Building Resilience: Understanding Cyber Risk in the Post-Pandemic World of Work

The global trend toward remote work has increased organizational attack surfaces, intensifying cybersecurity threats and increasing the risks to businesses in the post-pandemic world.

Guidehouse
Outwit *Complexity*

Guidehouse
Outwit *Complexity*

The COVID-19 pandemic triggered a paradigm shift in the way we work. During lockdowns, the traditional office setting was abandoned as employees began to work remotely. More than two years later, the trend toward remote work is continuing, with significant implications for cybersecurity and organizational risk.

This workplace disruption should have caused a reassessment of how we manage cybersecurity and handle associated risks. However, in many cases, businesses are still operating in essentially the pre-pandemic model, lacking resilience and effective risk management. Many are unaware of their current risk situation and the technical threats they are susceptible to.

> With remote work becoming the "new normal" all over the globe, setting a strategy for minimizing those risks and building resilience in the post-pandemic world is crucial."

The Post-Pandemic IT Landscape

Organizational Risk

Urgently implementing remote working protocols as a reaction to the COVID-19 lockdowns has put new demands on the IT infrastructure supporting organizations. This transition has enabled more endpoints, personal devices, and non-secure Wi-Fi networks to access mission-critical applications and data. As a result, for many organizations, the IT network's attack surface has increased greatly, creating a vast number of new vulnerabilities.

Today, with remote work becoming the "new normal" all over the globe, setting a strategy for minimizing those risks and building resilience in the post-pandemic world is crucial. Still, many organizations have not made the necessary investments to respond effectively to these growing threats.

Cybersecurity attacks are becoming more intelligent, coordinated, and targeted each day. With so much sensitive data now stored in the cloud, and accessible from remote locations, organizations must take steps to build resilience to match these threats.

As both customer and employee expectations for seamless, on-demand access to IT services continue to grow, maintaining business continuity is also more important than ever. Any unexpected outages, systems failures, or disruptions to digital services can have a negative impact on an organization. Whether these issues occur due to loss of power, adverse weather, or other circumstances, end-user tolerance for poor performance is at an all-time low.

Avoiding Common Pitfalls

Lack of Awareness and Communication

Communication of actionable risk information and organizational transparency are critical aspects of a resilient organization. However, too many businesses lack effective processes and channels of communication, from the top down and vice versa. This often results in failure to predict, manage, and recover from incidents such as system failures or data breaches.

Some business leaders are not aware of how critical their IT systems actually are in supporting their core operations, nor do they realize how damaging unplanned downtime could be. It's important to ensure clear, effective messaging throughout the entire organization regarding the role of the IT infrastructure and how to protect it.

The awareness of the organizational mission, and resulting priorities, must be validated and communicated by senior leadership throughout the entire organization.

In the event of an attack or outage, a strong asset management program requires understanding:

- What each system does/ who it supports.
- What other technology systems integrate with.
- What impact a system's failure will have on operations.
- What areas of the business will be affected.
- What needs to happen to resolve the issue.
- What communication is required to keep other business areas running.

Incomplete or Insufficient Contingency Plans

Even in organizations with good awareness of the potential risks they face, many contingency plans and disaster recovery processes are still insufficient compared to the reality of certain incidents. It is common for these measures to fail to cover the full range of possible risks or disasters that can impact the operations. Organizations must develop recovery plans with the foundational perspective that they will likely be attempting to reconstitute operations in "abnormal conditions"—during periods of reduced access and limited availability of common resources—staff, communications, etc. Prior prioritization of missions and supporting resources is necessary to ensure fast and efficient recovery operations.

Poor Asset Management

Asset management and asset intelligence are essential when aiming to build resilience. However, many organizations don't have an up-to-date list of all technology assets and data, nor a priority order based on the roles those assets play in supporting the organization. This prevents the development of recovery plans consistent with organizational objectives.

Underestimating the Challenge

Many businesses make the mistake of thinking resilience is a simple case of purchasing a point product or tool, switching it on, and leaving it to run. Additionally, some organizations also believe that compliance with industry standards and regulations is enough to achieve resilience. These are all potentially dangerous misconceptions. In today's post-pandemic world of work, cybersecurity is a complex, ever-changing issue that requires a long-term, companywide strategy and commitment.

Operations staff and IT teams must work together and communicate constantly to keep the IT infrastructure protected. This requires cybersecurity expertise, governance, and careful management of asset intelligence, alongside best practices and supporting technology solutions.

The rapid velocity and rapid onset of cybersecurity attacks means that resilience must be proactive, rather than reactive. Without this in place, organization could be exposed to severe risks. "Figuring it out when it happens" is a guarantee for greater costs and downtime following an unforeseen event.

The Importance of Resilience Today

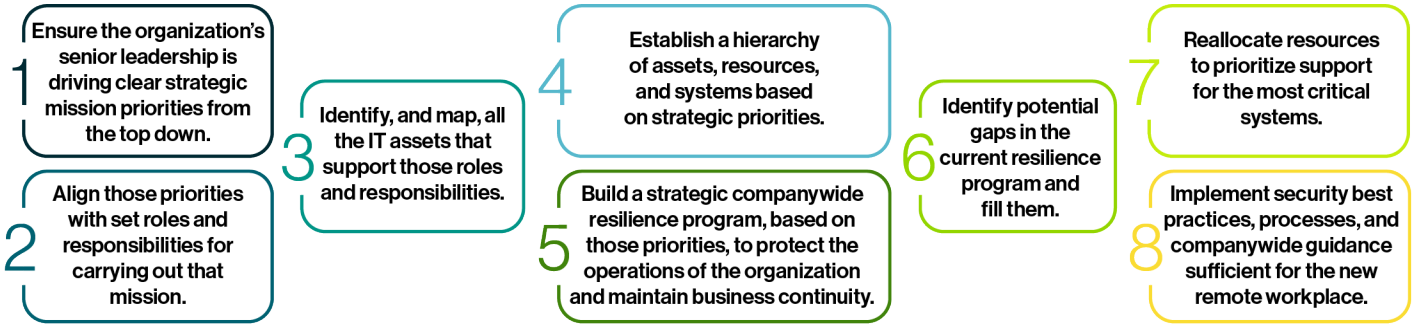
Why is building resilience, rather than just settling for basic compliance, so crucial today? Resilience is about ensuring an organization can continue to operate and perform as required. That means continuing to meet all its obligations, even when experiencing unexpected downtime or security issues.

In many cases, compliance has become a distraction from the goal of resilience for individual systems and organizations. Compliance is not the destination. It is a good start on the long journey towards true resilience.

True resilience requires key stakeholders to appreciate the risks and work together strategically to mitigate them. Resilience in the post-pandemic world of work is an ongoing, evolving process that needs to change with the organization and its circumstances. Businesses that fail to understand that, and fail to prepare accordingly, are operating at greater risk.

A Guide to Building Resilience

With so much risk to manage in today's digital business landscape, understanding how to set a strategy for becoming resilient is essential. Based on extensive experience successfully delivering cybersecurity and resilience programs for global organizations, Guidehouse recommends the following steps:



How Guidehouse Can Help

An organization's IT infrastructure is an intricate network of systems that rely on each other to keep the organization running and meet the expectations of stakeholders and customers. If one system within an IT portfolio is retired, that could have a trickle-down effect for the entire resilience strategy of a mission or business area in addition to the entire organization. This is why the channels of communication and transparency from the top down and back up become so important. Beginning with ensuring a detailed understanding of organizational data and technology assets, organizations must develop a comprehensive process to secure their infrastructure and promote constant vigilance around emerging risks.

With our extensive experience helping clients improve resilience and secure their organizations against cyber risk, Guidehouse can help organizations take a proactive approach to protecting their IT infrastructure, rather than waiting for incidents to occur before addressing their resolution.

As employees continue to embrace the trend toward remote work, organizations are exposed to more risks and vulnerabilities than ever before. This "new normal" brings with it the need for a renewed focus on resilience.

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 innovationv. 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 15,000 professionals in over 55 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**.

Contact

Marianne Bailey
Partner, Cybersecurity
mbailey@guidehouse.com

John Eckenrode
Director, Cybersecurity
jeckenrode@guidehouse.com