Securing Cloud Transformations
About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

ABOUT THE AUTHOR

FERNANDO MONTENEGRO
PRINCIPAL ANALYST, INFORMATION SECURITY

Fernando is a Principal Analyst on the Information Security team, based in Toronto. He has broad experience in security architecture, particularly network security for enterprise environments. He currently focuses on covering vendors and industry events in the endpoint security and cloud security spaces. Prior to joining 451 Research, Fernando worked in pre-sales and delivery roles with vArmour, RSA, SilverTail, Crossbeam and Hewlett-Packard. His areas of interest include security economics (particularly behavior economics), data science and network security. Fernando holds a BSc. in Computer Science and several industry certifications.
Table of Contents

Executive Summary 4

Introduction 5
   Figure 1: Barriers to broader implementation of public cloud services. 6
   Figure 2: Enterprise attitudes toward use of hosted cloud services 7

Cloud Transformation 8
   Figure 3: Factors used to build a business case for cloud investments. 8

Understanding Cloud Adoption Patterns 10
   Figure 4: The state of IT environments 10
   Figure 5: Primary environment for operating workloads today and in two years 11
   Figure 6: IT environments are not just hybrid (on- and off-premises) but also multicloud. 12

Organizational Systems and Culture 13
   Figure 7: DevOps processes are managed by lines of business 14

Understanding the Cloud Security Landscape 15
   Figure 8: Shared-responsibility model of implementing security in cloud deployments 15
   Figure 9: Experience level dictates organizations’ understanding of cloud security responsibilities 16
   Figure 10: Experience dictates adoption rates for key cloud technology controls. 17

Enabling Security Teams 18
   Figure 11: Skill sets inadequately addressed within organizations 19
   Figure 12: Vendor-based security tools used for off-premises cloud architectures and plans to acquire additional security services. 20
   Figure 13: Top ways organizations are addressing security concerns 21

Recommendations for Securing Cloud Transformation 22

Conclusions 24
Executive Summary

As organizations continue to strive for better business outcomes, particularly with the added pressure of the current health crisis, many have turned to cloud-based approaches. To support this shift toward ‘cloud transformation’ initiatives, security teams are being tasked with understanding and securing cloud environments. What can be learned from those organizations already on this journey? What are key trends, concerns and recommendations?

This study includes observations derived from in-depth interviews with executives directly responsible for securing cloud transformations at their organizations coupled with data from 451 Research’s Voice of the Enterprise research program.

Some of the key findings include:

• Cloud adoption patterns are increasingly multicloud.
• Security concerns are top of mind, but there’s increased confidence that they can be addressed.
• Shared responsibilities between providers and customers need to be well understood, and more experienced customers take on the responsibility of properly managing their cloud presence with both provider-offered and third-party components.

Key areas of focus are identity and access management, data security and cloud configuration management. The key recommendations span both strategic and tactical considerations. At a broader level, organizations must view cloud transformation as a long-term company initiative and build the necessary communications channels, capabilities and risk management practices to properly engage with the necessary stakeholders. Cloud security should not be treated as a separate discipline, but teams should be equipped to understand nuances from cloud security and deliver security outcomes while preserving agility. Looking ahead, we expect the drivers that led organizations to move forward with their cloud transformation initiatives to persist because of the need to support new regulations, new markets and new opportunities.
Introduction

After many years of increased adoption by a growing number of organizations, use of cloud-based environments has emerged as a standard way of creating, consuming and delivering IT services for a variety of use cases. This shift has resulted in massive pressure on organizations to adapt practices and thinking to incorporate cloud-centric services, technologies and methodologies. The scope of these changes includes virtually all of IT, from how common services such as internal messaging and communications are consumed to how customer-facing initiatives are designed and implemented.

Throughout this transformation, security has emerged as a top-tier concern. This reflects the increased value of these cloud-enabled systems, as well as the pace of technology change. Many stakeholders are unsure of the impact that the multitude of changes will have on the security of their cloud implementations.

This report presents key trends and recommendations as stakeholders consider what’s next in securing cloud transformation. The report builds on data from 451 Research’s Voice of the Enterprise research program, augmented by in-depth interviews with a select number of enterprises. Taken together, the data and interviews provide a broad view of how cloud transformation is affecting enterprises, including the challenges and their impact on security teams. The report also offers some recommendations for possible courses of action.

We understand there is significant demand for this type of guidance. As evidence of the importance of security, the data in Figure 1 below – derived from surveying senior IT leadership, not just security leaders, at a broad spectrum of companies – shows that information security is a significant barrier to broader adoption of cloud-based infrastructure services.
Figure 1: Barriers to broader implementation of public cloud services
*Source: 451 Research’s Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads & Key Projects 2020*

Q: Which of the following challenges – if any – are the greatest barriers to broader implementation of IaaS/public cloud for production applications at your organization? (Please select all that apply.)
*Base: All Respondents (n=69)*

- Information security concerns: 52%
- Controlling cost (cloud pricing structure or controlling/optimizing spending): 41%
- Vendor lock-in concerns: 32%
- Lack of expertise in management/orchestration of cloud platforms: 30%
- Control of data locality and/or sovereignty: 29%
- Migrating/integrating applications or data: 28%
- Maintaining compliance with industry regulations: 23%
- Difficulty applying existing IT governance to public cloud platforms: 22%
- Platform reliability concerns: 20%
- Loss of operational control: 20%
- Existing investment in owned/leased datacenters: 19%
- Organizational resistance to running workloads off-premises: 16%
- Other (please specify): 3%
- No barriers: 13%

That’s not to say that security challenges are too big an obstacle to be overcome; additional survey results show that senior IT leaders are increasingly confident that the topic can be addressed. As Figure 2 shows, many organizations (40%) now accept that hosted cloud can be used for mission-critical applications. That belief is even more pronounced in those organizations that self-identify as ‘digital transformation leaders’ (52%).
Figure 2: Enterprise attitudes toward use of hosted cloud services
Q: How would you best describe your organization’s policy toward use of hosted cloud computing (hosted private cloud, IaaS or PaaS) today?
Base: All Respondents
- Hosted cloud solutions can be used for any application including high-risk, mission-critical applications
- Hosted cloud solutions are limited to lower risk, non-mission-critical applications
- We don’t have a policy toward hosted cloud computing solutions
- We do not use hosted cloud computing solutions
Cloud Transformation

Organizations have been adopting cloud-based services regularly for several years, including a variety of business applications such as CRM, messaging platforms and back-end systems. At many organizations in North America, the migration from on-premises or hosted Exchange email systems to Microsoft’s Office 365 (or similar offerings from Google and other providers), alongside the adoption of cloud-based file hosting and sharing is often recognized a significant milestone in cloud adoption.

However, for many organizations, ‘cloud transformation’ is much more than adopting cloud-based services or simply moving workloads from traditional datacenters to cloud-based instances. Cloud transformation is often a key component in a broader reassessment not only of how the organization consumes or produces IT services, but of general business practices themselves. In that sense, ‘cloud’ is not simply a location for workloads, but a shift in thinking – a methodology – about how a business leverages new workloads, and how these workloads are designed, implemented and operated.

Underlying these initiatives are a variety of outcomes that organizations are looking for when they undertake cloud transformation. As Figure 3 shows, ‘agility,’ ‘scalability’ and ‘reduced footprint’ feature prominently in desired outcomes.

**Figure 3: Factors used to build a business case for cloud investments**
*Source: 451 Research’s Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads & Key Projects 2020*

*Q: What are the key factors needed to build a business case for IaaS/public cloud investments at your organization? (Please select all that apply.)*

*Base: All Respondents (n=65)*

<table>
<thead>
<tr>
<th>Factor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource scalability based on application/workload demand</td>
<td>46%</td>
</tr>
<tr>
<td>Hardware savings</td>
<td>40%</td>
</tr>
<tr>
<td>Improves efficiency of IT staff</td>
<td>37%</td>
</tr>
<tr>
<td>Faster time to market/agility</td>
<td>37%</td>
</tr>
<tr>
<td>Reduces internally owned/managed datacenter footprint</td>
<td>35%</td>
</tr>
<tr>
<td>Access to advanced capabilities embedded in public cloud platforms</td>
<td>31%</td>
</tr>
<tr>
<td>Improves application performance/availability</td>
<td>28%</td>
</tr>
<tr>
<td>Preference for consumption-based model for IT resources</td>
<td>28%</td>
</tr>
<tr>
<td>Software licensing savings</td>
<td>25%</td>
</tr>
<tr>
<td>Extends geographic reach</td>
<td>12%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>12%</td>
</tr>
</tbody>
</table>
These factors were also mentioned almost verbatim in many of the interviews. “Some of our primary objectives for migrating workloads into the cloud include agility,” said a respondent from a large-scale financial services firm. “Basically, the ability to get modern technologies in production faster. I would say that they are also related to cash preservation, so kind of the subscription-based nature of many cloud services or consumption-based model is preferable.”

Also, for many respondents, the ‘compelling event’ for their cloud transformation activities was triggered by contractual cycles, such as leases for traditional datacenters coming due, or refresh cycles for key applications. In those cases, organizations seek to migrate to the cloud quickly via transitioning their virtualized workloads. Some of the respondents mentioned that it was not uncommon for security teams to be involved in these activities much too late in the process, meaning security was left scrambling to learn how to secure the new environments. Sometimes they were involved too early and not involved enough, meaning that the security design would not reflect the final underlying technical architecture.
Understanding Cloud Adoption Patterns

How do cloud transformations affect the existing IT environment? While the expectation may be that many organizations – particularly smaller businesses – have a significant proportion of their workloads reside ‘in the cloud,’ the reality is that cloud adoption is much more nuanced. Organizations are aiming to create an integrated environment between on-premises and cloud-based resources. This means that not only do the environments need to coexist, but that cloud transformation is a long-term initiative that takes place incrementally. The broad survey data below illustrates this point.

Figure 4: The state of IT environments
Source: 451 Research’s Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads & Key Projects
Q: A hybrid IT environment leverages both on-premises systems and off-premises cloud/hosted resources in an integrated fashion. Which of the following best describes the current state of your organization’s IT environment?
Base: All Respondents (n=462)

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29%</td>
<td>Hybrid IT architecture currently in place</td>
</tr>
<tr>
<td>15%</td>
<td>In the process of implementing hybrid architecture</td>
</tr>
<tr>
<td>15%</td>
<td>Planning to implement hybrid architecture in the future</td>
</tr>
<tr>
<td>15%</td>
<td>No plans to implement hybrid</td>
</tr>
</tbody>
</table>

The individual interviews also confirmed this wholesale – all respondents indicated that their cloud transformation plans include varying degrees of workloads remaining on-premises on either company-owned or hosted datacenters. The reasons for this were, to a large degree, related to a cost-benefit analysis of migrating each workload. Many organizations said they take an opportunistic view of cloud transformation: when they are developing a new application, or an existing application is due for a refresh, they ask the question: ‘Does this belong on the cloud, and in which form factor?’

Still, organizations expect significant shifts in their workloads over the next two years, with segments such as adoption of IaaS gaining significantly at the expense of ‘traditional’ on-premises applications.
Figure 5: Primary environment for operating workloads today and in two years
Source: 451 Research’s Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads & Key Projects 2020
Q: Which of the following best describes the primary environment used to operate your organization’s workloads/applications today and in two years?
Base: All Respondents

<table>
<thead>
<tr>
<th>Environment</th>
<th>Today (n=433)</th>
<th>In Two Years (n=394)</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premises ‘traditional’ resources and infrastructure</td>
<td>17%</td>
<td>46%</td>
</tr>
<tr>
<td>On-premises private cloud IT resources and infrastructure</td>
<td>15%</td>
<td>15%</td>
</tr>
<tr>
<td>Software as a service (SaaS) and hosted applications</td>
<td>14%</td>
<td>27%</td>
</tr>
<tr>
<td>Infrastructure as a service (IaaS)/platform as a service (PaaS)/public cloud</td>
<td>12%</td>
<td>25%</td>
</tr>
<tr>
<td>Hosted private cloud</td>
<td>11%</td>
<td></td>
</tr>
<tr>
<td>Hosted, non-cloud infrastructure</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>None</td>
<td>&lt;1%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Finally, the data points to a poly-cloud scenario (often referred to as multicloud). Both broad surveys and individual interviews indicated wide adoption of up to three cloud providers at the same time.
When we explored this theme in the in-depth interviews, we found that the key driver for multicloud adoption has been the need to run different workloads with different cloud providers, often because of specific demands from the use case of each individual project. For example, while one cloud initiative might be delivering an IoT project leveraging AWS services, a separate third-party vendor may only certify the use of a certain cloud-based database back end if it is hosted on Azure or Oracle, while a machine learning project may favor Google Cloud. This has important implications for security; whereas project teams may only care about their specific cloud provider, a centralized team such as security needs to support all of them.
Organizational Systems and Culture

In addition to understanding the objectives of cloud transformation and how this process results in a broader technology landscape – multicloud environments, with a mixture of IaaS/PaaS, SaaS and on-premises, etc. – it is important to understand how cloud transformation affects the various stakeholders within organizations. As with other IT projects, we expect some of the key stakeholders to be the same, but with different perspectives as they relate to cloud:

- **Lines of business or business units.** These teams are evolving as they become more comfortable with technology, reaching out to the thousands of independent vendors with vertical solutions on their domains, which may result in broad usage of multiple cloud technologies or services.

- **IT engineering (developers and operations teams).** These teams will likely define, implement and operate a multitude of cloud environments, but they must be aware that they should do this under newer agile and DevOps project methodologies.

- **IT security teams.** Depending on internal company culture, security teams may be expected to have full operational roles in projects as they relate to security; they may have more limited participation, simply validating security choices, or as incident responders, etc.

The in-depth interviews highlighted these different roles for stakeholders – particularly security teams. Respondents indicated that security teams were often working to stay up to date on cloud initiatives from the other teams.

Although not directly related to cloud transformation, the figure below speaks to an adjacent area – DevOps – and points to a significant shift in organizational dynamics. According to the DevOps practitioner survey respondents, approximately half of DevOps processes are managed by the lines of business themselves, with IT having some central oversight.
Having a large set of parallel initiatives puts tremendous pressure on smaller, centralized teams, which can lead to negative consequences for both cloud engineering ‘tiger teams’ and security teams. While having smaller teams with domain expertise on cloud technologies may appear to be an effective and efficient manner of starting cloud transformation efforts, that strategy is likely to backfire because that small team will unlikely be able to cope with the increased demand for expertise from a variety of parallel projects. The better alternative is for the organization to work diligently on setting the expectation that the various teams must develop the necessary cloud technology skills to support their projects. A centralized team may indeed exist as a ‘center of excellence,’ but it should not have day-to-day responsibilities for operating each cloud project.

This same model applies to security: rather than force security teams to operate cloud security responsibilities across the organization, there needs to be a realignment of skills and responsibilities related to cloud security. While the security team can be a central point for escalations and research, individual projects should understand and apply guidance on security objectives.
Understanding the Cloud Security Landscape

The challenge that security presents to the adoption of cloud transformation initiatives is not lost on industry stakeholders. Notably, cloud service providers have invested billions of dollars in defining and delivering a wide variety of security controls and functionality within their platforms, while numerous third-party security vendors aim to complement those features to address different use cases.

Navigating how to implement security for cloud deployments is not a straightforward exercise of leaving the entire responsibility to the cloud provider. While there are many components in the overall architecture that are internal to the cloud provider, there are several interfaces that the provider makes available to customers and third-party vendors for their use. The general approach to security that all major cloud providers have arrived at is to frame the various roles and responsibilities within a shared-responsibility model. The generalized version of the shared-responsibility model is that, depending on the type of service being contracted, the provider is responsible for the underlying infrastructure of the service, while the client is responsible for configuring and using the service.

Figure 8: Shared-responsibility model of implementing security in cloud deployments

Source: 451 Research

<table>
<thead>
<tr>
<th>Always Customer</th>
<th>Overall Security Accountability</th>
<th>Cloud IaaS (*)</th>
<th>Cloud PaaS</th>
<th>Cloud SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identities and Access (IAM) – Application and Cloud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Governance – Security, Privacy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Monitoring and Response</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Varies</td>
<td>Application/Service Business Logic Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Framework and Services Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operating System Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Always Provider</td>
<td>Virtualization Layer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compute/Storage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Connectivity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical/Environmental</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) – Most deployments, except for ‘bare metal’ and similar offerings
While the division is quite clear in theory – basically, managing identities and access, governing data, security monitoring, and any configuration change that affects a service is the responsibility of the customer, regardless of which service is used – in practice, it has led to some confusion, leaving some customers with a distorted view of their cloud security responsibilities, a view that incorrectly places more burden on the cloud provider.

Unfortunately, such a view appears to be corrected primarily through experience. As Figure 9 below shows, customers had significantly different responses regarding how they would be notified of a cloud security incident based on their level of digital transformation experience.

**Figure 9: Experience level dictates organizations’ understanding of cloud security responsibilities**

*Source: 451 Research’s Voice of the Enterprise: Information Security, Budgets & Outlook 2020*

Q. What is the most likely way you would find out that your hosted cloud solution had been breached?

**Base: All Respondents**

- Our security monitoring infrastructure as applied to the cloud would tell us
- Our cloud provider would tell us
- Third parties (e.g., a credit processing company, the FBI) would tell us
- Other (please specify)

This gap is also clearly reflected in the technology choices. Figure 10 shows that there is a significant difference in adoption rates for key technology controls for cloud.
Figure 10: Experience dictates adoption rates for key cloud technology controls


Q: Which of the following security technologies or capabilities – if any – have you implemented in your hosted cloud? (Please select all that apply.)

Base: All Respondents

- Multi-factor authentication
- Encryption
- Identity management / authorization

The results indicate that the gaps go far beyond technology itself: organizations need to acquire a better understanding of cloud security topics in order to correctly take the responsibility of implementing and operating cloud environments in a secure manner.
Enabling Security Teams

There are obvious gaps in aligning security concepts to cloud transformation initiatives. A closer look – breaking it down by stakeholders – shows where those gaps are, and how they can be addressed:

- **Line-of-business stakeholders.** While they may understand the high-level security requirements, the multitude of service options likely makes it difficult for teams to understand what is required and what options are available. Another key concern is that, by and large, security metrics are rarely included in individual performance evaluations. In this case, security risks becoming an ‘unfunded mandate’ when compared to other individual metrics.

- **IT engineering (developers and operations teams).** Like those in line-of-business roles, these teams need to translate security requirements into practical implementations in their workflows, and they may also not be properly evaluated on security decisions. Furthermore, IT teams usually must contend with security artifacts – policies, content, tooling, processes – that may introduce delays to modern IT workflows.

- **Security teams.** Finally, security teams themselves face obstacles such as collaborating with the other teams in the manner and tempo required by modern workflows. There’s also the knowledge gap around cloud platforms themselves. As mentioned by a financial services respondent: “We try to create standards and guidelines for these public cloud platforms, but oftentimes those are tested by new applications that don’t fit into the guidance that we created.”

Interestingly, security teams are keenly aware of this knowledge/skills gap. In a recent survey aimed at security professionals, cloud platform expertise was clearly cited as the top skill most inadequately addressed in the organization. Notably, application security – also a key skill for developing better understanding of how to interact with engineering teams – came in second.
Indeed, when discussing the topic of skills, many respondents highlighted this area: “The biggest challenges we really had were just having a lack of knowledge about cloud security,” said a large financial institution respondent during the in-depth interviews. A similar feeling was echoed by a business service organization: “We don’t have people who know this in our internal organization. Building that capability has been a challenge for us.”

That said, all respondents indicated that the organizational structure is not changing significantly because of cloud transformation. Rather, it is much more about enabling the existing IT teams – including security – to upskill in cloud technologies and methodologies. In some cases, it includes leveraging resources from services partners while internal teams are scaling up. Many of the respondents indicated that upskilling their teams was a combination of cloud training and certifications while leveraging assistance from either the cloud provider or a specialized services partner. A business services firm respondent said: “Enabling our own employees who went through the [cloud provider] training courses and certifications and everything to get up to speed with where they can contribute for the journey.”

When it comes to security tooling, a significant number of respondents – both in surveys and interviews – indicated that they are aiming to integrate any cloud security technology into their existing IT workflows. To accomplish this, a significant number of respondents said they plan to use additional security products and services from third parties.
Figure 12: Vendor-based security tools used for off-premises cloud architectures and plans to acquire additional security services

Source: 451 Research’s Voice of the Enterprise: Information Security, Budgets & Outlook
Q: Which vendor-based security tools does your organization currently use for its off-premises cloud architectures? (Please select all that apply.)
Base: Respondents who use hosted cloud architectures (n=134)
Q: During 2020, does your organization plan to acquire additional security services for its off-premises cloud architectures? (Please select all that apply.)
Base: Respondents who spend on securing hosted cloud architectures via vendor-based security tools (n=103)

The range of controls, decisions and practices used to address cloud security concerns varies, but they are heavily centered on identity management and encryption/key management.
Figure 13: Top ways organizations are addressing security concerns

Source: 451 Research’s Voice of the Enterprise: Information Security, Budgets & Outlook

Q: Of the following, what are the top ways your organization is addressing security concerns with hosted cloud solutions? (Please select up to three.)

Base: All Respondents (n=195)

<table>
<thead>
<tr>
<th>Security Measure</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity management/authorization/access control tools</td>
<td>34%</td>
</tr>
<tr>
<td>Encryption/key management</td>
<td>26%</td>
</tr>
<tr>
<td>Usage of known vendor-supplied security tools</td>
<td>19%</td>
</tr>
<tr>
<td>Explicit service-level agreements (SLAs)</td>
<td>18%</td>
</tr>
<tr>
<td>Proven compliance with industry standards (e.g., SAS Type II)</td>
<td>16%</td>
</tr>
<tr>
<td>Explicit contractual responsibilities for security between</td>
<td>16%</td>
</tr>
<tr>
<td>the cloud provider and customer</td>
<td></td>
</tr>
<tr>
<td>A security operations center (SOC)</td>
<td>15%</td>
</tr>
<tr>
<td>Auditable</td>
<td>14%</td>
</tr>
<tr>
<td>Third-party testing or assessment of the cloud services</td>
<td>13%</td>
</tr>
<tr>
<td>Incident/forensics response support</td>
<td>12%</td>
</tr>
<tr>
<td>Providing regular results of security audits from known security</td>
<td>11%</td>
</tr>
<tr>
<td>testing companies</td>
<td></td>
</tr>
<tr>
<td>Dedicated infrastructure</td>
<td>11%</td>
</tr>
<tr>
<td>Re-architecting applications for the cloud</td>
<td>10%</td>
</tr>
<tr>
<td>Training in cloud security tools offered</td>
<td>9%</td>
</tr>
<tr>
<td>Transparency of infrastructure at the cloud provider via due</td>
<td>8%</td>
</tr>
<tr>
<td>diligence requests</td>
<td></td>
</tr>
<tr>
<td>Region-specific datacenter locations</td>
<td>8%</td>
</tr>
<tr>
<td>Provenance of the location of data</td>
<td>5%</td>
</tr>
<tr>
<td>References from other customers</td>
<td>4%</td>
</tr>
<tr>
<td>Assumption of liability for security breaches or outages</td>
<td>3%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>8%</td>
</tr>
</tbody>
</table>
Recommendations for Securing Cloud Transformation

Based on the input from the surveys and interviews, alongside other domain expertise related to cloud security, we can make several recommendations at both the strategic and tactical levels to help organizations maximize the chance of success for their own transformation activities.

• First, there needs to be broad understanding within the organization that cloud transformation is to be treated as a long-term strategic initiative. This implies an organization-wide discussion about aligning IT, security and risk management goals to broader business goals, as well as senior-level support for cloud transformation activities and phases. This is a much broader conversation than just with security teams alone; clarifying and agreeing on how the organization will approach cloud transformation is key.

• If the organization is also using the opportunity to significantly alter the workflow in adopting new technologies, such as adopting a more distributed model for new initiatives, then it becomes essential for executives to rethink responsibilities for risk management – particularly operations risk derived from cybersecurity – and how they should flow across the organization. Specifically, this means aligning responsibilities so that the underlying incentives and metrics for all teams – development and security alike – support the practices needed to secure cloud transformation.

• It is also necessary to make sure that all stakeholders are sufficiently equipped to discuss the relevant points of cloud transformation and security impact. This is not so much about creating technical cloud experts across the organization but, rather, allowing the different stakeholders to understand the nuances that cloud transformation will have on their specific areas of concern. For business leaders and development/engineering teams, this includes understanding the nature of security in cloud environments. For security teams, this means understanding the transformative nature of cloud services and how they affect the organization’s overall goals.

• The practice of selecting projects for cloud migration or transformation based on lifecycles appears to be an effective way of aligning these activities with the rest of IT workflows and should be encouraged. While cloud can be a ‘default’ option for new workloads – rather than ‘why cloud’ the question becomes ‘why not cloud’ – existing workloads may be migrated in a more measured manner. The criteria for selection will vary by organization, but typically include connectivity and latency requirements, scalability and availability needs, and projected lifetime business value.

• There’s also significant value in aligning the cloud transformation security efforts to a security framework. While there are specific cloud security frameworks – the Cloud Security Alliance’s Cloud Control Matrix is a potential candidate – organizations may also consider using provider-specific documentation and mapping those controls to existing formal or informal frameworks such as the NIST CSF, Cyber Defense Matrix or other governance frameworks. The key consideration here is that the cloud security framework should align clearly with the overall security and risk management framework that the organization already uses.
Once there is enough strategic alignment between security and the other stakeholders around cloud transformation, the preparation can turn to more tactical considerations. This assumes that by now, security and cloud engineering teams have aligned on the shared goals of cloud transformation security and are sufficiently motivated to address security concerns.

• First, clearly define and, if necessary, improve how and when security teams are made aware of cloud projects, and to what degree they need to be involved versus leveraging a ‘security champion’ within the project team. As mentioned before, it is not possible to scale the reach of security into a distributed workforce.

• Security teams must quickly be enabled to understand how the newer technology patterns are being implemented. At the same time, cloud engineering teams need to collaborate with security and risk management teams to translate security requirements from the various control domains – such as identity management, data security and application security – into specific requirements for engineering. At a minimum, teams should collaborate on performing threat modeling for cloud projects.

• Security controls must be inserted into the cloud engineering workflows in a manner that preserves the operational agility of those teams. This will likely take many forms, including but not limited to:
  - Providing meaningful insight to developers and engineers when they are creating and defining cloud applications or resources. One example is the integration of security guidance within developer tooling such as integrated development environments in a context-aware manner.
  - Support for security testing at multiple stages of the development lifecycle.
  - Increased use of practices such as infrastructure as code to minimize configuration drift of cloud environments from previously approved versions. Increased use of cloud security posture management and cloud workload protection tooling to correctly evaluate and monitor the new cloud environments.
  - Integration of security events and incidents into the existing incident response frameworks, but also integrating with engineering’s workflow – likely via defect tickets – so that fixes can be incorporated into normal engineering practice.
Conclusions

The path forward for organizations is to accept cloud transformation initiatives as a broad component of modern IT processes and adopt both strategic and tactical improvements as described above. This approach is independent of even broad disruptions in the macroeconomic sense, such as the current worldwide health crisis.

Indeed, the ‘people, process, technology’ model of process improvement holds true for cloud transformation:

- **People.** Enable all stakeholders to be conversational or fluent in cloud technologies and enable lines of communication among stakeholders to minimize surprises and accelerate learning.
- **Process.** Review how the organization manages projects to support the more dynamic nature of cloud projects, particularly as it relates to accelerating the feedback loops from learning.
- **Technology.** Rather than look at cloud as a separate technology domain, integrate cloud technologies into existing management and operations processes, including security operations.

Moving forward, we expect the following trends to continue to affect cloud transformation efforts:

- Cloud service providers will continue to release newer services covering specific business needs. These services will integrate into the provider’s broader identity and access management and monitoring frameworks but may do so in phased approaches.
- The broader combined usage of various edge technologies – from 5G networking to IoT deployments – and longer supply and value chains means data assets will be distributed over a much broader environment, which will require increased visibility into both the organization’s own environment and those of its key partners for security purposes.
- Given the essential role of technology, we will continue to experience increased regulatory oversight across multiple jurisdictions.

Organizations that can navigate the requirements and changes around the three key dimensions – people, process and technology – are likely to be in a better position to reap the expected benefits from their cloud transformation efforts.
RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. Find out how to thrive in a dynamic, high-risk digital world at rsa.com.

Adopting cloud computing? Realize the benefits and mitigate the risk with this Guide to Managing Cloud Transformation Risk.

Want to know more? Watch our webinar exploring the various cloud risks (security, resiliency, third-party, etc.) and providing recommendations to mitigate those risks through improved visibility, access controls and governance.

Ready to talk to RSA? Let the experienced members of the RSA Risk & Cybersecurity Practice guide you on your journey. Contact the RSA Risk & Cybersecurity Practice to get started. You can also reach us at: 800-995-5095.
About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000, 451 Research is a part of S&P Global Market Intelligence.

© 2020 451 Research, LLC and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication, in whole or in part, in any form without prior written permission is forbidden. The terms of use regarding distribution, both internally and externally, shall be governed by the terms laid out in your Service Agreement with 451 Research and/or its Affiliates. The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such.

451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.