tradition and meet the new world. No doubt about that. I call it Randcom 2.0—a future-proof online scheduling, routing, ticketing, and customer service system with 24/7 access via smartphones." James paused for a moment.

Ayn surveyed the room. Everyone seemed on board with James. And of course, why shouldn't they be? It is a humble venture to be ecologically friendly and affordable. And James truly believed in Randcom and its ability to benefit the people and ultimately, Zuidia.

"User experience, availability, and accessibility are primary right now," James continued. "We want people of all income levels to be able to ride a Randcom train, to be able to travel from city to city. Randcom's services will be good for Zuidia, good for our customers, and good for the global environment. We need to stay current though. Everyone is using their smartphones to purchase everything, so why not Randcom train tickets, too? I want us to have a better cyber-presence in Zuidia, that is what Randcom is going to invest in."

Ayn was feeling antsy. James was making good points and management was agreeing with him. But they were overlooking a major problem, the one problem that could make or break Randcom 2.0. Ayn thought about how idealistic James was being about Randcom; he wanted to focus more on marketing the trains as an ecological alternative to driving. Accessibility and cyber-presence were key to his vision, but his vision was lacking one aspect—accessibility is a minefield—it needs good security—cybersecurity. It is more important now than ever before.

Zuidia as a country had leapfrogged from a lack of telephone lines to a flood of inexpensive mobile devices and affordable mobile services. Randcom's customers were more mobile-savvy than security savvy. They wanted access; in fact, they demanded access. Whip out your smartphone, open an app, and book e-tickets on the fly.

This thought made Ayn nervous. E-tickets are a cool idea, but e-tickets require money-transfers, and financial information is perfect bait for virtual miscreants. If James wanted e-tickets available, then he needed to find a secure way to provide them to the customers.

James continued to speak about the future of Randcom. "Accessibility opens up multiple revenue channels and increases our profitability. We are helping our customers and the more they are aware that trains are ecologically sound and affordable, the more customers we will have. Accessibility, travel, reliability, and affordability; I repeat: it's good for us, Zuidia, the environment, and the people." James finished with enthusiasm. He believed in his plans and was pleased with management's silent affirmation.

James continued to push his vision for the company. "If we don't give people the ability to access service in a new world, even more so in an environmentally conscious world; then we are doing ourselves and the public a disservice." Look at the European sector. Rail-travel is changing the environmental footprint in Europe, affording so many people the chance to travel without emitting carbon hither and thither. Let's use the internet to give people the accessibility and affordability. Let's build it, claim it, and market it. Let's get Randcom 2.0 live." James bristled with self-affirmation. Randcom 2.0 had a bright future ahead and would benefit the economy.

It was Ayn's turn as all eyes in the room converged on her as being the technology messiah that would lead them to the Promised Land. Ayn agreed with the essence of accessibility. It came with a multi-million dollar investment promise, championed by the CEO. It would be a large technology undertaking. But James and the board seemed to have forgotten any cybersecurity investments as line items.

Ayn spoke up. "It's time." Ayn said to the room full of her colleagues, all of whom could only think about the bottom line, the short-term bottom line. "I agree that time is ripe for increased cyber-presence. But it's also time that we made some changes in vein. We need to update our cybersecurity before we launch our services online. An unknown ground full of uncertainty, that is the new threat. We must proactively build proper defenses before we lower the drawbridge. This must be our priority when we initiate Randcom 2.0."

Everyone looked at her intently. There was silence for a few moments before Hank Hector, the CFO of the company responded. Hank had joined the company when times were tough. He was James' financial hatchet-man. Any cost that could be spared, he spared. And Hank had done well in the past few years—operational cash flows were in the black.

"Ayn, I'm sure our systems are fine." Hank responded, piercingly. "We haven't been hacked. Our information is secure. Everything is password protected and our IT department can fix something if there is a problem. There is no use spending money on something that is already working. Besides, we don't have an earmarked cybersecurity budget. Let's think about a budget line item once Randcom 2.0 goes online. I agree with James; time is of the essence and we need to invest in our priorities right now. We're already resource starved. We can't keep adding costs in the middle of a launch."

Ayn felt disappointed, but not shocked. "But you're talking about the short-term budget," she said. "Think about it long-term. How much money could someone secure from this company, the costs of employee and customer information? Do you know how hard it would be to track down everything once the data and/or information was stolen? You can have spoofed IPs, global "zombie" servers controlled by malware. It'll be a complicated nightmare. Besides, think of the company's reputation, think of how many current and future customers we could lose if people didn't think our systems were secure. And that doesn't even include potential lawsuits." She paused for a moment to sip some water. She persisted—"the damage, the long-term costs, would be much more than simply updating our cybersecurity. We should invest in the short-term to save money in the long-term."

The room was silently taut. No one appeared to deny Ayn's points yet seemed reticent about committing to action. Ayn felt a sense of unease. Cybersecurity should be a shared call to action; cybersecurity cannot be left to IT alone. It requires executive championship. But not if executives, including the CEO, remain silent.

"Think about it," Ayn steadfastly continued. "The same demographic that you're trying to elevate, James, will be left for naught if our systems are breached. Even the best intentions are laid to waste. I know Randcom 2.0 is trying to increase accessibility and availability for customer convenience. But, don't think of security as an inconvenience; security and accessibility must go hand-in-hand. Right now, Randcom 2.0 isn't even ready to handle encryption. What happens if someone, anyone, gets into the system?" Ayn waited a second before continuing.

"Then comes demographics and education. Not to mention it, but the growing generation is getting younger and more connected, both in terms of our customers and our employees. Smartphones and tablets are everywhere but there is little knowledge among users about being safe with these new devices. That situation could really create a weakness for the company." Ayn desperately searched for some support among the blank stares. She was ready to wrap up. "Keep in mind, most of Zuidia isn't educated on the importance of cybersecurity, so we have both internal and external threats. For example, most of our customers are unaware and uneducated about even simple things such as creating strong passwords. That adds a lot of vulnerability for Randcom. The same group, now, entering and saving their financial information on Randcom 2.0 without a solid encryption in the background makes it the perfect play for a predatory hacker." Ayn finished, mentally exhausted.

As the meeting carried on, Ayn thought of all the issues that could arise from a breach in their system, of all the issues she knew of offhand. Technically, their systems did not have logical separation between various servers. From a process standpoint, Randcom had never prepared an IRP (incident response plan) to respond to a cyber-attack. At a people level, employees were barely trained in cybersecurity. All it would take is one attack, even one phishing scam, and the whole company could be compromised. But how could Ayn get the rest of the executives in agreement?

Taking stock

The next day Hank came by Ayn's office. She was tired and uneasy. Ayn wanted to do her job well, but she wasn't sure how she could if no one saw the importance in what she was saying. "Ayn," said Hank. "Let's talk about this cyber "stuff" you mentioned. You know, maybe we can find a little bit in the budget and we could do some minor changes."

Ayn looked up at him. "A compromise?" She said. "I'm happy to see that you've thought about it. I'm trying to do my job, Hank. I've been reading in the news lately that all these companies abroad have been getting hacked, money and information stolen, and then they don't know how to clean up the mess. I don't want that to be us."

"You're right," Hank said with a sigh. "I just read in the news this morning that another company was hacked with some randsomware, it cost that company millions to fix everything. So let's put a little money in and then we can advertise to our customers that we just updated our systems and now we are more secure than ever before."

"I like the idea. But what you're proposing is simply the tip of the iceberg. Throwing money at the problem is like trying to stop a hemorrhage with a Band-Aid. Besides, we can't afford not to be protected. Both of us know that a budget is not the same as changing the company culture

and mindset. We need to upgrade some of our system, but we need to reengineer our processes and educate our people too. We need to fix all aspects of the problem: people, processes, and technology. We can put money to tweak our systems, but when a good system encounters a bad culture, the bad culture wins. Our processes are old, our people, including our suppliers' employees and our customers, are not up to date with the changing environment. Plus, our technology is a mismatch of legacy and new systems threaded together to keep up with the Joneses. It won't protect us for too much longer. Adding a small line-item to the budget will not solve it, Hank."

Ayn paused. She needed to break it down for Hank. To get him to fully understand that there were more weaknesses in Randcom 2.0 than can be addresses with a few system updates. "Think about these three aspects, Hank. I can update the systems with a little bit of money, but this needs to be a company-wide change. Operations, marketing, sales, HR, and IT need to get on board."

Hank pulled up a chair. He had no doubts about Ayn's competence and wanted her to get her point across. "Nobody questions your caliber or intentions, Ayn. But yesterday's meeting might not have been the best venue for expressing your concerns. That too, right after James' vision of Randcom 2.0. So, why don't you break it down to me the specific issues? I can then take it back to James and see what can be sorted."

Ayn felt a sense of ease wash away her exhaustion. Finally, she had Hank's ear. Ayn took her tablet out and went on to explain.

"We are dealing with a three-headed Janus, Hank. Technology, processes, and people."

"Our technology at Randcom needs updating, we are all aware of that, even our customers know that. The technology is a company problem but it makes us vulnerable both internally and externally. We have to get it fixed. Randcom uses a combination of old systems and databases, not to mention out of date firewalls. We have more of a hodge-podge craft project than we do an actual system. Anyone with the slightest know how could easily take advantage of all the holes in our system. You and James need to realize that you can't always just buy the cheapest system or cheapest protection and assume all the pieces and parts will fit together. It doesn't work like that. A hacker could easily detect the smallest hole in our systems and we probably wouldn't have a clue! Not to mention our lack of logical separation in our systems- that makes us highly susceptible to a full-scale Ransomware attack. Remember the NHS attack? Well we could be next!"

She stopped to look at Hank. He seemed a bit dumbfounded. I don't think he quite understood the issue with the mismatched systems. But she knew that wasn't the end of vulnerabilities for Randcom. She decided to continue. You can't only protect one corner of the triangle and leave the other two vulnerable; the triangle will crumble.

"Then comes people. Our people, Hank, that's another worry of mine. Fixing this issue isn't as easy as spending some money for system upgrades and repairs. This will take time and education and commitment from all divisions of the company. I walk into the IT department and guess what I see! Passwords written on paper stuck behind monitors or under keyboards, people logging in and then leaving the computers unattended. Not to mention how many other employees use their personal cell-phones to do work for our company. All of these activities put Randcom at risk. Our people don't understand the importance of confidentiality, nor of security. Would our employees be able to tell the difference between an email from James or a fake email that looks like it's from James? Our employees can quickly become a vulnerability for Randcom since their behavior basically invites someone to hack us. But you know, a lot of the problem is with James and the company culture itself. We can't expect people to understand the importance of security if we don't promote it within the company culture first."

Ayn knew that training employees would take time. Even if Randcom were to update its systems, it wouldn't do the company any good if the systems were left unprotected by its own employees unaware of the lurking risks. Employees are often the quickest way to breach a system. Every employee creates a potential risk for Randcom.

Ayn cautiously noticed Hank's reaction. He hadn't drifted away. After a momentary pause, Ayn continued.

"We need to also focus on Randcom's processes, Hank. I've only been with the company for a short while and things were a bit of a cybersecurity mess before me, but I am working on fixing them. My next project is going to tackle some of the processes in the company. Do you know that as of now, employees are not prompted to change their password nor create strong passwords? This is basic security, a simple process fix.

In addition, when employees log onto their systems, there is no other requirement than just the password. We really need to add a few more layers of protection, something that would increase the complexity so it wouldn't be an easy breach for a hacker. But we can't start implementing a total process revamp unless our people understand the importance of it. The last time we ran an initial systems audit, we found that there is little separation of duties. The programmers are often rotated as testers and even database developers. Without any formalized process for security demarcation, anyone of them can easily create vulnerabilities. Then is our authentication process, I mean, what authentication process? I know of multiple instances where one of our sales people called IT about a link not working. It was a third-party link and IT ran the URL (link)

without verification. What if the link carried malware? And we don't even have a proper incident response plan in place. It could have been a disaster in the making."

Ayn stopped. She had made her point. She looked at Hank for his take on her concerns.

Hank felt overwhelmed from the information deluge. Yet, he appreciated every point that Ayn made. At the end of the day, a breach could turn Randcom 2.0 topsy-turvy and open up a litigious can of worms. The cost could be prohibitive.

"Well Ayn," Hank deliberately leaned forward to convey his sincerity. "It seems like you have a full report of the company. That's great, that's what we want you to do. True, we need to do something about them now, but that needs getting operations and HR together at the table. That might take a few months, given rollout pressures. But, I promise you, I'll get it done. Let's make this our next priority with a six-month timeline for deployment."

Ayn felt restless once again. "Hank, it's not that simple. The rollout makes Randcom 2.0 open to the public. Every hacker and half-baked script-kiddie will roll up his or her sleeves to penetrate our systems. It's a game to them, sometimes more malevolent than just a game. A six-month timeline is too long a horizon in an age when the mice get smarter than mice-traps in seconds. Rolling out Randcom 2.0 with cybersecurity on the backburner is not wise. I know James wants to create a competitive advantage with a quick rollout, but I'd rather be careful."

Hank and Ayn ended the meeting with the compromise to update the systems with the budget Hank could spare. She wasn't pleased but it was a start. Once at her desk, she emailed James about a cybersecurity workshop with HR and the IT department. It would be of the utmost importance to ensure that all the employees begin some sort of workshop on cybersecurity sooner rather than later.

Genesis of the Genie

Like a perfect storm, the story begins with Zuidia, a country, and Randcom, a company, trying to waltz in uncertainty.

Randcom began with a simple vision, to bring railways to the people of Zuidia. It was a company that began with an honest attempt to build Zuidia's infrastructure and take over the government built railway system. It was a young company, not beginning until 1980, when the nationalized railway system in Zuidia was first privatized. Since then, the company's main focus has been upgrading its rail services and its customers.

Randcom operated in a country facing an emerging but difficult period. Zuidia was an emerging economy. People that had missed out on land-lines and dial-up internet had suddenly leapfrogged into a cyber-age with smart devices. Yet, there were huge educational and income disparities. A new democracy and privatization were shifting the economy in uncharted territories. A large part of the population, once deprived of economic and social upliftment, was now being ushered into a new economy with new gadgets in waiting. With fresh money flowing into parched pockets, everyone wanted a smart device as a sign of being a "have" rather than a "have not." Gadgets were plentiful; cyber-education was not.

In Zuidia, people, no matter the income, were getting accustomed to being on some sort of smart phone, or tablet, or computer. In a country that had been suddenly bombarded by ubiquitous connectivity via cellphones and Wi-Fi, staying connected was the new "it." People were always on the Internet, replete with offerings, spam, and malware. With more smartphones and online shopping, not to mention social media, it was "cool" to be virtually connected, always. Many people in Zuidia did not see the harm in sharing passwords or in shopping on unsecured networks.

24/7 connectivity was also good for Zuidia. Zuidia's Internet penetration was the highest on the continent. E-commerce was booming and tax revenues from online shopping were beginning to rival High-street shopping. The government had been briefed about potential Internet threats and had proactively passed laws to protect consumer and corporate information.

It wasn't easy to find the trade-off between development and security. In fact, there was an underlying assumption that increasing security requirements such as asset protection and encryption would hamper business development. Conventional laws were in place for people's safety and protection of property, but there was a new landscape being crafted, and a different type of security was now necessary.

On paper and in legislative forums, the government appeared to be anything but complacent. Cybercrime was a prosecutable offense. Yet, the treatment was cosmetic. The cyber world stretched beyond physical borders, which made prevention difficult. In fact, lawmakers were mostly befuddled by unknown and uncertain vulnerabilities that could compromise consumers, systems, companies, and economies.

To make matters worse, Zuidia had a detached attitude towards cybercrime and cybersecurity. With no criteria for enforcement or monitoring, cybersecurity laws were just for presentation. Moreover, people and companies in Zuidia were complacent about potential dangers lurking behind every click, search, and download; they didn't understand the consequences. Cybercrime was on the rise and defenses were inadequate. It was reported that more than 50% of the adult population in this country had been a victim of cybercrime.

Despite the country being the third highest victim in the world for cybercrime, the government instituted cybercrime laws but not cybersecurity education. Without education and awareness, Zuidia could become an even easier target for cybercriminals because of the overall lack of cybersecurity knowledge.

The problem was evident in the statistics. Cybercrime costs in Zuidia were on the rise. In the past year, cybercrime cost Zuidia nearly 1.6% of its GDP. The government and policy makers understood the importance of having laws in place to deal with cybercrime. Having ratified the European Council Treaty on Cybersecurity as well as participating in UN talks on cybercrime and prevention, the government knew that if the more developed countries were making cybersecurity a priority, then this country should too. Zuidia's government felt that if a law was in place, the country was safe. Little did it understand that protection from cybercrime was more than a technology issue, it involved people and processes as well.

Then there was a new generation of criminals. A single push of a button could affect thousands of households and companies in an instant. Moreover, with media attention towards some hackers as modern day Robin Hoods and the open availability of hacking kits for curious "script kiddies," it was open season. The threats were invisible, hard to detect, and borderless, and there was little recourse.

It was within this landscape that Randcom was operating two divisions. The railway system division handled internal operations including timetabling, rail services, employee payroll, among others. The customer service division mainly focused on ticketing, access, and customer relationship management. Systems across the two divisions were loosely connected by middleware that seemed more like an afterthought than a deliberation. Randcom needed to stay competitive in a time when railroads appeared to be a thing of the past. In its drive to keep up with the times, Randcom used its IT group to tackle all technology requirements across both divisions. The same IT personal that was developing the CRM database could, in a few hops, also access ticketing information. There was no separation of duties.

Randcom had just launched the Rand Card. Much like the Oyster Card in the U.K., Rand Card would allow prepaid multi-transit advantages to customers. Sadly, Rand Card was only sold at the ticket counters or newsstands. Randcom announced that the Rand Card would be available for purchase online in a few months. Randcom was going to embrace the digital-era. What could go wrong?

A curious unraveling

It all began with a seemingly basic call from payroll. For some reason, payroll funds were short and HR wanted to know if it was a glitch in the system. Ayn was confused by the phone call but figured she would personally follow up with the IT department just to be safe. She reached out to her IT Director, Lev.

Lev responded within the next five minutes. All systems were good and validation checks were in place: no glitches, except an unknown stream of transactions that appeared to be cross-account transfers. But when he looked closer into the transfer schedule, it seemed suspect. Someone was siphoning funds to an external account.

Ayn had paused with a sense a dread. She understood all too well what had happened. Randcom 2.0 had just been compromised. Funds had been accessed and stolen through the payroll system.

Before Ayn recovered from Lev's response, she received another email from the customer support department. Strange, she thought, what could customer support want from her at this hour?

"Shouldn't customer service be escalating all matters to the supervisor and then to Lev?" Ayn thought? "Who knows?" she said out loud as she shook her head. There was no established escalation and incident response plan in place. She felt as if she was facing a typhoon in a tattered raft.

The customer service email signaled panic. Hundreds of customers were starting to complain that they had ordered a Rand Card from the website but hadn't yet received it, even though the customers had been charged. She tried to consider all the possibilities; did James launch the online Rand Cards already, without telling her? No, couldn't be. She searched for the website, she wanted to see it herself. Before she had finished reading Lev's response to the payroll funds shortage, Ayn found herself feverishly forwarding Lev the latest Rand Card crisis.

She opened the email and began to read. The more she read, the quicker she read. Customer support had forwarded her a series of customer emails, all with the same heading "Purchase your Randcom Tickets here." The email address, ticketsales@randcoms.com, appeared credible except for a minute detail; the domain, instead of randcom.com, read randcoms.com. Below it was a well-crafted message:

> To all valued customers,
> Randcom announces its brand-new online ticketing service, Randcom 2.0. We invite you to purchase a Rand Card as the next-generation ticket and save 15% off our regular fares. This special offer will end by midnight, the 17th of June, 20xx.

Please click this special link at www.randcardsforrandcom.com to purchase the Rand Card and activate your discount.
Sincerely,
James Rith, CEO
Randcom

She cautiously hovered over the www.randcardsforrandcom.com web address and looked at the real web link. It was an open IP address, 107.xx.xxx.xxx. She needed to see where the click would carry her. Ayn made sure her security was active and all virus and malware signatures were up to date before proceeding. She clicked. A site, phished and spoofed to look like Randcom, opened up. Simultaneously she did her application security. The site was trying to execute a Trojan bot onto her computer. This type of Trojan bot worked independently and secretly collected financial information and transferred it to a remote server controlled by criminals.

Ayn felt a cold sweat. How many customers have fallen for this? She thought. She took a deep breath; Randcom had just been hit on two fronts in such a short span of time.

She needed to tell the board. Ayn sent an email to James requesting an immediate conference call and telling him briefly about the crises. Within minutes James responded, suggesting a conference call in 15 min. It was 2 am.

As Ayn dialed into the conference call, her mind was racing. When was payroll breached? What else might have been compromised? Randcom's R&D, release data, the lot? When did the fake website get built? The timing was too uncanny. Were the two events connected? How much damage will it do to Randcom's customers and the Randcom brand?

Her head was spinning. It wasn't even 2 months ago that they updated their systems, added new software, and patched up a few vulnerabilities in the website. James and Hank gave her the budget to fix some immediate issues, and yet her worst nightmare was now a reality.

The phone was ringing now. With each ring, Ayn prepped herself about Randcom's system updates. The website was secure, firewalls were in place, and some intrusion detection for the application and content servers. All essential operating software had been updated. That had taken up the budget. Process reengineering and training were budgeted for the six-month horizon. She joined the call.

"Hi. Yes, its Ayn. Dialing in for the meeting. Where are we? Any new updates?" Ayn felt nervous.

James was frantic. "Ayn, tell me what happened? I thought we put money into our systems just 2 months ago! How the hell did this happen? Do we even know what they took? Should we tell the customers or keep quiet?" Randcom 2.0 was meant to be a game changer for the company and for the people, so how could something bad happen to something meant to do good? It just didn't make sense, James thought.

Ayn took a deep breath. "Yes. Hi James. I've been up all night. We implemented new software, made sure it was all up to date. Our payroll information resides behind our firewalls, not in the DMZ, you know, the publicly accessible demilitarized zone. So, it couldn't have been a total compromise of our systems. There is just no way for someone to externally get into our systems." Externally. That was the word—externally. Ayn's mind stopped racing and became more focused.

"James, remember I suggested a cybersecurity training program for our employees? I know you thought that a system update would be a one-time fix. But, what about our employees? Do they understand the importance of the data we handle? Do they know how to keep our systems secure internally, from our end? And do we vet our employees? They are the ones that are our 'trust interface' with the public. Do we have the right processes in place to ensure trust?" Ayn started to think of all the possibilities. People are always the weakest link.

James sat back in his chair. He did tell HR to do something about a cybersecurity workshop. But really, what wouldn't the employees already know? Just don't give our company information; it's simple, he thought. "Well, Ayn. HR and IT were expected to schedule cybersecurity workshops and training for the employees. But the Randcom 2.0 rollout was priority. And really, Ayn, do you think our employees wouldn't know how to be secure?"

Ayn felt her shoulders tense and her knees lock. Cybersecurity is a part of a company culture. If the CEO does not appear to care about championing cybersecurity, why should the employees care? The lax company culture about cybersecurity went all the way to the top. James had good intentions but was too complacent and trusting about the new threat landscape.

She raised her head and spoke into the phone, "James, most threats nowadays originate from inside companies, whether the employee intentionally or unintentionally acts. A culture of being unaware is still as big of a threat as being malicious. If our own employees are unaware of cyberthreats and vulnerabilities, then they can end up putting the whole company and our customers at risk." She wondered why she was the only one considering this possibility.

James's voice broke through her thoughts. "You know, Ayn. I trust my people. I don't think any of them would intentionally harm this company. And I can't imagine anyone wanting to target Randcom. I'm sure this is all a system malfunction or something. Just a glitch! Think about it, we aren't a bank or a healthcare company, we are

a train company; what valuable information could we possibly have?"

"James." Ayn said. "Lev, our IT director just emailed me the logs. It is not a system glitch. It was an intrusion. Perhaps a malware inadvertently installed by our employees. Lev is doing a complete sweep of all terminals and systems as we speak, and we'll know something soon. We ended up installing a bunch of new technology and software to speed up the rollout but we never changed the processes. With such a mish-mash of software and systems, we don't even have a formal process for patch updates and point-to-point encryption because an update to one piece of software could end up changing config files and other parts of the system could slow down or stop working. We don't even have a formal risk management process or even a process or incident response plan (IRP) for incidents like this." Ayn paused.

Ayn looked down to her computer screen. Lev's sweep report had just arrived. Multiple terminals were infected with a Trojan virus—the same Trojan virus. Randcom had always practiced file-sharing to increase collaboration and the file-sharing could have allowed the malware to infect multiple computers. Ayn took a quick stock and returned to the call.

"James, this is what we know. Some kind of malware infected our employee terminals and the file sharing service made matters worse. We think it is a keylogging malware, one that logs all the keystrokes and then sends the information back to the cybercriminals. That could have compromised userids and passwords. Lev is taking care of the issue but the harm is done. We know that someone was able to obtain employee passwords and information in order to infiltrate our system and siphon money from payroll." Ayn paused for a moment. She was exhausted, but the drive to know exactly what happened kept her going.

Ayn continued describing the situation in a controlled manner. "Also, we are aware that there was a fake website registered to an unknown party under the name randcardforrandcom.com that was selling our Rand Card online as the latest offering from Randcom 2.0. Now we all know that the Rand Card is currently available only at physical ticket counters. This spoofed website used a phishing attack to make people believe that Random 2.0 had just launched and that people could purchase Rand Cards directly from the phished website. We also know that this website managed to operate for 1 month without our knowledge, thus successfully stealing customer information and payment. I ran a WHOIS to find out where the attack and the IP originated but it looks like some anonymously registered overseas entity. But, the perpetrators could have masked it. They could be anywhere."

Ayn's voice now turned resolute. "What we don't know is whether or not these incidents were separate or orchestrated. We are calling in the federal branch. We have to figure out a way to respond to customers who purchased Rand Cards from the phished website. We have to find a way to communicate to our employees the payroll incident and how we are addressing it. Most of all, we have to address the loss of trust in Randcom to the public. How did this happen, like a perfect storm?"

Ayn took a deep breath. Even over the conference line, an anxious, eerie silence was palpable.

Hacking, she wrote

One month after the minor Randcom system update, in a quiet corner of an Internet cafe a few blocks from Randcom's corporate offices, Kira felt uneasy with excitement. The last company she hacked had gone well, or so she had thought. She was able to take enough money to last her awhile. But this time, it was different. Randcom had been heavily marketing Randcom 2.0, its new online train scheduling and ticketing system. People were talking about it and anticipating its release. Kira knew Randcom had spent millions creating the new system; it was all over the news. New systems have learning curves and vulnerabilities, she knew that. Three-pronged vulnerabilities: technology, people, and processes. Kira knew that it was easier to leverage vulnerabilities that were more acute than just technology—vulnerabilities in people and processes. And Kira knew that people were always the weakest spear in the cybersecurity triangle. She was going to go for it. Over a latte and a croissant.

Kira reminisced about her last attack. A few years ago, she had managed to siphon millions from a national bank in Zuidia, one that touted its "secure and safe" system to its customers. She had managed to penetrate the bank's system and maintain access for 3 days while the bank was closed for the holidays. It was a simple hack. Once she was inside the bank's systems, all she had to do was set up a few fake accounts at the bank with fake IDs. On the day of the cyber-robbery, she increased the withdrawal limit on these accounts from inside the bank's system and then transferred the money to external accounts at other banks. It was so simple, she mused. She had set up at another Internet cafe on the westside of town and was able to complete the heist while having her macchiato and scone, different tastes for different heists.

Kira's latest inspiration came from reading an article about international cybersecurity state-of-affairs. "The majority of cyber-crime, even the most sophisticated, is based on the simple exploitation of traditional IT access

credentials – cards, PINs, passwords (CPPs) – it's just so easy."[3]

Kira, nonetheless, felt uneasy and on edge. She was an employee at Randcom. It was unethical but Kira had lost her ethical bearings a long time ago. It was risky, but she might be able to hide her crime with a twin-flank attack. She had to set the stage.

Her first attack flank would come from outside the company. She had set up a fake website that lured customers to give personal information and credit card information in return for a railroad card sent via mail within 30 days. This would buy her a few weeks before customer complaints would flood the company. In addition, she was taking advantage of the fact that Randcom had announced it would make the Rand Card available for online purchase, but did not specify a date. Unwary customers were easy to fool.

As for the internal attack, she would go through the payroll system. Payroll was a legacy system, one that had rarely been upgraded or updated. With the newfound excitement about the Randcom 2.0 platform release, she assumed that no one in the company would even monitor the payroll software. The company spent a lot of money on firewalls and some IDS (intrusion detection systems) but mainly for services surrounding Randcom 2.0. Payroll would be "the" candidate for the breach. All she needed to do was use the spoofed email she used for her fake website and send payroll employees a credible "memo" email asking them to open an attachment hiding a keylogger malware. As long as the memo subject read something mentioning "Randcom 2.0," employees would open it with all urgency and little suspicion. People were always the easiest way to access any system, especially the Randcom employees.

Kira knew that every company falls prey to the same false notion: that technology is their only cybersecurity vulnerability. She would leverage her attack on three fronts: technology, people, and processes. Three points of weakness in a company and Randcom was no exception.

Technology

First, Kira knew that Randcom's systems were a product of evolution from the 1980s. There were legacy systems everywhere. What worked then was still in use, despite Ayn's minor upgrades. New software was band-aided to the legacy patchwork with some middleware and most advanced software was on the server-side. Client side applications were often outsourced with more emphasis on visual appeal at the presentation layer rather than ensuring resilience. Thus, it was what came to be a hodge-podge of different platforms, software, and web services. One didn't even have to be an employee to know this information; it was public knowledge and a quick Internet search revealed a litany of technology issues Randcom had suffered over time.

Ayn, the CIO, had recently been appointed and she wanted to revamp the entire architecture based on a robust, six-sigma software service management agenda. Ayn wanted all legacy systems to be moved server-side with better access control and software-as-a-service. Ayn's vision was well known and lauded by business and IT magazines. The change was coming in the next year or so. For a hacker, time was of the essence.

With the announcement of Randcom 2.0, Kira knew that Ayn could merely focus on minor software and patch updates. Randcom had recently been touting its new system upgrades for Randcom 2.0 to its customers. But overemphasizing Randcom 2.0 had left Randcom's legacy systems unprotected. As an employee, it was easy for Kira to know about vulnerabilities in the payroll system. Companies often think they need protection from external attacks and skimp on protecting themselves against internal attacks, as well. This was Kira's chance.

People

Whether it is a company or a country, people are the weakest link in the cybersecurity triangle. Randcom's executives barely championed cybersecurity as a part of the company culture. Cybersecurity was an IT buzzword. Kira knew that one did not need to be an employee to realize that the company culture reflected the country's lack-adaisical cybersecurity culture. Even as an employee, Kira knew of Randcom's little to no attention given to cybersecurity. Managers didn't care if employees shared passwords or left them written in the open. There was no clean desk policy. Employees could print any document and leave it in the open or copy it on USB devices. Like Zuida, her country, there were a modicum of policies but none cared about implementing or enforcing them. None cared if a personal phone or laptop was used for work purposes, especially because it saved the company money. And of course, Randcom had never run formal company-wide cybersecurity and risk training on even something as simple as a phishing scam. Even in a digital world, Randcom never educated its people on the dangers and risks to data as a corporate asset. Employee ignorance, phishing emails, and malware: that would be Kira's recipe and employees would be her channel for malfeasance.

[3] http://www.itweb.co.za/index.php?option=com_content&view=article&id=50608.

Processes

Kira had heard one too many times an adage: "Combine good technology, good people, and bad processes. Bad processes win." She knew that Randcom had rarely changed its processes in decades. There was no separation of duties. A payroll employee could also be assigned to help with building an employee benefits database with full access. Randcom interns were rotated across multiple departments but their old access privileges were never deactivated. That meant that an intern could access multiple different roles at any point of time.

Randcom had a cybersecurity process policy on paper: predict, prevent, detect, and respond. Predict risks and vulnerabilities by periodic systems audits; prevent cyberattacks by ensuring every system and terminal was secure; detect threats with proactive monitoring; and respond to attacks in a systematic way. But Randcom never implemented them. Frankly, Kira was certain that not even 10 percent of the company knew of Randcom's cybersecurity process or the policy. If Randcom were hacked, a lack of legacy system monitoring would let an attacker roam free for days before being noticed.

Finally, Kira knew the process employees used to log on to their accounts, a simple password verification. It was easy really. She couldn't even remember the last time Randcom requested password changes or data encryption. Most companies don't realize that the process itself is a form of security as well, especially internal processes. All she had to do was obtain a few passwords and she'd be in, nothing more than that. Nothing was encrypted so accessing data, including financial data, would be simple. It was a process waiting to be exploited.

Facing the fray

Dawn crept through the concrete and trees, glistening the glass panes at Randcom's headquarters. Ayn had stayed awake that night, piecing the puzzle together. As morning crept in, it was starting to make sense. For cybersecurity to work, the cybersecurity triangle of technology, people, and processes must work in unison. Even if the system was updated and secure, what happened if processes weren't well defined and employees weren't educated? A laissez-faire corporate culture towards cybersecurity does not help. Cybersecurity cannot be blind to unseen risks.

The answer, Ayn realized, lies in taking a proactive attitude towards cybersecurity. "When you invent a new mousetrap, mice get smarter," Ayn dryly mused. Randcom needs to be proactive across all fronts: technology, people, and processes. Technological proactivity needed a strong asset management and monitoring culture. Every system needed protection and continuous monitoring. From a people perspective, Randcom needed to indoctrinate in its employees and customers a culture of prevention and accountability. Finally, Randcom needed to reengineer its processes to creep out of antiquated ways of managing assets, auditing systems, preventing breaches, and responding to incidents.

But for now, first things first: How should Randcom communicate the two breaches to its employees and to the public? Some of, if not all of, Randcom's employees are also Randcom customers. That added to the complexity. Communicating the breaches was imperative. Yet, she was unsure about how to proceed. Should she wait for the Federal Investigators to brief her? Or should Randcom address it right then and there, in the open? What would be the fallout of each choice?

Perhaps this incident will be an eye opener for James. He held everyone's respect and his cybersecurity championship might finally start changing the company culture. But, what else? Who should educate the customers and change the customer culture? A country's culture often bears more influence than a company's culture. But, when both country and company cultures lack a culture with a cyber-secure focus, then everything is at risk. Zuidia needed a national culture, a proactive and preventative attitude towards cyber-awareness. Will this be a wake-up call for the government to create a more engaged culture of cybersecurity awareness, accountability, and enforcement? Could Randcom work with the Zuida government to create a public–private partnership to change the national cybersecurity culture? Too many questions, too few answers.

As Ayn heated some stale coffee in a microwave, a new email from Lev arrived. Lev had been looking at various web, access, and query logs to infer something that could shed more light on the two incidents. Lev's initial assessment confirmed Ayn's original suspicion. The fake website used to steal customer payments and the internal breach to steal from the payroll system were linked. It had to have been an employee that was familiar with the company, familiar with the software, and familiar with the general company culture about cybersecurity.

Lev's email portended something else. Something ominous. Perhaps, the perpetrators were not yet done. Lev heard that a new email was beginning to circulate, aimed at Randcom employees and customers. The email was another attempt at social engineering. The email was spoofed to look like a Randcom email. It was veiled as a update on the breach and asked all email recipients to click on another link, certainly to a phished website, to update their passwords for safekeeping. That would put more employee and customer information at risk. Ayn had forgotten to sip her coffee. She scrambled to craft another response. It was never-ending.

Ayn felt helpless. She was facing one or more perpetrator or perpetrators devoid of ethics and careless. There are anonymous, nameless, faceless entities lurking in virtual shadows—intent on causing mayhem and malfeasance. It was criminal. They left a path of destruction but few footprints. Where should she focus? Stop customers from purchasing fraudulent Rand Cards from the phished site? Isolate and fix the payroll system without knowing what else may have been compromised? Address the new social engineering crisis that could further compromise employee and customer personal and financial information?

One thing was certain. The Randcom brand had been tarnished for a long time to come. The damage to Randcom was more than money; it was trust. Randcom stood to lose its customers, its reputation, and its credit rating. This could invite a stream of litigation. Ayn knew that she needed to face the fray and craft a plan of action. She was always resolute, even in the face of adversity. She closed her eyes and breathed deeply.

As Ayn emailed the executive team to schedule an urgent meeting in the next hour, her video intercom buzzed. Federal investigators had arrived to help. Ayn readied herself for the first or many meetings and many a sleepless night ahead.

Teaching case discussion questions

- What is the ethical dilemma for Randcom between choosing greater public access and protecting consumer privacy? Is the CEO unethical? Why or why not?
- How should Randcom ethically communicate the hack to its customers? How would you handle the incident and create an escalation procedure that balances the company's well-being as well as that of the customers?
- From *technology and IS standpoints*, what would you recommend Randcom should have done to prevent, diagnose, and mitigate the breach? Establish an Incident Response Plan (IRP).
- From a *process standpoint*, forward three BPR (Business Process Reengineering) actions that would have mitigated the Randcom hack.
- From a *people standpoint*, propose three Cybersecurity training practices that would create a more prepared workforce that can better deal with cybersecurity threats.

References

Symantec. 2016. Global Forum for Cyber Expertise Initiative: Cybercrime and Cybersecurity Trends in South Africa. November.

My Broadband. 2014. Massive privacy, security flaw with Gautrain-linked site. *Naked Security*, October 2. https://nakedsecurity.sophos.com/2012/01/20/hackers-snatch-6-7m-in-south-african-cyber-bank-robbery/. Accessed 30 Jan 2018.

Vaas, L. 2012. Hackers snatch $6.7 m in South African Cyber Bank robbery. *Naked Security*, January 20. https://nakedsecurity.sophos.com/2012/01/20/hackers-snatch-6-7m-in-south-african-cyber-bank-robbery/. Accessed 30 Jan 2018.

Erica Diffee holds an MBA and a BA honours in Economics and a member of the *Phi Beta Kappa* society. She is also an author of a children's book, *Sella the Sharkie*.

Pratim Datta is an Associate Professor of IS, the PhD Director at Kent State University and a Senior Research Associate at the University of Johannesburg. Dr. Datta have over 30 journal publications and over 25 conference proceedings in journals such as *Journal of the AIS*, *Journal of Information Technology*, *European Journal of Information Systems*, *Information Systems Journal*, *Journal of Knowledge Management*, *Communications of the ACM*, *IEEE*, among others. Prior to academia, he worked for IBM and PwC.

Reproduced with permission of copyright owner. Further reproduction prohibited without permission.