IT STRADDLES TRANSFORMATION AND OPERATIONAL COMMITMENTS

From back offices, basements, and other bastions of anonymity, IT has been catapulted into the spotlight. As digital transformation sweeps through every industry, business leaders are realizing the central role that IT must play in improving top-line growth through new revenue opportunities and through better customer and partner engagement. Critical to new modes of doing business—in the cloud, using mobile devices, and increasingly through machine-learning and artificial intelligence (AI) applications—IT leaders and teams have a foundational role to play in this transition.

And yet IT teams remain largely engaged (and often overburdened) in the trenches. CEOs and the lines of business rely on IT for operational efficiency to ensure system performance, availability, and quality of service. They also expect IT to protect corporate network and data assets within a changing threat landscape, while complying with myriad, evolving standards and regulations. All despite a complex set of components that have accumulated (and aged) over time.

Not surprisingly, in its annual CIO survey, IDG found that 72% of respondents struggle to juggle business innovation and operational excellence requirements. And the number of challenges isn’t decreasing; 87% said they are increasing.¹

Acquiring skilled talent in all the areas IT needs to address, especially given staff and budget constraints, is getting more difficult. For midsize businesses, it may even be out of the question. To overcome these limitations, IT leaders must continue to meet day-to-day expectations and fulfill their new strategic mandates, while dealing with three root causes of the conundrum facing their IT teams.
UNPACKING THE TRIPLE BURDEN OF SMALLER IT TEAMS

As they consider how to support the growth and digitization of their businesses, IT leaders in midsize organizations are increasingly challenged on three fronts: limited and overworked human capital, fragmented and siloed technology, and accelerating security threats and demands.

IT VERSATILITY HINDERS GROWTH AND DIGITAL TRANSFORMATION

For IT leaders and their IT teams, versatility rules. Job roles must be defined broadly, not only because the organization is limited in size but also because they are in growth mode, expanding into new areas and tapping digital transformation ahead of a future return.

Versatility in IT, however, can thwart efforts to achieve expert-level proficiency. With the growing complexity of compute, storage, and networking technology—including the introduction of artificial intelligence—proficiency requires ongoing education and expertise in new technologies. Without such specialization, IT staff may not know how to extract the most value from technology investments or use them to their business’s greatest competitive advantage.

Specialization is also crucial—and scarce—in security and compliance management skills. Lack of expertise in these areas might result not just in failure to optimally utilize systems but also in a failure to prevent security breaches that can be very costly. For example, 22% of IT leaders in an ESG survey link factors that contributed to past security incidents to insufficient security skills. Midmarket organizations may consider hiring more security staff, or even adding outsourced security services, but these hires are tough to find (and costly if found) and often are out of reach given limited budgets. If IT leaders want to be seen as partners in strategic decision-making, they need to find time for staff to expand their skills.

They also need to find time to plan strategic improvements to corporate systems. Indeed, CIOs in larger enterprises are carving out the necessary hours. For those in midsize organizations, it may still be a luxury. It is difficult, for example, to justify spending time exploring how applications may be rolled out faster using cloud platforms when every staff member is fully booked supporting existing applications and systems. Indeed, 67% of cybersecurity professionals claim they are too busy with their day-to-day jobs to keep up with skills development and training.

However, giving in to these time pressures can result in staff constantly working in reactive, rather than proactive, mode. If IT security staff have their hands full rushing around in response to every unplanned IT or security issue, it’s hard to sit back and think about how to reduce the risk of future attacks and mitigate their impact.

FRANKENSTEIN IT CREATES A SYSTEMS MANAGEMENT MONSTER

In most cases, this overload on IT security staff is connected to amassing a hodgepodge of hardware, software, networking and security equipment, and services—some purchased through IT, some through the lines of business, and some by individuals who bring their own devices to work. Running a “Frankenstein-style” IT infrastructure—comprising disparate and isolated equipment, processes, and controls—requires staff to navigate a dizzying array of management interfaces, command sets, and response workflows.

Even purchasing suites of products from vendors in a technology area—endpoint, email, network, and so forth—requires significant monitoring and upkeep. Indeed, in a new survey of small and midsize businesses, the cost of ongoing maintenance, staff time needed to operate and maintain, and complexity were among the top reasons for a lower-than-expected ROI on technology.

At some point, most IT leaders reach their limit of technology and skills diversification, and they begin consolidating skill sets and technology platforms. As part of this process, they must rethink their IT and security architectures and how the individual pieces fit into a larger whole. This necessitates integrated product sets and offerings that use familiar interfaces that do not require wholesale retraining of staff.

IT leaders also opt for mature products with well-developed certification programs, with the objective of increasing the ease of finding appropriately skilled IT staff when required. Even so, they still face a range of technology stacks across IT, security, and compliance functions that require monitoring, maintenance, upgrades, and issue resolution. All of this adds up to valuable time spent running core infrastructure that cannot be spent on other business initiatives, such as new technology investigation, planning, and deployment.
SECFORINET

SECURITY IS BECOMING MORE COMPLEX AND DIFFICULT

Of all the responsibilities of the IT department, digital security is often at the top of the list. Security is nothing new to IT teams. They have always been responsible for a variety of security tasks, such as patching servers, managing digital certificates, maintaining firewalls, cleaning infected endpoints, and educating users on password protection and other facets of cyber hygiene.

What has changed in the past few years is the level of attention that cybersecurity has received from business leaders and shareholders, their interest continually stoked by recurring revelations about breaches and failures. The same people who seek the rewards of digital transformation—improved customer insight, streamlined supply chains, acceleration of business processes, and greater customer engagement—expect it all to be secure.

Larger organizations are responding to this change by creating dedicated security teams and end-user security awareness programs under a chief information security officer (CISO) or chief security officer (CSO). In midsize companies, IT leaders continue to shoulder the burden of the organization’s digital transformation, and the security thereof, without similar tools or end-user training.

However, it doesn’t take a large number of security-unaware employees to cause critical harm. Even one untrained employee who falls prey to a phishing scheme or works from an unsecure public network can wreak havoc on the business. And midsize businesses are less likely to be prepared. To wit: 65% of business respondents said that if their employer had a password policy, it was not enforced.

The predominant concern with security in this era of digital transformation is the expansion of the attack surface. Data is constantly in motion, traversing enterprise and cloud domains and reaching far-flung mobile devices and Internet of Things (IoT) components. This expanded attack surface provides cybercriminals with a much larger array of target vulnerabilities, making the attack vectors considerably larger and more dynamic.

As the variety, volume, and velocity of threats grow, the windows of action for the IT security staff shrink. There is less time to identify new threats, less time to detect intrusions, and less time to remediate before the organization is harmed. The race is on, not only to prevent, detect, and respond to threats but also to monitor and report on security events for compliance with a growing body of industry and government regulations.

22% of IT leaders link factors that contributed to past security incidents to insufficient security skills.
INCREASING THE VALUE OF HUMAN CONTRIBUTION

Digital transformation will continue to breed complexity, and technology can be seen as a complicating, as well as an enabling, factor. A pragmatic option for IT leaders would be to view technology as a tool to transform their roles, as well as the roles of their teams. They may choose from a variety of approaches:

- By automating operational tasks and reserving a portion of staff time to the role of strategy-focused specialists, IT leaders can maintain the uptime requirements of today’s business while also redesigning IT architectures for the future.
- By deploying technology that proactively identifies and monitors systems for indications of impending failure or emerging security compromise, and rapidly responds to them, IT leaders can avoid the fire drills that come with downtime.
- By selecting intelligent systems that come with out-of-the-box best practice configurations, ready-to-go reports, and more, midsize organizations can meet new security and compliance challenges with confidence.

Leveraging new technologies that automatically and proactively identify, monitor, alert, and guide responses to resolve systems and security issues frees up staff time for higher-value activities related to investigating, planning, and delivering new revenue-generating and even business-changing services built on new technologies. This is the essence of the value that IT leaders in midsize organizations can offer, as they take their place at the executive table.

3. Ibid.