RSA

RSA RISK FRAMEWORK FOR MANAGEMENT OF THE DYNAMIC WORKFORCE

HELPS ORGANIZATIONS ASSUME CONTROL OF RISK FROM THE DYNAMIC, GLOBAL WORKFORCE

As successful companies expand into new markets and increase their presence across their sector and the globe, their success breeds new challenges in maintaining the critical security of their most valued assets. The dynamic nature of companies' expanding workforces adds a level of complexity to employee access to key resources. Frictionless access that increases productivity, while maintaining critical country-specific compliance and data standards, becomes onerous as complexities increase. Ensuring access to critical resources through multiple access modalities, while employees work remotely and uniquely across geographies and cultural circumstances, creates challenges that test the capacity of a security department's abilities to ensure identity/access standards are established, corporate and consumer privacy regulations are followed, data residency restrictions are ensured, and systems are managed and maintained in support of multiple endpoints (smartphones, smartwatches, desktops/laptops and tablets) used by the dynamic workforce of today.

GOVERNANCE	IDENTITY	PRIVACY	DATA	SYSTEMS	
OPERATIONAL EXCELLENCE					
Roles and responsibilities defined Training and communications established Policies, processes, procedures, tools defined and integrated	User understanding of identity and access management and policies Employees, devices, and other assets authenticated fully Ongoing monitoring of unauthorized access	Accountability for privacy established, enforcement of classification standards, user standards for data handling Data residency established at local, national, international level	Roles and responsibilities established for executive and data owners, centralized management of data, presence of threat and vulnerability analysis across systems and infrastructure	Roles and responsibilities for management of anomalous activity, monitoring and management for all endpoints, existence of behavioral analytics for usage patterns Comprehensive policies and standards for usage	TOP 2
FOUNDATIONAL EFFECTIVENESS					ABOVE avg.
Governance processes established based on policy, processes and tools not entirely integrated	Some standards for identity and access, authentication across some assets	Some standards for privacy and handling of information established	Existence of data management but may differ across regions, some threat and vulnerability analysis	Snapshot monitoring of anomalous activity, existence of management processes, some standards and policies for endpoint usage	BELOW avg.
MINIMAL EFFECTIVENESS					
Basic processes and tools but not integrated, training ad hoc	Some roles defined for identity management, basic processes and tools	Privacy roles and responsibilities established but not well known, some standards for privacy	Some management of data but not standardized, little threat or vulnerability management	Ad hoc policies for endpoint usage, some monitoring	BOTTOM 2

The RSA Risk Framework for Dynamic Workforce helps organizations assess and improve their maturity across the following management domains: Governance, Identity, Privacy, Data and Systems. For each of these areas, RSA will apply its proprietary Cyber Maturity Quantification Tool that produces a profile of an enterprise's maturity in Dynamic Workforce Management, as well as an aspirational profile (long-term goal of third-party governance maturity status across the risk-management lifecycle). The comparison between current and aspirational states produces a gap analysis that can help organizations prioritize areas for improvement.

As with all RSA Risk Maturity Frameworks, the Cyber Risk Practice helps enterprises to assess their current readiness for managing risk with an approach that crosses an organization's traditional functional boundaries, using a maturity model that assumes the perspective of the CEO, COO, CCO, CIO and other senior executives.

The RSA Cyber Dynamic Workforce Maturity Assessment provides the following:

- Interviews and documentation with key business stakeholders to deeply understand business goals, objectives, risk tolerance and existing risk posture
- Administration of the RSA proprietary Cyber Maturity Quantification Tool to baseline risk maturity across the enterprise's usage of multiple endpoints
- Development of a gap analysis and roadmap that can be utilized to close existing gaps and move to a desired level of cyber risk-management maturity

ABOUT RSA GLOBAL SERVICES

The RSA Global Services team of 650 cybersecurity business advisory and technical consultants operates in more than 100 countries, and earned the "Strong Performer" rating in the Forrester Wave™ for Digital Forensics and Incident Response Service Providers.[1] With over thousands of engagements, RSA Global Services has helped secure many types of organizations, often designing and implementing comprehensive risk and security management programs.

RSA Global Services combines deep business advisory and security skills and broad risk-management knowledge to help the organization to assess and improve its dynamic workforce maturity status. Within the RSA Risk and Cybersecurity Practice, three groups provide critical security services:

- RSA Risk and Cybersecurity Advisory Practice (RCAP) delivers business-driven cybersecurity services focused on core business analysis, business impact assessment and cyber risk maturity assessment in the areas of cyber incident management, third-party management, dynamic workforce management and multi-cloud management.
- RSA Advanced Cyber Defense (ACD) delivers services to assess breach readiness, security operations center (SOC) or cyber incident response team (CIRT) assessment and design, incident response planning and testing, and "Expert On-Demand" services.
- RSA Incident Response (IR) helps customers design, manage and perform incident response functions via both proactive and reactive services. Available on a retainer or ad hoc basis, RSA IR extends the organization's security skills to deal with security incidents of all types and severities.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection, and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. For more information, visit rsa.com.

[1] The Forrester Wave™: Digital Forensics and Incident Response Service Providers, Q3 2017