Guidehouse
Outwit *Complexity*

Have You Reviewed Your Cloud Strategy and Security After the Kronos Ransomware Attack?

In December of 2021, Kronos, one of the world's biggest cloud-based HR management software providers, experienced a ransomware attack that led to a system-wide outage from which it's recovery was lengthy. The cyberattack left the company's enterprise and public clients without core functionalities, including payroll processing and scheduling, just ahead of the holidays.

While Kronos advised customers to rely on their own business continuity plans, including manual or semi-automated processing, many of their clients didn't have back-up procedures in place—which created major payroll issues that continue to impact both organizations and individuals.

Security is a Shared Responsibility

Hackers are using attacks that have maximum disruption by targeting third-party vendors and their customers. Security, often considered the sole responsibility of cloud service vendors, needs to be a shared responsibility.

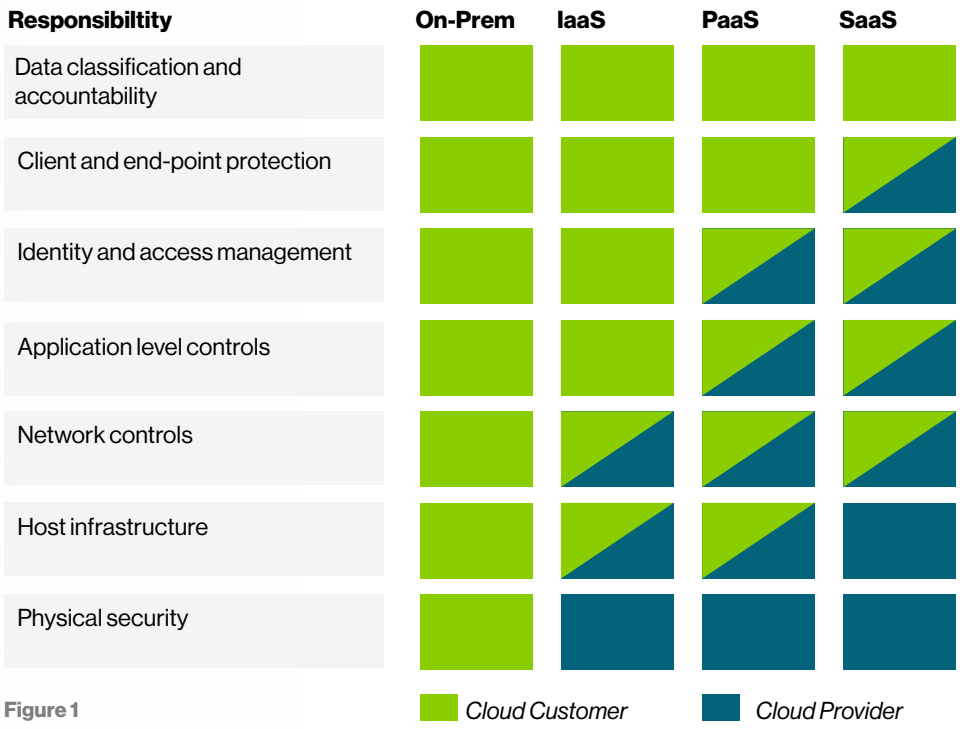

Figure 1

Healthcare providers are especially vulnerable to cloud-based ransomware attacks—deploying more cloud applications in their IT environment and having the highest proportion of information systems outside their direct control.

The Kronos cyberattack and other recent cloud security breaches demonstrate the vulnerabilities we all face, as well as the complexity our increased reliance on software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) solutions presents to our security architectures and business stability.

Hackers are attacking strategic targets with an aim of causing maximum disruption by going after third-party vendors and their customers. Too often, we assume that the vendors providing our cloud services are the only ones responsible for security on their networks. However, this responsibility is often shared, depending on the type of cloud services being deployed (see figure 1).

Healthcare providers are especially vulnerable to these types of ransomware attacks, as they tend to deploy more cloud applications in their IT environment and have the highest proportion of information systems outside the direct control of their internal information technology departments.

Cloud security compromises at the SaaS and PaaS levels have increased because:

- Organizations don't have a clear line of responsibility defined for security with the vendor
- Companies make incorrect assumptions about vendors' cybersecurity processes
- The belief that cybersecurity is "cloud native" gives false comfort

How to Assess Your Exposure

Cloud services incorporated into an enterprise's IT platforms broaden the attack surface and thus dynamically and exponentially increase the need for rigorous and holistic asset management and cyber defense strategies.

Employ a comprehensive cloud security framework that minimizes the impact of any one vendor in the event of a cyber incident.

The key challenge to understanding and addressing your cloud-related cybersecurity risks arises from the fundamental differences between each cloud vendor and platform. Therefore, there is no one silver bullet to secure your cloud and on-premise architecture. Cloud security starts with a well-defined operating strategy for your specific cloud environments, a detailed requirements definition and framework for new cloud environment acquisition, and an integration strategy that meets your cybersecurity requirements.

Enterprises must first have an inventory of all their cloud vendors and services, then apply a comprehensive cloud security framework to them that includes a strategy to minimize the impact that any one vendor has on your enterprise's operations in the event of a cyber incident. This encompasses an effective mitigation plan to enact when those services aren't available—which should be readied during the acquisition phase and operationalized over the course of service adoption and integration.

Figure 2

Your cloud security program needs to go beyond your SaaS vendors to include your custom subscriptions to PaaS and IaaS. These customizable platforms present more risk because they are often used for custom applications, sensitive data manipulation, advanced analytics, and storage platforms. This added exposure increases the responsibilities that must be managed within an organization's security architecture.

As cyber incidents increase and third-party cloud service providers become greater targets, ensuring that your enterprise has a holistic cybersecurity strategy that addresses its cloud-related security is critical for enterprise risk management and business continuity planning.

For more information, please contact:

Marianne Bailey
Partner, Cybersecurity
mbailey@guidehousefederal.com

Michael Ebert
Partner, Cybersecurity
mebert@guidehouse.com

How Guidehouse Can Help

Securing systems and data across multiple cloud environments is a complex and critical endeavor. Guidehouse helps organizations respond comprehensively to their business and cyber needs at all stages of the process by supporting them to address these key areas:

- Strategy, governance, and management
- Security architecture and services
- Threat and vulnerability management
- Identity and access management
- Information and data privacy protection
- Incident and crisis management
- Risk and compliance management
- Delivery and operations

For more information on Guidehouse's cloud cybersecurity capabilities, please see our Cloud Cybersecurity Solutions.

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 12,000 professionals in over 50 locations globally. Guidehouse is a Veritas Capital portfolio company, 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 **www.guidehouse.com**

© 2022 Guidehouse Inc. All rights reserved. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. GH-258a PS CyberAlert - Cloud Strategy