Techstrong Research

Building Resilient Organizations, Teams and Partnerships

COMMISSIONED BY

splunk>

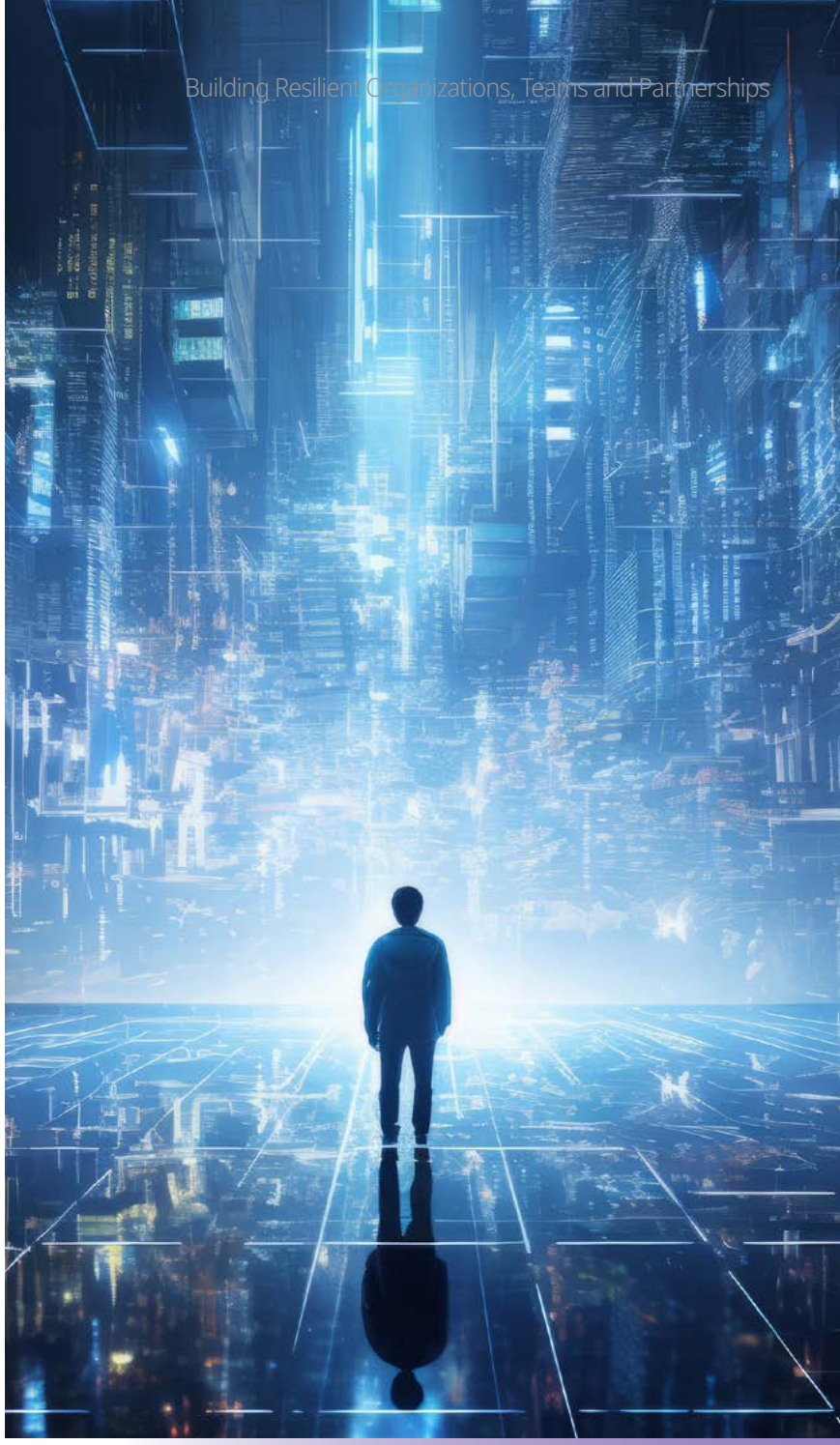
Introduction

THE RAPID SHIFT in technological dynamics over the past two decades has produced a business landscape where resilience isn't just an advantage—it's essential. As industries advance, challenges evolve and the lack of a firm foundation can adversely affect enterprises of all sizes.

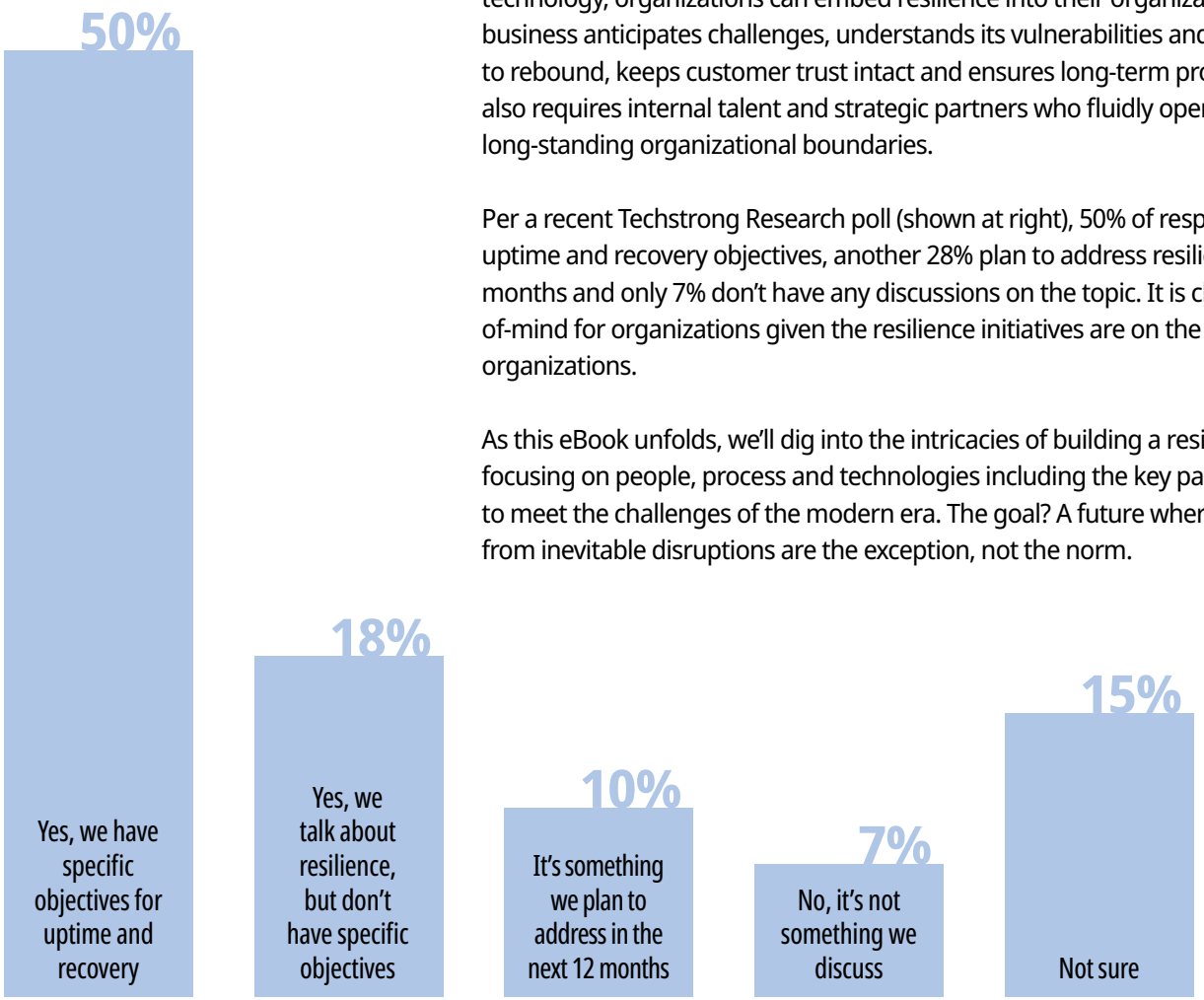
Today's business environment is characterized by volatility, uncertainty, complexity and ambiguity. Amidst this, market leaders are the ones who adapt faster than their competitors. Resilience doesn't just mean survival—it means fostering the ability to innovate, adapt and grow despite disruptions.

Every company is a digital company.

It's a hard truth: There's no modern business untouched by digital transformation. From small retail outlets leveraging social media for promotions to multinational enterprises deploying intricate cloud infrastructures, no organization goes untouched by technology. When these digital systems falter, it's not just an IT issue—it directly impacts business health. Downtime translates to lost revenue, eroded customer trust and a negative brand image.



Is resilience a critical business objective in your organization?



Resilience is Mission Critical

More than just a buzzword, resilience is the culmination of intelligent strategy and consistent execution. It's not built overnight. But, by aligning people, processes and technology, organizations can embed resilience into their organizational DNA. A resilient business anticipates challenges, understands its vulnerabilities and has the mechanisms to rebound, keeps customer trust intact and ensures long-term prosperity. Resilience also requires internal talent and strategic partners who fluidly operate across silos and long-standing organizational boundaries.

Per a recent Techstrong Research poll (shown at right), 50% of respondents have specific uptime and recovery objectives, another 28% plan to address resilience over the next 12 months and only 7% don't have any discussions on the topic. It is clear resilience is top-of-mind for organizations given the resilience initiatives are on the agenda of so many organizations.

As this eBook unfolds, we'll dig into the intricacies of building a resilient organization, focusing on people, process and technologies including the key partnerships required to meet the challenges of the modern era. The goal? A future where adverse impacts from inevitable disruptions are the exception, not the norm.

COMMISSIONED BY
splunk>

Getting People Aligned to Build a Resilient Organization

In today's fast-paced business environment, an organization's resilience hinges on its people. There's a longstanding belief that employees don't quit their jobs, but rather they reject their managers and leaders. Today's workers expect a vision from leaders that gives their work meaning and relevance–they demand leadership, and rightfully so.

Yet leadership alone isn't enough. Building an effective talent pipeline ensures organizations are prepared to address the evolving challenges of cybersecurity, IT and operations. Security, observability and operations do not cleanly follow traditional organizational structures, often blurring the lines between boxes on the org chart. In this changing landscape, soft skills like communication, problem-solving and critical thinking have become more essential than ever. Furthermore, there's an increasing appreciation for individuals from non-traditional backgrounds, as organizational diversity can introduce fresh perspectives and innovative solutions to staid environments.

As we dive deeper into the age of digital transformation, chief technology officers (CTOs) are tasked with meeting increasingly high customer expectations and maintaining organizational resilience amidst evolving security threats, while simultaneously adapting applications and handling the intricacies of scaling. Often, there are noticeable skill gaps within organizations, which has shifted the focus toward external partnerships. More companies are leaning on the experience of both software technology providers and managed service providers, looking to them as trusted strategic advisors and sources of scarce knowledge, expertise and resources.

When examining the challenge of finding qualified cybersecurity staff, respondents from a recent Techstrong Research poll highlighted the lack of candidates with the required knowledge and experience, as well as a lack of time to sufficiently train internal staff. Compounding the issue are increasingly common hiring freezes driven by a global economic slowdown. These data points make clear the reality that finding, growing and retaining staff is a top priority to building a resilient organization.

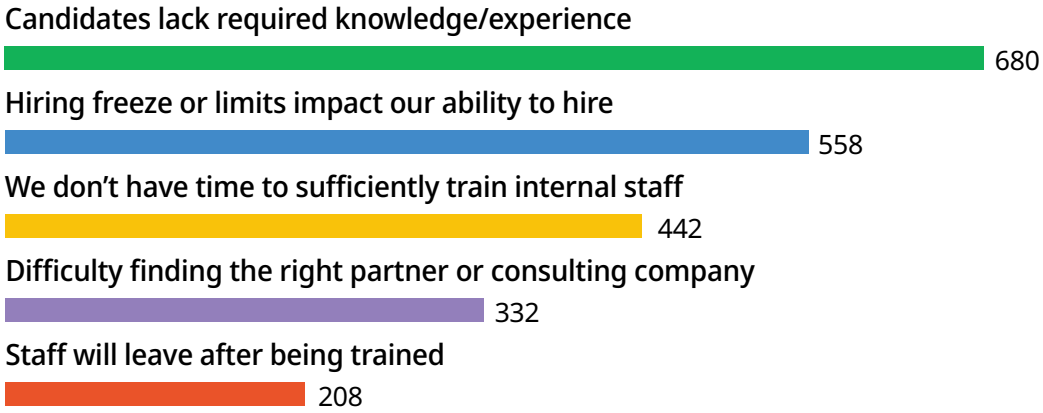
"Connecting security and IT people to how their work affects the outcomes that matter to the business and the value creation process is a real critical skill for leaders today."

CORY MINTON
FIELD CTO - AMERICAS
SPLUNK

COMMISSIONED BY

splunk>

Issues in finding qualified staff ranked most important to least important



The emergence of generative AI is transforming how we perceive the jobs and skills needed today and in the near future. What were once considered advanced knowledge workers or specialized skills can potentially be handled by generative AI and machine learning. Because of the rapid ascension of generative AI, leaders across the organization are asking how this technology can be utilized for increased revenue contribution, improved customer experiences and for operational efficiencies. Acquiring the latest AI skills and new approaches that leverage AI presents a prime opportunity to utilize external partners and advisors. New approaches to problem-solving and the latest in best practices evolve nearly every day in the fast-paced world of generative AI.

However, even amidst rapid technological growth, nothing replaces the wisdom accumulated through experience. In an era where technical skills can quickly become outdated or replaced by AI, the insight gained from years of experience provides priceless value. This also highlights the criticality of continuous learning and training to ensure an organization remains nimble, adaptable and resilient.

By intricately weaving together the principles of strong leadership, timely talent acquisition and understanding how teams utilize tech to drive efficiencies, companies are not only equipped to weather challenges but can emerge stronger, more energized and ready for the future.

"Partnering with a professional services organization or systems integrator shortens the time to value of new digital workloads, ensuring they're secure and up and running."

CORY MINTON
FIELD CTO - AMERICAS
SPLUNK

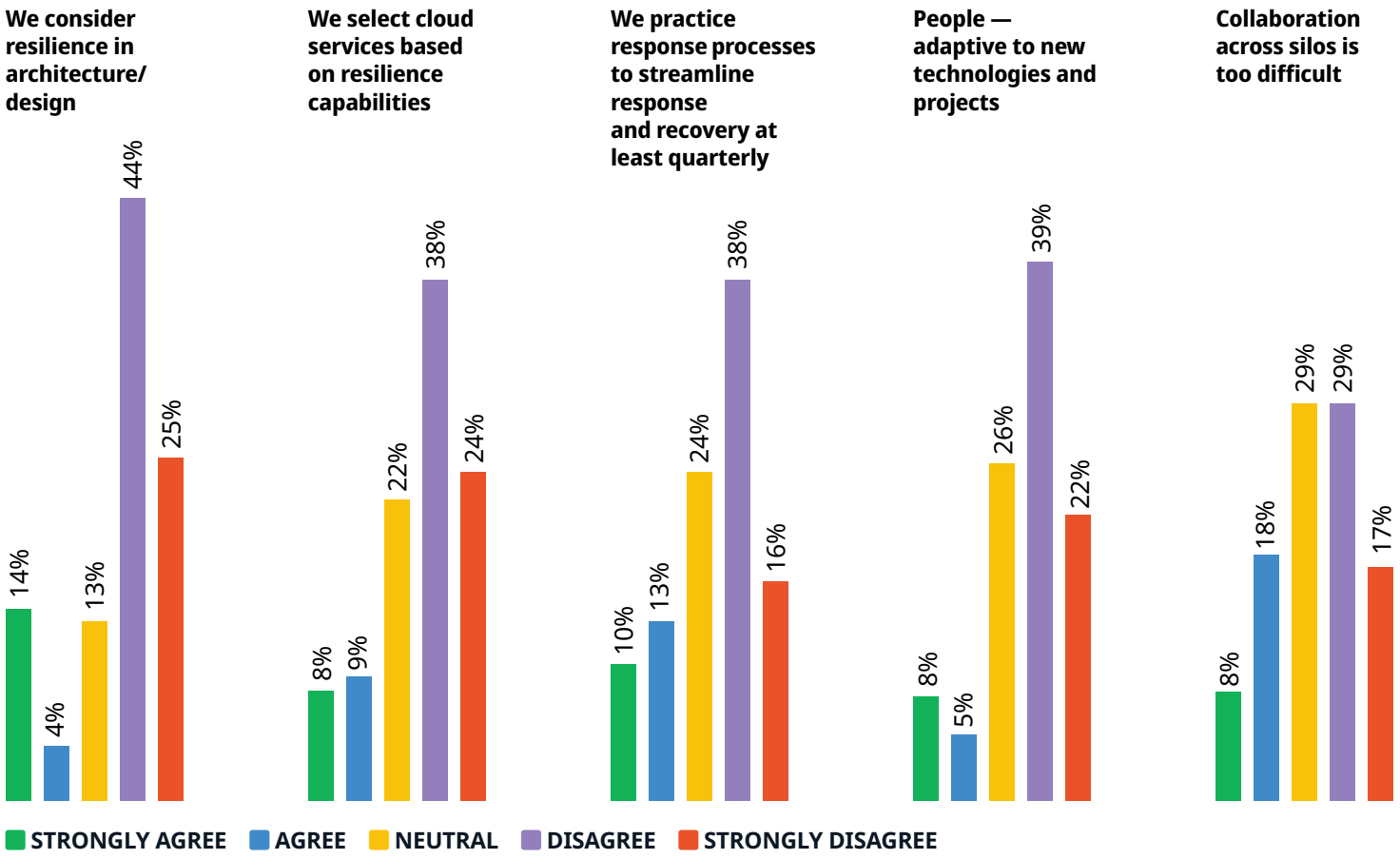
Processes Underlying a Resilient Organization

The increasing complexity of the macro and digital business environment has made it necessary to adopt truly cross-functional processes. With an ever-growing multitude of data sources, applications, tools and integrations, it's become clear that cross-functional collaboration needs to be expanded across both security and observability. The metaphorical "walls" that have traditionally separated security from IT operations and other important segments of the organization must be dismantled. Leadership roles, such as CIOs, CTOs and CISOs, are now converging and their functions are no longer distinct silos but overlapping and interdependent domains.

With the right tools and experts, cross-functional collaboration can knit formerly isolated functions into a cohesive flow of information and work, resulting in outcomes that benefit both customers and the organization as a whole. Concepts such as a 'Center of Excellence' can provide a foundation for alignment and collaboration, offering shared services spanning across business verticals based on insights and data. When internal expertise isn't sufficient to break down silos and create cross functional processes, external strategic partners and advisors who see these problems every day can step in to help organizations overcome seemingly insurmountable challenges.

An example of where cross-functional alignment is mandatory is regulatory reporting and compliance. Regulatory scrutiny, championed by bodies like the SEC, can no longer be an afterthought for business and IT strategies. It mandates a holistic, cross-functional view of the organization and a myriad of processes. Few processes are higher profile than timely breach disclosure. Should any incident or issue materially impact the business, it's a non-negotiable duty to apprise shareholders quickly and effectively.

Do you agree or disagree with the following statements about resilience?



As you can see from the chart above, according to the recent Techstrong Research poll, we've got a lot of work to do to really embed the concept of resilience into business processes. For example, 69% of respondents don't consider resilience in architecture/design, 62% don't select cloud services based on resilience capabilities and 61% don't believe their people are adaptive to new technologies and projects. That's problematic when you want to really embrace organizational resilience.

Yet, organizations have already embraced a practical embodiment of this ideology—DevOps. With its inherent emphasis on cross-functional workflows, DevOps underscores the need to embed security within software development, infrastructure and operational frameworks. The mandate is clear: Innovate while safeguarding data. So organizations do have the capability to embrace resilience, but they may not recognize it yet.

However, it's vital to recognize the limitations. A DevOps team, despite its prowess, may lack intricate knowledge of security nuances. For instance, scenarios like a financially motivated 'Tempest Strawberry' attack on the organization might escape the scrutiny of DevOps but would immediately raise alarms within the security group, given the potential ramifications. Additionally, external guidance from service providers and governmental bodies, such as the Cybersecurity and Infrastructure Security Agency (CISA), remains invaluable to ensure activity within the broader business community is considered.

Leading organizations have addressed these issues by obliterating these silos, fostering productive collaboration between operational functions, redesigned processes to leverage shared data sources of truth. This alignment, founded on the principles of transparency, agility and shared expertise, paves the way for resilience—allowing the organization to adapt and prosper irrespective of the challenges it confronts.

The Role of Technology in a Resilient Organization

Software is purchased for one reason only—to address business needs. Such software often aims to simplify tasks, align workstreams,expedite processes and protect the organization's critical data and resources. In essence, teams and individuals seek tools that eliminate hurdles in their workflow. By doing so, the software enables the construction of robust, resilient systems.

However, with the advent of multi-cloud platforms, there's a looming danger of reverting back to the age of silos. What's imperative now is an aggregation point—a space where data from various sources is consolidated, offering a comprehensive view of the environment. And more tools are added seemingly every day, causing clutter and further complicating the technology environment. Streamlining is essential.

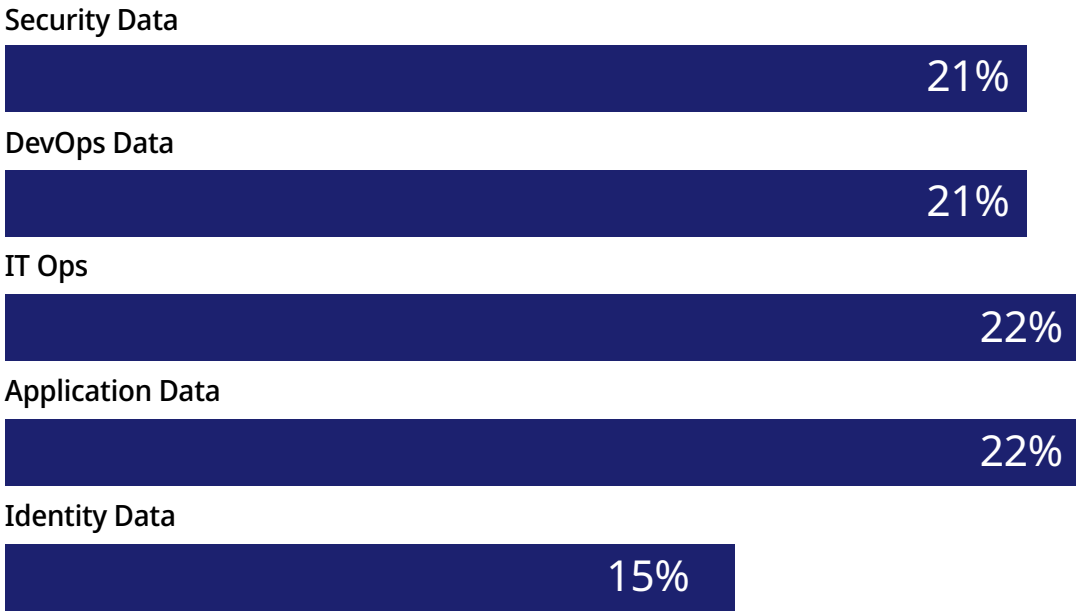
Historically, technology has always been a tug-of-war between innovators and disruptors. This relentless back and forth, though quicker now, remains fundamentally unchanged. Consider generative AI, a groundbreaking innovation. Yet, despite its game changing potential, it arrives with age-old questions: How does one navigate its associated risks? How is its intellectual property secured? Can the results be trusted? Given that resilience implies an inherent flexibility to adapt—technology solutions must be malleable to evolving business needs, emerging security threats or the ever-changing technology environment.

Central to this discourse is the need for a machine data "system of record." This system would serve as the definitive source of security and operational data, and its efficacy hinges on the consistent collection and analysis of the right data for each process and use case. This is where platforms like Splunk come into play, bridging the gap between IT operations, security and the growing world of DevOps. Their role? Ensuring a seamless digital business operation and flow of information that fosters resilience.

Referring back to the Techstrong Research poll, we can see below that many data sources are aggregated for operational processes, including application data (22% of respondents), IT Ops (22%), DevOps and security data (21% each). Interestingly, only 15% leverage identity data, which can provide significant intelligence about access before, during and after an attack.

Initiating this journey toward resilience means harnessing technology adeptly, tweaking the monitoring ecosystem, and focusing on the continual acquisition of relevant insights. Given the prevalent skills deficit and talent drought, external technology experts stand as pivotal assets. They guide organizations, steering them towards a path where resilience isn't just an ideal—it's a reality.

Do you aggregate and leverage the following data/telemetry sources in your operational processes?



"Resilience is bringing business and cybersecurity leaders together in part by the threats like ransomware that consistently and continually impact every aspect of a business."

RYAN KOVAR
DISTINGUISHED SECURITY STRATEGIST AND LEADER OF SURGE SPLUNK

COMMISSIONED BY splunk>

Summary

In the modern business landscape, resilience is a critical success factor. This eBook delineates the foundational tenets of building a resilient organization, starting with the pivotal role of leadership. Leaders don't merely guide; they craft compelling visions that energize the organization and make clear the importance of each individual's contribution. Their foresight recognizes the value of both traditional and non-conventional, internal and external skill sets, especially as digital transformation intensifies the demands on IT and security sectors.

Next is the critical importance of cross-functional processes. By embracing models like DevOps, organizations can champion collaboration, improve security and innovate quickly and effectively. Simultaneously, technology stands as both an enabler to catalyze action and a challenge to be managed. While software streamlines business functions and multi-cloud environments offer expansive platforming options, the threat of reverting to isolated silos and unaligned functions persists. Solutions like Splunk serve as an integrator, bridging gaps and serving as the source of truth, all of which bolsters resilience.

Yet, amidst this dance of leadership, processes and technology, the real champions are people. And it's always been this way. They are the linchpin, making innovation, competitive advantage and resilience possible. Your people navigate the complexities and rapid shifts of today's business environment, not tools. For organizations to truly flourish, they must cultivate environments where individuals can learn, grow and engage with external partners to build expertise in new domains, accelerate time to value and deploy new capabilities that move the needle for business. In essence, resilience is not just about robust systems or cutting-edge tech—it's about empowering the people who make it all possible.