Cyber Risk Specialists: Masters of Mitigation in the Digital Age

Written by: Joshua Bucheli, Talent Community Manager at cyberunity and John Corona, Independent Risk and Cybersecurity Consultant

"If you don't invest in risk management, it doesn't matter what business you're in, it's a risky business" – Gary Cohn

As digitalisation surges forward ubiquitously, so too do the risks associated with this new cyber-frontier.

But first thing's first… what is 'cyber risk'?

Put simply, **cyber risk** is the risk associated with depending on cyber resources (i.e., the risk of depending on a system or system elements that exist in or intermittently have a presence in cyberspace) (NIST, 2017, 2021). That's to say, it is the risk of financial loss, operational disruption, or damage, from the failure of digital technologies employed for informational and/or operational functions introduced to a system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system. Cyber-crime or cyber insecurity, especially cyber-attacks, are on the rise and increasingly jeopardise critical systems and processes – something that threatens virtually all businesses due to the exponentially growing interconnectivity and dependence on cyber space.

There are several reasons why it is important that companies be aware of their cyber risk exposure. Risk awareness allows for informed decisions and risk-savvy approaches when it comes to new IT and cyber investments; executive boards, boards of directors, and regulators mandate transparency in the form of risk appetite statements; and disclosure of a company's cyber risk exposure is often a condition when negotiating cyber-insurance premiums. In short, this new breed of risk awareness is vital for all the same reasons that enterprise risk awareness is. What sets it apart, is the sheer velocity and scope with which it is impacting businesses – a state of affairs which necessitates a highly specialised breed of risk specialist.

Where does cyber risk stand today?

The current state of the cyber risk landscape is an increasingly precarious one – the scope of active threats is increasing, attack vectors are expanding, and the potential for harm is growing, (see Figure 1). The fact that data is often distributed rather than being stored centrally further complicates the cyber risks and associated security challenges faced by corporations, especially in the context of increasingly common hybrid clouds.

According the WEF 2023 global risk report (World Economic Forum, 2023), "Widespread cybercrime and cyber insecurity" is one of the top ten risks the world will face within the next 10 years (Figure 1). Other global risk assessments concerning business risk mirror these results, also including cyber risk in their top 5 (PricewaterhouseCoopers, 2022) / (Allianz, 2023) / (AON. 2022).

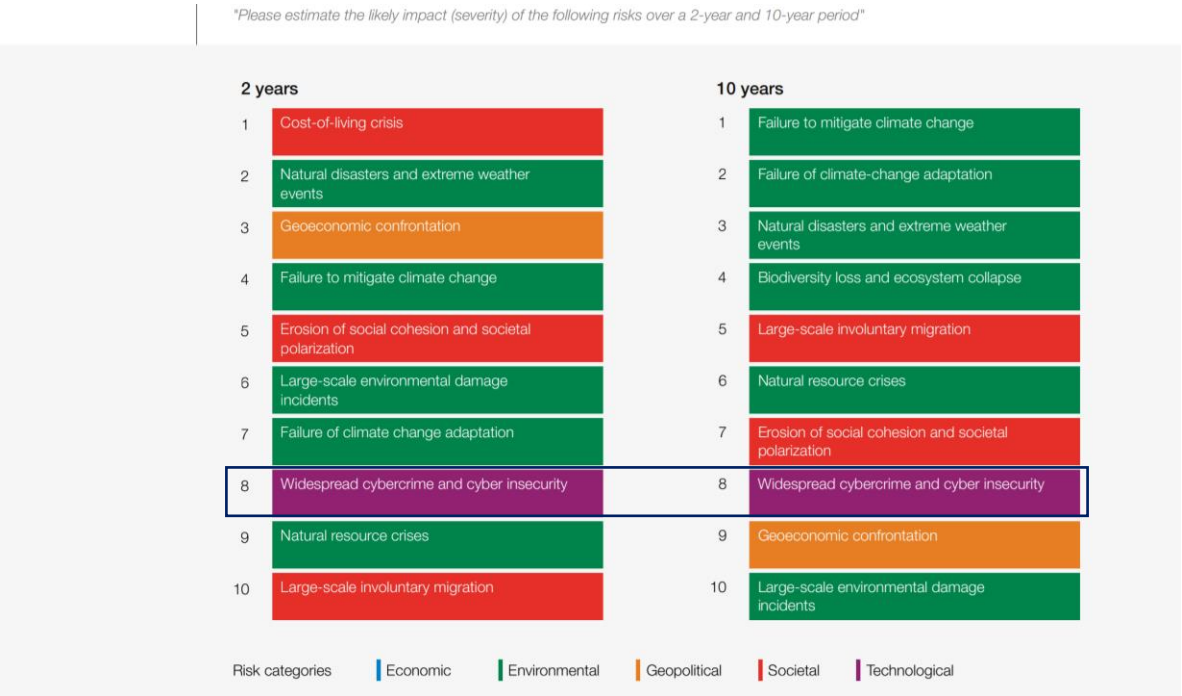

Figure 1: Global risks ranked by severity over the short and long term (World Economic Forum, 2023)

The fact that cyber risk is rising in prevalence and potential impact is compounded by the fact that businesses are not (or at least do not feel) adequately equipped to contend with these new risks. As illustrated in the annual WEF risk survey, participants perceive their risk preparedness as low, with only around 25% rating their risk management as effective or highly effective in terms of preventing or mitigating the impacts of cyber risks (Figure 2).

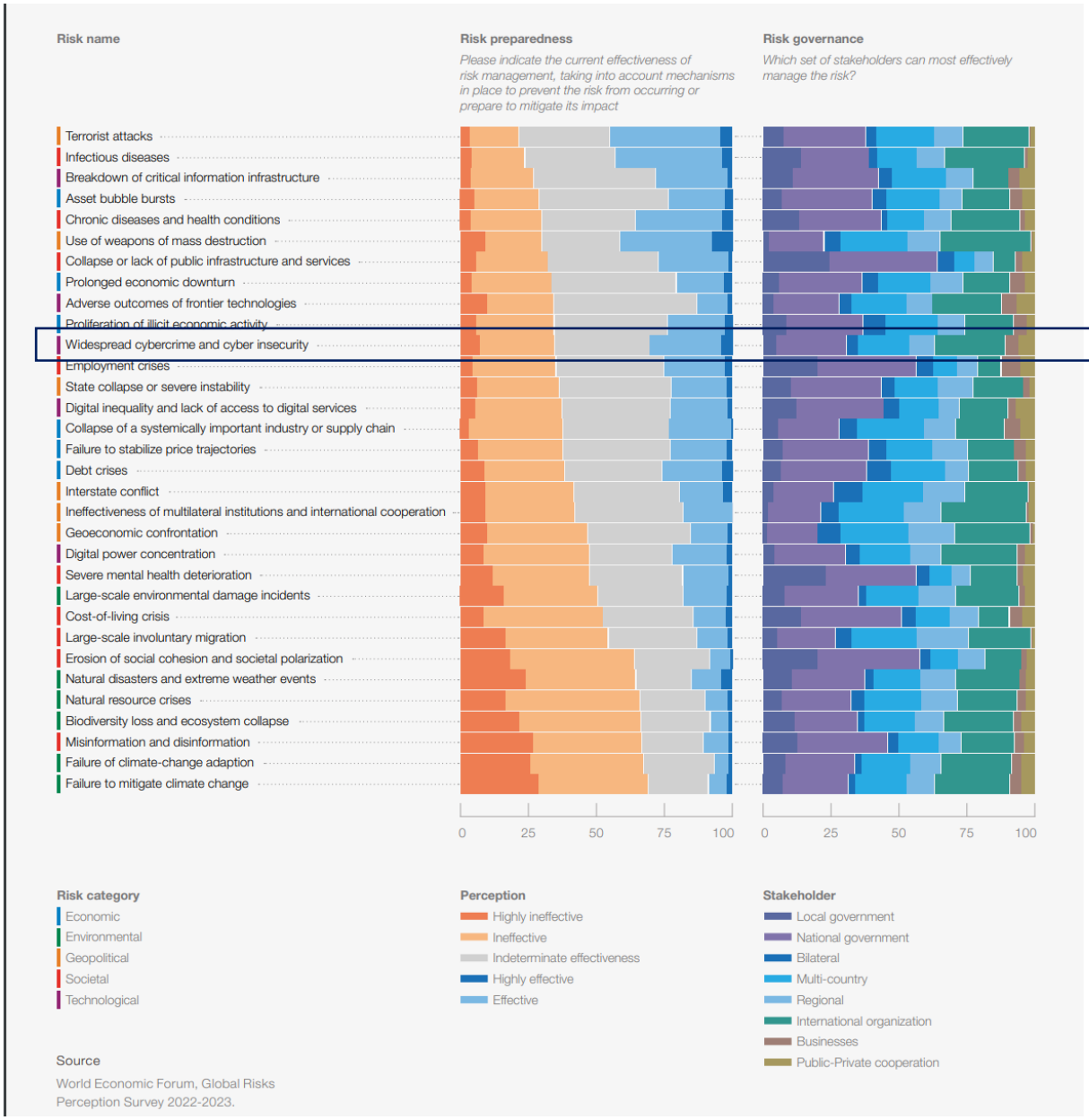

Figure 2: Perceptions around preparedness and governance (World Economic Forum, 2023)

Several global risk assessments and surveys have gone on to show that businesses are currently amongst the least prepared stakeholders when it comes effectively managing these cyber risks (Figure 2).

In response to the already considerable, and steadily increasing, global cyber risk exposure, policymakers around the world have taken action. For example, the SEC in the USA has proposed specific rules for cyber risk management, strategy, governance, and incident disclosure (Microsoft, 2023).

Within Switzerland, a new National Cyber Security Centre (NCSC) has been established to help keep cyber risks in check, issuing a strategy covering ten areas of action including threat situation, crisis management, and cyber defence to name a few (NCSC, 2023) (see also the National Test Institute for Cybersecurity).

Nevertheless, where regulations do exist, they are often fragmented, with several laws operating parallel and sometimes in conflict with one another (EBA, EU 11/19 Guidelines on ICT and security risk management (EU), federal bank regulatory agencies 10/20 – Sound practices to strengthen operational resilience (USA) being well known examples). When it comes to businesses like infrastructure providers (e.g., cloud providers) comprehensive risk-related regulation is often missing altogether.

Where is cyber risk heading?

With the advance of paradigm shifting new technologies like the Internet of Things (IoT), Big data, Artificial Intelligence (AI) / Machine Learning (ML) and the general digitalisation of critical business processes, companies are relying more and more on such technologies. This reliance carries with it considerable risk-related implications, the complexities of which necessitate extra know-how and expertise. One new innovation, and the game is changed – think of ChatGPT and the entirely novel risks that it has foisted upon businesses almost overnight (Bloomberg Law, 2023).

All of this is compounded by the myriad new regulations that are in the pipeline in the US, China, Russia, India and the EU which businesses will increasingly need to comply with – not to mention integrate into their risk management frameworks (*Harvard Business Review*, 2022).

In short, new technologies, greater cyber exposure (and reliance), and new regulations are going to subject enterprises to new risks. These new risks are difficult to foresee and will require specialised professionals in order to be identified on an ongoing basis. Not only will enterprises need to invest in uncovering key cyber risks – once uncovered and codified into a risk inventory, these risks will inform further investments and budgeting for everything from core business expenditures to (cyber) insurance.

Cyber Risk Specialists: The Key to Cyber Risk Governance

Currently, businesses typically situate the responsibility for cyber risk either within a key function in their IT department or within a function independent from their IT department that reports directly to an executive board member – i.e., the Chief Risk Officer, General Counsel, Chief Financial Officer. To allow for effective risk management, such setups need to ensure that links between risk managers and IT managers are established and actively maintained. Not only this, but it is vital that these individuals are properly empowered to influence the running of business processes and IT systems in the name of risk mitigation.

More often than not, regulated and large businesses implement their cyber risk management by integrating cyber risks into their broader enterprise risk management processes. While this is a common and valid approach, a dedicated cyber risk assessment process is advisable due to the substantial and complex organisational effort, qualified specialists, and data-driven risk processes required to effectively tackle cyber risks.

Small and medium enterprises (SME), currently dedicate less time and fewer resources to cyber risk management, if at all, with such responsibilities often being delegated to a CIO or a dedicated CISO. Whether this is purely a question of resources, or a tendency to underestimate cyber threats, it is clear that, by and large, SMEs are investing minimally in, and allocating less than sufficient budgets to matters of cybersecurity (NZZ, 2019).

The role of cyber risk management focusses on business processes across the board, including, but not limited to any and all core IT processes. By supporting the running of and by guiding changes to businesses through real-time risk assessments and risk consulting, such specialists ensure that decision-makers have the necessary insight to make informed decisions based on specific risk profiles.

Hard Skills and Qualifications

By now it should be clear that cyber risks are more than merely an extra tick-box that needs to be added to existing risk management frameworks. It is an entirely new modality of risk that will have a profound impact on how risk in general is thought of and approached by businesses. Accordingly, it is going to require a new generation of risk management professionals with a particular set of skills and expertise.

Of course, traditional risk management skills like risk identification, quantification, assessment, prioritisation, and mitigation, as well as compliance and regulatory awareness combined with knowledge of risk management frameworks like COSO and ISO 31000 will remain par for the course. However, in order to be able to apply these skills to the everchanging environment that characterises cyberspace, complementary contextual knowledge of IT (more specifically, information security) is also essential.

The first and most direct track is to pursue an academic foundation (bachelor/master) in Information Technology, Computer Science, or Cybersecurity (see for example**,** HSLU's dedicated BSc. Information and Cyber Security) and to supplement this with further training and/or certification in risk and security management (see for example, ISACA's CRISC, SCIC's CRM, or cyberunity's education partner, the SCI's Information Security Risk Management certification). Many top universities (see for example, Harvard or IMD) also offer top tier risk management trainings and postgraduate certificates.

Alternatively, a more recent track has also become available for those who wish to pursue a federal diploma in ICT security at a college of higher education instead of a BSc. or MSc. (see for example, the Cyber Security Specialist EFA or the SCI's Cyber Security Specialist Federal Diploma). Combining these qualifications with the aforementioned further education in risk management will also provide aspirants with the necessary background for a promising cyber risk career.

Finally, there are also options for lateral entrants – economics or business administration (bachelor/master) graduates, for example, bring many transferable soft skills which, when coupled with further training in IT, risk and/or security, lend themselves well to a career in cyber risk management (see https://www.ausbildung-weiterbildung.ch/it-risk-management-info.aspx for an overview of different providers in Switzerland).

Soft Skills - Beyond technical Know-How

Strategic and Proactive Mindset

Perhaps the most important soft skill that effective cyber risk specialists must bring to the table is the ability to think strategically. To analyze, manage, and mitigate risk, one must understand an organization's vision, mission, goals, how they interface with its processes, and what factors might prevent their achievement. Beyond this, understanding the interactions between different risks and how mitigation strategies may affect them differently is key. This requires big-picture thinking – the ability to assess a situation from a broad perspective and develop plans that consider multiple risks,

their intersections, and potential outcomes.

Aspiring cyber risk specialists will also need to be able to think proactively. A good risk specialist thoroughly assesses an organization's risks. A great risk specialist, however, goes beyond this by anticipating risks before they become a problem.

Rather than just asking 'what risks do we face today?', effective cyber risk specialists/managers must constantly ask themselves, 'what risks could we face in the future?'. Time is of the essence when it comes to cyber threats, and it is a lot easier to prepare for the problems of tomorrow if one has the skills and foresight necessary to think about them today.

Effective Communicators, Coordinators and Facilitators

IT risk specialists and managers operate at the crossroads between technological- and management teams within organizations. Consequently, they need to act as coordinators and facilitators between these parties, using well developed communication skills to interface these stakeholder interest groups, facilitate communication between them, and coordinate their efforts going forward.

Once risks are identified and prioritized and corresponding mitigation strategies are conceptualized, these risks and strategies must be formulated clearly, concisely, and in such a way that is understandable for and convincing to non-technical leaders and decision makers. Following this, action items resulting from these reports must be communicated to technical specialists who implement the respective changes within systems. As such, the ability to adjust one's communication strategies for both technical and non-technical audiences is essential.

Beyond this ability to code switch effectively between technical and non-technical communication styles, aspiring risk specialists can set themselves apart from the competition by emphasising their knack for persuasion, diplomacy, and for instilling trust in stakeholders. After all, being understood is worth very little if advice is not heeded and acted upon, something that often comes down to how trustworthy one comes across.

Analytical Thinking

Finally, and at the risk (pun intended) of stating the obvious, analytical thinking – the ability to approach a problem through systematic logical reasoning – is the foundation upon which cyber risk specialists must base the rest of their skillsets.

Cyber risk specialists are tasked with identifying risks and room for improvement within IT architectures. They develop plans for the mitigation of these risks, often evaluating data, and assessing models to do so. This is a rather difficult task without an affinity for sound and systematic logical reasoning. One might think that this goes without saying, especially considering that the brunt of the educational programs that one must complete to become a qualified risk specialist are analytical in nature. Nevertheless, the point cannot be overstated.

Quantitative versus Qualitative Risk Management

Before we conclude, there is a final point worth noting – namely, that cyber risk specialists tend to come in two general varieties: the quantitative or analytically minded and the big picture or pragmatically oriented. Though the line between the two is rarely clear cut, and a combination of both is ideal, it is important that aspiring cyber risk specialists understand the differences between the two.

Quantitative approaches to risk tend to place more weight on numbers and percentages, employing data analysis, quantitative assessment techniques and using statistical models to analyze, measure, represent, and mitigate risks to IT architectures. Pragmatic approaches to risk, on the other hand, employ a 'macro' lens and are more likely to use a more qualitative approach to assess, prioritize, and develop recommendations for addressing risk.

It is important to note that the two are anything but mutually exclusive and a complementary mix of both approaches is needed to ensure that risks are managed effectively. However, not all stakeholders are equally receptive to both. As such, the mark of a top tier risk specialist is the ability to tactfully combine the two based on a given scenario or audience.

Ultimately, as cyber risks continue to grow in prevalence and severity, almost to the point of ubiquity, corporate survival will increasingly rely on the implementation of robust risk-governance and management. Such governance is impossible without the expertise of highly qualified, well-rounded, and IT-affine risk specialists – a set of professionals that are still few and far between.

The best way to avoid the war for talents that is plaguing the current cybersecurity (and indeed the cyber-risk) -scene, is to KNOW YOUR TALENTS. If companies want to equip themselves appropriately for the current cyber risk landscape, they need to approach, build, and maintain relationships with specialists who can make that happen *before* they need them.

After all, what good is risk management if it happens after the fact?... Risk management is a proactive affair – and that goes both ways. Just as risk specialists need to be proactive when identifying cyber risks if they are to effectively protect businesses, businesses need to be proactive in reaching out to and establishing ties with such specialists if they want to protect themselves.