Information Security Architect

About Us

Xinja is building the first, Australian, independent 100% digital bank designed entirely for mobile. We are building a bank with our customers and designed in their interests. Neo banking will disrupt the existing banking model and create a whole new generation of experiences.

Developing the first neobank in the country is an exciting and challenging task. Our ethos is based on a win-win with our customers; if they do well, so do we. We believe it's time Australians had access to the kind of technology that just allows them to get a lot more out of their money, with less angst.

We extend that attitude to our people and our partners. We look after our staff, and trust them with significant responsibility, but support them well. This is a great opportunity to be part of building a great company, and a fabulous brand.

Our 10 golden rules

To be successful at Xinja you are going to need to be happy working with our 10 golden rules

1. No dickheads... however good they may be. No dress code. No power trips because of a hierarchy. Intellect and implementation is all that matters.
2. Everything is in the cloud.
3. We use real time data to evaluate our business and we reward staff on a quarterly basis with an entirely discretionary bonus. No one gets a bonus if our investors aren't making money and our customers aren't happy.
4. We are here to make money, that's why we exist, and we don't screw people over to do it. We don't lie to our clients in person or in marketing. We don't engage in immoral lending, if our grandmother would think it was wrong, then it is. We aim to make lots of money ethically and we are proud of it.
5. No one is entitled to work at Xinja. It a huge honour to represent people's hopes of a new bank and we earn that honour every day.
6. We look after our people bloody well. We stand by them if they are in genuine need.

7. We are truthful and direct with each other. Everyone says what they think in a robust, challenging, edgy environment. That means we won't be the right place for everyone to work, and that's ok.
8. We only hire people better than us. We never, ever settle because we need a body. We do psychometric testing to get the best people, every time.
9. About half our team, executive and board will be female, if they aren't we aren't recruiting the best people. We actively seek all types of diversity combined with brilliance.
10. If you discriminate against someone because of who they love/sleep with, you're a dickhead...please see rule 1.

The Role

The Information Security Architect plays a strategically critical role in defining and assessing Xinja's security strategy, architecture and practices. The security architect will be required to effectively translate business objectives and risk management strategies.

Responsibilities

The Information Security Architect will:

- Develop and maintain a security architecture process that enables the enterprise to develop and implement security solutions and capabilities that are clearly aligned with business, technology and threat drivers.
- Develop security strategy plans and roadmaps based on sound enterprise architecture practices.
- Develop and maintain security architecture artefacts (models, templates, standards and procedures) that can be used to leverage security capabilities in projects and operations.
- Track developments and changes in the digital business and threat environments to ensure that these are adequately addressed in security strategy plans and architecture artefacts.
- Participate in technology projects to provide security planning advice.
- Determine baseline security configuration standards for operating systems (e.g., operating system hardening), network segmentation, and identity and access management (IAM).
- Develop standards and practices for data encryption and tokenisation within the organization based on the organization's data classification criteria.
- Conduct threat modelling of services and applications that tie to the risk and data associated with the service or application.

- Conduct security assessments of internal systems, applications and IT infrastructure as part of the overall risk management practice of the organization.
- Provide guidance to the Security Operations team in conducting vulnerability assessments and other security reviews of systems, and prioritize remediation based on the risk profile of the asset and guidance from the CISO or other executive management.
- Coordinate with DevOps teams to advocate secure coding practices and escalate concerns related to poor coding practices to the CISO.
- Coordinate with the privacy officer to document data flows of sensitive information within the organization (e.g., PII or ePHI) and recommend controls to ensure this data is adequately secured (e.g., encryption, tokenization, etc.).
- Validate IT infrastructure and other reference architectures for security best practices, and recommend changes to enhance security and reduce risk where applicable.
- Validate security configurations and access to security infrastructure tools, including firewalls, intrusion prevention systems (IPSs), web application firewalls (WAFs), anti-malware/endpoint protection systems, DLP and AWS infrastructure components etc.
- Review network segmentation to ensure least privilege for network access.
- Liaise with the vendor management team to conduct security assessments of existing and prospective vendors, especially those with which the organization shares intellectual property, PII, ePHI, regulated or other protected data.
- Evaluate the statements of work from these providers to ensure that adequate security protections are in place. Assess the providers' SSAE 16 SOC 1 and SOC 2 audit reports (or alternative sources) for security-related deficiencies and required "user controls," and report any findings to the CISO and vendor management teams.
- Liaise with the internal audit (IA) team to review and evaluate the design and operational effectiveness of security-related controls.
- Support the testing and validation of internal security controls as directed by the CISO or IA team.
- Review security technologies, tools and services, and make recommendations to the broader security team for their use based on security, financial and operational metrics.
- Conduct incident response exercises with colleagues throughout the organization and incorporate lessons-learned into existing security architectures and practices.
- Liaise with the business continuity management team to validate security practices for both disaster recovery planning (DRP) and business continuity management (BCM) testing and operations when a failover occurs.
- Key relationships include; Application and information owners, CISO, CIO, Chief risk officer (CRO), Chief privacy officer (CPO), Information security manager (ISM), Enterprise architect and Project management office.
- Regularly report relevant cyber security metrics into the required stakeholder(s).

Requirements and Qualifications

- Bachelor's or master's degree in computer science, information systems, cybersecurity or a related field.
- Professional security management certification is desirable, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) or other similar credentials.
- Experience in using architecture methodologies such as SABSA, Zachman and TOGAF
- Direct, hands-on experience managing security infrastructure such as firewalls, IPSs, WAFs, endpoint protection, SIEM and log management technology
- Exposure to Static Application Security Testing (SAST) tools.
- Direct, hands-on experience using vulnerability management tools
- Working knowledge of the methodologies to conduct threat-modelling exercises on new applications and services
- Full-stack knowledge of IT infrastructure (e.g., applications, databases, operating systems, Hypervisors, IP Networks, Storage Networks, Backup networks).
- Direct experience designing IAM technologies and services (e.g., Okta, Amazon Web Services' [AWS'] IAM, Azure AD)
- Strong working knowledge of IT service management (e.g., ITIL-related disciplines):
- Experience designing the deployment of applications and infrastructure into public cloud services such as AWS and/or Azure.

Business-related skills:

- Strategic planning skills — The security architect must interpret business, technology and threat drivers, and develop practical security roadmaps to deal with these drivers.
- Communication skills — Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate information security and risk-related concepts to technical and nontechnical audiences at various hierarchical levels.
- Financial analysis —evaluate the financial costs of recommended technologies. Specifically, the security architect will need to quantify purchasing and licensing options, estimate labor costs for a given service or technology, and estimate the total cost of operation or the ROI, or payback period for services or technologies that are replacing existing capabilities.

- Project management skills — financial/budget management, scheduling and resource management.

Key behaviours and competencies:

- High level of personal integrity, as well as the ability to professionally handle confidential matters and show an appropriate level of judgment and maturity.
- High degree of initiative, dependability and ability to work with little supervision while being resilient to change.
- Must be a critical thinker, with strong problem-solving skills, always open to learning and developing on personal growth.