ZOHO

Balancing the strengths and vulnerabilities of emerging enterprise technology

Cyber resilience series, Q3 2024

Continually refining strategies for the adoption and use of new technology helps organizations maximize their investments—and mitigate evolving threats.

Artificial intelligence, IoT, and other emerging technologies have accelerated innovation and enabled striking process transformations across industries. However, the rapid adoption of new technologies has also given rise to cyber security threats that are both novel and profound.

Many executives are still struggling to understand the risks associated with cutting-edge technologies (such as AI, ML, and quantum computing)[1], although most acknowledge that those risks are significant. A staggering 96% of executives fear that generative AI has made their companies vulnerable to a breach within the next three years[2].

Staying ahead of cyber threats has always required a substantial investment of funds and resources. Now, in an era of smarter, more capable threat actors, business leaders are beginning to question whether the costs are sustainable[3]. In the most cyber resilient organizations, executives are shifting focus from threat prevention to the development of agile strategies for incident response. But for these strategies to be effective, an org-wide culture of knowledge sharing and ongoing stakeholder education is essential.

> *Data breaches caused the exposure of 22 billion records in 2022, despite $150 billion in cyber security investments the previous year.*
>
> [PwC, 2024]

A purpose-built tech stack

In 2023, 89% of org leaders planned to increase their technology budgets, with more than half investing in AI and 46% allocating funds toward IoT[4]. With each new implementation opening businesses up to a range of new risks, rigorous standards for software selection have become more crucial than ever.

Before expanding their tech stacks, executives should aim to identify the precise areas of business they intend to

[1] PwC, 2023 | [2] IBM, 2024 | [3] World Economic Forum, 2022

[4] PwC, 2023

improve and determine whether a given solution will support the necessary growth. This will likely require collaboration across departments, and consultations with stakeholders who can highlight processes and initiatives that aren't supported by existing systems.

Top 5 tech investment priorities in 2023

- 58% - AI
- 46%- IoT
- 35% - Virtual reality
- 34% Augmented reality
- 33% - Advanced robotics

- PwC, 2023

At the most basic level, a lean, purpose-built tech stack presents fewer vulnerabilities for malicious actors to exploit. But it is also more easily monitored, enabling IT and security teams to isolate threats when they emerge, and deploy robust response protocols across the organization.

Unfortunately, even businesses that set out to limit their implementations may struggle to do so. A growing number of employees are turning to unsanctioned applications[5] to address evolving market demands and more complex job responsibilities. To minimize the usage (and risks) of Shadow IT, a shift from one-off applications to more comprehensive software suites may be necessary. Through a unified, integrated application ecosystem, leadership can achieve greater degrees of trackability and transparency across the organization.

After the initial application selection process, ongoing feedback and evaluation is often essential. By routinely assessing implemented solutions, and the degree to which they support organizational goals, business leaders can more easily maintain a streamlined and effective tech stack.

[5] Businesswire, 2022

Stakeholder training and education

With 82% of data breaches linked to human error[6], an organization's employees can have a powerful impact on cyber security and resilience. It is therefore crucial to ensure that stakeholders across functions are in sync about how technology should be used and how threats should be managed. This is more easily achieved when education surrounding new technology extends past the software onboarding period and becomes a routine feature of organizational culture.

Ideally, training will equip employees with strategies for identifying and responding to modern cyber threats. Employees should, for example, be able to identify an AI-generated phishing email or recognize signs of poisoning in the company's ML models. The most impactful training programs will also familiarize employees with internal protocols for incident response, exploring the granular roles they will be expected to perform in the event of a breach.

Whether a business chooses to relay this information through webinars, in-person training sessions, or a regularly-updated knowledge base, it is important to ensure that the results of its efforts are measurable. This requirement is often overlooked—A government study of UK businesses found that only 19% had actually tested their employees' cyber attack responses[7].

With a 360-degree view of internal processes, business leaders can quickly test and assess their incident response strategies. Zoho Analytics helps you evaluate execution at the organizational, departmental, and individual level.

Businesses that possess the necessary resources may benefit from designating a team to assess employee reactions to signs of a data breach or external tampering with company software. At the very least, org leaders should monitor incidents over time and track trends in employee responses. Through these efforts, they can address any clear gaps in stakeholder knowledge and take the necessary action to prevent repeat incidents.

[6] Verizon, 2022

[7] CRC Northwest, 2022

A balanced approach to modern technology

Despite the associated risks, refusal to adopt emerging technology is not a viable option for modern businesses. And paradoxically, it may not be the most secure option either. When implemented and managed strategically, many cutting-edge technologies can actually improve existing security systems and processes.

> *There is a critical difference between embracing a new solution and trusting it implicitly. Companies don't need to fear emerging technology—they simply need to remain vigilant of the risks and be open to adjusting their strategies as those risks evolve.*

Shailesh Davey
Chief Technology Officer at Zoho

SSO, for example, can enhance security for routine processes by bringing an extra layer of protection to the apps employees use every day. It also reduces password fatigue, which can cost businesses as much as $670.36 in productivity per employee each year[8]. Meanwhile, AI can be used to monitor vast amounts of data for anomalies—and when companies opt for embeddable AI tools, they benefit from features like data analysis and consolidation, while avoiding the risks of sharing their data with multiple third-parties.

Zoho Zia

Zia, Zoho's AI assistant, brings diverse functionality to your apps while keeping your data safe within the Zoho ecosystem.

Whether an organization can deploy new technology in a way that supports, rather than detracts, from its security goals largely hinges on its willingness to evolve usage policies and training strategies as the threat landscape demands. In the near future, organizations that capitalize on the strengths of new technology without becoming complacent in its performance will be in the best position to remain competitive, profitable, and resilient.

[8] Beyond Identity, 2022