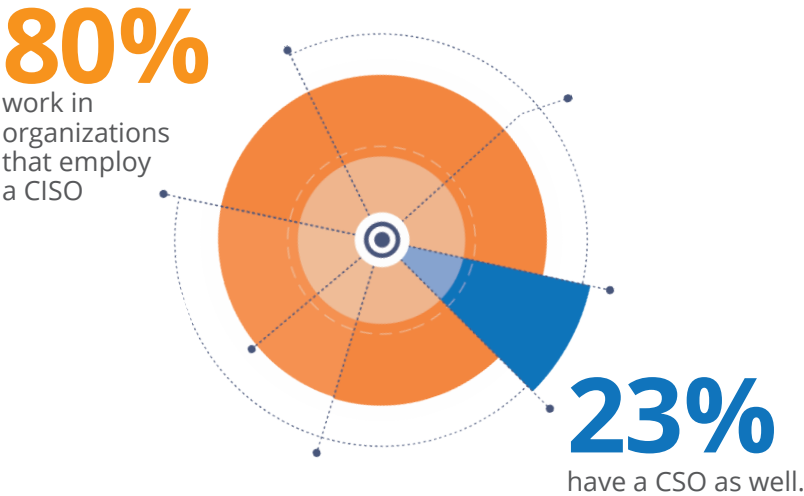


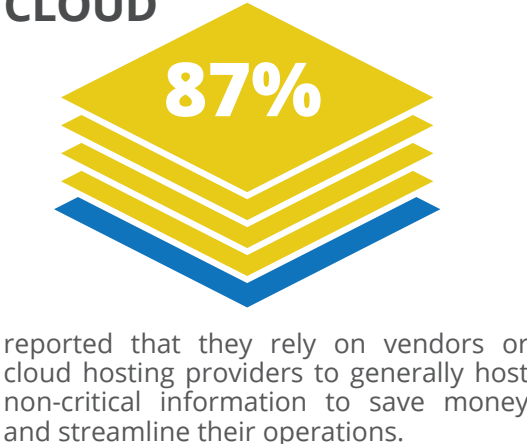
THE SHIFTING CYBERSECURITY LANDSCAPE

How CISOs and Security Leaders Are Managing Evolving Global Risks to Safeguard Data

THE EVOLVING ROLE OF THE CISO



CISOs ARE CAUTIOUSLY ADAPTING TO THE CLOUD



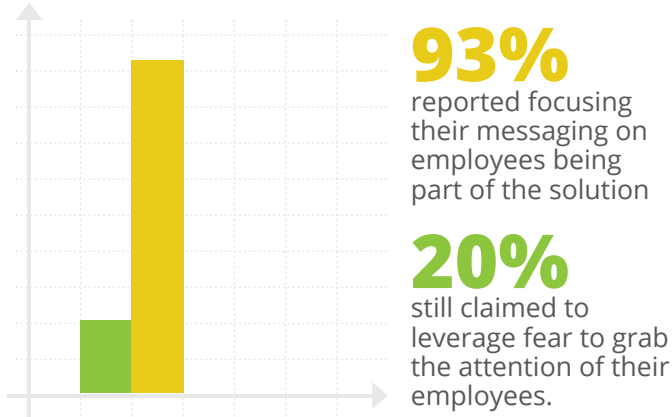
OUTSIDE SUPPORT IS ESSENTIAL



MANAGED SERVICES PROVIDERS TYPICALLY SUPPORT CYBERSECURITY



SECURITY MESSAGING IS EVOLVING WITH TRAINING AND COMMUNICATION TRENDS



SECURITY AND BYOD POLICIES AROUND

100%

OF RESPONDENTS

reported having data privacy and incident response plans.

13%

DESCRIBED THEIR

privacy policy or program as "insufficient or incomplete."

80%

REPORTED HAVING

a Bring Your Own Device (BYOD) plan.

63%

BELIEVE THAT

BYOD plan gadgets contain company-sensitive

SUCCESS OF SECURITY INVESTMENTS IS MEASURED BY RISK REDUCTION

93%

of respondents focus on risk reduction as measure of return on IT security investments.

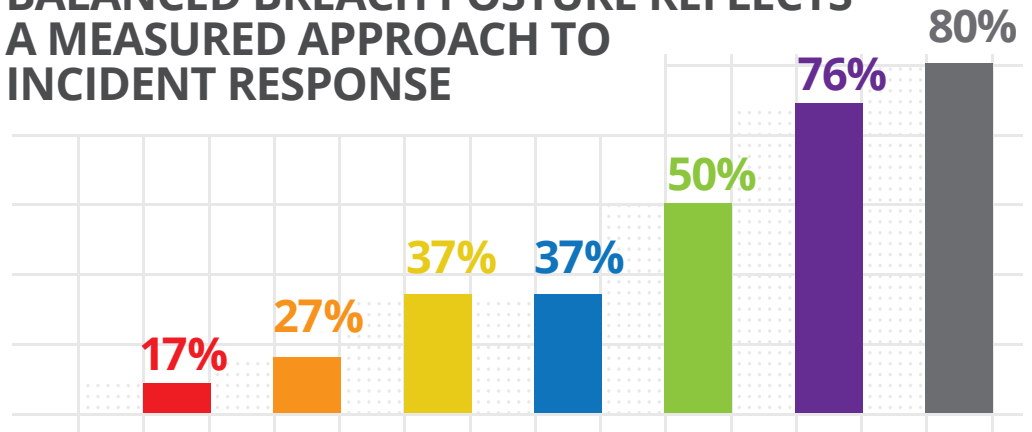
70%

are interested in improved detection capabilities.

20%

characterized the amount they had spent on IT security in the past two years as insufficient.

BALANCED BREACH POSTURE REFLECTS A MEASURED APPROACH TO INCIDENT RESPONSE



- worried most about ransomware or malware
- focused on cyber attacks
- concerned most about an employee mistake
- characterized their information security it as proactive
- described their information security posture as equally reactive and proactive
- ranked user threats as their greatest area of weakness for enterprise security visibility
- concerned somewhat or very concerned that they had already been breached

DATA MANAGEMENT IS A MYSTERY FOR SOME

77%

of respondents claimed to have a data map of their organization's information landscape.

30%

described their organization's data management as "ineffective or out of date."

97%

can identify critical-value data within their networks.

60%

have a way to know what people do with the critical-value data after it is accessed.

83%

have the means to identify who accesses critical-value data.