Healthcare Facilities Need a Holistic Digital Identity Strategy, Not Uncoordinated Solutions, Imprivata Research Reveals

More than two-thirds believe identity management is important to their security strategy, yet less than half are using key identity and access management tech

WALTHAM, MASS, USA, June 29, 2022 /EINPresswire.com/ -- As more healthcare facilities take steps to strengthen their security posture, protecting against all cyber threats hasn't been easy. Healthcare facilities are struggling with implementing and enforcing holistic digital identity management strategies, according to the new Imprivata report released today titled, Security and Digital Identity in the Healthcare Industry. The findings show that despite 69% of respondents saying identity management is important to their organisation's security strategy, 51% have still experienced a security incident in the last year.

> "
> Now, healthcare enterprises must put the right technologies and processes in place to enhance security and prioritise compliance in the face of rising cyber threats"
> *Gus Malezis, CEO at Imprivata*

Imprivata, the digital identity company for mission and life-critical industries partnered with research firm WBR Insights to survey 200 security leaders at healthcare companies across the US and UK. The results shed light on how healthcare organisations like hospitals, clinics, and medical systems are approaching security risks.

Responses indicate that healthcare organisations have made significant progress in protecting their systems from cyberattacks and data breaches, with over 75% claiming their security strategy has become more robust and comprehensive. However, the fact that more than half (51%) suffered a cybersecurity incident in the past year suggests a different approach is needed to enhance security.

"Healthcare organisations have been put under significant strain, not only by the ongoing pandemic, but by the sheer volume of cyber threats that plague this sector at rates higher than any other," said Gus Malezis, CEO at Imprivata. "Now, enterprises must put the right technologies and processes in place to enhance security and prioritise compliance in the face of these rising threats."

Nearly two-thirds (63%) of respondents are currently using compliance, audit, and risk reporting technologies to combat these threats. However, only half of the respondents surveyed are using multifactor authentication (MFA), a core security technology that requires multiple verification factors to gain access to data and applications.

Other critical identity and access management solutions that are being used by less than half of respondents include single sign-on (46%), privileged access management (PAM) (42%), and role-based provisioning and de-provisioning (35%). These solutions, including MFA, represent the foundation of a zero-trust architecture (ZTA). High complexity and poor user compliance are cited as top roadblocks to implementation, while 73% said lack of budget is not a challenge for their identity management strategy.

Using one of these solutions is better than none, but the lack of a holistic cyber strategy can leave detrimental gaps and vulnerabilities. Of those that experienced a security incident, 51% cited the incident involved theft of customer personally identifiable information.

"While security leaders understand the threats they face, it's clear they need better, more efficient solutions to break down internal barriers. Working with a seasoned partner that understands clinical workflows can help ensure deployment is successful through implementation and beyond," said Malezis.

Investing in cyber insurance is also one of the highest priorities for healthcare organisations in 2022, according to 39% of respondents. Over a third (35%) do not currently have cyber insurance, with 39% citing cost as the primary reason. In fact, 70% of respondents with cyber insurance said their insurance premium has increased between 11% and 50% in the past year.

However, healthcare organisations are implementing digital identity solutions to reduce the cost of cyber insurance, with MFA and PAM cited as the most common measures put in place, according to 56% and 40% of respondents, respectively.

From costly cyber insurance to the uptick in cyber incidents i¬¬n the last year, these trends indicate a holistic digital identity strategy and coordinated solutions are needed to reduce cyber threats and compliance risks while overcoming internal roadblocks to implementation and enforcement.
To read more about how healthcare organisations are approaching security and digital identity, download the full report.

About Imprivata
Imprivata is the digital identity company for mission- and life-critical industries, redefining how organisations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enable organisations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by

establishing trust between people, technology, and information. For more information, visit
For more information please visit: www.imprivata.co.uk

Press Contacts
Melloney Jewell◻
Imprivata◻
+44 (0)208 744 6500◻
Mjewell@IMPRIVATA.com ◻

Andreina West
Andmar
+ +44 1491281297
email us here
Visit us on social media:
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/579005016