Our Priorities

Our priorities within 1 to 2 years:

- Digitalisation & automation e.g., digital spend analytics, chatbots. Process simplification with technology enablement providing better understanding and insights through data and information.
- Develop an effective Supplier Relationship Management framework (including risk management), with clear roles and responsibilities. Standardising ways of managing strategic suppliers and contracts will reduce risk of contractual benefits leakage and opportunities.
- Continuous process improvement towards zero audit tolerance. Balancing the need for more efficient process that meets the current business needs while keeping control and governance in place.
- Review long tail vendors for spend and supplier optimisation. Though low value spend (purchases below RM5K) is a small percentage of Maxis total spend (<1%), a continuous review would facilitate better spend and supplier management.

Our medium-term plan in the next 2 to 5 years:

- Enable AI and predictive technology (extreme automation). This minimises administrative tasks which would allow staffs to focus on more strategic tasks.
- Move towards more strategic partnership with suppliers whereby channels are established to discuss performance, issues, value add activities including innovation and sustainability.

OUR CYBERSECURITY

Built a stronger cybersecurity culture and enhanced system resiliency

Ensuring robust cybersecurity of our systems and safeguarding data privacy is a critical and top priority for Maxis. The industry we operate in directly exposes us to numerous cyberthreats, especially when considering the large network that we operate and the millions of customers we support. As such, it is vital for us to invest in security infrastructure, create policies, processes, procedures and implement solutions that will strengthen our defense against the growing sophistication of would-be attackers, while ensuring that our business objectives can progress unimpeded.

Protect the Brand and Ensure Compliance

Embed Security in DNA

Strengthen Cyber Resilience and Support Digitalisation

"I am Maxis" embodies our commitment that all of us are responsible for cybersecurity. Our employees and partners are required to adhere to our cybersecurity policies and ensure that the necessary cybersecurity controls are implemented, monitored and reviewed. We also encourage active participation in our cybersecurity awareness programmes and provide updates on cybersecurity threats through our internal communication channels and through dedicated campaigns.

The Cybersecurity Management department is accountable for more than the cybersecurity posture of our networks and IT systems but also partner with the business to ensure that Maxis continues to remain resilient against cyber threats and protect our key assets. Cybersecurity as a whole is governed by members of the Maxis Management Team and also provide periodic reports to the Audit & Risk Committee regarding posture, current and potential security threats as well as measures taken to manage the identified risks.

Enhancing Cyber Resilience

The potential for security threats increases indirectly as a result of digitalisation initiatives and thus prompts the need to review our strategies to enhance cybersecurity resilience. By definition, resilience means the ability to anticipate, withstand, recover from, and adapt to adverse conditions, attacks, or compromises on systems.

Acknowledging that human error is a major factor in cyber security breaches, we continue to enhance cybersecurity resilience through our security awareness programme

for stakeholders comprising our first line of defence. This includes our employees and key vendors, amongst many others. Numerous activities were held in the year under review, including awareness campaigns, targeted awareness programmes, monthly advisories, refresher modules, periodic phishing simulations and an annual Safety & Security Day. The phishing simulation, which is held quarterly, has helped to ensure that employees are aware about phishing activities and how to respond accordingly in such situations.

In our effort to improve our cybersecurity resilience, we also work closely with our key vendors to ensure security compliance, especially in the context of the Personal Data Protection Act 2010. We strive to ensure our customer data are well protected and take extra effort to ensure the compliance of all parties working with Maxis who have access to customer data. As part of this, we are enhancing our systems to ensure the correct classification of digital documents to protect both customer data and sensitive business information or strategies

On our strategy to thwart Ransomware attacks, which has increased globally lately, several simulations and campaigns were conducted to ensure our processes, especially our Incident Response in handling such situations are intact and effective. In the cloud setup for example, we continuously assess potential security gaps and introduced measures that prevent common threats such as Cloud Distributed Denial of Service (DDOS) and Advanced Persistent Threats.

With several activities and security controls deployed thus far, the Governance team within Cybersecurity Management is also looking rigorously at the effectiveness and compliance of all the systems deployed either in the cloud or on-premise to ensure we have a secured and safe environment now and in the near future.

Empowering Digitalisation

In supporting the Maxis' digitalisation initiatives where systems are increasingly being hosted on the cloud, the Cybersecurity team requires all applications to go through the compliance requirement of ensuring good hygiene. We are adopting the DevSecOps approach that automates the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery.

In line with this approach, a few security processes in the area of testing were introduced where applications are scanned to detect code-related vulnerabilities as part of the Static Application Security Testing (SAST). Any vulnerabilities found must be remediated before the applications are allowed to move into the production environment. In addition to this, there is also the Software Composition Analysis (SCA) tool that calculates digital signatures for all libraries and detects the vulnerable open-source libraries and manage the open-source elements of their applications. Finally, there is the Dynamic Application Security Testing (DAST) at the last leg of testing that would analyse web applications while in runtime and identify any security vulnerabilities or weaknesses. All these stages of security testing are part of the DevSecOps approach in ensuring our support towards a secured digitalisation and cloud initiatives in Maxis, and align to the Zero Trust and Security by Design strategies.

Industry Collaboration

The Cybersecurity team also participated in a few industry-related activities organised by MCMC and Malaysian Technical Standards Forum Berhad (MTSFB). The initiatives were meant to develop standards in the area of cybersecurity and build the foundation work to get the environment ready to support digitalisation initiatives. We see these initiatives as an important contribution that will benefit society and the security industry.

Priorities in 2022

As the complexity of cyber threats increase and our attack surface continues to expand, our focus moves to risk based prioritisation, cloud security, compliance and technology enhancements. This will be achieved through the adoption of security by design practices, adoption of zero trust strategies and the implementation of best practice security standards that are aimed at protecting our brand, ensuring compliance, embedding security in our DNA, further strengthening cyber resilience and supporting our digital transformation ambitions.

In the short term, we will continue maturing our cybersecurity management and standardising our security operations and practices, amongst many other initiatives that will span over the longer term such as enabling greater automation and the use of predictive analytics and Artificial Intelligence (AI) for security monitoring, detection and incident handling.

On the Data Protection front, we have prepared a roadmap with a number of initiatives including the enhancement of current data protection capabilities by implementing new solutions that would address current gaps to better protect customer personal data and confidential data from potential data breaches.

The ISO certification in Maxis will continue to be re-certified to ensure our security processes are meeting international standards. For example, our Voice and Data Core network infrastructure has been ISO27001 certified since 2012 and we are expanding the scope in 2022 to cover our data centre in the cloud, in line with the Group's digitalisation programmes.