Journal of Information Systems Education

Volume 33
Issue 4
Fall 2022

Teaching Case

Information Security Management in Distress at SkillPlat

Ivano Bongiovanni

Recommended Citation: Bongiovanni, I. (2022). Teaching Case: Information Security Management in Distress at SkillPlat. *Journal of Information Systems Education*, 33(4), 338-356.

Article Link: https://jise.org/Volume33/n4/JISE2022v33n4pp338-356.html

Initial Submission:	23 September 2021
Minor Revision:	31 December 2021
Accepted:	7 February 2022
Published:	15 December 2022

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 33(4), 338-356, Fall 2022

Teaching Case
Information Security Management in Distress at SkillPlat

Ivano Bongiovanni
Business School
University of Queensland
Brisbane, 4000, Australia
i.bongiovanni@uq.edu.au

ABSTRACT

In this role-playing teaching case, students impersonate Selective Consulting, a fictitious, Australian-based company tasked with assessing the information security practices of SkillPlat, a provider of apprenticeship and traineeship services. The case develops around the one-week visit paid by Selective Consulting to SkillPlat's headquarters, during which the consultants identify several issues that denote poor information security management practices by the company. After analysing the case materials (the main text, plus seven exhibits), students write a report in which they assess the pros and cons of SkillPlat's information security management practices, offer recommendations for improvement, and indicate other sources of information that could be useful for a more detailed analysis. The report is expected to cover various topics in information security management: policies, user behaviours/human factors, governance, security practices, risk management, physical security, protection of personally identifiable information and privacy, organisational culture, etc. This teaching case has been successfully utilised with two cohorts of Master students as an assessment piece, at the end of a course on cybersecurity management. The present case requires students to offer solid arguments in favour of their assessment and recommendations, tapping into their knowledge of the subject and external resources (e.g., industry reports, academic papers, etc.). This Teaching Case needs to be accompanied by its Teaching Notes.

Keywords: Information assurance & security, Case-based learning, Risk assessment, Teaching case

1. INTRODUCTION

Headquarters of Selective Consulting, Monday

It is a beautiful Monday morning. You are slowly enjoying your cappuccino in your office. As you are putting down a to-do list for the upcoming days, Martine, one of the Personal Assistants of Selective Consulting, the consulting firm you work for, asks you to urgently meet your boss in her office.

"Hey Karen, did you want to see me?" – you ask your boss.

Karen is one of the most successful partners at Selective Consulting. She welcomes you in her office with her usual smile and asks you to take a seat.

"I have to ask you a huge favour. Last week I was approached by the Chief Executive Officer (CEO) of SkillPlat, have you ever heard of them?"

"The training company?" – you ask.

"Precisely. Their CEO is a very good friend of mine and has asked me if we could run an assessment of their information security management systems. They are getting ready for an audit in the coming months and would like to take all the necessary steps to improve their cybersecurity posture before this happens."

"Not a problem. What's their timing?"

Karen takes a deep breath and shows her best smile ever: "Friday. They want a complete report by Friday."

"What?! Are you kidding me?"

Karen does not react to your surprise and lets her words sit in your mind for a little while.

"Apologies Karen, I did not mean to be so abrupt…I mean, Friday is in 5 days! How is this going to be feasible?"

"I understand. I told the CEO that such a deadline is quite ridiculous, but he did not seem too concerned. He asked us to do all we can." – Karen replies, with all her self-control. Then, she continues: "Look, if you manage to make them happy, you will be considered for your next review toward earning partner status".

You smile back, shaking your head: "One day, you will need to tell me how you always convince me, Karen…"

"I will. So, I suggest you start working on this immediately. You are excused from all your other commitments. The SkillPlat project is your priority now. Feel free to involve whomever you think will be helpful. I want the full report in my inbox by Friday at 4:30 pm. I am forwarding you an email that SkillPlat's CEO sent me over the weekend: you will find more details on what you are expected to do."

You leave Karen's office a bit concerned, but also excited. This is one of those challenges you love so much…

One hour after your meeting with Karen, a pop-up sound catches your attention. She has forwarded SkillPlat CEO's email:

From: ktaylor@selectiveconsult.com.au
RE: SkillPlat Project

Hey,

Thanks again for accepting this job in such a short notice. I knew I could count on you. Please find below the email that Jerry Thomson, CEO of SkillPlat, sent me over the weekend. Also, I took the liberty to speak with your

colleagues Matt and Patricia and asked them to help you on this one. They are at your complete disposal.

Good luck!
Karen
Partner, Selective Consulting

From: jerry.thomson@skillplat.com.au
To: ktaylor@selectiveconsult.com.au
RE: Information Security Management at SkillPlat: A Comprehensive Report

Dear Karen,

Great talking to you on Friday and reminiscing our days back at uni. As I mentioned, we would love to have a **comprehensive report assessing the status of, and providing recommendations on, information security management at SkillPlat**, in preparation for our audit in the coming months. The report should have two parts:

Part 1 should be a synthesis of what you found, with pros and cons of our information security management system.

Part 2 should be an overview of the practical steps we could take to improve. The more in detail these practical steps are, the better. Since we acknowledge that you will not have much time to collect the information needed for your report, in part 2, we would also like you to **assess what sources/documents/materials you would need to investigate, to provide us with a more complete report, if you had more time** (this could be utilised for a follow-up project).

The topics we would like to be covered are the following ones: governance, policies, procedures, compliance, risk management, culture (including awareness, training, and education) and ethics.

Thanks in advance; looking forward to reading your report and seeing you soon!

Jerry Thomson
CEO, SkillPlat

2. MAIN TEXT

Headquarters of Selective Consulting, Monday

You waste no time and immediately call Jerry Thomson to ask for some basic information to start this project:

"Jerry, could you please give me a brief overview of your business? Size, employees, main customers, a bit of history, etc."

"Sure, no worries. So SkillPlat was founded as a private company in 1980 and has always been very loyal to its original mission: connecting greatly-skilled people with potential employers, whilst delivering outstanding training, both on the job and in the classroom. We offer a wide range of customised solutions for the modern workforce. We basically have two types of clients: as a business-to-consumer organisation, we identify apprenticeship and traineeship opportunities for people who need a job and to acquire new skills or strengthen their existing ones; as a business-to-business organisation, we offer exceptionally skilled workers to employers in need for human resources. Plus, we take care of all the insurance and contractual arrangements, dramatically reducing the paperwork for both employers and employees. As a training organisation, we also offer a wide range of traditional and flexible training programs, ranging from IT skills development, to carpentry, to horticulture and farming, etc. Long story short: think of any possible training need one may have, and we offer a course in that area, either directly, or through one of our two affiliate colleges, Alba and Oasis. SkillPlat has a total of around 50 employees and an annual turnover of around AU$20 million, which classifies us as a medium enterprise. Since 1980, we've had a total of around 50,000 customers and helped hundreds of organisations find skilled workforce. We have delivered thousands of training programs and courses and we are today a key provider in two States for apprenticeship and traineeship services."

"Could you please tell me more about what apprenticeships and traineeships are?" – you ask.

"Sure. So, an apprenticeship or traineeship can be full-time or part-time employment. They mix work and structured training. Through them, people develop skills that will help them find a job and career for life. Apprenticeships last around 3-4 years and are usually offered in the trade industries, like building, carpentry and construction, or engineering, or electrotechnology, and many others. Traineeships are usually shorter, 1-2 years, and include employments in business administration – for example in administrative, accounting, HR, and local government positions – hospitality, retailers, etc. Once placed with a public or private business (the host employer), our apprentices and trainees are formally trained, either on-the-job or with us or with an agreed institution, for example our two affiliate colleges." – Jerry explains.

"How do you make sure your apprentices and trainees are happy at their workplace and the employers are happy with them?" – is your next question.

"We have around 15 local officers who regularly inspect each workplace (on average once every 10 weeks). In this way, they can monitor progress, ascertain whether safe work practices are implemented and check that the appropriate on-the-job training is provided. The local officers are the backbone of our organisation and constitute a very precious connection between the employees, the employers and ourselves. They are our eyes and ears on the territory!"

"You mentioned affiliate colleges. What are these?"

"Yes, so we have an affiliation with the Oasis Community College and the Alba College. Through these two institutions, we offer our training courses and programmes. We send our apprentices and trainees to their facilities and have them attend their courses, to then get accredited with us. The two colleges offer our students discounted fees and in exchange receive a constant influx of guaranteed students from us. Also, if the two colleges have students that are interested in apprenticeships or traineeships, they send them to us. I must admit, Oasis and Alba are the cheapest colleges in this sense, and we are lucky to be doing business with them. But the quality of their services is still pretty good."

"Couldn't you simply offer those courses in-house?"

"Obviously not. It would cost us much more. Imagine hiring all those teachers and trainers… It's much cheaper to outsource this to the two colleges. We are all in the same 'supply chain' if I can use this expression. However, we do maintain some courses in-house and the teachers are either the local officers themselves or some people we casually hire as trainers (or mentors, as we call them). We have 5 of these which, together with the 15 local officers, brings the total up to 20 trainers."

"Speaking of which, how are you internally organised?" – you then ask.

"I will send you a copy of our organisational chart as soon as we finish our call. Broadly speaking, we try to be as

lean as possible, maintaining a somehow agile organisational structure. So, we obviously have a board of directors, composed by the main shareholders, a mix of public and private actors, plus some individual investors. As the CEO, I report directly to the board on the running of the organisation. Together with me, there are four C-Suite people: Judith, our Chief Operations Officer, who is in charge of the apprenticeships and traineeships and of the connections with the employers; Sandy, our Chief Human Resource Officer, who supervises all aspects of HR within our organisation, recruitment, payroll, but also the safety aspects of apprenticeships and traineeships and training; Wong, who is our Chief Financial Officer, and deals with all things financial management; and finally Rupert, our Chief Information Officer (CIO), who is the tech wizard and deals with all aspects of IT within SkillPlat. I reckon you may want to have a chat with all of them, but probably I would start with Rupert. Do you want me to organise a meeting for the two of you?" – Jerry asks.

"That would be great, thank you. Any time tomorrow sounds good. I will come to your headquarters, if this is OK?"

"Sure, not a problem."

"If I'm not wrong, I didn't hear you mention a marketing team?"

"You're right, we don't have a proper one. Our corporate relationships managers and local officer at times do a bit of marketing work, but the largest chunk of it is outsourced to a marketing and communications company called MarketProPlus. They're the leader in the area and, despite costing us a lot of money, perform incredibly well. Most of our recent growth is actually thanks to their amazing campaigns for us."

"I see. So, my colleague Matt would like to come and visit you guys this afternoon; could this be arranged?"

"Absolutely. I will ask my admin to prepare a working space for him. We have heaps of hot desks that are usually used by visitors, students, and some employers. You know, they love to come and work remotely from here, especially the ones with whom we managed to establish a solid, long-standing rapport. Did you have any other questions for me? I have a meeting starting in 10 minutes, and I should not be late for this one. You know, we had a bit of an issue with a former local officer of ours…"

This remark raises your curiosity: "Oh really? Can I know what this is about?"

"Sure thing. So, we had this guy with us for five years in one of our branches in the north part of the state. He left four months ago. He was on the team in charge of a very important project, a bid for an AU$800,000 government-sponsored grant for the professional development of around 1,000 employees in several local city councils. After resigning, he immediately joined a competitor who ended up winning the bid and being awarded the government grant. And guess what? Their proposal looked incredibly similar to ours and had a slightly lower price." – explains Jerry, in a sad tone.

"I see. And what are you going to do now?"

"Well, that's exactly what we are going to discuss today. We hired some lawyers to understand if this happened by pure coincidence or if this person has done something wrong. In which case, we want to know how we can proceed."

"I would love to be updated on this one, if you don't mind…" – you cautiously ask, understanding the sensitivity of this matter.

"I don't see this being a problem. Let me have a chat with our lawyers. May I ask you; why are you interested in this? I don't think there has been any external attacks or anything cybersecurity-related in this circumstance…"

"Well, you don't need an external attack to have an information security problem."

"Ok. I thought you guys were all about hackers, viruses and dodgy individuals entering a company's networks. Anyways, if you don't have other questions, I'd better go. I shall see you tomorrow here. Have a great day!".

Headquarters of Selective Consulting, Tuesday

As promised, Jerry Thomson has sent you SkillPlat's organisational chart (see Appendix A). Some minutes later, you call your colleague Matt and ask him to go to SkillPlat's headquarters, where they should be waiting for his arrival. You task Matt with interviewing as many people as possible, to collect information about how the company manages its cybersecurity.

Headquarters of Selective Consulting, Tuesday

You do an online search for SkillPlat and find their website. At first sight, everything seems to be OK: the website employs the *https* protocol, and the company has published several organisational policies on privacy, records management, and ICT (Information and Communication Technology). You email Patricia and ask her to have a look at them. Out of curiosity, you click on their Login button. A page opens, where you can select which category of user you are and enter the restricted access areas. Categories are Apprentices and Trainees, Timesheets, Students, and Candidates. You try to log in each of them: obviously, you don't have passwords and credentials but can still have a look at the user interface of the login pages, which looks something like this page (see Appendix B).

"Ok, interesting…" - you think.

You keep searching online and spot one article from a local newspaper (see Appendix C) and one publicly available Facebook post from SkillPlat's Facebook page. The article talks about a training course launched two years ago at SkillPlat and contains information on the type of training delivered in an interview given by Rupert Maddox, the CIO. The Facebook post refers to a social media campaign recently launched to promote a new cohort of trainees and apprentices starting on their jobs with their employers. The campaign (#showsomeexcitement and #SkillPlat) asks students, apprentices, and trainees to post on their social media a picture of themselves holding their SkillPlat ID card. So far, trainees and apprentices have shared around 300 photos: some of them are screaming in excitement at the camera, others are simply smiling, others have their arms happily raised up in the air. Almost all of them have their ID cards clearly visible in their hands, which shows how proud they are of belonging to the 'SkillPlat family'.

"Mmmhh…a probably effective marketing move, but at what cost? I will need to take a closer look at their ID cards." - you think, as you scroll the photos of the campaign.

Headquarters of Selective Consulting, Tuesday

Matt calls you from SkillPlat's headquarters.

"Hey Matt, did you make it there? How's things?" - you ask him.

"Hey boss. All good thanks. I installed myself in one of their offices. There's another desk for you. The CEO, Jerry, welcomed me, but he almost immediately left because he had something to discuss with one of their suppliers. Everyone's been super-nice so far. Are you coming straight here tomorrow morning?"

"Yeah, we've got so much work to do, I don't have time to come to my office. Let's meet there at 8am. Did you have a chance to talk to anyone?"

"Except the CEO, not really. But I managed to get Internet access through their wireless system. Well, it was quite easy, to be honest. Their Information Technology (IT) guy was not in, so one of their receptionists handed me a printed card with a set of credentials they use for guests when no one from IT is around."

You farewell Matt and hang up. As you pack your stuff and head home, you have a feeling this will be a long week…

Headquarters of SkillPlat, Wednesday

The next morning, you reach SkillPlat's headquarters by 8am. Matt is not there yet. You use this time to wander around SkillPlat's premises. The building is more like a big warehouse and has a nicely decorated garden at the front. On the right side of the main sliding door, there is a swipe access card system and an electronic doorbell. Instructions on a plate ask visitors to ring the bell to gain access to the main lobby of the company. Students, apprentices, trainees, and staff members – the instructions say - can access by simply swiping their ID cards. As you walk towards the side of the building, you notice another door, kept open outwards by a large shelf. A couple of meters past, along the same wall, you can notice a few bags, apparently full of papers, with the large tag "for shredding" on them. No gate separates that area from the main road.

It's getting late, and you decide you will go through the onboarding process. You will meet Matt inside. Following the instructions on the main sliding door, you ring the bell. After a couple of seconds, a receptionist, whom you can see through the glass-door, asks you about yourself and the purpose of your visit.

"Oh, I'm sorry. Yes, Jerry mentioned that you would be here early this morning. I'll let you in." – she says.

Margaret, the receptionist, asks you to sign in the visitors' register: you provide your full name, contact details and reason for visiting and ask her if and how you could get Internet access.

"Albert is the IT person on duty this morning, but usually does not come to the office until 9am. Here, take this card…this is the system we use in these cases."

Margaret hands you a card probably like the one Matt was provided with the day before. Your username is: SkillPlatGuest and the password is…well, you guessed it right: *password123*.

You thank Margaret for her kindness and ask her to show you the hot desk you will be using for the next couple of days. Luckily, the room is spacious and very bright.

"Margaret, I know your students and staff members have ID cards to access the premises. Do you happen to have one I can quickly see?" – you ask her.

Margaret shows you hers (see Appendix D). You look at it, then ask her: "I was wondering if the students have similar ID cards?"

"Yes, exactly the same. The only difference is that, under category, they have 'student/trainee/apprentice'. And obviously the ID card number changes" – Margaret explains. You thank Margaret and install yourself at your hot desk.

Headquarters of SkillPlat, Wednesday

You and Matt have managed to organise an interview with Rupert Maddox, the CIO at SkillPlat. He's been on the role for more than 20 years. Given his position and experience, he will be able to give you a lot of information for you to use in your report.

Rupert does not seem to be in his best mood, but you can't complain about this. After all, two consultants asking questions about information security would make anybody nervous.

"First of all, thank you very much for your time today, Rupert." – you start – "We will try to be as quick as we can."

Rupert simply nods in silence. To make him feel at ease, you start with an easy question:

"So, I was reading yesterday an article on the Internet saying that some time ago you have engaged all your employees in a quite extensive cybersecurity training program. Can you tell us a bit more about this?"

"Well, of course we did. I mean, we wanted to abide by the recommendations of the government. I mean, we didn't have to do it, but we wanted our employees to understand the importance of information security. We had a bunch of security managers from different companies come and give keynote speeches and involve us in simulations. We discussed past episodes that occurred at SkillPlat, what went wrong, and areas for improvement. We touched upon several topics: governance, awareness, cyber-response and obviously all the most common types of attacks. We also had one day dedicated to social media." – Rupert explains enthusiastically.

"That's interesting. And how did the employees react to this initiative?"

"At the beginning, they were very sceptical. I mean, we absorbed two full days of their time and, you know, here everyone has a lot of things to do every day. But after all, they were very happy with it."

"What do you think worked particularly well?" – is your next question.

"I guess the fact that a lot of that training was based on the concept of staying safe online in general, and not only at work. I mean, when you teach people how to use their social media properly, what to be wary of, spear phishing, social engineering and those sorts of things, they feel safer at home and, consequentially, they know what to do at work."

"This is very true. And I read every employee participated?"

"Well, that was the intention. Unfortunately, six people could not make it. Four staff members were on maternity leave, one person was at the hospital and another person was about to leave the organisation, so we thought it would be okay they did not participate."

"Have you had a chance to have the absentees attend another course?"

"Unfortunately, no. We had purchased the training course from an external provider, and we paid for exactly the number of attendees we had."

"I see. And are those people still working for SkillPlat?"

"Mmhh…yes, actually they are. Obviously except for the person who left."

"Have you organised similar training initiatives after that one?"

"Have you got an idea of how much money these programs cost? No, we couldn't afford it. I mean, it would be great, but Jerry would never be able to justify such an investment with our board. You know…it's about information security management. Our board of directors thinks it's a waste of money. Don't get me wrong, I don't believe training is a waste of money, but I know we must balance our investments. I can already imagine what would Wong, our Chief Financial Officer, say if I were to ask for more money in cybersecurity training…"

"So, what other types of training have you organised in the meantime?"

Rupert takes some seconds to think about an answer. Then, a bit embarrassed, he replies:

"Well, I guess apart from our normal information security and privacy onboarding training and our information security and privacy yearly course, not much…"

"What do these consist of?"

"They are basically interactive webinars: participants – our staff members – can take them when they want, either from home or at their desk. They are 10-15 minute videos. In some parts, there is delivery of contents: definition of information security, data breach, examples of cyber-attacks, etc."

"So, employees take these courses when they join the company and then once a year?"

"Well…Yes."

"And how do you keep track of the need for employees to take the course every year?"

"We don't have a register or anything similar. It's up to the employee to make a note of the need to take the course. I guess this is something we have to work on, as if an employee forgets about the information security and privacy course, we have no way of reminding them."

You slowly nod, thinking that, after all, this is not the most absurd way of keeping track of training records you have heard of in your career. Some companies you worked for in the past do not even have yearly training…

"I wanted to ask you something about your role now. As a CIO, what are your main responsibilities?" – you continue.

Self-confident, Rupert answers immediately: "Well, I am the leader in all things IT. Having joined this company more than twenty years ago as an intern, I really climbed the ladder and made my way to the top. As a CIO, I make most of the decisions in terms of IT investments, information security, systems, networks, etc. This is also because no one at the executive level has any IT background. I graduated while I was working, and this allowed me to apply all the knowledge I acquired at uni on the job. I obviously have a team of four people working for me, plus I can count on the admin staff, when needed; but, to be honest, I don't know how SkillPlat would do without me. Sometimes I would like the responsibility to be a bit more shared, but I also get paid quite well and this is my duty, after all."

"Can you tell us what the most common issues are that you have to deal with?"

"IT-related stuff: Internet going down for whatever reason; new equipment to be tested; our providers messing things up; visitors or students or staff members not being able to login; and so on."

"And in terms of cybersecurity?"

"Ah! I was expecting this question…It's your job after all, right? Well, nothing major, really. We had one successful malware attack and an attempted ransomware attack in, say, the last 12 months."

"Interesting. What happened there?"

"In the first case, which happened exactly one year ago, a newly hired employee clicked where they were not supposed to click and installed a malicious .exe file which, when executed, triggered a number of alerts in our intrusion detection system. Luckily, the security manager was on duty and immediately isolated the infected machines. We had someone come in from outside and take a look at the whole thing: no data or information were leaked outside, and the malware was removed. In the second case, a local officer was found working from remote on his personal laptop and not securely connecting through our virtual private network (VPN). You need to know that we have a company policy whereby all the traffic generated from remote needs to transit through our VPN. One day, the local officer accessed an insecure website and as a result was the victim of a successful ransomware attack in which the perpetrator managed to take control of several folders on their computer. The local officer immediately called me – I remember, it was like 1am – and, panicking, told me what happened. The day after, we got our security manager to take a close look at our system and scan whether the perpetrator had managed to access it. Luckily, they did not, maybe because they did not realise the damage they could have been able to produce. We helped the local officer clean their machine with no further damage."

"Were there any lessons learnt from these two instances?" – you ask, curious about these cases.

"In the first case, not really: I had a chat with the employee and joked with him about the fact that his curiosity 'almost killed the cat'. He's a good friend of mine, these things can happen after all, so I did not make a big fuss about it. In the second case, yes. We immediately issued an urgent newsletter to all staff members in which we reminded them to use the VPN when working from remote."

"Thank you. We are quite interested in the information security policies that you have in place. Can we have a chat about these?"

Rupert checks his watch and apologises: "I'm sorry guys, but I have to get back to work now. As for the policies, I suggest you go and talk to Stella, our Security Manager. She's in today, you'll find her in the office or at the cafeteria."

Headquarters of SkillPlat, Wednesday

The Parlour is a buzzing little café just opposite SkillPlat's building. When Matt and you enter, you immediately realise that almost everyone in there is from SkillPlat, having their mid-morning coffee or something to eat. SkillPlat's staff members wear nice, blue polo shirts with their name tags on. You take a seat in a quiet corner and Matt orders an espresso for both of you. As you wait, you have a chat about the interview with Rupert:

"Quite a character, that Rupert" - starts Matt - "I can't really figure out how good of a CIO he may be. I mean, they're certainly doing some good things, but other aspects of what he shared with us left me a bit surprised and worried."

In that moment, a SkillPlat employee approaches your table. Her name tag reads Stella.

"Hi! My name is Stella. You two must be from Selective Consulting. Rupert just told me you wanted to have a chat about our information security policies?"

Stella is SkillPlat's security manager and looks eager to assist you. Matt immediately takes the floor, introduces the two of you, and orders another coffee for Stella, who takes a seat at your table.

"So, we do have a Corporate Information Security Policy (CISP) and we're actually in the process of setting up policies and procedures for different organisational areas. I'm happy to share the CISP and an example of another policy with you. It would be great to receive some feedback from you in your report!"

You then ask Stella to elaborate on her role and on how the IT department works.

"As you probably know, I am part-time in this job. The position was full-time until a couple of years ago, but then they decided that the fact that we haven't had any major breaches ever justified a reduction in costs. Hence, they put me on a 0.5FTE. I can't really complain about it, though: this gives me a lot of time to work on my own venture, which is my real passion, a mobile pet-grooming business. At SkillPlat, I am basically in charge of all things information security: networks, software, hardware, processes, technology, you name it. The only thing I am not really covering at the moment is the human side. And by this, I

mean training, awareness, education, etc. Those are a bit like grey areas for SkillPlat, at the moment. We always end up hiring external consultants."

"Rupert was telling us that not much has been done in those areas either?" – Matt asks.

"I guess that's pretty accurate. What can you do…the board of directors always thinks about *bang for buck*. They probably believe that there's no need to spend much money in training when we are likely not going to be targeted by external attackers…"

"Yet, you did have a couple of instances…as Rupert mentioned…."

"Oh, did he mention those to you? Well, if he did, I guess there's nothing wrong with me giving you my opinion. You know what really happened? We got so lucky. Incredibly lucky. Especially the ransomware thing. That was much more than a near miss. I tell you what, that episode could have cost us the whole company. The malware attack through that email, well, I get it that curiosity may push an employee to click where they shouldn't, and we improved our application controls after that. The employee was a childhood friend of Rupert and I'm pretty sure the event was not even mentioned to anyone in the company. But the ransomware…big warning there. And I can't say that things have changed much after that. We have this company policy based on which all traffic goes through the company's VPN, but apparently employees don't always follow it. Rupert put out an urgent newsletter asking everyone to be more careful, use their VPN, avoid dodgy websites even when working from home, etc.; but that was about it."

"Stella, Jerry, the CEO, mentioned the recent case of a former employee that apparently had insider information that provided an advantage to their new employer in a bid with the government…"

Your question strikes Stella right on her forehead, like an arrow. The security manager does not reply immediately but checks a couple of times if anyone can hear her. Then, at a lower volume, she says:

"Look, this is a bad one. I know the guy. He's always been quite a dodgy person. He left the company on a bitter note. Rupert, in particular, could not stand him. Unfortunately, this person was in charge of this bid. He was immediately replaced, but a big mistake was made: his email account was not disconnected until two weeks after he left, and the preparation for the bid was in full swing at that time. So, internal emails kept circulating. Recipients were under an old mailing list, and this person was still part of it. I'm sure he kept checking his work email during those two weeks. He could certainly download attachments and read emails about SkillPlat's proposal for the bid. That's how he could use such information at his new employer's advantage. And that's how they won the bid."

Matt is on a roll: "Jerry said this is being investigated. We're interested in what went wrong there."

"As I was telling you, we're developing our security policies. I'll send you the one on email usage for you to have a look. It has been approved already, but all feedback would be very valuable. Email disconnection is usually in the hands of our IT Managers, but there's not a warning to alert them when a disconnection needs to be done. Usually, a communication gets triggered from HR informing the IT Manager on duty that someone does not work for us anymore and IT does the disconnection straight ahead. This time, for some reasons, either such communication did not happen, or the IT Manager simply forgot about the disconnection. Those guys, frankly speaking, are quite busy…I'm sure we could use more IT managers to take some burden off their shoulders."

"Stella, is SkillPlat following any specific frameworks?"

"You know, being a medium enterprise there's just so much we can do. So, we decided to adopt a bottom-up approach, starting with baby steps to then escalate, for whatever possible, to more established management models such as ISO27001 or NIST. Well, at the moment, we're not anywhere close to getting an accreditation. It may take years. But for us it's important to start, at some stages, no?"

"Now, the CEO mentioned that SkillPlat partners with two colleges for the delivery of most training courses. How do you organise information sharing with these two colleges?"

"Yes, the Oasis Community College and the Alba College. I would say that 80% of our students, apprentices and trainees go to the Alba College, as they are leaders in their field. Once the students pass their courses there, they get accredited with us. The Alba College has often been considered a best practice in terms of cybersecurity. I know the security managers there and they all have some of the best certifications available in the market: CISSP, CISCO, CISM, etc. They are very strict on information sharing: they prepared an information sharing policy that is the best policy I've ever seen: complete, understandable, comprehensive, rigorous. In one word, nearly perfect. I feel very confident with doing business with the Alba College. On the other end, the Oasis Community College is a very small organisation and only 20% of our students go there. They are always tight with money and are desperate with increasing enrollments. Why do we do business with them? Well, mainly for two reasons. First, they offer a couple of brilliant courses which are not delivered by any other colleges nearby. Second, well, their principal is our CEO's wife."

Matt and you look at each other with a dubious expression on your faces. Stella continues on: "Yes, I know, it sounds quite strange and smells like conflict of interest everywhere. Anyways, - hurries Stella - this has nothing to do with information security. The problem is that, well, in terms of cybersecurity, the Oasis Community College is almost a disaster: their IT manager is also their network admin and their security manager. The poor guy has to do pretty much everything. Loss of personal information and malware-infected machines have been quite a problem in the past at that college. I don't know how they haven't been on the news yet. Probably because they're a small fish. Now, Rupert, our CIO, is worried about this issue and has mentioned it several times to Jerry, our CEO. But as you can understand, Jerry gets quite defensive when it comes to the Oasis Community College."

"So, how do you manage the potential risks deriving from your relationships with the Oasis Community College?"

"We try to keep ourselves as separated as possible from them. I'm not an expert in contracts, but I believe the affiliation we have with them is quite light, in the sense that the students are effectively *their* students: Oasis collects, stores, and manages their information when they are there. We do the same with our students when they are here with us. The downside is that students often complain about this separation: *"Why do I have to enter the same information twice, once for SkillPlat and once for Oasis? Can't you guys talk to each other?"* they often tell us. And they're absolutely right, but we don't want to take risks. Still, there are instances in which you need to share some basic information: we always hope Oasis won't lose it. Our Risk Committee has its hands full with assessing risks associated with doing business with the Oasis Community College."

"Speaking of which, we had a look at SkillPlat's organisational chart and could not see a Risk Management function. Don't you have one?" – you ask.

"Actually, we don't, in proper terms. How we do risk management is through an ad-hoc committee called the Risk Committee. I am a member of the committee together with Rupert the CIO, Judith the COO, Sandy the CHRO, and our safety manager. Judith is in charge. The committee deals with operational risks (the financial ones are managed by Wong and his finance team) and these include cyber-risks too. When we discuss cyber-risks, the IT managers are invited too. The Risk Committee meets once a month or upon request by any of the committee members. Its main function is managing risks: once we identify a new one, we assess it and treat it. Obviously, the risks I mainly deal with are of cybersecurity nature. If you're interested in how the process works, I'm happy to share with you the minutes from our last meeting."

"This would be great Stella, thank you!"

"Ok, I'd better get back to work now. I'll send you the promised documents."

Later, as expected, you receive an email from Stella, with the promised documents: SkillPlat's Corporate Information Security Policy (see Appendix E), an example of a sub-policy, the Email Acceptable Usage Policy (see Appendix F), and the minutes from the latest meeting of the Risk Committee (see Appendix G). The following day could be a decisive one in terms of the information you will be able to collect for your final report.

Headquarters of SkillPlat, Thursday

You start your day by paying a visit to Marko, one of the IT managers. His office is located at the back of the main building of SkillPlat. You knock at the door, but no one answers. You decide to wait, when a desktop computer on a desk inside the office catches your attention: the screen is still on, no one is at the desk, but the computer clearly appears unlocked.

"Hey, I'm here." - a sudden voice at your back - "You must be the consultant?"

You can perceive a hint of sarcasm in the voice of Marko, who immediately goes past you without shaking your hand and heads back to his desk.

He then looks at the screen and, confused, says: "I…I…always lock my computer, I was just at the toilet."

You offer Marko your best smile. You have more than 15 years of experience in this job, and you know when someone is lying.

"No dramas Marko. I wanted to ask you something: what is the usual procedure you use to grant visitors like me access into your wireless network?"

He seems embarrassed: "Yeah, look, yesterday it was a bit of an exception with that little card and the *password123* thing... There's usually someone from IT on duty all the time, so when a visitor comes in, we deal with usernames, passwords, etc."

You remember that Margaret, the receptionist, gave you a very different version… Your conversation with Marko goes on for some more time, during which you realise the IT manager is very distracted. You decide to tackle the issue headfirst: "Sorry if I am being very honest Marko, but you seem to be thinking of other things? Maybe we can re-arrange our conversation for tomorrow?"

Marko sees your point: "I'm sorry, you're right. It's just that I will be by myself this week and the following one as Albert, the other IT manager, is away. I've got so much on my plate that I can only think of my agenda getting bigger and bigger. You know, we're so understaffed in IT. I think we should hire one or two more people, but for now there seems to be no budget for this."

"I perfectly understand. Let's just leave it for now, if I need more info from you, I will let you know."

Marko looks relieved, as you leave his office.

Headquarter of Selective Consulting, Thursday

Before you head home to have some rest before the big day, you receive an email from Patricia, with her analysis of the reports that SkillPlat publicly shares on their website: a Privacy Policy, a Record Management Policy, and an ICT Usage Policy.

From: patricia.krueger@selectiveconsult.com.au
RE: Publicly available policies from SkillPlat's website

Hi,

I analysed the policies you downloaded from SkillPlat's website, and I am briefly summarising what I found. First, I believe we can agree that for an apprenticeship and traineeship platform to make three such important policies publicly available is a great testament to their willingness and motivation to be trusted by their partners and clients.

Privacy Policy: This policy informs whoever lands on SkillPlat's website of how the company handles personal information and complies with legislative requirements in terms of privacy. The policy contains heaps of details on its purpose, scope, responsibilities, and document owner. It clearly articulates what collection and use of personal information are and how disclosure of personal information (including to service providers) is regulated. The policy explains how privacy is guaranteed when users access SkillPlat's website, the usage of cookies, and the collection of certain statistics for business purposes. In the document, there is also a section dedicated to the security of personal information electronically stored on SkillPlat's premises, how such information is used and the company's intention to abide by industry best practices in this field. Legislation on disclosure of data breaches is also expressly mentioned in the document, with details on how SkillPlat intends to notify the required authority should a breach occur. Finally, the document regulates access to information (which is guaranteed upon request and when another person's privacy is not infringed) and modes for correcting inaccurate/outdated information held by SkillPlat. The document is signed by the Chief HR Officer, with contact details provided in case of necessity. The document was approved three weeks ago.

Record Management Policy: This document is intended to inform stakeholders on how SkillPlat's record management system works. The policy does not illustrate scope, responsibilities, and document ownership, but does provide some details around its purpose. In sum, the policy explains that all SkillPlat employees and staff members must create full records that adequately document the official business activities of the company. Also, staff should not alienate, relinquish control over, damage, alter or destroy SkillPlat's records. Signature of the document is by the CEO. The document was approved one month ago.

Communication and Information Technology Policy: This policy regulates the usage of information and communication technology (ICT) at SkillPlat. After

describing the purpose, scope, responsibilities and ownership of the policy, the document is divided into three main areas, around which ICT usage is regulated: marketing and advertising; Internet and emails; and social media. In terms of marketing and advertisements, the policy states that SkillPlat engages only in practices that are compliant to relevant legislation and that the CEO is to be considered the public face of the company. As for Internet and emails, the policy states that employees and learners are provided with Internet and email access for business and learning purposes and the Internet should not be used for illegal, immoral, or unacceptable use. A significant section is dedicated to social media, where employees and learners are invited to use social media with high ethical standards, respect, integrity, transparency, and honesty. The document is signed by the CIO and was approved six months ago.

I believe it is obvious that the three policies present some interesting differences in the ways in which they are drafted, their contents, etc. It may be worth mentioning some of the above elements in the final report, what do you think?

Tomorrow morning, I will be in the office at 7 am, so we can start writing the report.

Patricia

Tomorrow you will finalise the last pieces of information and work with Patricia and Matt on the final report.

3. EPILOGUE

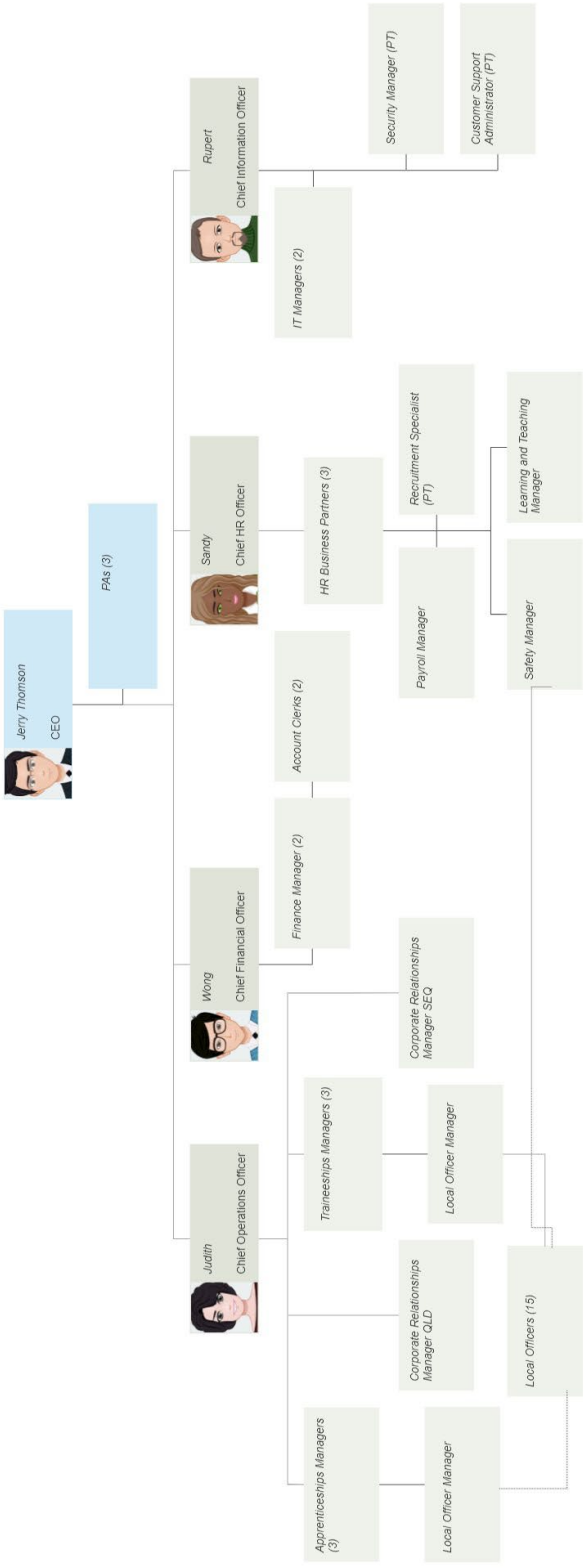
Headquarters of Selective Consulting, Friday afternoon
Done! You have just pressed the 'Send' button for the email you prepared for Karen, with the report about the information security management system at SkillPlat. Patricia and Matt proudly look at you. You thank them for their help: you would not have been able to do this without the invaluable support of your colleagues.

AUTHOR BIOGRAPHY

Ivano Bongiovanni is a lecturer in information security, governance, and leadership at the Business School, University of Queensland, Australia. He holds a Ph.D. from QUT. His academic experience includes appointments with Bocconi University (Milan, Italy), QUT (Brisbane, Australia) and the University of Glasgow (UK). His industry experience includes appointments with the Italian Department of Police and the Organising Committee for the XX Winter Olympic Games. Besides conducting research on information security management and cybersecurity leadership, he regularly facilitates design-led workshops and leads projects in this area.

APPENDICES

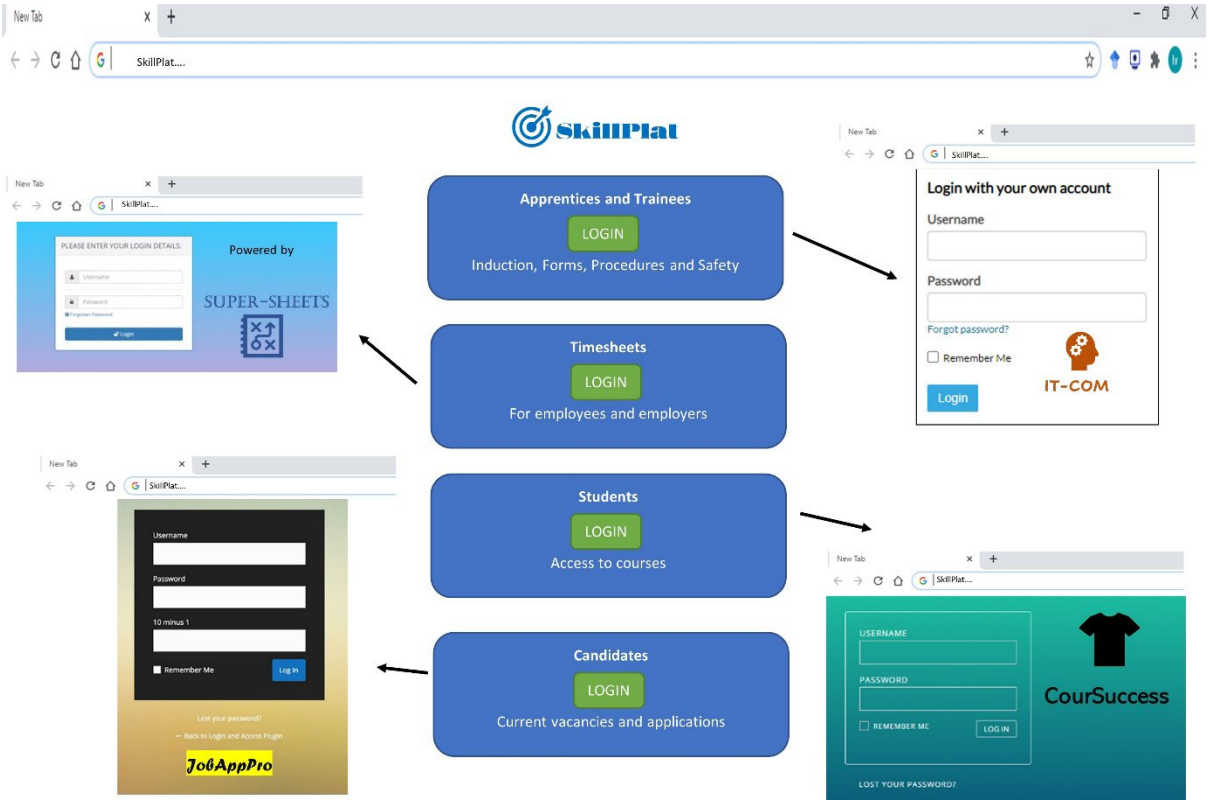
Appendix A. SkillPlat's Organisational Chart



Note: PT indicates Part-time employment; PAs: Personal Assistants

** Made with smartdraw.com and avatarmaker.com*

Appendix B. Login Pages from SkillPlat's Website



Appendix C. Newspaper Article about SkillPlat's Training Program

CYBERSECURITY NEWS
Information Security? It's no joke at SkillPlat!

Local training organisation to train all employees in cybersecurity

Our correspondent, 27 March 2018

In the light of the entry into force, last month, of the legislation on the notification of data breaches, local apprenticeship and traineeship platform SkillPlat has decided to engage all its employees into an ambitious training program on information security. The company, that has around 50 employees and a number of sub-contractors (caterers, cleaners, tradespeople, etc.), has been particularly responsive towards the government recommendation for SMEs to start taking information security seriously.

"We firmly believe that information security should be everyone's priority these days and we decided to massively invest in a comprehensive cybersecurity training program for all our employees." stated Mr. Rupert Maddox, the company's Chief Information Officer "That's why, with the help of several security experts, we are going to deliver a two-day, full-time information security course for all our employees."

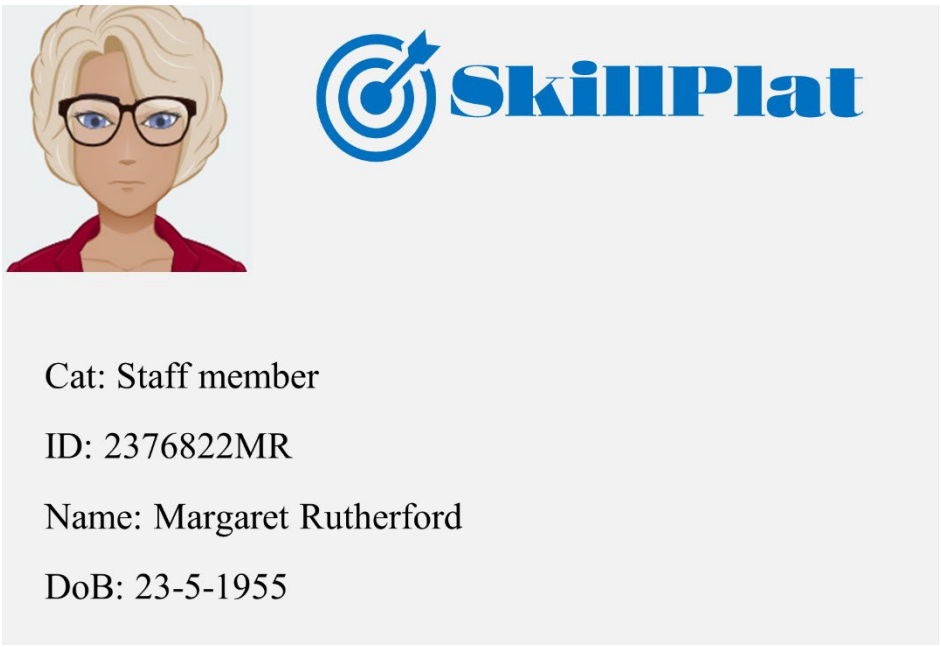
SkillPlat's employees will learn the basics of information security, from how to protect customers' data and privacy, through the usage of corporate social media, to how to spot suspicious emails and what to do in such cases.

"We will also have a keynote speaker come and talk about the legislation on the notification of data breaches: how it applies to SkillPlat, what to do in cases of breaches and how to communicate with our stakeholders." continued Mr. Maddox.

This initiative is the first of its kind for the loc and the CIO further elaborated on its importance: "As a platform, we manage at any given time heaps of personal information: of our students, trainees and apprentices, of the employers that work with us and of numerous stakeholders. When I joined this company twenty years ago, everything was done on paper and there weren't as many regulations on privacy and information security. Today, we primarily operate online. Yet, we do have a number of legacy systems that would require an update, systems for which Internet connection was not in-designed but retrofitted once it became available and convenient to do so. This presents several warnings, which our employees have to be aware of".

The training program will begin in two weeks. Mr. Maddox estimates that in around two months all employees will have completed it.

Appendix D. Sample ID Card of SkillPlat



*Avatar created by using avatarmaker.com

Appendix E. Corporate Information Security Policy for SkillPlat's

SkillPlat - Corporate Information Security Policy

Table of contents:

1. The importance of information to SkillPlat

SkillPlat is a company which is IT intensive, meaning that most, if not all of SkillPlat's operations are highly integrated and dependant on its IT assets. These IT assets include the data and information of customers, employees, etc, as well as the information processing systems which store, process and transmit these assets. Therefore, these IT assets, in all their forms, can be seen as the life blood of SkillPlat, and must, therefore, be suitably protected against all risks. Properly protecting and securing these IT assets is critical to SkillPlat's survival. Furthermore, SkillPlat is subject to a wide range of legislative, regulatory and contractual agreements and specifications, which also require the proper protection and security of all these IT assets. The purpose of this Corporate Information Security Policy is to state the commitment and support of management to such protection and security, and to specify the environment which will be used in SkillPlat to protect these IT assets from all types of threats, whether internal or external, deliberate or accidental.

2. What is Information Security?

Information Security is seen as the discipline used to maintain the following three basic characteristics of information and data: Confidentiality, Integrity and Availability. This Policy therefore specifies the environment which will exist in SkillPlat to ensure that the confidentiality, integrity and availability of SkillPlat's IT assets and information processing systems are maintained at all times.

3. Why SkillPlat needs Information Security

As stated above, SkillPlat's IT assets are critical to the company's very survival. However, for SkillPlat to be a competitive player in the market, SkillPlat must also share such information assets with other external players, for example, customers, employers, financial institutions, etc. This sharing, of course, results in increased risks to these vital SkillPlat information assets. To protect SkillPlat's information assets during internal as well as external use, and also to conform to legislative, contractual and statutory requirements regarding its IT assets, Information Security is one of SkillPlat's prime responsibilities. This responsibility is shared by all employees of SkillPlat – from the highest to the lowest level.

4. The Information Security Commitment of SkillPlat's Board

The Board of SkillPlat realizes the strategic importance of its IT assets and information processing systems, and the subsequent protection of these assets. Full support and commitment is given by the Board to the enforcement of all aspects of Information Security on all levels of SkillPlat. This commitment is formulated in terms of the following Policy statements, and the Board also mandates disciplinary action against any stakeholder of SkillPlat who does not comply with the content of this Corporate Information Security Policy and its constituent sub-policies.

5. Scope

This Policy applies to:

5.1 All SkillPlat's IT assets stored, processed and distributed via SkillPlat's information processing systems;

5.2 Any person who had been granted authorization to access SkillPlat's IT resources, including, but not limited to, permanent, temporary, third party, contractual employees and users;

5.3 All business partners and clients (including apprentices, trainees and employers) that access SkillPlat's IT assets in any way.

6. Information Security Statements in this Corporate Information Security Policy

Statement 6.1

SkillPlat will have a proper Information Security organizational structure to manage Information Security according to this Corporate Information Security Policy and its constituent sub-policies.

This structure will:

- ensure that security roles be assigned to all users;
- that all users are aware of the content of this Policy;
- that all users are aware of the disciplinary consequences of not complying with this Policy;
- coordinate and review the continuous implementation of this Policy.

Statement 6.2

All IT assets in SkillPlat will have a documented way in which they are handled, including:

- being reflected in a company-wide inventory;
- having a nominated owner who will ensure proper rules for the handling and protection of such assets.

Statement 6.3

SkillPlat's Personnel (Human Resource) policies must incorporate detailed measures to support the implementation of this Corporate Information Security Policy. These measures must include termination of employment, non-disclosure and confidentiality clauses, job-oriented Information Security responsibilities and reference to disciplinary action for nonconformance.

Statement 6.4

SkillPlat will have a proper infrastructure to enforce physical and environmental security in order to protect information-related assets.

Statement 6.5

SkillPlat will have the proper measures, including responsibilities and procedures, in place to ensure the correct and proper management and operation of all its information processing and communications facilities.

Statement 6.6

SkillPlat will have the proper measures in place to ensure that only properly authorized people have (logical) access to its information facilities.

Statement 6.7

SkillPlat will have proper measures in place to ensure that Information Security is taken into account during the acquisition, development and maintenance of all software systems.

Statement 6.8

SkillPlat will have a proper system for managing Information Security incidents.

Statement 6.9

SkillPlat will have proper measures in place to ensure the business continuity of all its information processing systems.

Statement 6.10

SkillPlat will have proper measures in place to ensure compliance to all legal requirements, as well as to the Statements of this Corporate Information Security Policy.

7. Sub-Policies

The Corporate Information Security Policy of SkillPlat is supported by the set of SkillPlat's Information Security Sub-Policies in which each of the Statements above is specified in detail.

8. Responsibilities

7.1 SkillPlat's board and senior management: drafting, amending, and promoting this CISP in order for all employees and stakeholders of SkillPlat to be aware of it; ensuring that this CISP gets regularly updated, based on changing business requirements or environmental factors (e.g., technology); deciding on cases of major breaches to this CISP.

7.2 Chief Information Officer: supervising compliance to this CISP, with the help of the IT team; reporting to the board of directors on compliance to, updates on, and progress of, this CISP; deciding on some cases of violations.

7.3 Security Manager: ensuring compliance to the CISP's sub-policies, where needed; supervising the security of the IT infrastructure of SkillPlat; liaising with employees and other stakeholders to ensure the operational implementation of information security procedures and measures; report to the Chief Information Officer; consult the Chief Information Officer and the board of directors on case of breaches.

7.4 Users: ensure compliance to this CISP and related sub-policies.

Note that this Responsibility list is not comprehensive, but merely acts as an example.

9. Compliance Clause

Where there is belief that a breach to this CISP (Statements 6.1 to 6.10) has occurred, the company's disciplinary procedure will be activated. If an employee or other stakeholder is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's/stakeholder's disciplinary record. Responsible for the assessment of the appropriate penalty will be the Chief Information Officer/Chief Human Resource Manager or the Board of Directors, based on the severity of the violation(s).

Appendix F. Acceptable Email Use Policy for SkillPlat

SkillPlat - Acceptable email use policy [internal only]

Introduction

Use of email by employees of SkillPlat is permitted and encouraged where such use supports the goals and objectives of the business.

However, SkillPlat has a policy for the use of email whereby the employee must ensure that they:

- comply with current legislation;
- use email in an acceptable way;
- do not create unnecessary business risk to the company by their misuse of emails.

Scope

The present policy applies to any employee, staff member, senior management team member, executive, board member, contractor, visitor, etc. having a [user]@skillplat.com email.

Reference

Up: The present policy originates from SkillPlat's Information Security Strategy.

Down: The present policy is implemented through a number of procedures whose drafting in written form is currently under-way. In absence of a written procedure on how to implement the present policy, current unwritten organisational arrangements stand.

Unacceptable behaviour

The following behaviour by a SkillPlat employee is considered unacceptable:

- use of company communications systems to set up personal businesses or send chain letters
- forwarding of company confidential messages to external locations
- distributing, disseminating, or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating, or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- accessing copyrighted information in a way that violates the copyright
- breaking into the company's or another organisation's system or unauthorised use of a password/mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-business-related matters
- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus or malware into the corporate network

Monitoring

SkillPlat accepts that the use of email is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business. In addition, all of the company's email resources are provided for business purposes. Therefore, the company maintains the right to examine any company-owned systems and inspect any data recorded in those systems. In order to ensure compliance with this policy, the company also reserves the right to use monitoring software in order to verify the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with employees.

Non-compliance: sanctions

Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record. Responsible for the assessment of the appropriate penalty will be the Chief Information Officer or the Board of Directors, based on the severity of the violation(s).

Agreement

All company employees, contractors or temporary staff who have been granted the right to use the company's email services are required to sign this agreement confirming their understanding and acceptance of this policy.

Appendix G. Risk Committee Minutes (SkillPlat)

SkillPlat – Meeting Minutes

Date: 15 October
Location: SkillPlat, meeting room 306
Time: 10am – 1pm
Subject: **Risk Committee monthly meeting: Emails erroneously sent to external recipients: Risk Management.**
Participants: Security Manager, CIO (Committee Vice-president), CHRO, COO (Committee President), IT Manager (x2), Safety Manager.
Apologies: none.
Next meeting: 15 November, 10am – 1pm

Agenda:
- Emails erroneously sent to external recipients: Risk Management
- AoB

Introduction and goals of the meeting:
After several similar instances occurred to competitors in the South-East Queensland area, as reported by the Security Manager, a requirement to put in place a structured process to manage the risks associated with emails being erroneously sent to external recipients arose. The Risk Committee (RC) agreed that such risk should be carefully managed by SkillPlat and decided to prepare a risk management process. The meeting finalised the risk management practices associated with this type of risk, including overview of the risk (risk identification), risk analysis, risk assessment, risk treatment, risk monitoring and ongoing review of the risk management process.

Sources:
Main source for the newly established risk management process was the ISO/IEC31000:2018 framework. It is worth noting that the adopted risk management process conforms with the ISO/IEC27001:2015 framework "Information Technology – Security Techniques – Information security management systems – Requirements", with particular reference to Part 6 – Planning).

Scope and Definitions:
Several definitions were proposed during the meeting to scope the purpose and boundaries of the risk management process described in the present minutes:

1) The Security Manager suggested that the process should cover *"All instances of communication erroneously sent to external recipients via email from SkillPlat's staff members, employees, visitors, contractors and other stakeholders in relation to their business for, and with, SkillPlat, provided that such communications utilise SkillPlat's internal email system, identifiable through the [username]@skillplat.com domain."*
2) The CIO suggested specifying the following exclusion cause: *"The process described in this document should not cover instances of communication erroneously sent to external recipients via email from email systems not identifiable with the [username]@skillplat.com domain, including, for example, [username]@gmail.com or [username]@live.com.au."*
3) The COO suggested specifying the following exclusion clause: *"The process described in this document should not cover instances of communication deliberately sent to external recipients via email, which should be the object of a specific risk management process, to be discussed in future RC meeting."*
4) The Security manager suggested that by *erroneously* the present document means *following an act of unintentional nature including, but not limited to, negligence, unskillfulness, recklessness*.
5) The RC voted on the aforementioned points 1-4 and approved them unanimously.

Risk Identification:
SkillPlat is a company that largely relies on email communication by their employees for their business. The large number of emails sent on a daily basis, from the company's facilities and from remote (e.g., employees' households or other connected location) increases the chances of having information erroneously and accidentally shared by SkillPlat's employees with unintended recipients. This can result in financial costs, competitive disadvantage and/or reputational damage.
Whilst acknowledging the importance of timely communication, this Committee recognizes the need to have procedures in place, in order to mitigate risks associated with email communication erroneously sent to external stakeholders.

Risk analysis:
The risk identified in the present document manifests when an employee or whatever person in possession of a *[username]@skillplat.com* account erroneously sends an email to an unintended external recipient. Examples of such instances include, but are not limited to, erroneous inclusion of unrelated recipients in the To:, CC: or BCC: fields; typos in the recipient's email addresses; or incorrect assessment of who the recipient(s) of an email should be.
Consequences of this type of risk largely vary and depend on factors such as type and nature of the erroneous recipients; the content of the email; the degree of confidentiality of the email; etc.

Risk assessment:

Risk assessment is performed by estimating the *likelihood* (L) and *consequences* (C) of the risk under analysis and rating the resulting risk on a pre-established risk matrix. The risk matrix adopted by this RC and, as a consequence, by SkillPlat is indicated at the bottom of this document (Figure 1).

After careful discussion, the RC has decided to consider all external email communications as potentially conducive of sensitive and/or commercial in confidence information. As a result, the risk assessed in the present document was rated as being *likely* (L) and *extensive* (C). This results in the risk being rated 8 on a 0-10 *magnitude* scale, where 0 is non-existent risk and 10 is a risk of maximum magnitude.

The RC has then evaluated the presence of potential risk controls capable of mitigating the magnitude of the risk under discussion. SkillPlat has a contractual arrangement with EmailSoft for the provision of email classification services. Before sending an email, SkillPlat's employees are automatically requested to classify it based on its content. This obliges them to carefully consider, before sending it, the content of an email and its intended recipients. At the same time, the software progressively 'learns' about the content of emails and is capable of flagging cases in which the classification of the operator may not match the content of the email.

According to the Security Manager, EmailSoft's solution greatly reduces the likelihood and consequences of instances of email erroneously sent to external recipients. It does not nullify the risk, however, as operators can still bypass the system (depending on the machine, EmailSoft has been found slowing some OS down) and avoid classifying the information or erroneously select the recipient(s).

The residual risk was therefore rated as being *possible* (L) and *moderate* (C). This results in the risk being rated 6 in terms of magnitude.

Risk treatment:
In the light of the risk assessment and the existing risk mitigation strategies, based on indications provided by ISO/IEC31000:2018, the RC has decided the following procedures for risk treatment:
- When an employee realises that he/she erroneously sent an email to an external recipient, the aforementioned employee is required to perform an immediate assessment of the information contained in the email and of the erroneous recipient:
- If the above assessment results in an instance where operational, financial or reputational damage to SkillPlat will most likely not occur, the employee is requested to simply notify the erroneous recipient of the email communication and take action as appropriate;
- If, on the contrary, the above assessment results in an instance where operational, financial or reputational damage to SkillPlat will most likely occur, the employee is requested to immediately notify their line manager for actions to be agreed upon with maximum priority. In these cases, the line manager is requested to notify the CIO.

The RC has also agreed on the following options for risk treatment:
- All employees must never disable the email classification system, unless specifically required by their line manager;
- Conversely, employees must carefully pay attention to warnings and 'red flags' raised by the email classification system and act upon them;
- Admin credentials only allow deactivation of the email classification system;
- In case of doubt, employees must seek advice from their line manager;
- Training courses (onboarding/induction and refresher) will be delivered to all employees on topics such as the email classification system and recognising sensitive/commercial in confidence information in an email;
- Communication on the aforementioned issues (e.g., newsletters) will be regularly circulated throughout SkillPlat to raise awareness on this risk.

Risk monitoring and ongoing review:
The CIO will be responsible for regular, six-months reports to this RC on the implementation of the procedures here illustrated and on the overall assessment of this risk in general. Besides this, the CIO will regularly report to this RC in case of urgency when, for instance, external circumstances are believed to have changed for whatsoever reason the risk assessment illustrated in this document.

Closing remarks:
The Risk Committee agrees that this document constitutes a substantial component of SkillPlat's Risk Register and reiterates the importance for the company to create a unique Risk Register document. Further discussions on this topic will take place in the next meetings of the RC.

AoB:
None.

Signed,
The Risk Committee

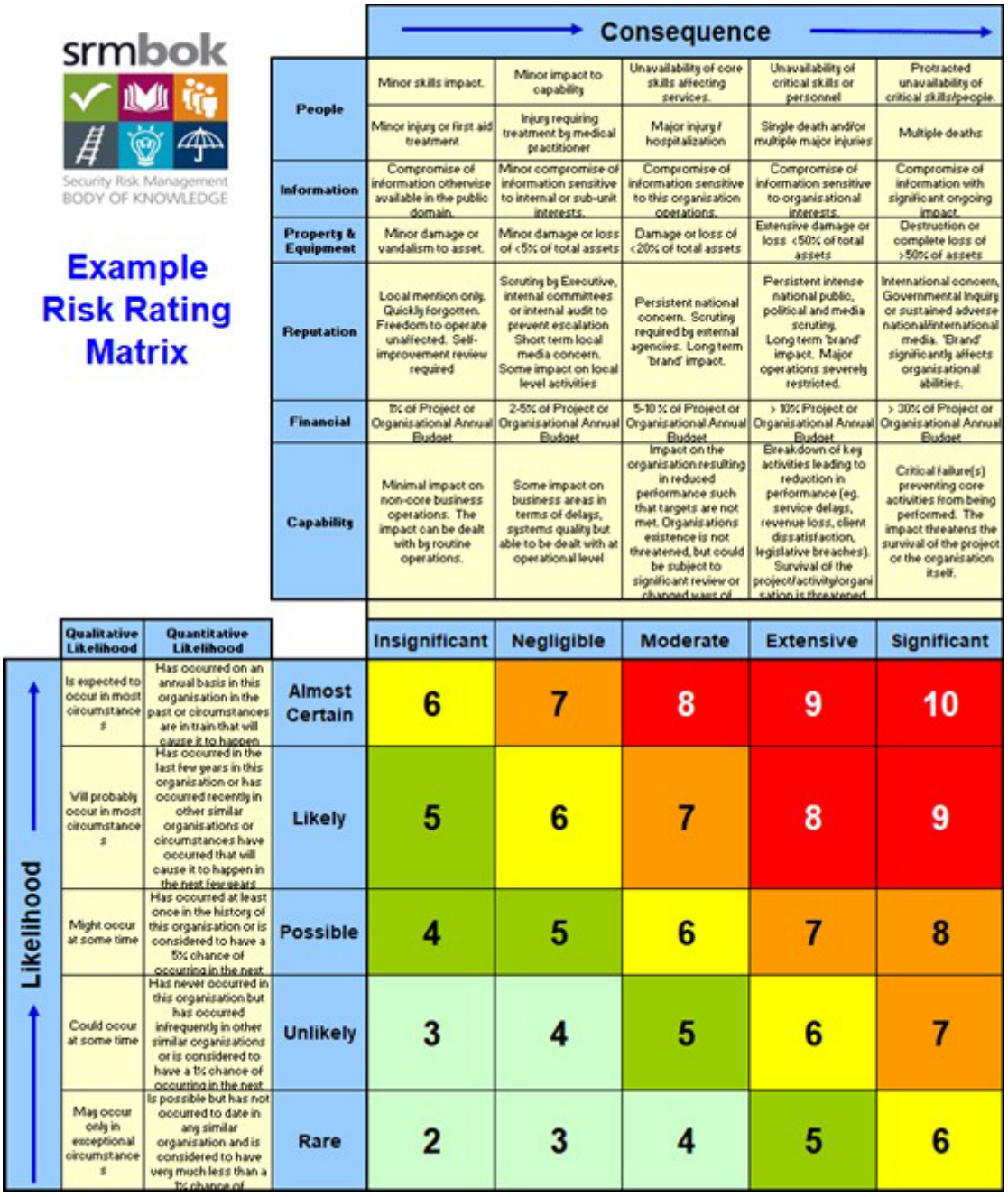
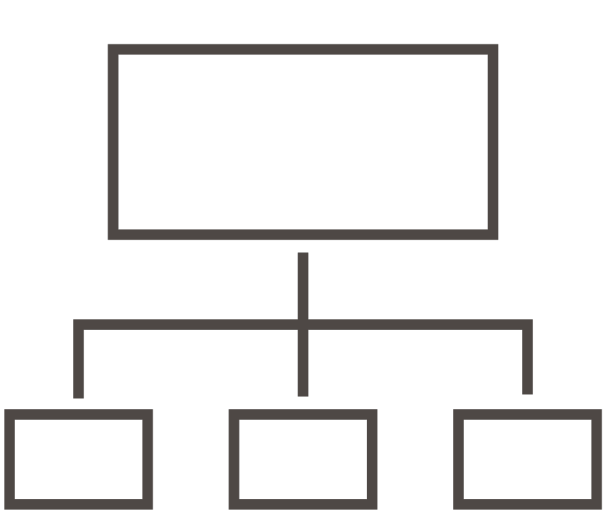


Figure 1. Risk Matrix (from Talbot & Jakeman, 2009: *Security Risk Management Body of Knowledge*. Hoboken, NJ: Wiley)



Information Systems & Computing Academic Professionals

Education Special Interest Group

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 2574-3872