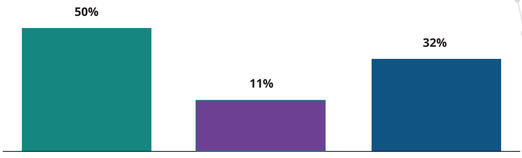
sonraí SECURITY

Almost One-third of US Companies Under-Resourcing Cloud Security Despite Escalating Risks

Spending on cloud services is high

With more than half of respondents having spent more than $10 million and 11% having spent more than $100 million in the last three years, security preparedness is low, with almost one-third (32%) saying they are doing less than they need to, or nothing at all, to ensure security of their cloud resources.



Half of respondents having spent more than **$10 million**

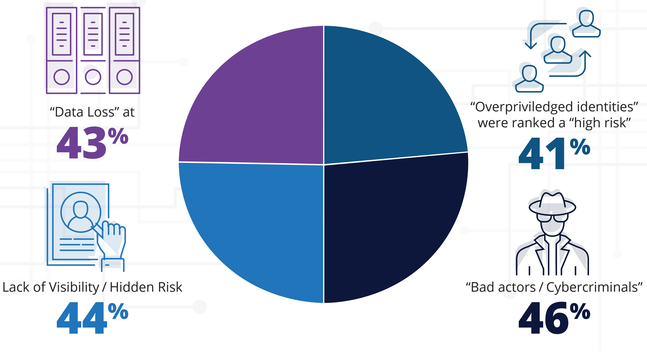
11 Percent have spent more than **$100 million** in the last three years

32% say they are doing **less than** they need to, **or nothing at** all, to ensure security of their cloud resources.

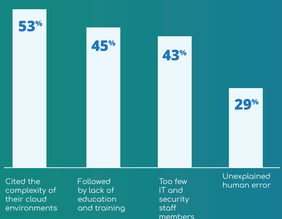
7,750 identities had access to sensitive cloud data

Respondents reported having an average of 7,750 identities with access to sensitive cloud data, estimates that production deployments of Sonrai Dig would suggest are exceedingly low.

When ranking the severity of several types of threats:



Regarding the reasons they occur:



Cloud misconfiguration also stood out as a leading cause of breaches

37%

of respondents said that they had increased significantly in the last year.

In addition to outside hackers and insider threats, the THREE most common, and often overlooked, causes of data breaches include:

Overprivileged Identities

Identities with significantly more privileges and access than are required to carry out the duties assigned to them introduces a significant risk to the cloud.

Human Error

Human mistakes will happen and will not be deliberate at times, but these errors can still wreak havoc in an organization. One example we commonly see is an employee who takes shortcuts leaving sensitive data in locations where it is not adequately protected.

Unauthorized Access

Due to the complex nature of cloud environments, having visibility into which identities have access to data and resources is increasingly difficult. Organizations need to secure all crown jewel data and enforce policies to prevent unauthorized access to the cloud environment.

Survey Respondents:

- The 101 respondents had a minimum of $50M in annual revenue and 1,000 employees.
- Ninety percent were headquartered in the U.S, with 67 percent also having non-U.S offices.
- Business segments represented included fintech (16%), healthcare (14%), manufacturing (14%), education (8%), government (8%), technology (8%) and insurance (6%).
- Seventy-four percent of respondents operate hybrid cloud environments, with 44% using multiple public clouds.
- Seventy-seven percent have spent $50M or less on cloud services in the last three years, with 13% having spent $50.1-100M and 11% having spent more than $100M.
- Cloud security solutions applied varied widely amongst respondents, with 90% using provider-supplied cloud security, 41% using identity access management (IAM), 22% using cloud security posture management (CSPM) and 18% deploying identity governance solutions. Fourteen percent report using dedicated container security solutions, and 11% use data classification tools.

Visit www.SonraiSecurity.com to learn more about public cloud security platform that provides a complete risk model of all identity and data relationships, including activity and movement across cloud accounts, cloud providers, and 3rd party data stores.

sonraí SECURITY