Appendix A: Security Maturity Model

	Minimal to comply	Security controls focused	Threat focused to protect	Agility to grow the business
Digital transformation strategy	Digital transformation initiated at function or line of business level, but uncoordinated with enterprise strategy.	Digital transformation initiatives are tied to enterprise strategy but with short-term focus and tactical solutions.	Integrated, continuous enterprise wide digital transformation innovation in place.	Digital initiatives transforms market and customers by creating new business models and services.
Security business objectives Objectives, leadership, cross-function, culture	Business-level planning focused on meeting external or internal compliance and legal requirements. Cybersecurity planning is reactive and highly tactical.	Cybersecurity planning focused on protecting core business assets and processes. Security is treated as a silo function and perceived as a barrier to digital transformation initiatives.	Cybersecurity planning aligned with digital transformation objectives to prioritize cybersecurity as a business concern, leveraging accreditation to improve external confidence.	Continuously review and optimizes digital transformation initiatives in alignment with risk assessment. Processes in place for business to govern execution of security throughout business lifecycle.
Digital risk management Strategy, management, governance, compliance, data protection	Risk management seen as a legal issue for meeting external or internal compliance requirements.	Risk management framework employed to baseline risk estimation and guide the application of appropriate security controls. Risk is treated in technical terms.	Economic and external assurance framework and organizational processes applied to continuous risk management. IT risk is seen in context of business risk and a part of strategic requirements.	Data-driven performance metrics in risk estimation and cost-benefit model for use across the business and programs. Risk treated in business opportunity terms.
Security program Policy, architecture, operations, monitoring, controls, SDLC, metrics	Cybersecurity handled by IT, focusing on basic authentication, perimeter-based security, and standard threat protection mechanisms.	Cybersecurity program build around protection of users, data, and applications through application of essential security controls.	Cybersecurity program aligned with risk strategy and employs capabilities to continuously monitor for and respond to threats.	Cybersecurity program implements processes and technical architecture across enterprise. Cybersecurity capabilities enable business processes.
Digital platform Virtualization, cloud, network, mobile, IoT	Basic cybersecurity and asset management solutions for digital platforms to conform with external and internal compliance requirements.	Distinct cybersecurity controls across applied across physical, virtual, internal, and external digital platform environments.	Cybersecurity controls augmented for threat monitoring and response across digital platforms and employ risk model for external services.	Integrated, automated security controls across digital platforms based on a distributed security model that focuses on securing users, data, and applications.

Note: SDLC is systems development life cycle.

Sources: International Data Corporation; A.T. Kearney analysis