ZOHO

Beyond tech talent:

Strategies for building a cyber resilient workforce

Cyber resilience series, Q3 2024

As cyber threats become more complex, executives are applying a range of new strategies to cultivate security-conscious employees.

In an era of evolving threats, forward-thinking organizations are focused on cultivating cyber resilient employees—individuals with the expertise to identify threats promptly and the skills to respond using available company resources. But as tech talent shortages persist, and new threats continue to emerge, many businesses are struggling to build workforces that support their cyber resilience goals. More than 90% of executives have observed organizational skill gaps relating to cloud computing security, management of AI and ML systems, and zero-trust implementation[1].

59% of business leaders and **64%** of cyber leaders rank talent recruitment and retention as a key challenge for managing cyber resilience.

[World Economic Forum, 2023]

Businesses that fail to address these gaps may open themselves up to critical consequences ranging from regulatory noncompliance to the loss of consumer trust. To prevent irreversible damage—and ensure the structured and timely deployment of incident response protocols—proactive executives are reevaluating the skills that are most essential to cyber resilience, and reconsidering the ways they've traditionally populated tech roles within their companies.

Defining essential skills

When business systems are compromised, employees who can respond to technological disruptions by quickly pivoting to manual processes, communicate status updates across departments, and collaborate with regulatory bodies are often invaluable. Just as tech experts are essential for bringing systems back online, critical problem solvers and skilled communicators can be essential for maintaining business continuity. With this in mind, a growing

[1] ISC2, 2023

number of employers are looking beyond IT talent to recruit or nurture candidates with a range of soft skills.

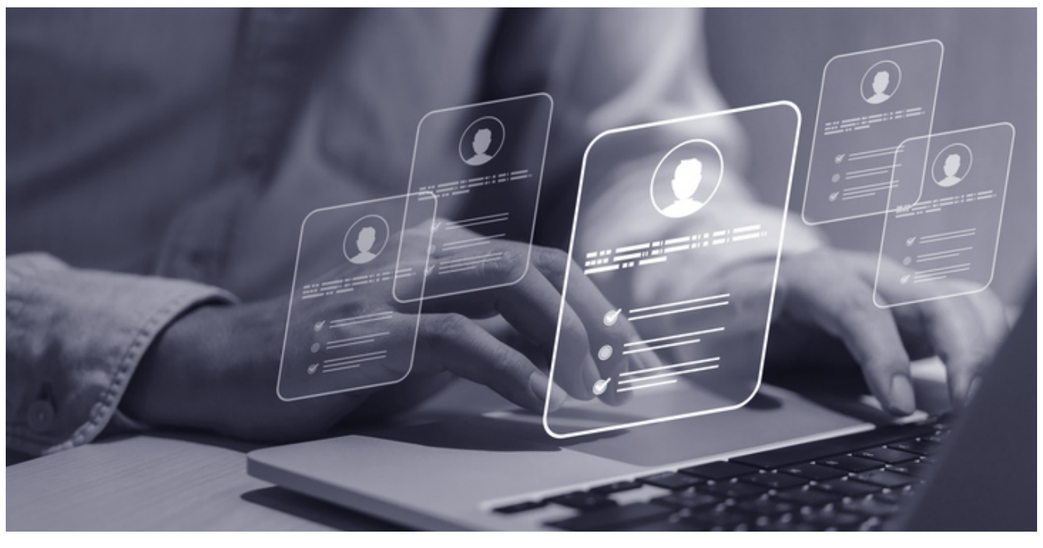
> *Prompt troubleshooting is crucial during a cyber incident—but it's only the first step toward business recovery. Complex threats demand a comprehensive response, which will require a diverse range of employee skillsets.*
>
> 
>
> **Shailesh Davey**
> Chief Technology Officer at Zoho

The most crucial employee skillsets often vary between organizations and industries. In the finance sector, for example, familiarity with relevant laws and experience working with government regulators can help protect an organization from compliance violations during a disruption. In retail, executives may prioritize swift and transparent customer communication.

As part of their cyber resilience strategies, organizations should aim to determine which skills will help them achieve their highest-priority needs in the event of an attack, breach, or similar incident. Defining these skills can help shape future talent recruitment efforts, and sharpen the focus of employee training programs. From an employee's perspective, it can bring greater clarity to the company's incident response protocols by emphasizing the strengths and talents each team is expected to contribute.

Reimagining the recruitment process

Across industries, employers are casting a wider net in terms of candidate experience and education. More than half have expressed a willingness to provide on-the-job training to high-aptitude candidates, and to create opportunities for the growth of entry-level employees[2]. This practice can give org leaders an opportunity to work with employees early in their cyber security



[2] ISC2, 2023

journeys, and to shape their training around the company's core values and philosophies.

90%

of org leaders would be willing to pay for employee cyber security certifications.

[Fortinet, 2023]

Ideally, flexible hiring criteria will also make space for a broader range of backgrounds and perspectives within the organization. In the long term, this could result in more innovative and effective ways of addressing evolving threats. But there are short-term benefits to be gained as well.

A diversity of skillsets can prove invaluable in the event of a cyber incident. For example, an IT employee with communications experience can be deployed to relay details about patches or repairs to stakeholders across the organization. Ultimately, the more talents a company can leverage during an attack, the more agile and comprehensive its response will be.

Designing trackable training programs

A recent Cisco report found that businesses are 27% more resilient when their employees are confident in the company's policies, procedures, and documentation[3]. But even in security-conscious organizations, employees often struggle to transfer cyber security education to daily work activities. Nearly half of executives still worry that their employees wouldn't know how to respond to a phishing email, despite years of security awareness training[4].

Zoho supports org-wide transparency, communication, and trackability, so you can take data-based action toward your company's training goals.

Their concern highlights the importance of looking beyond the initial design of a skills development program to track its outcomes over time. Testing and benchmarking help

[3] Cisco, 2022 | [4] Business Wire, 2023

org leaders identify where their security training is successful and where it breaks down. Using this information, they can design more relevant and effective programs based on the skills required for various employee roles.

Establishing trackable training processes may require an investment of time and effort upfront, but it is an often-crucial step toward long-term business health. The threats facing businesses are increasing in both scope and complexity; meeting them head on requires a cross-organizational commitment to data-based strategies. In many cases, an investment in accurate and reliable training data is the key to taking cyber security from theory to practice and taking an organization from cyber aware to cyber resilient.

Why Zoho for Enterprise?

Proven software, customer commitment, tremendous value.

Scalability & Reliability

Zoho for Enterprise reduces the cost of infrastructure, unifies existing apps, and solves complex business problems for increased enterprise fitness, resilience, and scalability.

Customization & Extensibility

Through granular customizations and powerful in-house developer platforms, Zoho lets you orchestrate workflows, streamline data management, and deploy world-class solutions at scale.

Security & Privacy

From owning our own data centers to GDPR compliance features, Zoho enables enterprise organizations to focus on core business priorities, rather than data management.

Enterprise Services

From data migration to consultation and implementation, our team is armed with the in-depth product knowledge and industry expertise to meet your unique technical requirements.

Are you ready to transform your organization?

We’re here to help. Have a 15-minute, no-obligation call with one of our **Business Architects** to get all your questions answered.

Find us at **zoho.com/enterprise.** |