EINPRESSWIRE

Keeper Security Releases Cybersecurity Disasters Survey: Incident Reporting & Disclosure

Research finds 40% of organisations have experienced a cybersecurity incident, yet 48% did not disclose those incidents to the appropriate authorities

LONDON, UNITED KINGDOM, September 26, 2023 / EINPresswire.com/ -- Keeper Security, the leading provider of cloud-based zero-trust and zero-knowledge cybersecurity software protecting passwords, passkeys, secrets, connections and privileged access, today released findings of its Cybersecurity Disasters Survey: Incident Reporting & Disclosure. The findings reveal widespread shortcomings in reporting cybersecurity attacks and breaches, both to internal leadership and external authorities.

> The numbers point to a need for organisations to make significant cultural changes around cybersecurity, which is a shared responsibility.”
>
> *Darren Guccione, CEO and co-founder of Keeper Security.*

Cybersecurity incident reporting falls short
Keeper's survey shows a lack of policies for cyber incident reporting, despite the growing risk of cyberthreats. Nearly three-in-four respondents (74%) said they were concerned about a cybersecurity disaster impacting their organisation, and 40% of respondents said their organisation has experienced some type of cyber disaster. Despite these concerns, reporting breaches to a company’s leadership team and to proper authorities is often avoided.

External reporting: 48% of respondents were aware of a cybersecurity attack that their organisation did not report to the appropriate external authorities.
Internal reporting: 41% of cyberattacks were not disclosed to internal leadership.

Incident reporting is low; guilt is high

Of those who admit they've failed to report an attack or breach to leadership, 75% said they felt "guilty" for not doing so. Fear, forgetfulness, misunderstanding and poor corporate cyber-culture all contribute to widespread underreporting of security breaches. The top three reasons why an attack or breach was not reported to leadership:
Fear of repercussion (43%)
Thinking reporting was unnecessary (36%)
Forgetting to report the incident (32%)

Organisational cultures do not prioritise cybersecurity

Despite the potential for long-term financial and reputational consequences, poor disclosure and transparency practices prevailed. Failure to report was largely based on the fear of short-term harm to the organisation's reputation (43%) and potential for financial impacts (40%).

Respondents also cited a strong need for senior leadership to demonstrate a vested interest in the organisation's cyber posture, and stand beside their IT and security teams, providing the resources and support they need to report and respond to attacks.
A combined 48% of respondents did not think leadership would care about a cyberattack (25%) nor would respond (23%).
Nearly one-fourth of all respondents (22%) said their organisations had "no system in place" to report breaches to leadership.
"The numbers point to a need for organisations to make significant cultural changes around cybersecurity, which is a shared responsibility," said Darren Guccione, CEO and co-founder of Keeper Security. "Accountability starts at the top, and leadership must create a corporate culture that prioritises cybersecurity incident reporting, otherwise they will open themselves up to legal liabilities and costly financial penalties, and place employees, customers, stakeholders and partners at risk."

Best practices

In the current high-risk security climate it's critical for enterprises to encourage transparency and honesty in cyber disaster reporting, and to adopt best practices, policies and procedures to safeguard against ongoing threats. Some of the most effective ways to prevent cyber disasters, including password and privileged access management, are the simplest, yet most critical to protecting organisations.

Download the full report here to learn more.

Methodology

Keeper commissioned an independent research firm to survey 400 IT and security leaders in North America and Europe to gain their insights on cyber disaster incidents, reporting and recovery. An independent research firm conducted the survey in 2023. Keeper characterises 'cybersecurity disasters' as any event that severely impacts the confidentiality, integrity or availability of an information system.

About Keeper Security
Keeper Security is transforming cybersecurity for organisations around the world with next-generation privileged access management. Keeper's zero-trust and zero-knowledge cybersecurity solutions are FedRAMP and StateRAMP Authorised, FIPS 140-2 validated, as well as SOC 2 and ISO 27001 certified. Keeper deploys in minutes, not months, and seamlessly integrates with any tech stack to prevent breaches, reduce help desk costs and ensure compliance. Trusted by thousands of organisations to protect every user on every device, Keeper is the industry leader for best-in-class password and passkey management, secrets management, privileged access, secure remote access and encrypted messaging. Learn more at KeeperSecurity.com.

Charley Nash
Eskenzi PR
charley@eskenzipr.com