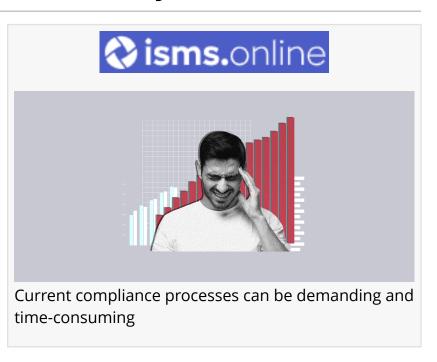# 100% of U.S. businesses surveyed incur fines for data breaches or violation of data protection rules over the last year

Only 16% of businesses cite main motivation for compliance and robust information security is to avoid fines and penalties, according to ISMS.online research

NEW YORK, NY, USA, June 26, 2024 /EINPresswire.com/ -- Over the past year, a full 100% of U.S. businesses surveyed have incurred fines for data breaches or violation of data protection rules, according to research into the ['State of Information Security'](#), by [ISMS.online,](#) the auditor approved compliance platform. The findings highlight the complexity of mounting

Current compliance processes can be demanding and time-consuming

legislation and the challenges of meeting multiple compliance requirements.

As data breaches continue to surge, government entities and trade bodies are trying to meet these challenges with updates and implementation of regulations and compliance mandates.

> **"**
>
> Businesses are failing to recognize that compliance & security come hand-in-hand, & if they want to protect their information, meeting regulatory requirements will put them in a good position to do so"
>
> *Luke Dash, CEO, ISMS.online*

Equally, businesses must continue to prioritize cybersecurity, with many responding by taking the discipline to the board room. Gartner anticipates that by 2026, [70% of boards](#) will include one member with cybersecurity expertise in a move to help defend not only against attacks but reputational damage, as well. Many organizations have continued to invest either the same amount or more in cybersecurity over the last 12 months in anticipation of both the sophistication and frequency of anticipated threats.

Despite continued investment, ISMS.online's survey of 518

information security professionals in the U.S. found that businesses are still falling foul to data breaches. The average U.S. fine for data breaches and violation of data protection rules now amounts to $317,062. That said, only 16% of businesses cite that their main motivation for compliance and robust information security is to avoid fines and penalties. The need to remain competitive (36%), increased customer demand (33%), and protecting customer information (33%) rank as the top three motivations.

"Businesses are failing to recognize that compliance and security come hand-in-hand, and if they want to protect their information, meeting regulatory requirements will put them in a good position to do so," said Luke Dash, CEO of ISMS.online. "It also demonstrates their willingness to put customer data first, which enhances loyalty, reputation and competitiveness as well as easing financial repercussions."

This is supported by the findings given that a mere 19% of respondents believe that complying to avoid fines and penalties has provided a decent return on their investment in information security compliance programs. The majority (33%) cite that the best ROI for compliance initiatives is appealing more to investors looking for companies with low cyber risk.

Dash continued, "The landscape is certainly changing when it comes to compliance and fines. It is staggering to see that all of the businesses surveyed have received fines over the past 12 months, yet it seems that these penalties are now seen as a small part of the compliance story."

"Businesses previously saw compliance as a way to sidestep hefty fines and negative publicity, however as our research shows, competitive advantage, reputation and protecting information are now seen as the main benefits of compliance," Dash added.

Positively, businesses recognize that building effective information security foundations is essential for compliance, and it is encouraging to see that 51% of the U.S. ISMS.online survey respondents noted that their businesses plan to increase their information security budget by up to 25% in the coming year to do so. This provides critical assurances to customers, shareholders and regulators.

The research also found that current compliance processes can be demanding and time-consuming with over 60% citing that it took between 6-18 months to meet compliance with CCPA and other U.S. state privacy laws alone. In fact, 6-18 months was a sweet spot for many American companies to meet a host of regulations, including HIPAA (56%), PCI-DDS (54%) and SOC2 (57%).

"This is just a snapshot of the legislation businesses are facing and these rising regulatory fines, as highlighted by the ISMS.online research, prove there's still some way to go. But compliance doesn't need to be as onerous. As auditors, it's our job to identify conformity with standards and, therefore, aid businesses in meeting the mounting requirements within these to help them reduce the risk of a breach.

"There are solutions now that can streamline and automate these conformity audits, reducing manual tasks and enabling successful audit engagements. Being able to eliminate the frustration of sorting through diverse and complex systems and making audits more straightforward could be the difference between saving thousands or losing hundreds of thousands and your reputation to boot," said Warwick Tams, Head of Sales - Alcumus ISOQAR.

-ends-

About ISMS.online
ISMS.online is revolutionizing the way businesses across the globe handle data privacy and information security compliance. The cutting-edge SaaS platform provides a comprehensive roadmap to robust and scalable governance, risk and compliance for organizations of all sizes and maturities. With a global presence and over 25,000 users, including enterprise clients like Moneycorp, Siemens and Ricoh, ISMS.online simplifies complex processes across over 100 standards and regulations, empowering organizations worldwide to secure and scale their compliance with ease.

Research Methodology
ISMS.online commissioned leading independent market research firm Censuswide conducted the research. With a sample of 1,526 respondents who work in information security across 10 sectors including technology, manufacturing, education, energy and utilities and healthcare in the UK (502), USA (518) and Australia (506). The research uncovers the main information security and compliance challenges facing organizations in these regions. The survey fieldwork took place between March 22, 2024 and April 2,2024.

Sarah Hawley
Origin Communications
+1 480-292-4640
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/722790486