Cyber resilience:

Fortifying business operations in an era of unprecedented threats

Cyber resilience series, Q3 2024

The scale and frequency of cyber attacks are increasing rapidly. Strategies for normalizing operations and regaining consumer trust can help businesses stay viable in the worst case scenarios.

Bolstered by advancements in technology, cyber threats are becoming more complex—and more prevalent. In 2023, 82% of CEOS were anticipating a successful attack in the near future[1], and by the end of 2024, attacks on businesses are expected to cost the global economy USD $10.5 trillion[2]. With industry regulations widely pending, it has fallen to business leaders to mitigate the risks of AI, IoT, and other emerging technologies within their organizations. However, research shows that more than a third of companies lack formalized plans for risk management, and only one in four is focused on cyber resilience[3].

Top three cyber-related threats facing businesses:

- *Cloud-related threats*
- *Attacks on connected devices*
- *Hack-and-leak operations*

[PwC, 2024]

While robust security measures, formalized data governance policies, and strict vendor vetting can help protect critical business systems, the pace at which new threats are emerging has made some degree of vulnerability inevitable[4]. It is therefore crucial for organizations to develop comprehensive plans for maintaining business continuity, minimizing losses, and preserving customer relationships in the event of a damaging cyber incident.

Assess risks and prioritize systems

Restoring the organization's core business functions after an attack or breach is crucial to cyber resilience—and a predefined strategy can bring efficiency and precision to the process. Collaborating with managers and SMEs helps org leaders determine which teams are most vital for business continuity, which tools those teams require to perform their primary responsibilities, and how various cyber incidents would impact access to those tools.

[1] Tech Republic, 2023 | [2] Forbes, 2023
[3] PwC, 2024 | [4] Harvard Business Review, 2023

This type of cross-functional input gives org leaders, who traditionally benefit from a bird's-eye view of operations, a more granular understanding of core business processes. As a result, they're better positioned to make informed decisions about the allocation of IT and security resources in the event of an attack.

> *It is no longer realistic for businesses to prevent disruptions to their digital systems altogether. Rather, the goal should be to prevent a disruption to one team or function from triggering a domino effect across the organization.*

Saravanan Muthian
Chief Information Officer at Zoho

Ideally, a restoration strategy will limit downtime across the organization. However, some degree of system and departmental prioritization is essential for minimizing damage. Transparency surrounding these decisions is key, as it will give stakeholders a sense of what to expect in the immediate aftermath of an incident, minimizing frustration and friction as IT teams work to restore normal operations.

Evaluate the business ecosystem

Third-party relationships are often a necessity, but in the context of cyber resilience, they can be a source of significant vulnerability. The vast majority of executives have concerns about the cyber resilience of small and mid-sized businesses in their ecosystems, and 58% feel that their own organization is more cyber resilient than its suppliers and partners[5].

[5] World Economic Forum, 2022

This is why effective cyber resilience strategies often involve an assessment of the organization’s full business network. Evaluating the security protocols employed by vendors and partners—and their plans for recovery should those protocols fail—can limit the risk of supply chain disruptions and help contain damages within the company that suffered the initial breach.

98%

of organizations have a relationship with one or more vendors that have experienced a data breach in the last two years.

[Harvard Business Review, 2024]

The most thorough organizations incorporate cyber resilience measures into their terms and conditions for business relationships. This could involve outlining protocols for how the organization’s data will be handled, and when and how its members will be informed of an incident.

While this level of diligence may extend the vetting process, it is often essential for tightening control over external activities that could impact internal processes, as well as the primary organization’s revenue and reputation.

Develop and disseminate an incident response plan

While shoring up vulnerabilities and getting systems back online are primary goals after a cyber incident, additional measures are often required for successful business recovery. A formalized incident response plan, which defines roles across the organization, can have a powerful impact on cyber resilience. Such plans (when implemented alongside a designated incident response team) have been known to reduce the cost of a cyber incident by $2.66 million[6].

An effective emergency response requires prompt action and accountability on the part of all stakeholders. The trackability supported by Zoho’s applications helps ensure that org members are taking appropriate actions at appropriate times.

[6] IBM, 2022

The most crucial steps and responsibilities for business recovery often vary by industry. However, all businesses can benefit from assigning team members to communicate status updates across the organization, draft correspondence to affected customers, and ensure compliance with legal requirements.

Employee training sessions or formal team meetings can help businesses familiarize employees with their assigned roles. Essential information can also be conveyed through a handbook or knowledge base that employees can access on demand. However the company chooses to disseminate its incident response plans, clear and proactive communication surrounding its expectations for stakeholders helps ensure that all teams are well prepared should a breach or attack occur.

Take steps toward continuous improvement

Alongside powerful advantages, emerging technology has given rise to more persistent and pernicious threats. Staying ahead of new threats may not always be possible, but defined protocols for identification and documentation can be pivotal for preventing similar incidents in the future.

Zoho helps enhance transparency and communication across your application ecosystem—so your teams are always in the loop about breaches, patches, and plans for the future.

Ultimately, cyber resilience can never guarantee protection from malicious actors—but it can prepare businesses to learn from their vulnerabilities. When businesses can demonstrate an understanding of their security limitations, and a commitment to continual improvement, they are better positioned to earn the trust and confidence of both internal and external stakeholders going forward.

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.** | ZOHO