Working Paper

"Managing IT Risks"

Written by: Jean-Roch Sibille

Date of submission: 06/12/2020

Table of Content

Introduction

I have been working in the financial industry since about 15 years, focusing primarily on risk management related topics. One thing is for sure; my vision of risk management has never ceased to evolve.

My professional career started with the back-testing of pricing models as an intern on the trading floors of banks, at the time when credit derivatives were the new popular thing (i.e., Credit Default Swaps, nth-to-default, CDO, CDO^2, etc.). I really enjoyed it because it combined deep technical theories with practical market considerations. I actually liked it so much that I decided to do a PhD on the subject, just to make myself sure that I got the math right. By the time I finished my PhD though, this exciting topic had turned into a risk management debacle. Credit derivatives were indeed at the base of the 2008 crisis and pricing models were blamed as one of its major causes.

The crisis had two impacts for me. Firstly, it landed me a job as a consultant doing model validation. Since no one knew anymore how to price complex credit derivatives, the research and models I had worked on were directly applicable. Secondly, it shaped my first perspective on risk management: you should better measure your risks and be serious about modelling them.

Confident in that learning, I continued working as a consultant for about 5 years. I validated a large number of models for banks and insurance companies related mostly to pricing, risk and capital models with the deep conviction that by modelling better, you could protect financial institutions.

However, contrary to my initial belief, I learned that most often the issue at stake was not with the modelling as such. The vast majority of modellers and technical professionals are highly dedicated and competent at their job, and in most cases, financial institutions face modelling risk for reasons external to the methodology itself. The most frequent risk factors are actually related to the quality of the data and inputs, the many observable and hidden expert judgements, the nature of the assumptions (e.g., risk neutral vs. real world or point-in-time vs. through-the-cycle), the model understanding and its use by the business, the lack of stress and out-of-sample testing, the missing documentation and key person risk, etc. This assessment led to my second perspective about risk management: you should never lose sight of the bigger picture. It is not because the math is right that the risk is properly evaluated or steered by the company.

Nevertheless, one aspect of my job somewhat frustrated me. As a consultant, going from company to company and from one model to another, you get the opportunity to learn a lot quickly, especially when you validate models and do not build them from scratch. This helps you growing fast as a professional, but there is also a very limited sense of ownership. You arrive at the company, you spend a few weeks analysing the model and you finalize the project when you deliver your validation report, including recommendations for the company to follow. Afterwards, you leave the company and you will probably never know what has become of your recommendations and whether they really made sense. The only way I could really understand what managing risk meant was to get on the other side of the fence and join a financial institution. Shortly after realizing this, I moved to a management role in the risk department of an insurance company.

To begin with, I had to learn to let go of the technical dimension of the job, which was hard for me as I was used to being recognized exactly for that expertise. I was an expert on asset side and banking related topics, and I became suddenly responsible for a large team of highly skilled actuaries focusing on the liability side. One thing I quickly understood is that as much as banks are all about assets, insurance companies are all about liabilities. One theory I figured out at the time was that actuaries invented MCEV and risk-neutral pricing, just to avoid talking to their investment colleagues. What can be better than a world where all assets earn the same return?

More seriously, I had no choice but to trust my team, and as said before, technical people are usually very good at what they do, so I knew it should work. I focused then on what I could do to promote better risk management aside from computing risks. Under the guidance of a Chief Risk Officer that came from the business, I realized a lot could be done so that the great work performed in risk measurement would actually help the company in making better decisions. This requires credibility towards the business, a solid sense of materiality and prioritization, and strong communication and influencing skills. This experience of focusing on the business impact helped me shape my third perspective of risk management: reporting risks is not enough, the risks have to be explained to and understood by the business in order to create a sense of ownership and accountability when decisions are taken.

Being appointed to my current position as Chief Risk Officer modified my perception of Risk Management yet again. In my previous role I considered that my job was to lead my team in identifying critical risk topics, ensure the business understood those risks and then communicate effectively what decision the management needed to take to mitigate the risks at an acceptable level. As a Chief Risk Officer, I am also a final decision-maker and responsible for all the potential risks, even the ones I might not be personally aware of. This made me discover a few additional aspects of the risk management function.

Firstly, it is not really possible to know at every point in time what are all the risks, neither can you be informed in real time of all risk generating decisions being taken, especially in disrupted times such as the current Covid-19 pandemic. It is also not practical to have a risk manager involved in every instance where a risk taking decision is being made. To overcome this, the basis is to have a strong governance in place with clear thresholds, limits, approval requirements, etc. but this is not enough. On top of a clearly defined governance, everyone in the company has to be risk conscious when making decisions, irrespective the governance and guardrails. This highlights a key responsibility for the risk function: to foster a healthy risk culture inside the company.

Secondly, as a decision maker, if I declare a risk as acceptable, it means the company will effectively take that risk. Regularly, stakeholders point out that the risk management function is impeding business initiatives, and use it as a reason not to pursue activities fraught with risks. This is certainly true, as the role of the risk function is indeed to say no when the risk intensity is just beyond acceptable. In other instances though, the risk is bearable, or can be so if minor adjustments or mitigation actions are taken. Such positive decisions are very important, because in such cases the risk management team can prove itself as a valuable partner, and act as a business enabler by defining the conditions for a risk to be acceptable for the company. Furthermore, as the risk function is not incentivized based on business performance, the fact that the risk function also supports active risk-taking activities can be very valuable to the management of the company as it provides a more neutral point of view than the business. Hence, my latest perspective is: risk management has to be implemented at a global company level through the promotion of a healthy risk culture and the risk function has to act as a business enabler to facilitate decision-making.

Much more can be said about managing risks, but hopefully this short review of my professional journey can be helpful to understand how perspectives can change through time, even if the subject matter stays the same. I look forward to continuing this evolution as I learn new insights.

Aside from the more personal views shared in this introduction, I would also like to talk about one of my most recent experiences, namely managing IT risks. As you can read from my background, I have no specific experience or knowledge about IT. Nevertheless, I am responsible in my role to monitor, report and provide steering guidance on all forms of risks, including those related to IT. In addition, IT risk has become one of the most critical areas for financial institutions at large, including insurance companies. Therefore, the objective of the next sections would aim at providing some insights on how to handle such risks. It will be covered in three sections:

- Section 1 “The Risk Strategy”: this section provides a general view on what the role of risk management is in defining the risk strategy of the company and how it can provide a useful framework applicable to IT Risks.
- Section 2 “IT Risk Challenges”: this section identifies some of the critical challenges that are specific to the management of IT Risks.
- Section 3 “Managing IT Security Risk”: this section exemplifies how a sub-segment of IT Risk, the IT Security Risk, can be approached through a standard risk framework.

1. The Risk Strategy

Before going into the details of managing IT risks, we need to establish what the role of the risk management function is and what it means for a company to establish a risk strategy.

Firstly, what is the role of risk management? Essentially, the objective of the risk function is to secure a sustainable future for the company. This means to protect the company on the one hand (e.g., to keep it away from bankruptcy), and to support the success of the company on the other hand (e.g., to ensure it is profitable in the long term). The former is the traditional role people associate with risk management, while the latter is also critical, and often more complex. It means that the risk function has to help the company to take manageable and controlled risks. More precisely, it has to ensure that the levels of risk are acceptable and fit within the company risk appetite. To enable this, one critical dimension is to regularly assess the risks and to communicate the results to the leaders of the organization, typically the Board of Management (BoM). The BoM will then have the responsibility to set a level of risk appetite for the reported risks, consistent with the available resources and targets of the company. In case the appetite is equal or higher than the predefined risk level, the risk can be accepted. In case the appetite is lower, the risk function will drive actions to reduce the risk level within the appetite.

The comprehensiveness of this exercise is of paramount importance to the success of the company, as, even if risks go unreported, they obviously still do exist. A company does not decide what its risk profile is, as such; it can only decide what aspects of the risk environment should be measured, how they should be addressed, and what levels are to be considered as acceptable. This also means that for non-reported risks, the appetite is in theory “infinite” as the management of the company is unable to steer them.

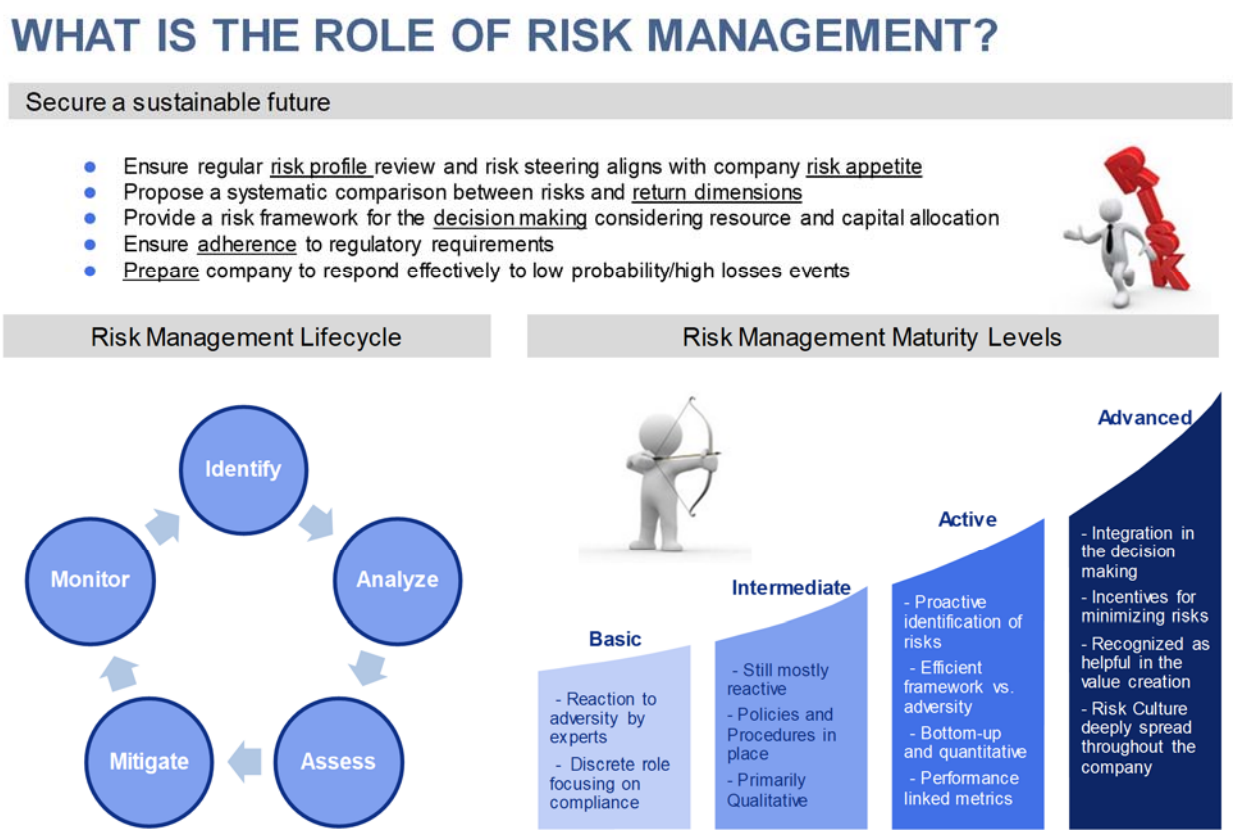

Figure 1: The Role of Risk Management

While the role of the risk function is clarified (see as well the above chart/graph for more details), we should also keep in mind that the risk profile of the company is a continuously moving target.

The internal and external environment of a company is indeed constantly changing, therefore, risk strategies have to go beyond simply evaluating the risk profile at one moment in time. In the case of IT risks, it is for example necessary to follow the continuous increase in sophistication of cyber-attacks. Similarly, the impact of changes in the business environment, such as new developments in regulations or business practices (e.g., using lower-cost cloud services for data storage or block chain to secure payments) also require a detailed evaluation.

Additionally, alongside the constant tracking of environment changes, risk managers need to develop a risk approach in line with the company strategy. For example, the decommissioning of obsolete systems, the launch of new products or the review of a digital platform all impact the IT risk profile of the company.

This stresses the need for the risk function to be timely and comprehensively informed of the important decisions taken by the company as they will likely impact the risk strategy, which itself can shape the business strategy, as one has to adjust to the other. The figure below provides a visual on how the different dimensions are connected to each other.

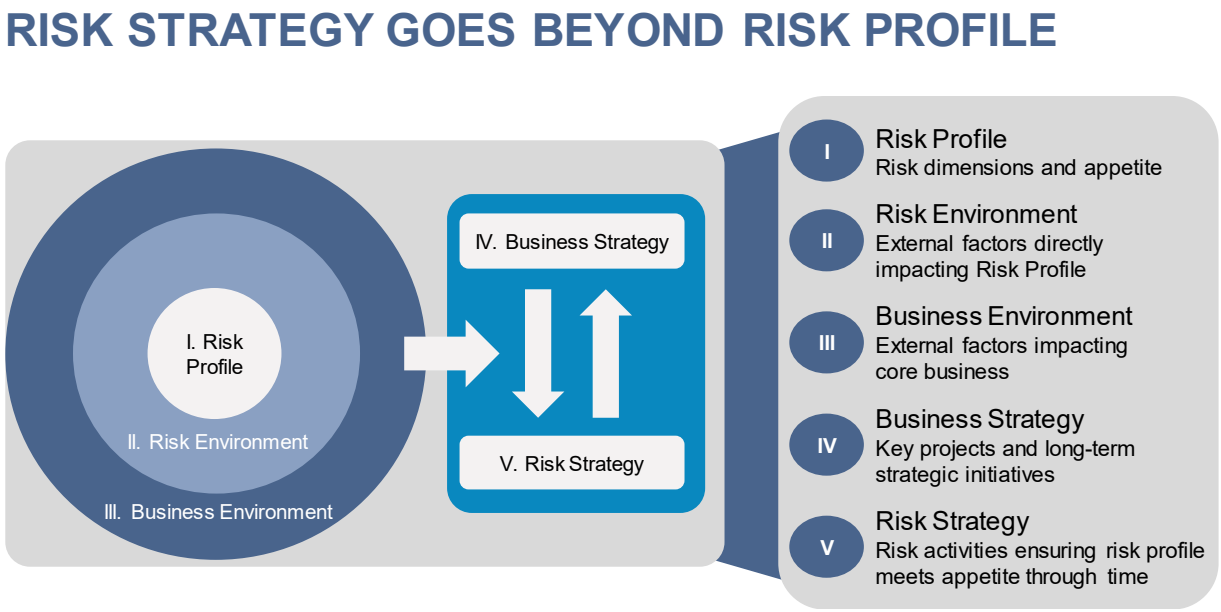

Figure 2: The Risk Strategy

2. IT Risk Challenges

The goal of this section is to shed some light on the environment around IT risks as we just learned how critical it is to understand the global picture to set a comprehensive risk strategy. In particular, the section identifies some of the critical challenges faced when managing IT risks.

Defining and Measuring IT Risk

The first challenge of the IT Risk domain is simply to provide it with an exhaustive and actionable definition.

IT risks cover all the risks associated with the development, operation, ownership, use and maintenance of IT infrastructure and applications. The risks associated with the different categories mentioned can then materialize in many different ways. For example, it can be risks related to the misconfiguration of a system, change management failures, stability issues preventing users from accessing their applications, loss of critical data, corruption of backup solutions, issues with access management, weaknesses in malware protection, performance issues reducing productivity, etc. It is beyond the scope of this paper to provide an exhaustive list even if creating such a list is critical for every company.

After defining the scope and the nature of the risks, the next step is to measure for each risk scenario, the likelihood of the occurrence of a risk event, the severity of its impact and to identify metrics that can be tracked to evaluate the situation over time. This is standard risk management practice, but difficult to apply systematically given the large scope of IT risks. An example is the access management of software users. Typically, it is not unusual to see applications being accessed by more people than required. For most applications, the negative impact of having too many users with access is negligible. However, if some applications contain strictly confidential information, the impact can be much higher, including the breach of legal and regulatory requirements. In that case, there should be regular controls in place for these applications in order to identify potential accessibility issues, as there will be no risk appetite for such access breaches.

The example of access management is relatively straightforward. Depending upon the type of access at stake, it is a situation where the risk appetite should be easily identifiable and measured through time. Now, some IT risks are much more difficult to measure and steer. For example, take the risk of IT

instability. In our new working from home environment, we are probably all experiencing issues with using IT applications, be it applications used for web conferences or to access information on our company's servers.

Naturally, we would probably all have no appetite to experience such issues. However, a perfect level of quality is likely to have a very high cost associated with it, given the large number of causes that can create stability issues. From a risk management point of view, we should ask ourselves the question of what level of instability can therefore be tolerated. For example, can we accept at the company level one stability incident per month that lasts a maximum of 1 hour? The role of the affected unit within the organization might also affect the decision made in this respect. Depending on the answer to that question, the accountability of the business function might be affected as well as the way the risk will be measured and steered. This stresses the importance of having, in addition to a catalogue of IT risks, a list of metrics associated with different risk scenarios.

Finally, aside from the IT risks that can be directly mapped to the definition provided, there are a series of risks that are linked IT risks. Amongst those, we can mention cybersecurity risk (which we will be discussing in the next section) IT project risk (related to significant IT initiatives such as decommissioning of obsolete platforms or the centralization of databases), third-party and outsourcing risk, incident management and risks around the quality of the IT control environment. All of these additional risks should ideally be dealt with consistently with the general management of IT risks.

Setting Roles and Responsibilities in Managing IT Risks

Given the significant level of complexity of IT risks, as explained above, another major challenge is to define a suitable governance that ensures an efficient identification, reporting and steering of the risks. This topic is relevant for managing most of the other risks faced by the company, but given the necessary expertise to handle IT risks, there is a higher probability of having silos within the company that fail to communicate and collaborate optimally. More specifically, the following functions are usually involved: the IT function (i.e., the Chief IT Officer or CIO), the IT Security function (i.e., the Chief Information and Security Officer or CISO), the Compliance function (i.e., the Data Protection Officer), the Operations function and the Risk function. Depending upon the complexity of the company structure, each of these

functions might have local and group/holding company equivalent. Some functions, or specific responsibilities of the function, might also be outsourced to a third party.

Moreover, any conflict of interest between and inside the various functions should be identified and mitigated. Given the complexity of simply understanding the nature of the risks, the same IT experts are often responsible for developing IT solutions, identifying the risk scenarios, reporting the risk metrics and defining what an acceptable level of risk could be. It is easy to see that such a set-up is prone to biases. To overcome this situation, it is best practice to segregate the different reporting lines (e.g., the CISO should not report to the CIO) and to empower second line functions like risk and audit with their own expert capabilities.

Increase in Legal, Compliance and Regulatory Requirements

Another challenge that has grown recently when it comes to managing IT risks is the dramatic increase over the last years in legal, compliance and regulatory requirements combined with an increased interest by regulators to discuss IT risks with financial institutions. The objective is not to make here an exhaustive list, but be it in the US, Asia or Europe, many texts have been released recently, such as the GDPR in Europe (General Data Protection Regulation), the New York DFS cyber rules or the US Privacy Laws (GLBA, CCPA and HIPAA) with an extensive impacts on the companies set-up. Each of these texts has a direct influence on how IT risks need to be managed and reported, internally and externally.

Engaging the Senior Management

The last challenge mentioned here is the difficulty to communicate and engage with senior management. The challenges are numerous. There is, of course, the technical complexity of IT and its dedicated jargon, but there is also the difficulty to describe the enterprise-wide implications of the different risks and to assess their materiality. If these cannot be presented correctly, the management will not be in a position to set its risk appetite and decide how to deal with the various risks, be it by avoiding, accepting, mitigating or transferring it. In addition, the amount and variety of risk scenarios and risk metrics associated with IT risks may give a sense of helplessness to management. This feeling, often combined with a false perception of security (many institutions have not faced, yet, a significant IT risk event), often leads to a weaker level of effective oversight by senior management.

Considering these various challenges, my conviction is that the risk function is well positioned to play a strong role in overcoming them. It is independent from other reporting lines, has the overall understanding of the risk profile of the company and is expected to cultivate a healthy sense of materiality and prioritization. Of course, there are a few conditions for this to work. Firstly, the role of the risk function needs to be clarified within the company governance and be impactful in the decision-making process (e.g., through a dedicated IT Risk Committee chaired by the risk function). Secondly, it requires the risk function to hire dedicated IT risk experts.

3. Managing IT Security Risk

Now that we have covered the goals of risk management and presented some of the key challenges around IT risks, the objective of this section will be to highlight how these risks can be managed in practice using IT security risk as an example.

As mentioned before, we need first to understand and measure the risk. To achieve this, we will use a cybersecurity breach scenario called the “cyber kill chain” which has been developed by Lockheed Martin and has become a benchmark in the industry.

Figure 3: The Cyber Kill Chain

The cyber kill chain scenario describes all the steps that are involved in a cyber-attack

- Step 1 – **Reconnaissance**: The intruder choses a target, gathers public information and look for vulnerabilities
- Step 2 – **Weaponization**: The intruder develops malware to exploit a specific vulnerability
- Step 3 – **Delivery**: The intruder transmits the malware to a victim, for example using phishing
- Step 4 – **Exploitation**: The malware begins executing on the target system
- Step 5 – **Installation**: The malware installs a backdoor or another form of access for the intruder
- Step 6 – **Command & Control**: The intruder gains a persistent access to the victim’s system
- Step 7 – **Actions on Objective**: The Intruder initiates end goal actions, such as data theft, data corruption, or data destruction

This scenario has two main benefits. Firstly, it makes the story sufficiently clear and simple to understand for non-experts. Secondly, it allows us to decompose cyber risk in multiple steps whose risks can be separately assessed. See below the table describing how each step can be evaluated.

Steps	Risk Assessment	Key Information and Metrics
Reconnaissance	Determine attack likelihood and potential danger of the attacker. - Who is likely to attack and why? Cybercriminals, state-sponsored attackers, hacktivists, etc. - What is the attacker interested in? Money, recognition, revenge, etc. - Why would the company be a potential target? How does our IT defences compare to peers?	- External vulnerabilities report - External IT defence assessment - Penetration tests - Disclosures and public information - Company profile and reputation
Weaponization Delivery	Identify the most likely forms of attack and the success probability from the attacks. - What are the various forms of attack? Harmful software, viruses, ransomware, phishing, vishing, infected websites, etc. - How likely is it that an employee falls victim to an attack? - How effective are the spam filters and firewalls?	- User behaviour report - Phishing campaign results - Security Incident Handling - Penetration Tests
Exploitation	Determine the strength of the company "outer shell", the risk that the malware begins its execution in the system. - What defences are in place to avoid malware execution? - How efficient is the company at identifying and closing external vulnerabilities?	- External security company scoring - External vulnerabilities report - Control compliance report
Installation Command & Control	Determine the strength of the company "inner shell", the risk that the intruder gains a permanent access to the system. - How much risks could be caused by access management issues? - How efficient is the company at identifying and closing internal vulnerabilities? - What is the toxicity level of our applications and internal devices? - Do we have aging issues and should we decommission or replace?	- Toxicity level reports - Internal vulnerabilities reports - Hardening guidelines - Penetration tests - Identity awareness
Actions on Objectives	Estimate the potential damage from an attack. - What is the information that the attacker will be interested in? Company data, customer or employee details, policy information, etc. - How could the stolen information be converted into a financial gain? Data ransom, dark web data sales, stolen policy credentials, etc. - What are the potential costs to the company? Regulatory fines, legal settlements, investigation costs, reputational damage, etc.	- Compliance reports - Penetration tests - Anti-fraud/money laundering reports - Logging & automated detective measures - Vulnerabilities remediation time

Figure 4: Cyber security risk assessment table

When considering the overall risk profile, it is key to understand that all the steps of the cyber kill chain are interconnected. This means that the risk of a cybersecurity breach is going to be a combination of all the risks contained in the different steps. If you consider the example of a company that has a high risk of being targeted due to its size and reputation but that has a low exploitation risk due to a strong outer shell, the totality of the risk should not be so high. As an opposite example, if the company is not very known and not a potentially profitable target for cybercriminals but is very weak to resist even basic forms of attacks due to outdated software and firewalls, the risk might still be material.

As we understand from these examples, what this scenario analysis allows us to do is to explain the risk level of the company in an intuitive manner, ground it into measurable risk factors and highlight areas of weaknesses and strengths. This is all we need to engage with the management of the company to set the risk appetite and start reporting and managing the risks.

Now, there is one element of cyber security we have not discussed yet, namely the defensive and detective actions. Indeed, in addition to the defence mechanisms active at the different stages of the kill chain, the company can also perform activities on an ongoing basis to try to detect and stop cyber-attacks. To identify these, let's first look at a typical phishing attack risk scenario.

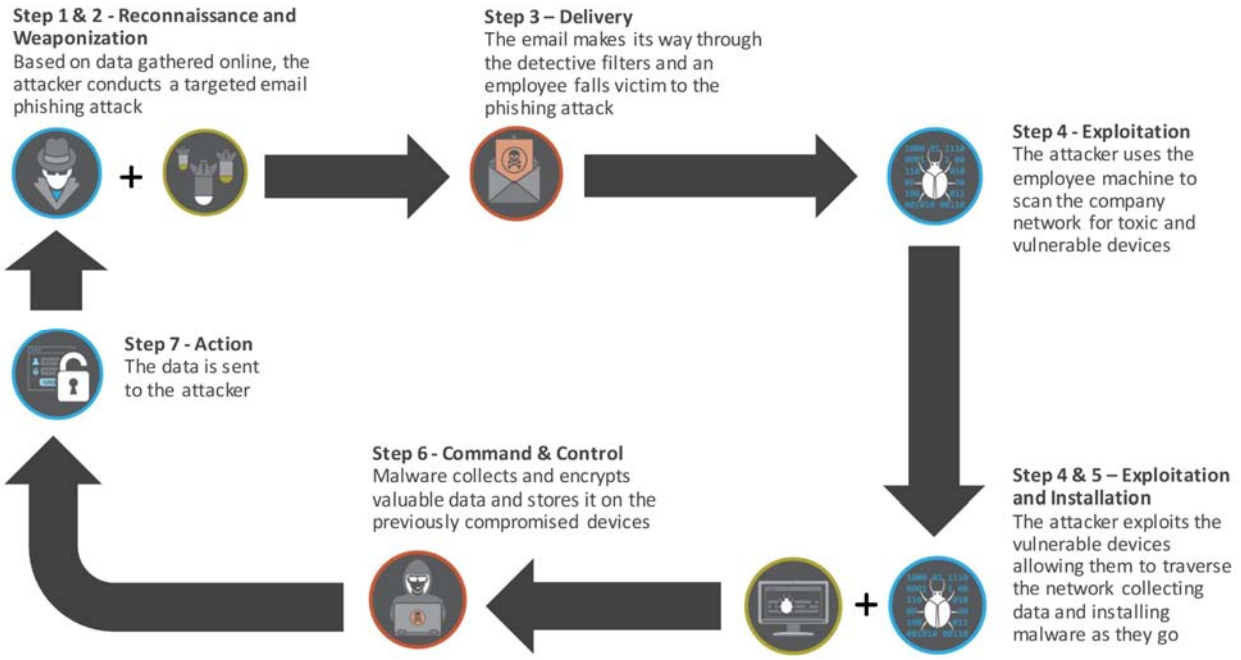

Figure 5: Phishing attack risk scenario

Taking then this phishing example in consideration, the next figure will show examples of both indicators and defences that can be used against the attack. If any of the defence mechanism is successful, the attack will be stopped, as all the steps have to happen successfully. Collecting data on successful defence actions is therefore important in assessing the overall risk. Similarly, data around detection can help to properly assess the risk level, even if results can be misleading. If no suspicious activity gets detected, it does not mean that nothing is happening. To get a better assessment of detection capabilities, one of the techniques frequently used is the penetration test that involves asking an external party to try to penetrate the systems of the company without being noticed.

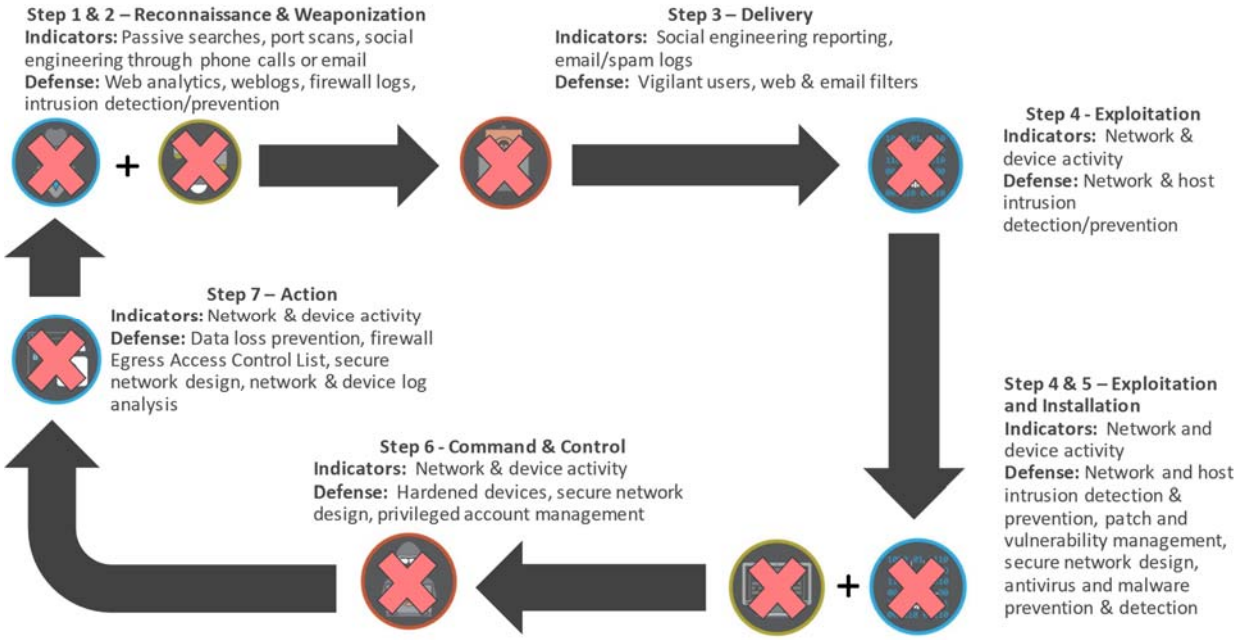

Figure 6: Detection and defensive techniques against phishing attacks

Including the risk assessment of detective and defensive actions against cyber-attacks, we should now have identified all the elements necessary to evaluate the cyber-security risk profile of the company. The next step will be to communicate it and assess if it meets the company risk appetite. Depending on the results, the appropriate measures will have to be taken.

4. Conclusion

As we have seen throughout this document, risk management faces multiple challenges. To start, it is complex by nature because it needs expertise in many business disciplines while keeping a holistic, strategic and forward-looking perspective. Then, it requires creativity to constantly imagine what can happen next and what can happen differently. Finally, it requires strong communication and influencing skills. Risk messages have to be simple, accurate and balanced to best support the company strategy.

All these aspects are easily observed when managing IT risks. The subject requires deep knowledge as well as an important strategic oversight. IT is a constantly evolving theme, driving risk managers to continuously imagine new scenarios. Lastly, it needs to be presented in a logical and understandable way to make appropriate decisions and properly set the company risk appetite which will then drive the risk strategy.

To conclude, these dimensions also capture well the reasons why I have enjoyed so much working in risk management over the years. It forces you to constantly learn about new topics while keeping the overall understanding of the company risk profile and business strategy. It builds on your creativity as it challenges you to think differently. It pushes you to improve vital communication and consensus building skills to ultimately drive the best risk informed decisions.