Cyber Implications of IT Modernization and Cloud Migration

Changes in the way IT services are designed, delivered, and maintained create new cybersecurity challenges and risks.

Today's cyber threat landscape pits cybersecurity experts and their chief information security officers against often well-funded and highly innovative adversaries, ranging from organized syndicates and nation-states to hacker-for-hire opportunists looking to make a fast score. Securing critical and high-value digital resources is just one of the challenges. As information technology capabilities change to meet the needs of the business, the cyber attack surface changes as well. IT modernization and cloud migration strategies can provide increased cyber protection, but attackers at the same time are pivoting to pursue new potential entry points for attacks, leveraging those same capabilities.

Leaders bound by tight business processes and tighter budgets can take steps to further reinforce and secure their digital estates against attackers by understanding the threats and focusing on the most significant risks to the organization. By zeroing in on the most critical assets and focusing on meaningful, inherent threats and the related vulnerabilities, organizations can keep digital initiatives on course, strengthen their security postures and enable meaning business outcomes.

Key Cyber Challenges

Several business and IT trends with positive benefits for the broader organization introduce new challenges for cybersecurity, including:

1 Cloud adoption

Cloud adoption: As workloads and critical data are distributed across a variety of public and private cloud providers, data centers, and third-party software-as-a-service providers, there are more possible points of entry and surface areas to be attacked and potentially exploited.

2 Remote work

Remote work: Remote work can expose sensitive data and credentials in a variety of public and private settings.

3 Internet of Things (IoT) proliferation

Internet of Things (IoT) proliferation: The ever-growing range of small, low-power, and increasingly sophisticated devices that can collect and process data make it increasingly difficult to map out the full range of vendors participating on any given organizational network.

4 Third-party infrastructure

Third-party infrastructure: Organizations of all shapes and sizes are increasingly moving away from owned-and-operated data and computing centers to a variety of outsourced, hosted, and cloud-provisioned digital infrastructure and service solutions.

Because of the significant capability and positive business impacts, movement in favor of these trends will doubtless continue. But IT and business leaders also increasingly recognize and admit the growing risks, complexity, and challenges faced through IT modernization. For example, the Cloud Security Alliance (CSA) reported survey results in October 2022[1] finding that just 39% of IT and security professionals have a high level of confidence in their cloud data security. Only 4% said they felt they had enough security for all data. Guidehouse recommends enabling logging and continuous monitoring of all cloud services as an important first step in closing such gaps.

Addressing the Implications of Modernization and Cloud Migration

Since IT modernization continues to proceed and gather pace, organizations should take steps now to address the cyber impact before being forced by an event or incident to do so. Guidehouse recommends reinforcing IT and security strategy and discipline in several areas, including:

Data Governance: As both storage and processing tasks are increasingly farmed out to a multi-cloud environment, organizations must have a clear understanding of how data is used and protected at each step in the process. This should include mapping out joint responsibilities, where relevant, through a shared responsibility model, among cloud and middleware vendors. Carefully monitoring and evaluating the security programs of partners and suppliers to ensure they meet and exceed relevant security standards.

Application Hardening: With application processes spanning multiple clouds for processing components or other dependencies, Guidehouse recommends a development approach that prioritizes application hardening as a matter of course. This includes using a continuous integration/continuous development (CI/CD) pipeline model, infrastructure-as-code, and careful guardrails that prevent developers from incorporating code or vulnerabilities into productions.

Secure Architecture: Organizations should consider implementing zero-trust architecture and policies across both modern and legacy systems and applications, conducting strict and continuous monitoring of all configurations, and automating the enforcement of policies through orchestration technologies.

User Access Control: Access should be based on, at a minimum, a role-based access with all users authenticating into applications as general users through contextual authentication, which utilizes a wide range of signals (device, past user history, IP address, etc.) to continuously determine whether a user should have access to an application. This removes the outmoded notion of a security moat to protect the perimeter. User access practices should also be carefully monitored during transitional periods between on-premise and cloud resources, when credential management may be complicated by the need to manage multiple logins to access the same resources depending on whether the legacy (on-premise) or migrated (cloud) system is needed.

Posture Management: This discipline compares application, system and development stack configurations against expected secure and compliant standards and automates alerts and remediations when configurations do not meet or drift from known secure configurations.

Training and Awareness: Because email will continue to be their primary vector for exploitation for bad actors, organizations must continue to focus on awareness and training. Automated phishing simulations and gamification can demonstrate the harm these attacks can cause, and provide instructional materials to inform how to identify and report potential threats.

Artificial Intelligence (AI) and Machine Learning (ML): Organizations can use machine learning to automate the detection of irregular behavior, spotting activity, system usage and application anomalies that could be signs of a threat, exploit, or breach. Enabling detailed logging (available through most major public clouds as well as specialty cloud vendors) and leveraging AI to sift through large volumes of data can help relieve the workload on human IT and security specialists. AI can also be applied to further automate processes, including account provisioning and configuration management.

Strategy Beyond the Cloud

Modernization also provides an opportunity to realign security practices not specifically tied to cloud services and other distributed computing. In today's digital ecosystems, organizations cannot afford to ignore the very real risks arising when any facet of interconnected and essential components of doing business is overlooked. Organizations need to have a better understanding of threats and vulnerabilities to be able to manage risks.

An important place to start is by reviewing and reevaluating vulnerability management processes and practices. Many organizations rely solely on industry risk scores for identified vulnerabilities without understanding the real risks within the context of their IT environment. With the vast number of vulnerabilities organizations cannot afford to waste time remediating every single vulnerability. Instead organizations need to focus attention on those vulnerabilities that pose the greatest risk.

Without applying that context properly, many organizations overcommit resources to addressing vulnerabilities that may be high on the Common Vulnerability Scoring System but pose little to no risk in their environment. This approach fails to consider that the system identified with a critical vulnerability may not be public-facing, may not have access to data of any real value, or may otherwise be isolated and materially unimportant. At the same time, systems rated as just medium risk may actually be public-facing and contain data or other resources that would be materially damaging to lose. Risk scoring and resource allocations to secure systems should take into account not just the technology but the underlying organizational value and impact of a potential loss or exploit.

Develop proficiency around understanding software bills of materials (BOMs). This will provide a better view into the exposure surfaces and vulnerabilities of a wide range of devices and services, including IoT equipment and cloud services. Cybersecurity is now more than just a home game—it also takes concerted effort by a vendor ecosystem and due diligence by customers. Software BOM tracking makes it more manageable to work with third-party vendors to understand how they manage their responsibilities and how their vulnerability management plans may affect you in the event of a misconfiguration or breach.

Where possible, shift the response posture to detections, exposures, and other cyber incidents from one of manual intervention to automated response. Automated management of security-related support tickets is just the beginning. Automated remediation can make it easier to remediate mis-configurations and drift and can disable or quarantine misconfigured or vulnerable devices and system to minimize the blast radius of any potential exploit or compromise.

Make sure that the network teams involved in the segmentation of high-value applications and data are also involved with the teams developing and configuring those resources. In the October 2022 CSA survey, 45% of respondents named "inadvertent exposures due to misconfiguration" one of their top three cyber worries[2]. Because complexity creates more opportunity for misconfiguration, coordination, communication and documentation across IT deployment and security teams needs to be a priority to keep this complexity from causing issues down the line.

And finally, senior leadership and top IT governance figures should remain committed to speaking with one voice and communicating to the entire organization that security is a shared responsibility.

How Guidehouse Can Help

Guidehouse professionals have worked with large enterprises and federal agencies alike to evaluate, adjust, and reinforce secure practices even in the midst of significant IT modernization and cloud migration campaigns. Through technical expertise and diligent change management, we work to close and tighten potential gaps, identify, and adjust misaligned policies, and educate developers in modern CI/CD pipeline practices.

Ensuring cyber readiness in the midst of transformation is a difficult lift for even the most well-resourced organization. It now seems practically impossible to do everything well in order to comprehensively secure the tech estate. By focusing on the fundamental basics internally, you build routine and reflex, ensuring a culture of security by default that will help protect your organization even as the tools and attacks change. Working with experts such as Guidehouse professionals to evaluate the security of your cloud foundations, your readiness for further modernization and transformation in the cloud, and the resilience of cloud workloads puts a fresh team on the fast-changing challenges to come.

Contact Guidehouse to discuss a cloud health assessment.

[1,2] New Study from Cloud Security Alliance and BigID Finds That Organizations Are Struggling to Track, Secure Sensitive Data in the Cloud", October 20, 2022, New Study from Cloud Security Alliance and BigID Finds That | CSA.

Contacts

Matt Phillips, Director
Cybersecurity
maphiliips@guidehouse.com

Anil Krishnanda, Director
IT Strategy
akrishnanada@guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 17,000 professionals in over 55 locations globally. Guidehouse is led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit guidehouse.com.

https://guidehouse.com/services/cybersecurity

@GHTechsolutions http://linkedin.com/showcase/guidehouse-technology-solutions/