INTRO

IVK is a mid-sized fictional company on a rise after a metaphorical fall involving the previous CEO and some stakeholders. The replacement CEO; Carl Williams is hired to turn the company around. He picks Jim Barton, a Loan Operative manager famous for picking fights with the previous CIO, Bill Davies, to ironically fill Davies' place. Several Chapters in, and a lot of learning on Barton's case, we reach our first major issue in Chapter 11. One, that, could tear down whatever Williams had built up. A DoS attack and some recorded tampering in client databases. This is a big deal because the client databases held everything that was needed to commit identity theft. Three solutions are given. Do nothing, shut down the company, or build a mirror site from development files and shut down the original product. This event concludes with the firing of two senior staff members, an unethical and risky decision by Williams to hide everything and do nothing, and Barton receiving an unhealthy dose of anxiety and guilt. In the following chapter, Barton becomes paranoid that Williams wants to use him as a scapegoat if things go south. That if Williams' coverup plan fails, he'd be dragged down with him. He continues to ask himself why he didn't get fired until he gets a rude awakening in the form of an email from Williams. Williams tries to encroach on the IT area by sending several controversial and biased articles on IT and its management. The email formatting tells Barton that Williams has lost faith in him. Barton then makes measures to find better ways to communicate with Williams from the IT view.

Three chapters later, a new set of issues come to light. Talent is a rare thing, and having many unique talents is rarer. One such talented individual is Ivan Kroffsky. Ivan is a bit eccentric; he believes that software should not be patented and in protest, he turns malicious. He actively works on a side project to flood patent passing offices with fake patent requests in what is essentially a DoS attack. Worse even, Ivan wants to do this on company computers, and does so on company time, conflicting with the high priority Alpha3 project he is placed on. Ivan is one of a few yet to be identified hard to replace individuals within IVK, and the one who makes Barton realize he really should identify them for future endeavors. No real solution other than speaking to Ivan could be offered. They suggest "big brother"-ing all employees in the future, it is not a good way to keep the talent happy, so they move on. Later in the same chapter, Barton meets John Cho, another one of these talented, tough to replace individuals, at a jazz gig. Cho and Barton's relationship has been a strained one and Barton uses this opportunity to gain a unique view on collaboration to repair the relationship some.

Chapter 18 picks up in the middle of a meeting between Barton and Williams as they discuss how to manage and reduce the risk for the IT department. After some self-reflection on Williams' decision in Chapter 11, the CEO and CIO settled on a way to prioritize and categorize risk and cost of protection. This is to be their standard moving forward and is represented by overlapping goals on the scale of Tolerable and Intolerable with high and low-cost risks.

BACKGROUND

In a grouped fashion, let's start with Bill Davies. Bill Davies was the previous CIO, but not a well-dressed or well-spoken one in Barton's opinion. This led to Barton taking him lightly, and what could be kin to bullying Davies. Barton would knock Davies down for being too technical or for wearing a cartoonish tie. And after Barton takes on Davies' job, he suddenly realizes that Davies was actually well respected by his team. This leads to Jim developing a new acronym for himself; UWGDF, Understand What Got Davies Fired. Because he realized, he didn't actually know what got Davies Fired. After he gets ahold of a private peer review on Davies, he found the most likely reason. "Davies had a tendency… …to pull back into the confines of his familiar IT world when faced with difficulty, especially conflict with an executive from the business side." [5,

p. 82] The ironic thing that Barton doesn't seem to realize here, is it's likely Barton who was the "executive from the business side". The Irony continues in full by chapter 8. Barton had shut down and made Davies and Cho into a laughingstock when they shared information about a security hole in a presentation. He had used it as an opportunity to deny their funding and to redirect the funding to a Loan Operative project. This is what caused the hole to remain as a vulnerability, leading to the tampering in the client databases.

Carl Williams is a major character throughout the novel. In the very first chapter, we realize that he holds Barton in high regard, even stating that he liked Barton's work in loan operations. But that point directly causes conflict for Barton when, in chapter 9, he realizes that Williams has every reason to see him as a threat and rival for his position as CEO. There is even more evidence to Barton being a threat because he was considered for a COO position and tended to be invited to lunches with higher-ups. Becoming a major form of confusion for Barton when, in chapter 11, he dodges a punch and doesn't get fired. The DoS attack happening under Barton's watch would give a perfect opportunity to remove a rival, but Williams didn't. Most of chapter 11 focuses on Barton's worrying about this, specifically what Williams might have planned for him. By the end, we still don't know the reason why Williams didn't fire Barton. But we do know they seemed to be on much better terms by chapter 18.

At its peak IVK IT held a value of $75.12, and after its tumble, landed at $30.72. Barton takes note of this starting in chapter 5 when things are still relatively calm, and we watch as it gradually rises, until hitting a bump during the DoS attack, only to rise again gradually. The numbers are relevant because in chapter 18 William acknowledges that the $30.75 went up to $50, clear evidence of Barton's success.

The June attack essentially took out the website services for the company, and then blocked out customer support by sending every second, 3 emails containing the word gotcha. This is the DoS attack mentioned everywhere. It was clearly a malicious attack.

DISCUSSION

In chapter 11, the major points to look at for us was in the options and decisions made after the DoS attack. Three options were presented and we commented on each in terms of ethics and commercial benefits. The first was; do nothing, which we felt was a very risky option. It is not necessarily a wrong one or a bad one, but it is not ethical and has a chance of failing spectacularly. The second was; shut down the company. This option would essentially publicize the event, and since the company was already on thin ice, this could spell the end for the company. So, an ethical one, but not a corporate one. The third and final one; build a mirror site from development files. We felt that this option was the best of the two. It avoided a fatality for the company from publicizing the issue, and would also repair the security holes to prevent it from happening again. However, despite being ethical and one to prevent the company from failing, it is the most expensive. It cost more money than they likely could afford at the time. Which is probably why Williams chose to do nothing. While being a major risk, it was probably the best option of the 3 for the company surviving. As Williams mentions in chapter 18, only big and stable companies can afford to play it safe.

Chapter 12 seemed to focus around a major question: why wasn't Barton fired, but two other senior executives were? The executives only went against the decision, while Barton was seen by Williams as a rival, plus Barton brought up and caused the event directly. We threw around ideas for a while about this and adopted Barton's as the most likely. Theory one; Williams needed a scapegoat to keep around if his decision to do nothing fails. Theory two; Williams might have

found beforehand that the company can't afford to replace Barton. Theory three; Williams might respect Barton on a personal level. All of these have points to support them, but the one we agreed on is that Williams respected and still needed Barton. We believe this because Williams first and foremost, had identified Barton as a rival. In order to even be considered a rival for CEO, you'd need a lot of redeeming qualities. Williams also mentions how much he liked what Barton did as early as the first chapter, even stating that if anyone could make the jump to CIO, it would be Barton. So, we definitely feel that Williams might even believe there may be consequences to firing Barton, especially with Barton's connections to higher-ups.

In Chapter 15 we meet Ivan Kroffsky, a real eccentric in our opinion. We all felt alarm bells in our heads when we read about him wanting to use company computers to attack patent processing servers. Not to mention building the software to do it on company time. We felt that even though he's talented, IVK should not be that lenient towards him. Cho is another hard to replace talent but we feel that Cho and Ivan are not even comparable. While Cho takes time off to use towards his Jazz band, the experience helps develop team skills and is not a potential liability. We don't feel there is any other solution other than to tell Ivan off and make sure he's on the same page as the rest of IVK. The other solutions like tracking employee contribution and stuff we know from personal experiences is a standard, but not an active one. It should only ever be done as a form of log to look back on if something goes wrong or for peer reviews.

Chapter 18 was relatively uneventful. It was mostly a confirmation that Williams had made the right decision and didn't regret it. We know that Williams was hired because he's turned around the failing status of several companies, so we know he has experience with making risky decisions. We fully agreed with the risk management concept they came up with. So there was nothing really to speculate on or discuss other than what could be linked from chapter 11.

CONCLUSION

We stand by the decision for Carl to do nothing in regards to the DoS attack, even though it may not be ethical or effective. This is mainly because the company is in a difficult position in terms of growth and finances. We also firmly believe that Carl respects the work Jim Barton does and for who he is a person. Jim's previous position as the directory of Loan Operations lives to tell the tale, so despite the fact that Carl did not listen to Jim, he would be hard-pressed to fire him. We then have Ivan Kroffsky who should stop working on his personal projects on company time. It is important to support your workers and their passions, but not at the detriment to the company. It can inspire others to do the same and lead to drainage of company resources and money. Ivan should just spend the vast majority of his time working for the IT projects of IVK, because that is what he was hired to do**.** In summary, IVK is a company that took a lot of damage from the DoS attack, has a somewhat difficult communication executive pipeline, let's talented workers work on their own projects and takes great risks in their executive decisions. This combination surely sounds like a long-term disaster in the making, unless things change.

Q1. For the most part, Jim Barton, let his IT team do the dirty work in figuring out what may have happened on the day of the DoS attack. One of his workers Cho even spent 40 hours straight trying to figure things out. As the CIO, putting your best resources in charge of such situations is the right thing to do, and with Jim's level of experience in IT, it was the correct decision. It was good that the IT team was able to put together a list of possible choices of what could be done regarding the DoS attack. This laid all the possible options on the table and the one that everyone (not only Jim) agreed upon as the best decision would be the one to go to Williams. Later on, Jim reaches out to Maggie and Jonathan (the kid) for advice. Normally, it's best not to involve people who don't know anything about the company, but considering these unusual circumstances, where

Jim is new to being a CIO, it might have even been beneficial. When it's time to make a critical decision, sometimes it's good to get the advice of other people because it's not like everyone knows what to do at all times, especially in Jim Barton's situation.

Q2. The decision this question is referring to is when Carl Williams decided not to shut the company down for security upgrades, system repair, and maintenance. This was certainly a difficult decision for the CEO to make, so it is not a simple yes or no type of answer. We believe that Carl Williams did make the right decision for the success of the company and corporate realm, but not from an ethical or legal perspective. In Canada at least, companies have to inform Canadian consumers when their privacy is breached, according to the Digital Privacy Act [1]. Under the assumption that information was leaked during the DoS attack, what Carl did was illegal - you have to notify someone that their privacy may have been breached. On top of his decision being illegal in today's world, it was also unethical because vital personal information may have been leaked from individuals. It is not good business practice or moral to fail to inform someone that their social security number, address and contact information have been leaked to an unknown third party. A great analogy would be if someone you don't know was going through your wallet or purse, and your friend knew about this but didn't tell you. Disregarding this law and playing devil's advocate, what Carl did was the best thing to do for the success of the company. His utmost desire is to have the company succeed, so make sure no one knows of the successful DoS attack and information leakage, would maintain confidence in shareholders and customers/clients. Deciding not to shut the company down will show consistency with IT infrastructure because no one likes to see it when a website or service is down. A good example of this is the Google search engine, because it is rarely, if ever, down [2].

Q3. Jim Barton's and IVK Corp's priorities are to never reveal to anyone that IVK experienced a DoS attack, find a way to improve IT security infrastructure without shutting down the company and finish any outstanding projects that will show IVK is a successful company. Essentially, the CEO wants to hide the DoS attack from the history books for the company as much as possible. In addition to this, Jim's priorities and responsibilities have increased because two other executives got fired after arguing with the CEO. Jim is now the CIO and directory of Loan Operations so he must wear two hats for the company. This added level of responsibility is difficult and makes Jim's job more challenging because he has to prioritize the functionality of two departments – luckily, he is familiar with the role. IVK Corp must remain a solid company in the eyes of the public and simply continue with their day-to-day business ventures.

Q4. The meeting on June 30th was the meeting where Jim Barton informed Carl Williams about what the company should do in regards to the DoS attack. Many executives were in this meeting along with Jim Barton and Carl Williams. In quick summary, Jim Barton explains what the company should do, many other executives agree, and two other executes get fired for standing their ground in front of Carl Williams. It is interesting and important to point out that Jim Barton enters the meeting as IVK's CIO and exits the meeting as IVK's CIO and temporary director of Loan Operations. We believe that Carl Williams still has some respect for Jim Barton, despite bringing up the idea of shutting the company down. By the same token, Jim Barton may be only still around because he would fit perfectly as a scapegoat for Carl. We don't think Jim Barton's standing in IVK was affected for better or for worse, as he was just doing his due diligence as the CIO. His job is to inform the CEO of the best plan of action for the IT department in times of DoS

attacks. One thing Jim Barton could have done better provided a stronger argument to Carl Williams to shut the company down. It was pretty good, but Jim Barton may have underestimated Carl William's stubbornness to do things his way, or the highway, literally. Interestingly an article on cio.com, "How to Argue with the CEO — And Win" provides some interesting advice for CIO's such as getting other people to back you, playing the CEO's desire to be successful, putting your job on the line, and anticipate the CEO's questions [3]. These are some pieces areas Jim Barton should have touched upon more, to be better prepared in convincing Carl Williams. With that being said, he is still a fan favourite of Carl Williams, but this time with some added pressure because he has to juggle two roles for the time being. Jim Barton did his best, and at that meeting, it just wasn't good enough, so in this circumstance, he should just go along with the CEO and learn better for the next time he has to convince the CEO.

Q5. Jim Barton should reconnect with his IT team and tell them what the CEO has decided. At the end of the day, it is up to the CEO to decide the plan of action for the company, when it comes to moments like these. If something bad were to happen to the company, Jim Barton made his recommendation at the meeting and all the executives were witnesses to his recommendation. Jim could be blamed for any events that come to pass but at this point it the CEO's fault for not listening to Jim. It's ironic because the meeting ends off with the notion of possibly keeping Jim as a scapegoat for any future problems that occur, but it was Carl himself that decided not to listen to the CIO to shut the company down, so he can't use Jim as a scapegoat. As mentioned originally, Jim should inform all his employees of the CEO's decision to not shut the company down. Assuming that shutting the company down for security maintenance was the optimal course of action, the entire IT team should join forces and convince the CEO to do so. This should only be the recommended course of action if the entire IT team truly cared about the company and were not afraid to lose their jobs. It's a difficult position, but if the CEO closes themselves off, it leaves the company vulnerable [4]. If the CEO disagrees once more, they can all give their resignation letters. You can't run this company with no IT department and it takes many weeks to ramp any new employees up. That course of action is starting to get unethical, but if the security of the company's data is what matters most, sometimes extreme measures must be taken.

Q6. In my opinion, I think the doctrine of completed staff work [6] fosters a toxic communication environment. Communication within the workplace should be a two-way street, where an employee should be able to bring ideas and designs to their manager without repercussions. This has a positive impact on workplace culture [7], where employees feel like they don't have to "tiptoe" around their managers, and on the actual finished product, which will now be a reflection of managerial input and employee input. At IVK, it seems like this is not the case, as evidenced by William's unwillingness to accept different opinions on what to do after the attack and even firing people who disagree with him.

Q7. I agree with Maggie's assessment that Barton is "Totally screwed". I feel that Barton is between a rock and a hard place when it comes to his future at IVK. On one hand, William won't really listen to anyone and acts wildly and is chaotic, which doesn't allow Barton to bring ideas to him out of fear of losing his job. On another hand, Barton is also a part of the executive team, and if IVK goes down Barton would go down with it (and potentially ending his career). Another factor is the environment that Barton has to work in, which is a toxic environment that is being fostered by William behaves towards his employees.

Q8. I don't believe that IVK should implement a system to monitor the performance of employees. There is no way to implement a system that monitors employee performance, without it also monitoring what an employee is doing [8]. It is incredibly hard to quantify what leads to a high performing employee. For example, in the book, Cho spends a lot of time with his jazz band which directly translates to him being happier and performing better at work. Another reason is that it's hard to measure how hard someone is working from just their computer, for example an employee could be working hard by writing out ideas on a whiteboard or on paper. This doesn't necessarily translate directly to a metric but may still improve productivity. However, I think that having an organic way of measuring success could be useful. For example, team managers could have code reviews and see how much employees have done in certain periods. This comes off more natural and less "Big brother" like and could be a way to decide who needs more training and who is okay on their own.

Q9. I think a company like IVK should take a measured but firm approach to its risks and tradeoffs. Even if IVK is really confident in something it is pursuing, it is entirely possible at any moment for a completely unexpected outcome. One strategy, as Williams points out, is to play it entirely safe and only make bets when you are absolutely confident in what you have. This strategy works well if IVK is an incumbent in the market, but as Williams points out, IVK is not and needs to bet big to win sometimes.

Q10. I think that a CIO should pursue senior management and oversight when managing IT risk because if they don't, the people that will push changes might not always consider IT. Executive members that don't know much about IT will not be able to correctly understand the requirements that need to be satisfied when discussing risks to IT. For example, Williams isn't really aware of how things in IT work, shown by his frustration at Barton's solutions to the attacks. However, Barton correctly understands the solutions and what would work best. If a CIO is part of the group of people that push changes, (senior management) then the needs of IT are represented properly.

REFERENCES

[1] Connolly, Amanda. “Companies Will Now Have to Tell Canadian Consumers When Their Privacy Is Breached - and Do It Quickly.” *Global News*, Global News, 5 Apr. 2018, globalnews.ca/news/4122202/data-breach-canada-privacy-commissioner/.

[2] Metz, Cade. “Here's How Google Makes Sure It (Almost) Never Goes Down.” Wired, Conde Nast, 3 June 2017, http://www.wired.com/2016/04/google-ensures-services-almost-never-go/.

[3] Levinson, Meridith. “How to Argue with the CEO--And Win.” *CIO*, CIO, 13 June 2011, http://www.cio.com/article/2407728/how-to-argue-with-the-ceo--and-win.html.

[4] Charan, Ram. “How to Prevent a Faltering CEO from Damaging Your Company.” *Strategy Business*, 5 Apr. 2018, www.strategy-business.com/article/How-to-Prevent-a-Faltering-CEO-from-Damaging-Your-Company?gko=7832b.

[5] Austin, Robert D., et al. *The Adventures of an IT Leader*. Harvard Business Review Press, 2016.

[6] *The Doctrine of Completed Staff Work*, govleaders.org/completed-staff-work.htm.

[7] “Importance of Good Communication at the Workplace.” InCorp Global, 29 Nov. 2018, www.incorp.asia/hr/importance-of-good-communication-at-workplace/.

[8] Bowman, Robert. “Is New Truck-Monitoring Technology for Safety -- or Spying on Drivers?”*Forbes*,ForbesMagazine,14Feb.2014, www.forbes.com/sites/robertbowman/2014/02/11/is-new-truck-monitoring-technology-for-safety-or-spying-on-drivers/.