RSA Risk Framework for Dynamic Workforce Risk

Managing risk in a complex & changing work environment

Introduction

Digital Transformation is a journey underway in organizations across the globe. Defined as an organization’s rapid adoption of technology and increased integration of business processes, Digital Transformation creates opportunities to gain strategic efficiencies and capabilities by providing a technology model that improves continuously and is guided by data. The outcome is smart, actionable insights, and the ability to act on those insights faster than the competition, which enables the delivery of better, more innovative products and services.

One important element of Digital Transformation is the shifting nature of the workforce. Organizations gain huge benefits from the combinations and options available in staffing, including remote and mobile workers, multigenerational teams, and traditional, contracted and gig economy workers. Digital technology is a critical enabler for this agility and efficiency, supporting the communication and collaboration capabilities that drive the modern enterprise.

However, a dynamic workforce creates challenges that span the organization because every functional area is experiencing its impacts. For digital technology in particular, it becomes more difficult to secure a dynamic workforce because you substantially grow the complexity of important activities ranging from authentication and access control to data privacy to cyber incident response. These complexities in turn increase the digital risk, and consequently the business risk, that a dynamic workforce brings.

For example, cloud solutions can introduce blind spots in an organization’s threat-monitoring program. Virtualized and containerized applications can be provisioned outside of normal IT processes, often by non-IT personnel in line-of-business roles. Different clouds and applications rely on different identity and access systems and may be incompatible with enterprise systems and standards. And many of the same risks of other third-party relationships apply as well: privacy, resiliency, performance and security (both physical and technical) must be considered,
Thus, the benefits received from dynamic workforce computing must be balanced against the risks assumed:

<table>
<thead>
<tr>
<th>BENEFITS</th>
<th>RISKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexibility—Blend work modalities</td>
<td>Identity Lifecycle—Multiplies number of</td>
</tr>
<tr>
<td>Cost—Optimize staffing with contract/</td>
<td>identities to create and manage</td>
</tr>
<tr>
<td>gig workers</td>
<td>Access Control—Complex to design</td>
</tr>
<tr>
<td>Diversity—Capture ideas from diverse</td>
<td>and maintain access across locations and</td>
</tr>
<tr>
<td>workforce</td>
<td>devices</td>
</tr>
<tr>
<td>Globalization—Employ workers</td>
<td>Threat Detection &amp; Response—Protecting IT for</td>
</tr>
<tr>
<td>wherever they reside</td>
<td>mobile workers</td>
</tr>
<tr>
<td>Mobility—Empower people to work</td>
<td>Data Privacy—Personal information</td>
</tr>
<tr>
<td>without constraints of place and</td>
<td>and company IP are available from anywhere</td>
</tr>
<tr>
<td>time</td>
<td></td>
</tr>
</tbody>
</table>

Like all risks, dynamic workforce risk is not binary—you can’t eliminate it completely, or at least not without forsaking all the benefits that dynamic workforce computing delivers. The task is then to identify, mitigate and continuously manage dynamic workforce risks, and continuously improve and maintain the maturity of your dynamic workforce risk program.

To address this need, RSA has created the RSA Risk Framework for Dynamic Workforce Risk. Like other RSA Risk Frameworks, it’s based on a maturity model that helps customers fully assess and effectively improve their capabilities. It provides a lens to analyze the full range of dynamic workforce risk requirements, using detailed questions and applying expert analysis.

RSA Risk Frameworks are based on established and understood industry risk frameworks, including ISO 31000 and NIST SP 800-161, as well as cybersecurity frameworks, including NIST Cybersecurity Framework (CSF) 1.1 and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide (CSRC). However, the RSA Dynamic Workforce Risk Framework goes beyond the broad standards to leverage RSA’s deep experience (including industry-specific experience) in helping customers address and manage dynamic workforce-related risks of all types.

Figure 1: RSA Dynamic Workforce Risk Framework (simplified)
Dynamic Workforce Risk challenges

The dynamic workforce brings fundamental change to both operational and technology domains in an organization. Culturally, the workforce is an evolving mix of generations and types of workers, each with their own traits, preferences and work styles. Baby boomers work side by side with Gen Xers and millennials. Each group carries expectations about things like privacy and flexibility, while exhibiting skills with different technologies. For example, traditional workers value face-to-face interactions and email, while the youngest workers prefer to operate via "consumerized" applications like videoconferencing and short messages. This increases the modalities and devices that identity, security and risk functions must manage.

Changes in the mix of workers also drive complexity. Traditional full-time employment is being extended and in some cases replaced by contingent (contract) personnel and “gig economy” workers—people who work for different organizations, at the same time or sequentially, and deliver great flexibility in executing dynamic workloads. However, this can increase difficulty and risk in areas such as authentication or data privacy.

Digital Transformation initiatives also increase complexity and risk. “Bring-your-own-device” (BYOD) strategies increase the variety of devices to support, at the same time offering less control than traditional corporate-managed devices. SaaS applications, while valuable for their ability to empower collaboration across distances and time, introduce blind spots for your cybersecurity program, while adding complexity to identity and access management.

In fact, bad outcomes from dynamic workforce risks are in the headlines daily. In 2013, Edward Snowden, a contractor working at the United States National Security Agency (NSA), revealed thousands of classified documents stolen using NSA-issued credentials. And compromised credentials, often for cloud applications, continue to be a preferred technique for malicious actors ranging from state-sponsored hackers to cybercriminals.

Simply put, as businesses leverage the benefits of an increasingly dynamic workforce, the risks from these strategies also increase. The number, complexity and velocity of these risks make it difficult to track and respond effectively. Furthermore, the oversight of dynamic workforce elements becomes increasingly important to ensure that the quality of products and services delivered continues to meet required standards.

There are three primary drivers of risk, which RSA calls the “3 M’s”: Modernization (Digital Transformation), Mandates (such as GDPR and other privacy laws) and Malice (skilled and well-resourced attackers). Dynamic workforce risk is impacted by all three.

With so many relationships to track, the complexity of dynamic workforce governance can be difficult to understand and manage. Many organizations struggle to maintain the staff or resources to cope with this increased complexity.

Often, dynamic workforce responsibility is spread across different teams within the organization. Dynamic workforce risks are not identified, assessed, treated and monitored consistently across all lines of business. Each team talks about risk using different language with different measurements, controls and reporting. As a result, it becomes difficult to find a single source of "truth" for dynamic workforce risk and performance. Without a consistent enterprise view of dynamic workforce risks, the executive team does not have a clear enough picture of risk to make well-informed business decisions.

The RSA Risk Framework for Dynamic Workforce Risk

The RSA Risk Framework for Dynamic Workforce Risk is a professional services offering from the RSA Risk & Cybersecurity Advisory Practice (RCAP). Like all RSA Risk Frameworks, this services engagement delivers a business-centric model of consultancy that addresses a specific, major problem facing boards of directors today, including cyber incident risk and third-party risk, as well as risks from the dynamic workforce and multi-cloud environments.

RSA Advisors bring the tools and experience to help organizations assess their current readiness for managing a risk, and to implement a customized strategy for rapid and continual improvement.

Utilizing the RSA Risk Framework for Dynamic Workforce Risk, RSA Advisors help organizations advance programs and processes to clearly identify, effectively mitigate and continuously manage dynamic workforce risk. This process targets the difficult but critical task of assessing and managing the risks associated with the full range of dynamic workforce elements.

These risks grow commensurately with the Digital Transformation and globalization that drives an increasingly interconnected world. Even the best-run organizations face business impacts arising from dynamic workforce failures, including regulatory compliance violations, data breaches, fraud, business interruption and reputational damage.

As with all RSA Risk Frameworks, the Dynamic Workforce Risk Practice helps assess a company’s current readiness for managing this risk, with an approach that
crosses an organization’s traditional functional boundaries, using a maturity model that supports the perspective of the CEO and board members. The RSA Dynamic Workforce Risk Assessment provides the following:

- Conduct of interviews with key business stakeholders to deeply understand the business’s goals and objectives relating to dynamic workforce deployments
- Gap Analysis between current state program posture and desired dynamic workforce risk program posture, including comparison to industry best practices
- Identification of types of risks to mitigate and continuously manage, as well as processes to track dynamic workforce controls, certifications and risk-management processes
- Administration of the RSA proprietary Dynamic Workforce Risk Management Program Quantification Model to baseline current risks arising from potential outcomes due to failures of dynamic workforce suppliers
- Evaluation of strengths and weaknesses of dynamic workforce risk-management processes as related to customer industry, business goals and risk tolerance
- Development of a roadmap that can be utilized to move to a desired level of dynamic workforce risk-management program maturity with time to value as a driver in the roadmap
- Readout of results to stakeholders

At the conclusion of RSA Dynamic Workforce Risk advisory engagement, clients should have a clear understanding of risk-management maturity across the relevant categories and demonstrate the ability to identify, mitigate and manage risk at the highest level of effectiveness. Additionally, clients should have in place a strategic roadmap to both improve maturity in key areas and sustain capabilities already in place, even in the face of evolving or increasing risks.

In many organizations, RSA can apply its Dynamic Workforce Risk Framework and begin making demonstrable impact in 4 to 12 weeks. A typical Assessment and Gap Analysis with interviews and presentation of final deliverable requires a team of two to three RSA Professional Services Advisors, and may vary depending on the complexity and size of the environment as well as the amount of interviews/surveys required. The model presumes 10 to 12 interviews plus an online assessment component.

**How it works**

Different representations of the RSA Risk Framework for Dynamic Workforce Risk highlight different aspects of the model. Figure 2 shows the leading indicators of maturity across four main areas of dynamic workforce risk: Ecosystem, Governance, Identity and Compliance. A detailed scoring system behind these categories and ratings allows organizations to assess maturity for every area and baseline an initial score based on the company’s risk tolerance. This tally can then be used as a reference point from which to prioritize investments, adjust strategy and take other actions that advance dynamic workforce risk management.
• **Governance**—The ongoing process of integrating policies, processes, procedures and tools

• **Identity**—The management of identity and access (e.g., single-factor, multi-factor, identification) across all users and modalities

• **Privacy**—The definition and enforcement of classification standards and data residency requirements

• **Data**—The establishment of roles and responsibilities for data ownership and the centralized application of vulnerability and threat analysis processes

• **Systems**—The confirmation of roles and responsibilities for systems that monitor and manage endpoints and apply behavior analytics to detect anomalous usage patterns

Organizations at the most mature level achieve Operational Excellence optimizing dynamic workforce security and minimizing business risk. They do this by coordinating and integrating IT and business risk functions across the entire dynamic workforce risk domain. Other characteristics of maturity include automation of key processes, advanced analysis capabilities and continuous improvement of elements such as the incident-management lifecycle.

The RSA Dynamic Workforce Risk Framework engagement assesses the types of capabilities that exist at each level of the model. In many cases, maturity progresses from manual processes to siloed digital processes to highly automated, integrated processes. Organizations at intermediate levels of maturity tend to rely on spreadsheets or online tools, coupled with nonintegrated point solutions, and open source or free tools. The problem with this approach is that it rarely provides a holistic view of the risk environment and typically yields a slow and incomplete response. Lacking the insight, visibility and playbooks capable within today’s dynamic workforce risk programs puts organizations at a strategic disadvantage, making it more likely that a risk will turn into a problem, and that the problem will have a substantial negative impact.
How RSA Solutions map to the RSA Risk Framework for Dynamic Workforce Risk

RSA provides a rich portfolio of products and professional services that enable organizations to unify disparate IT security and business risk functions, advance their maturity model and reduce risk. As shown in Figure 4, RSA Risk and Cybersecurity Practices and RSA product suites address every area of mature dynamic workforce risk management, across Governance, Identity, Privacy, Data and Systems.

RSA Risk & Cybersecurity Advisory Practice (RCAP) is the umbrella practice for the critical components of Digital Risk Management, and helps customers implement solutions that protect against risk, ensure compliance and accelerate business objectives. Within RCAP are:

- **RSA risk management practice**, which helps organizations advance their capability for continuous risk improvement and helps ensure that risk programs are well-coordinated and aligned with identified business tolerance levels when it comes to reducing dynamic workforce risk.

- **RSA Advanced Cyber Defense (ACD) and RSA Incident Response (IR)**, which help organizations design and deploy effective cyber-defense systems and respond to attacks, respectively. Industry expertise has been earned through thousands of proactive and reactive engagements across the globe.

- **RSA identity & assurance practice**, which helps organizations resolve the two big challenges related to dynamic workforce access to systems. Authentication is the process of continuously validating the identity of a person or resource, while identity governance ensures that access is restricted only to what should be available to any specific identity.
RSA Product Solutions are industry-leading software tools that empower organizations to address the critical domains of Integrated Risk Management, Threat Detection and Response, and Identity and Access Management. These include:

- **RSA Archer® Suite**: which delivers Integrated Risk Management (IRM) to increase visibility and insight into true business risks and empower organizations to make better decisions throughout the risk-management lifecycle.

- **RSA NetWitness® Platform**: which is an advanced security information and event management (SIEM) and threat defense solution that aligns business risk context to security risks so that security teams can rapidly detect and understand the full scope of a compromise and its associated risks.

- **RSA SecurID® Suite**: which facilitates business by allowing legitimate users to quickly and easily identify themselves, while mitigating the risk of unauthorized users gaining access to the network and other resources.

**Conclusion**

The RSA Risk Framework for Dynamic Workforce Risk provides a maturity model for developing a mature, business-driven strategy that is informed by—and accommodates—both IT and business risk functions across the dynamic workforce risk domain. Organizations can apply products and solutions from the RSA portfolio to fully operationalize the model at the highest levels of maturity. In doing so, they can reduce risks to revenue/mission, reputation and compliance while safely pursuing opportunities that allow them to thrive.

To find out more about using the Risk Frameworks to assess and optimize your organization’s risk-management strategy, please visit [rsa.com/risk-frameworks](http://rsa.com/risk-frameworks).

**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](http://rsa.com).