TED ROGERS SCHOOL OF MANAGEMENT | Ted Rogers Leadership Centre

Cyber Breach at an Insurtech's Third-Party Vendor

Board Oversight under Stress

Ilona Niemi, Ph.D., MPM

* All opinions represented in this case are personal and belong solely to the author. Any such opinions do not necessarily represent the views of the author's employer or any other persons, institutions or organizations with whom the author may be associated.

Ethical Leadership Case Study Collection Case Number 023-001
April 2023

Toronto Metropolitan University

Table of Contents

Introduction **1**
Insurtech Aurum **1**
Anyone in Charge of Third-Party Risks at Aurum? **3**
Where is the Board's Risk Oversight? **5**
Aurum's Management under Pressure **7**
Rewriting Aurum's Strategy and Governance **8**
Questions **10**

Cyber Breach at an Insurtech's Third-Party Vendor

Board Oversight under Stress

Ilona Niemi, Ph.D., MPM

Ethical Leadership Case Study Collection
Case Number 023-001
April 2023

Ted Rogers School of Management,
Toronto Metropolitan University

Keywords: Board Governance, Board Oversight, Risk Appetite, Data, AI, Cyber Risk, Third-Party and Nth Party Risk, Privacy Risk, Data Privacy and Protection, Financial Services, Insurance, Insurtech, Digitalization, Customer Trust and Brand Reputation

Introduction

At 5pm on January 25, 2023 the cyber breach at Brainy is in the national and international headlines. Based on the initial reports, private records of 15 million people across the globe have been impacted. It is thought that significant amounts of personal information have been exposed and it is not known who is impacted, how, and where in the world. Five minutes later at 5:05pm the Chief Marketing Officer (CMO) of Aurum, a rising Auto Insurance Insurtech, sees the headlines in her newsfeed wondering why the company impacted sounds so familiar to her. Within two minutes the CMO gets confirmation from her team that Brainy is one of Aurum's vendors. Aurum's customer service chatbot receives the first inquiry regarding Brainy's cyber breach at 5:11pm.

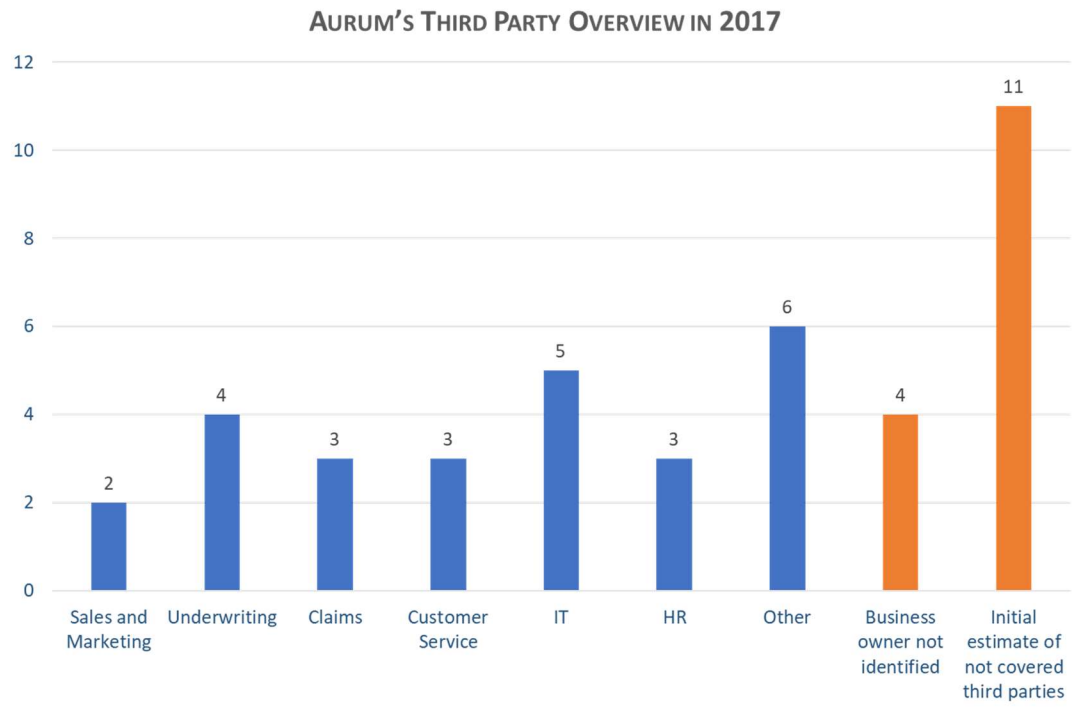
Brainy is a third-party vendor providing artificial intelligence (AI) services for Aurum's claims data. Aurum is only one of Brainy's dozen auto insurance customers globally, leveraging Brainy's cutting edge capabilities. Brainy's success story has been based on the large quantities of insurers' and other data that has enabled it to develop superb capabilities to analyze damages in real time using 3D images of damaged vehicles. Now Brainy's biggest strength has turned against it. The chair of Aurum's board's risk committee, Frida Lynx – onboarded just two weeks earlier – is on the train late afternoon on January 25, 2023 reading the evolving news on Brainy's cyber breach. She wonders whether Aurum is impacted, and if so, how to take care of the insurer's worried customers.

Insurtech Aurum

Aurum is the first fully digital auto insurance platform, and is based in Montreal, Canada. It was started by a former executive of a large global insurance provider from Europe back in 2013, and since then that person has served as the Chief Executive Officer (CEO) of Aurum. The CEO of Aurum had worked in his forming career years in the Asia Pacific region and closely observed the rise of early adopters of the fully digital insurance customer experience. Since its inception Aurum's customer platform and claims service have gained global and local attention and received several awards. In particular, the company's AI-driven claims

processing – allowing to resolve a significant portion of auto claims within minutes – has been the focus of global attention and has been rated very positively by customers.

Aurum's business model is built on financial ecosystem thinking in which identifying the right third-party providers and ensuring that any cutting-edge technology can be leveraged effectively and efficiently are the keys to success. The first few years at Aurum have been a whirlwind; a structured approach to setting up and managing third-party partnerships was never prioritized, and the need for the specific skill set to standardize the onboarding of vendors had not been fully recognized. An initial inventory of the various third parties in use was started in 2017, as shown below, but it was never finalized.



The company's strategy from early days has remained to avoid any unnecessary investments in infrastructure, in order to manage their cash flow and keep a strong balance sheet. As a digital provider targeting Generation G and Millennials in particular, Aurum's values focused strongly on the importance of maintaining customer trust and being a good and ethical steward in insurance. The CEO had never missed an opportunity to speak about customer trust and its linkage to Aurum's brand reputation.

Aurum had kept growing consistently, and in a sustainable way, making investor money flow in. When the global COVID-19 pandemic situation deteriorated leading to significant shutdowns of public life in spring 2020, most traditional insurance providers had struggled to provide a digital experience bringing insurance services straight to people's homes, and so this was Aurum's opportunity to shine. Regardless of the across-the-board COVID-19 related rate reductions and insurers' own rebate programs, Aurum experienced a strong and steady business during the pandemic, and it was consistently able to provide up to 15% lower premiums on average than its more traditional counterparts.

Late 2020 in the midst of the pandemic, the Board of Directors had unanimously approved Aurum's new three-year strategy of going global and diversifying offerings by building life insurance capabilities. It had also been agreed that going public by mid-2023 was required in order to change the narrative regarding the company from a story about a startup to one about a serious insurance provider. Only by doing so could Aurum start challenging the current, established insurance players in the auto and life segments. As of January 2023, Aurum's planned Initial Public Offering (IPO) was just over six months away, in the second half of 2023. The investor negotiations were already at an advance stage, and all seemed to be set for going public. Also, momentum was building for the planned global expansion, expected to begin taking effect in late 2023 with selected European countries.

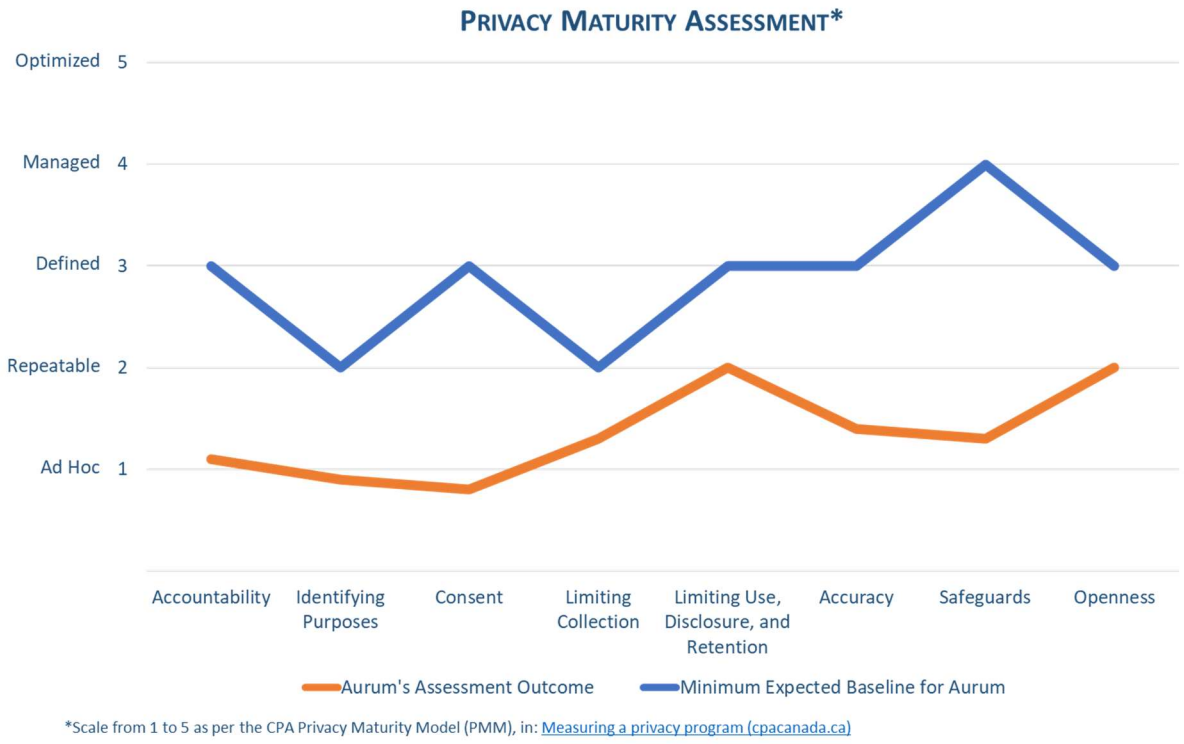
Anyone in Charge of Third-Party Risks at Aurum?

Since 2013, Aurum's focus had been on expansion, and on beating investor expectations. Speed was believed to be of the essence in any decision-making. Decisions about Aurum's third-party vendors had been decentralized and everyone on the management team had been able to authorize partnerships. Aurum's governance had not been maturing in a way that matched the growth in the size of the company. Given the entrepreneurial spirit and family-oriented decision-making at Aurum, risk discussions were effectively side conversations. Also, the culture emphasized the difference between Aurum and traditional insurance companies, leading indirectly to executives frequently questioning the applicability of the traditional regulatory and control frameworks to Aurum's business model.

Brainy, the third-party targeted by the cyber-attack, had been the focus of an intense discussion within Aurum's management team about six months before the crisis in January of 2023. Aurum's "triple hat officer" – the individual responsible for risk, compliance and privacy – had brought two privacy complaints to the management team's attention. In both cases, customers were worried about their personal information being used without proper consent. The risk/compliance/privacy officer had verified that one of Brainy's subcontractors had started using Aurum's data for new purposes without obtaining approvals from the company and without having acquired proper customer consent. Aurum had sent a written warning to Brainy in response to what Aurum referred to as a breach in contractual obligations. Against the guidance from the risk/compliance/privacy officer, the management had decided not to spend time or money to further investigate Brainy's practices and those of its subcontractors. These two privacy issues were never reported to the risk committee of the board of directors, nor were the subsequent regulatory investigations that had been triggered by the complaints. Generally, there was an atmosphere of trust at Aurum and a belief that strong values and respect for contractual obligations would take care of any risks.

The in-house risk/compliance/privacy officer, who had been with the company in various roles since the beginning, had been busy with customer-facing matters in the newly created role. The sole focus of the work was to react to business inquiries and further improve the digital customer platform. Motivated by the successful completion of a cyber risk certification program, Aurum's risk/compliance/privacy officer initiated a structured review of privacy risks. The assessment showed an immature control framework. To make this assessment more concrete, the industry data below regarding third-party privacy risks was integrated into a report to management.

The review had not been received well by the management team. The management team felt that the measurement standard used was not the right one for Aurum's culture and business model. Management unanimously agreed on postponing any work in this area due to the significant investments it seemingly required. Given the immaturity of Aurum's risk framework, no discussion of this topic took place at the board of directors and no decision about risk appetite was made at the board level. The risk/compliance/privacy officer followed the guidance provided to the privacy risk review by the management team and continued the day-to-day work as if nothing had ever happened.



*Scale from 1 to 5 as per the CPA Privacy Maturity Model (PMM), in: Measuring a privacy program (cpacanada.ca)

Where was the Board's Risk Oversight?

During the initial years of Aurum's expansion, the board of directors had not spent any substantial time on issues related to risk/compliance/privacy oversight – the boards focus was on growth, going public, and other pressing matters. The pandemic had been a wake-up call for Aurum's board, and had highlighted the absence of basic risk protocols at

Aurum. This had led to a broader discussion at the board, and to the recognition that Aurum needed to have risk/compliance/privacy knowledge and expertise in order to successfully support its new strategy. Frida Lynx, a European Union based risk, compliance and privacy professional, was onboarded as the new chair of Aurum's board's risk committee on January 15th 2023, just ten days before Brainy's cyber breach. The hope had been that Frida Lynx would institute a larger shift within Aurum's risk culture and within the ranks of the peer directors and management. A seasoned risk executive, Frida had seen it all while working in Europe. She was the former Europe, Middle East, and Africa (EMEA) Chief Risk Officer (CRO), later the Chief Compliance Officer (CCO), and most recently had acted as the Chief Data Protection and Privacy Officer (CPO) of a well-known American social media platform. During the six years in her CPO role, Frida Lynx had been part of her company's program to prepare for the significant and groundbreaking changes in the European Union's privacy law in 2018. She also unfortunately had had experience in dealing with the substantive fines that could be levied under this legislation as well as the negative reputational implications of being fined. During the interview process for the role of risk committee chair, Frida had been constantly reassured that there were no major, urgent risk issues at Aurum to fix.

It is now early in the evening on January 25th, two hours after news of Brainy's cyber-attack had gone viral across the globe, Frida Lynx has started to realize that Aurum has some serious governance issues to tackle in both the short and long term. Frida Lynx steps off the train and dials the number of Aurum's CEO. She feels restless and full of questions. She feels even more so when she finds out that the CEO had, just five minutes earlier, been brought up to speed on the developments at Brainy. The initial thinking across the ranks at Aurum was that the breach was Brainy's issue, one that Brainy could deal with internally. The management team at Aurum has now been made aware that Aurum's customers' data is most probably seriously compromised, along with data from other insurers and customers of Brainy. Frida Lynx stops asking the CEO her list of prepared questions, realizing that there really are no answers, at least not for now.

To Frida Lynx' relief, the CEO informs her that there is a business continuity plan in place at Aurum, and it has just recently been tested in collaboration with external auditors. The CEO

activates the business continuity plan while carrying on the conversation with Frida. Of course, this is two long hours too late in Frida Lynx' opinion, but Frida figures it is better late than never. Frida leaves the call by assuring the CEO that she is "here to help."

Aurum's Management under Pressure

Aurum's management learns very quickly that the cyber-attack at Brainy has compromised personal data of their over 1.1 million customers and third parties. It means that effectively everyone who has been insured by Aurum, or who is a claimant of Aurum, has been affected one or the other way by this privacy breach. The data exposed consists mostly of names, addresses, date of births, social security numbers and driver license numbers. The quantity of credit card numbers exposed is not known yet. But it is clear to all stakeholders that a lot of sensitive personal information has been compromised, and that it is getting serious for Aurum's team for the first time since the company's launch in 2013. Aurum's management team, under the leadership of the CEO, starts feeling immense pressure from customers, investors, regulators, and the board of directors. All of these stakeholders want to know now what is going on at Brainy, and the details of Aurum's plan of action.

In the days following the privacy breach, Aurum's management hires a consulting company to lead the complex investigation, to ensure that Brainy takes the right actions regarding Aurum's data, and to make sure that Aurum's stakeholders are informed in a timely manner. The investigation reveals three significant improvement opportunities at Aurum:

1. Immature data protection and privacy frameworks;
2. A lack of oversight over third parties due to limited onboarding and integration processes;
3. A discrepancy between the attitude to risk embodied in Aurum's corporate culture, on one hand, and the company's actual practices, on the other.

Internally this breach also prompts a healthy discussion regarding the state of cyber risk protection at Aurum itself.

Based on the initial calculation of the costs and effort, fixing this all could jeopardize the timeline for the company's planned global expansion. The consulting company supporting Aurum's course of action has made very clear to Aurum's management that this breach could easily have a very different outcome and price tag on it. The new Canadian privacy regimes, both in Quebec and at the federal level, will soon start imposing fines up to 5% of global revenue or CA$25 million, whichever is greater.

Aurum's business model is based on trust and being a good steward of data. Although several other insurers and companies have been affected by the breach in a similar way, it has had a very serious and specific impact at Aurum, namely the loss of a large number of customers. A further decline in customer counts is seen when both the Canadian privacy commissioner and a lead regulator, highlight the deficiencies in Aurum's management and mitigation of third-party risks and name Aurum explicitly in their reports.

As the crisis unfolds, a number of options are assessed, with an eye to restoring Aurum's brand. Cutting ties to Brainy is not an option, given that the success of Aurum's business model has been 100% reliant upon its claims processing capability, and given that there is no substitute technology available in the marketplace yet. Aurum's management is aware of this, and the thought has always been to first scale and go public with the company, and ideally thereafter acquire Brainy.

Rewriting Aurum's Strategy and Governance

The mid-2023 date previously set for going public is no longer viable in the wake of the Brainy's privacy breach, and nor is the European expansion planned for late 2023. Two of the three critical investors involved in the plan for going public have started seriously reviewing their positions regarding Aurum's prospects. They are very concerned to learn from news media about Aurum's unexpected strategic, operational, governance and ethical challenges.

On behalf of the Board of Directors, Frida Lynx naturally assumes the lead for reacting to this breach, in close coordination with the chair of the board. Based on her past experiences, Frida knows that time is of the essence when communicating with stakeholders and she knows that all solutions will be imperfect. Aurum's management team, led by the CEO, aligns with Frida on varying options, as well engaging in discussions with key investors and other relevant stakeholders.

Following Frida's guidance, the CEO announces Aurum's plan to tackle its short-term strategy and its longer-term governance challenges. The plan includes a commitment to significant investments in governance, risk, cyber, compliance, privacy, and ethics capabilities over the next three years. It also establishes a new timeline for going public and for expansion in Europe. Frida Lynx is satisfied with the outcome, and she knows well that there is only one chance to get this right in the eyes of the public and investors. Can Aurum shift its culture and deliver on the plan?

Questions

1. Why did Aurum's CEO and management team decide not to prioritize risk governance? Why did they consistently ignore the opportunities to improve over the years?

2. Should Aurum's CEO resign or get replaced due to this breach? Please discuss the pros and cons of your response.

3. Why do you think the risk/compliance/privacy officer failed to speak up and to try to get the board of directors up to speed regarding the governance deficiencies detected?

4. How would you rate the board oversight of Aurum's CEO and management team?

5. Why did the board of directors not identify the governance weaknesses earlier? What was the biggest impediment to establishing good board governance and oversight at Aurum?

6. How should Frida Lynx act on the need for a discussion of the company's risk appetite framework with the management team?

7. What recommendations should Frida Lynx now make to the board to ensure that the three-year strategic investment on governance, risk, cyber, compliance, privacy and ethics capabilities will be a success?