Achieving Identity and Access Assurance Requires a Holistic Approach

Identity and access management systems are just one element of what's needed to counter identity-related cyberattacks. Solutions must also leverage threat intelligence and be aware of business context.

Given the volume and diversity of cyberattacks today, it can be easy to lose sight of one characteristic that many share: The vast majority of successful attacks occur because users' identities and credentials have been compromised in some way. In its annual "Data Breach Investigations Report," Verizon found that more than 80% of confirmed breaches occurred via account takeovers and use of stolen passwords. As the attack surface expands with digital transformation, the journey to the cloud, and mobility, digital risk management and specifically access management becomes even more of a challenge.

This reality drives home the critical importance of verifying that people—as well as applications and devices—are who they claim to be before granting them access to sensitive systems and data. Doing so is the primary role of identity and access management (IAM) systems.

But providing a more complete and effective solution to reduce identity aspects of digital risk and drive Identity and Access Assurance (IAA), which is the confidence that users are who they claim to be and that they have the right level of access, requires more than just a discrete IAM component. What's needed is a complete approach that encompasses not just IAM functionality but also real-time threat intelligence; leveraging threat intelligence will provide visibility into risk that is beyond the context of identity. Also required: a full understanding of business context, especially the ramifications of successful cyberattacks against different digital assets.

Such a comprehensive approach also requires close attention to organizational structures and dynamics. That is, the responsibility for providing IAA can't be pigeonholed in one enterprise department. Identity-based threats and vulnerabilities must be understood and addressed collaboratively across an organization's IT, security, and risk management teams.

A recent survey in which IDG queried 100 decision-makers at organizations with 2,500 or more employees, confirmed the importance of achieving IAA as a high-priority that requires an appropriate security strategy. The respondents all held director-level or higher titles and had responsibilities in one or more relevant areas such as IT, IT security/security operations centers, risk management, and/or compliance/audit.

The survey identified a variety of challenges as well as benefits associated with delivering holistic IAA, and respondents with different roles in IT, security, and risk management groups had some different perspectives regarding the path to IAA. Despite the challenges and differences in opinion, however, virtually every respondent confirmed the strategic importance of taking a well-rounded approach to managing identity aspects of digital risk and delivering IAA. Finding a partner that can provide both the products and professional services required to implement sophisticated solutions to drive IAA is one of the most effective means by which organizations can protect their digital assets and, ultimately, their long-term success and viability.

IAA Threats and Challenges

Although there were many areas of general consensus among those surveyed, as noted, there were some differences in perception, depending on the respondents' organizational roles. Those differences included their assessments of the most-threatening attack vectors and the difficulty of blocking them.

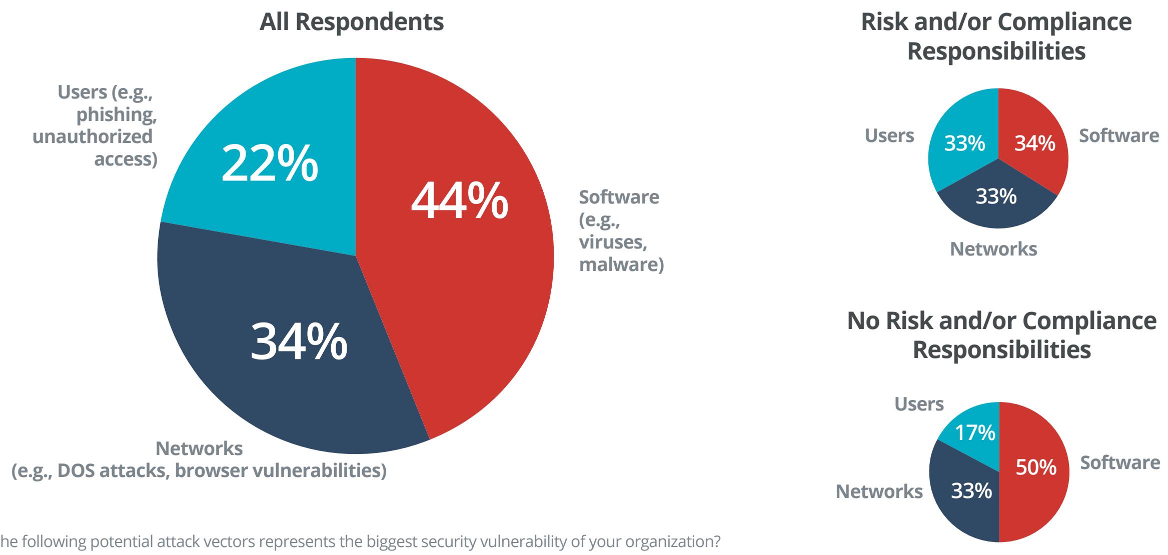
Overall, the largest group of respondents (44%) identified viruses, malware, and other software vectors as the biggest security threat among three broad categories of risk. About one-third (34%) said network and browser vulnerabilities posed the most significant threat, whereas 22% cited user-sourced breaches from phishing or other attacks.

Survey respondents with risk and compliance responsibilities, however, saw the threat danger from each of these three categories as being roughly equivalent. This finding suggests that those most directly charged with assessing and countering risks are more likely to understand the peril associated with user identity compromises.

As for the difficulty of defending against each of these three categories of attacks, the respondents overall saw a rough equivalency of that challenge for all three.

Figure 1. Biggest Security Vulnerabilities, as Seen by Different Corporate Groups

Users are more likely to be perceived as a top security vulnerability among those with risk and/or compliance responsibilities.

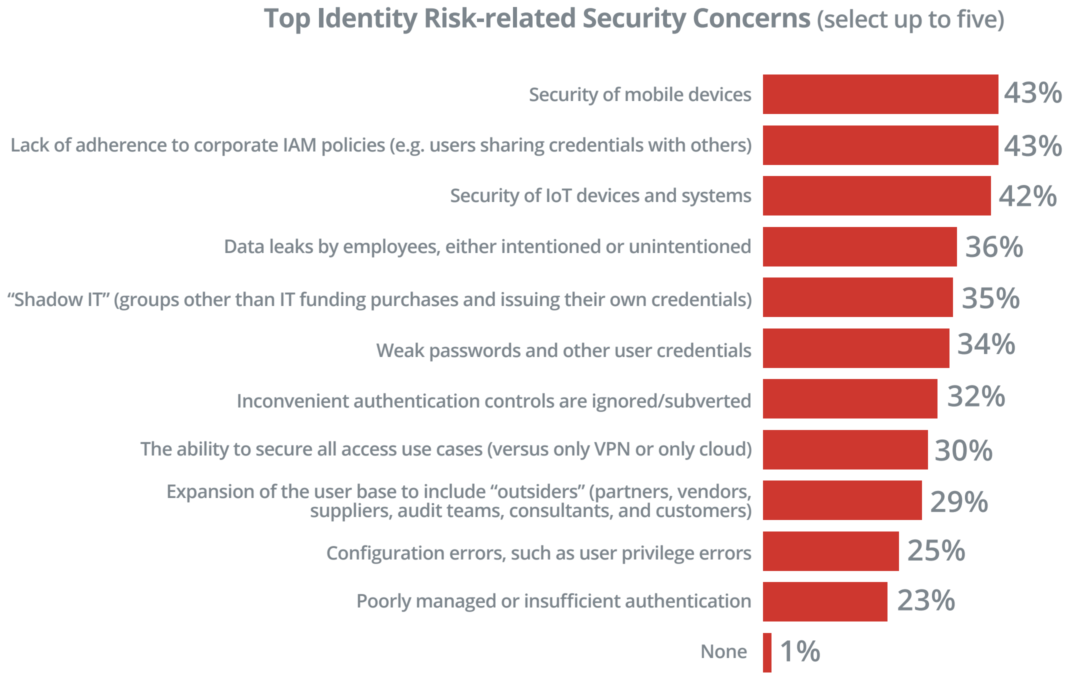


Q: Which of the following potential attack vectors represents the biggest security vulnerability of your organization?

When asked about their specific concerns related to identity-based risks, the 100 decision-makers cited nearly a dozen issues, as shown in Figure 2. Failure to adhere to corporate identity access management policies was tied with the security of mobile devices as the top risk-related security concern.

Figure 2. Top Identity Risk-related Security Concerns

Mobility device security, IAM policy enforcement, and IoT security are among the top identity risk-related security concerns at enterprise organizations.



Lack of adherence to corporate IAM policies is particularly challenging for smaller enterprises (2,500–4,999 employees) (53% vs. 33% among all others).

Source: IDG

Not surprisingly, organizations face a variety of obstacles when it comes to deploying digital risk management solutions. The top two obstacles—each cited by more than half of the respondents—were cost and budget constraints and user adoption challenges. Close behind was the difficulty of integrating risk management solutions into existing environments.

Multifaceted IAA Seen as a Critical Component to Digital Risk Management

The findings of the IDG survey indicate that there is a broad understanding of the strategic importance of achieving IAA. The survey asked respondents to rank the importance of user IAA on a 10-point scale, ranging from its just being a basic tactical need at the low end of the scale to being an integral part of an encompassing approach to identity aspects of digital risk management at the upper end. More than half (57%) placed IAA's importance in the highly strategic 9–10 range, with the average rating from all 100 respondents hitting 8.3 on the scale.

Furthermore, the importance of IAA has grown notably over the past two years, as shown in Figure 3, with nearly half (49%) of the respondents saying IAA's importance increased significantly during this period.

This growing importance was reflected in the ubiquity of deployments of solutions to drive IAA. At the time of the survey, 96% of the enterprises had one or more identity-related solutions already in place to drive IAA. Of the 4% that didn't, all were currently evaluating such solutions.

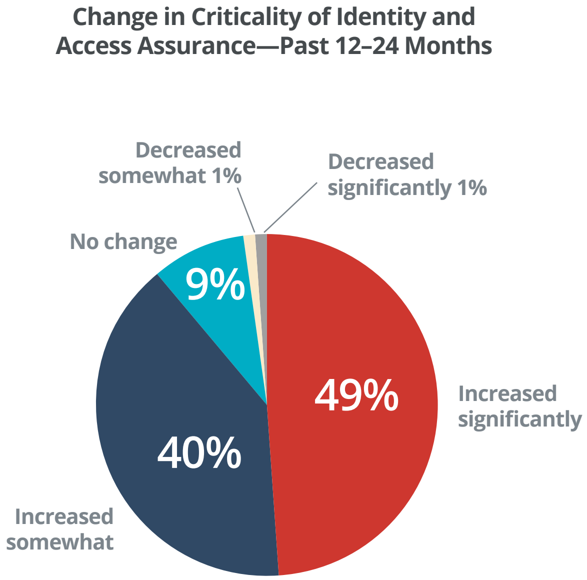
But what does a "holistic" approach to to drive IAA as part of an overall digital risk management strategy mean? The survey characterized such an approach as consisting of three primary elements:

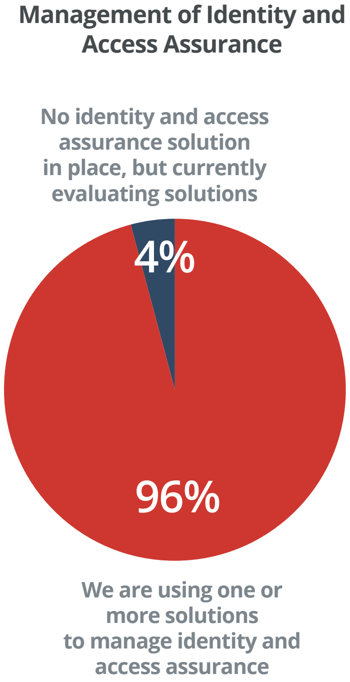
- **Identity insights**—the confidence that users are who they claim to be at the time of access (based on user profile and typical behavior)
- **Threat intelligence**—providing insight into the security status of devices, networks, and cloud environments connected to each user
- **Business context**—the impact on the business of rogue access to an application or an asset

Defined in that way, holistic digital risk management driving IAA was deemed critically important by 18% of the respondents, very important by 70%, and somewhat important by 11%. The reasons for this importance were reflected in a long list of perceived benefits that the respondents said such a comprehensive approach could provide (see Figure 4). On average, each respondent identified more than four of the benefits listed.

Figure 3. Growing Importance of IAA

Almost 9 in 10 respondents report that identity and access assurance has increased in importance versus other security areas. Most organizations have one or more solutions in place to address it.

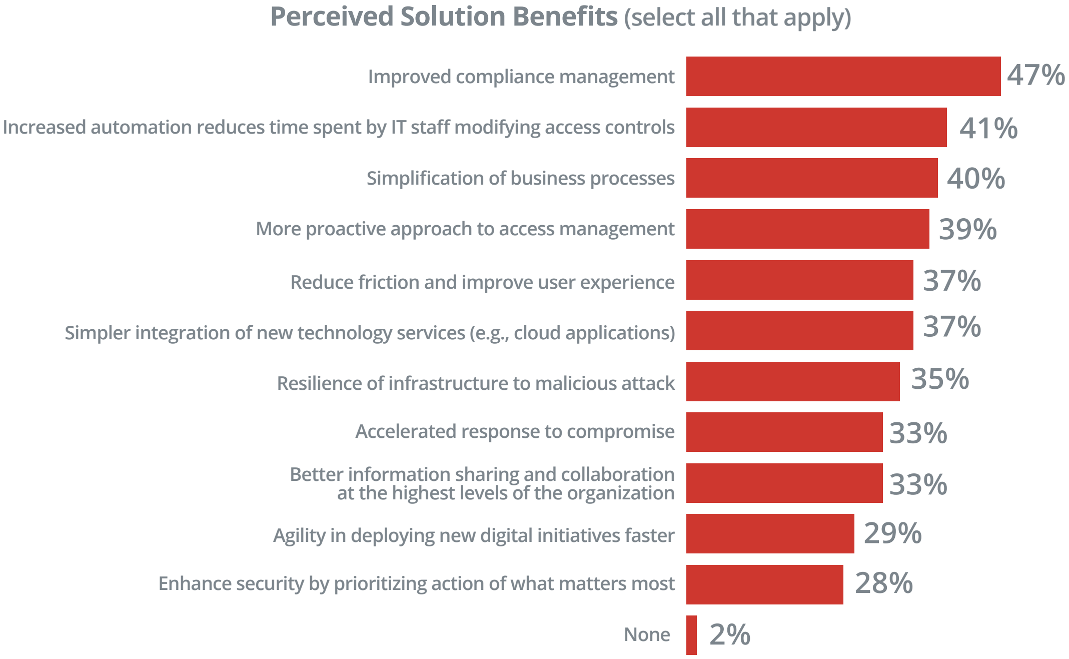




Source: IDG

Figure 4. Perceived Benefits of a Holistic Approach to IAA to Reduce Identity-related Digital Risk

Respondents associate multiple benefits (4 or more, on average) with a holistic solution that brings together identity insights, threat intelligence, and business context to provide secure access to all users, across all applications.



Source: IDG

Given that virtually all of the respondents consider a holistic approach to IAA and risk management important, often critically so, it's not surprising that more than 90% also claimed to have multifaceted strategies that include identity insights, threat intelligence, and business context elements.

When evaluating solutions for comprehensively managing the identity aspects of digital risk, the survey respondents gave essentially equal weight to three criteria. One of the three was finding a solution that could be applied pervasively across all use cases. A second was the need to take an intelligent, risk-based approach that uses analytics to prioritize actions based on the value and sensitivity of the digital assets involved. The third criterion is to deploy solutions that emphasize convenience and drive user adoption. Having these three criteria fulfilled will provide a holistic approach to IAA.

Collaborating to Share IAA Responsibility

No identity solution, holistic or not, can be successful at managing digital risk without corporate-wide buy-in that backs it up. Most importantly, this backing must involve the IT department, the security operations center, and the organization's compliance and risk management teams. (Individual business units and their employees, of course, must do their part as well.)

The IDG survey respondents broadly claimed to have a high level of cross-team collaboration when it came to managing digital risk. As was the case with perceptions of the nature of the digital risk faced, though, viewpoints about organizational cooperation varied with the respondents' corporate role.

Overall, nearly 80% said there is either a very high (39%) or high (40%) level of cooperation and collaboration across multiple functions in their organizations when it came to managing digital risk. Once again, however, those respondents with frontline risk and compliance responsibilities were more circumspect in their assessments of this unity.

Only 29% of the risk and compliance managers rated cross-function collaboration as very high, compared to 57% of those with no risk and/or compliance responsibilities.

A clue to this disparity can be found in the responses to a related survey question. The respondents were asked to identify the respective involvement of different teams when it came to evaluating identity-related threats and setting identity management priorities. All told, 77% of the respondents said the IT department was involved in these activities “to a great extent.”

By comparison, just 46% said risk management and governance teams were involved to a great extent in evaluating identity-related threats and in setting management priorities. And only 38% said compliance and audit teams were deemed to be that involved. In order to combine identity insights, threat intelligence, and business context, stronger collaboration is required. This requires teams to break down the silos and work together to share the responsibility and share information to effectively manage identity aspects of digital risk and drive IAA.

RSA Pioneers a Holistic Approach to IAA

RSA, a pioneer in business-driven cybersecurity solutions, counts 94% of the Fortune 500 among its 30,000 corporate customers worldwide. The company is now driving the industry toward a more comprehensive approach to IAA, by offering a wide range of IAA-focused products and services that provide the pervasive, intelligent, and convenient solutions customers require.

The RSA SecurID® Suite, RSA‘s identity solution, encompasses both access assurance, with RSA® Identity Governance and Lifecycle, and identity assurance, with RSA SecurID® Access, to address the full range of challenges encountered when giving users secure access to digital resources across complex IT environments.

The RSA SecurID Suite provides users with fast and convenient access to resources—be they on-premises systems and data or cloud-based services—from any device, at any time, and from any location.

For IT, security, and risk managers, the suite supports many forms of multifactor authentication, including various mobile-optimized authentication options to support today’s distributed and mobile workforces. As part of its pervasive reach, it also provides wizard-based connectors for rapid onboarding of new applications.

The RSA SecurID Suite provides intelligence, by delivering risk-based authentication, and intelligent access certifications, by leveraging machine-learning algorithms. These algorithms take into account known information, such as a recognized device or a user’s login credentials, as well as risk indicators, such as a login occurring from a new location.

In addition, the RSA SecurID Suite factors in the business context of any access request. That assessment includes the potential impact on the business if rogue access to a sensitive application or data occurs, prioritizing actions based on the criticality of access violations.

RSA SecurID Suite also leverages identity context to simplify how access is governed and to streamline access requests and fulfillment, providing a complete and integrated IAA solution that delivers both convenience and security while eliminating “islands of identity.”

Complementing the RSA SecurID Suite are several additional RSA offerings that contribute threat intelligence and business context to the identity risk evaluation, including:

- **RSA NetWitness Platform**—a security information and event system that applies threat intelligence and behavior analytics to detect, prioritize, investigate, and automate the response to threats
- **RSA Archer Suite**—empowers organizations to quickly implement risk management processes based on industry standards and best practices—leading to improved risk management maturity, more informed decision-making, and enhanced business performance
- **RSA Fraud & Risk Intelligence Suite**—an omnichannel solution that combines risk-based authentication and analytics solutions for web, mobile, and e-commerce, as well as fraud intelligence services

RSA also offers consulting services designed to help companies address both the technical and the organizational demands associated with achieving holistic IAA. The RSA Identity Assurance Practice includes the RSA SecurID Access Practice and the RSA Identity Governance and Lifecycle Practice.

» For further information about how RSA solutions can help you achieve your IAA goals, see **RSA.com**

By developing and deploying holistic IAA solutions that take into account identity insights, threat intelligence, and business context, organizations can greatly reduce their vulnerability to identity-based cyberattacks.