Michał Kałuziński

Senior Risk Steward - Technology and Cyber Security Risk HSBC

A Senior Risk Steward in Technology and Cyber Security typically oversees risk management strategies within an organization's technology and cybersecurity departments. Their responsibilities may include identifying potential risks, assessing their impact, and developing strategies to mitigate or address them effectively. They often collaborate with various teams to ensure compliance with security protocols and regulatory requirements, as well as to implement measures to protect against cyber threats. Additionally, they may provide guidance on security best practices and contribute to the development of security policies and procedures.

Masters in Law from Jagiellonian University in Krakow

1. what are the biggest cybersecurity risks you face on a day to day basis, or what keeps you up at night?

2. how do you use data science to help you solve your issues?

3. what are the fundamental skills you need to know to do your job appropriately

4. how has the landscape changed since you graduated in 2013?

5. where do you see the industry in 10 years?

1. What are the biggest cybersecurity risks you face on a day to day basis, or what keeps you up at night?
   1. As a Senior Risk Steward in Technology and Cyber Security at HSBC, one of the most significant cybersecurity risks I encounter on a daily basis is the ever-evolving threat landscape. This includes emerging cyber threats such as ransomware, phishing attacks, and advanced persistent threats. Additionally, ensuring the security of our systems and data amidst the rapid pace of technological advancement presents ongoing challenges. Ultimately, what keeps me up at night is the potential impact these risks could have on the confidentiality, integrity, and availability of our critical systems and information.
2. How do you use data science to help you solve your issues?
   1. Data science plays a crucial role in our efforts to mitigate cybersecurity risks. We utilize advanced analytics and machine learning algorithms to analyze vast amounts of data in real-time, allowing us to detect anomalies and potential security breaches more effectively. By leveraging data science techniques, we can enhance our threat detection capabilities, identify patterns indicative of malicious activity, and respond proactively to emerging cyber threats.
3. What are the fundamental skills you need to know to do your job appropriately?
   1. The fundamental skills required for my role encompass a combination of technical expertise, risk management proficiency, and strong analytical capabilities. Proficiency in cybersecurity principles and best practices is essential, including knowledge of network security, encryption protocols, and vulnerability assessment techniques. Additionally, a deep understanding of regulatory requirements and industry standards, such as GDPR and ISO 27001, is necessary for ensuring compliance and effectively managing risk. Strong communication and collaboration skills are also critical for engaging with stakeholders across the organization and facilitating effective risk mitigation strategies.
4. How has the landscape changed since you graduated in 2013?
   1. Since I graduated in 2013, the cybersecurity landscape has undergone significant transformations driven by rapid technological advancements and the proliferation of digital ecosystems. Cyber threats have become more sophisticated and pervasive, with threat actors continuously adapting their tactics to exploit vulnerabilities in increasingly interconnected systems. The rise of cloud computing, mobile technologies, and the Internet of Things (IoT) has expanded the attack surface, presenting new challenges for cybersecurity professionals. Moreover, the regulatory landscape has evolved, with stricter data protection regulations and heightened compliance requirements shaping the way organizations approach cybersecurity risk management.
5. Where do you see the industry in 10 years?
   1. Looking ahead, I envision the cybersecurity industry undergoing further evolution and innovation over the next decade. As technology continues to advance, we can expect to see continued convergence between cybersecurity and emerging fields such as artificial intelligence, quantum computing, and blockchain. This convergence will present both opportunities and challenges, as we seek to harness the power of these technologies to enhance cybersecurity defenses while also addressing new and evolving threats. Additionally, the growing interconnectedness of digital ecosystems will require a more holistic and collaborative approach to cybersecurity, with increased emphasis on information sharing and collective defense mechanisms. Overall, I anticipate that cybersecurity will remain a critical priority for organizations across sectors, driving continued investment in talent, technology, and risk management strategies.