IT Security

Subsector: Enterprise

Job Family: Information Technology

Impact Level

Today, this role is responsible for overseeing the programs, protocols and escalation processes for security incidents, and working towards enhancing security operations as well as cybersecurity solutions.

Medium Impact

Consolidated Activities

	Today	Future
Security Strategy and Standards Setting	Execution involves human judgment and technical expertise in aligning enterprise security vision and underlying initiatives with business strategy.	Human interaction and technical expertise will remain key in advising top management on information technology security matters.
Cyber Risk Mitigation and Network Disaster Recovery Plan Development	Execution requires deep technical expertise and can be time consuming due to the need for independent reviews of information and formulation of recommendations.	Machine learning will be used to identify potential cyber-security incidents and potential network abnormalities. Working through raw data and leveraging unsupervised machine learning algorithms, abnormal information security activities can easily be detected. However, human judgment will remain critical in formulating corrective actions and appropriate controls to mitigate technical risks.
Penetration Testing and Results Reporting	Automated penetration testing software for real time information is already being adopted today. Dashboards that are able to visualise the testing and results are also common to help determine issues and quickly counter threats.	Automation of the security testing allows the human tester to focus their time and expertise on actually simulating realistic threats.

In the next **3–5** years ...

Methods of security breaches would be increasingly complex and difficult to prevent, hence, this role will leverage AI tools to predict anomalies and take a preventive approach to manage cyber threats with varying levels of complexity and determine the optimal course of action.

Skills Differentiators:

- **Cybersecurity:** The job holder will continuously upskill to be able to handle and address increasingly advanced data/online threats.
- **Systems Thinking:** The job holder will possess strong understanding of how systems work within the context of larger systems, ensuring successful implementation/integration of security solutions.
- **Stakeholder Engagement:** The job holder will need to be able to coordinate/maintain productive working relationships with stakeholders and achieve buy-in to ensure successful roll out of new security measures.
- **Risk Awareness:** The job holder will possess in-depth knowledge of risk – including strong understanding of emerging risks, inherent process and system risks – to develop comprehensive cyber-attack prevention plan.
- **Business and Financial Acumen:** The job holder will possess commercial awareness to work effectively with business units in developing security measures and strategies to combat security vulnerabilities – in a way that is aligned across the organisation.

RPA | Advanced Analytics | AI