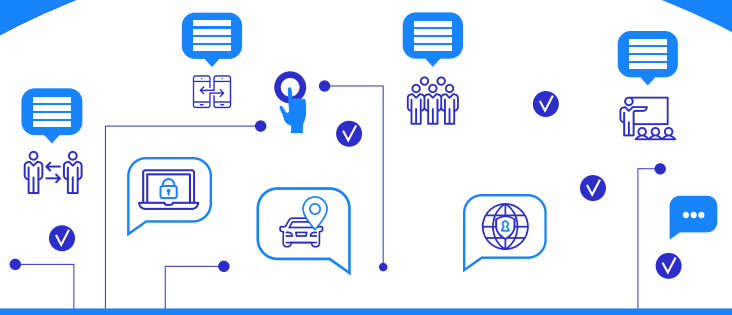
Security for the Hyperconnected World

LANE COOPER

Contributing Editor, CIO, CSO, Computerworld, Network World



EMPOWERING THE SECURELY CONNECTED WORKFORCE

BlackBerry® Secure™

WORLD TOUR

SURVEY GOAL

The Global State of Information Security® Survey is conducted annually to explore how businesses are embracing a modern approach to threat management and information sharing.

TOTAL RESPONDENTS

9,500

COLLECTION METHOD

ONLINE QUESTIONNAIRE

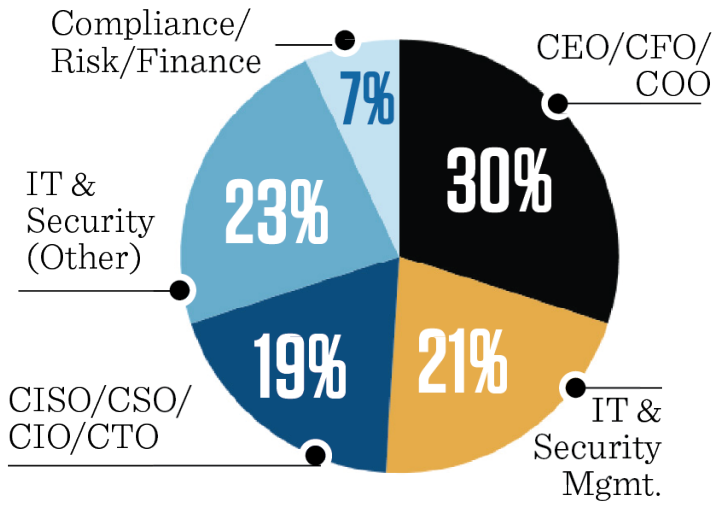
REGION

North America	38%
Europe	29%
Asia Pacific	18%
South America	14%
Middle East, Africa	1%

AUDIENCE BASE

CIO and CSO's audiences, as well as clients of PwC from around the globe were invited via email to participate in the survey.

JOB TITLES



AVERAGE COMPANY SIZE

21,751 EMPLOYEES

AVERAGE REVENUE

$4.1B

TOP REPRESENTED INDUSTRIES

Technology	19%
Financial Services	10%
Industrial Manufacturing	8%
Consumer Products & Retail	8%
Consulting & Professional Services	7%
Education & Non-Profit	7%
Engineering & Construction	7%
Health Industries	6%

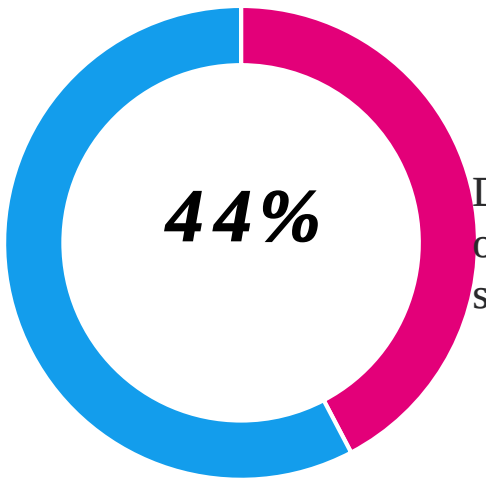
IDG

Strategic Trends

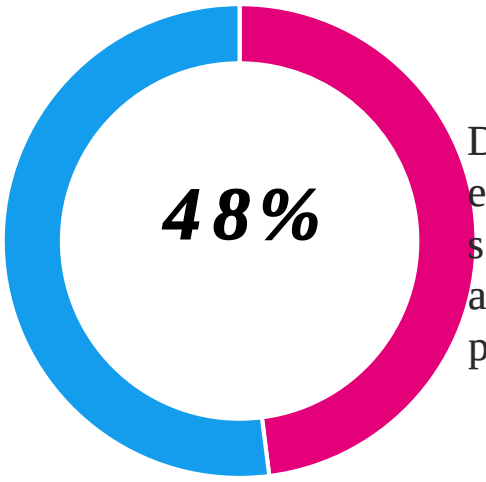
THE HYPER-CONNECTED ENTERPRISE

- Leveraging mobile and cloud technology to improve operations and competitive position through optimized communication and collaboration.
- Beyond human collaboration and communication...applying emerging technologies like IoT and artificial intelligence...to enable digital transformation.
- As more systems are connected to environments that are often not owned -- nor fully controlled -- by the enterprise, risk rises to unprecedented levels.
- Threats at the end point have never been greater or more complex.

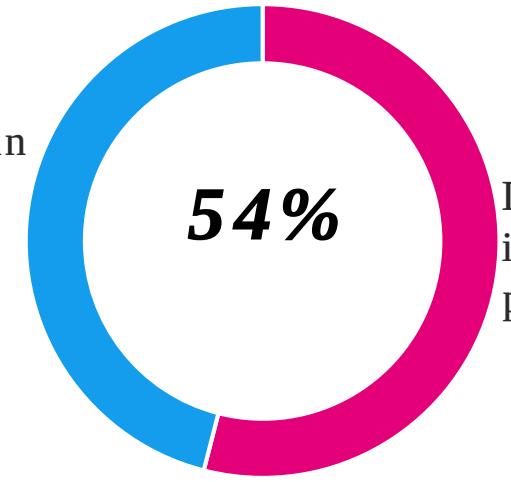
Getting Back to Basics...the Shortfalls



DO NOT have an overall information security strategy



DO NOT have an employee security awareness program



DO NOT have an incident response process

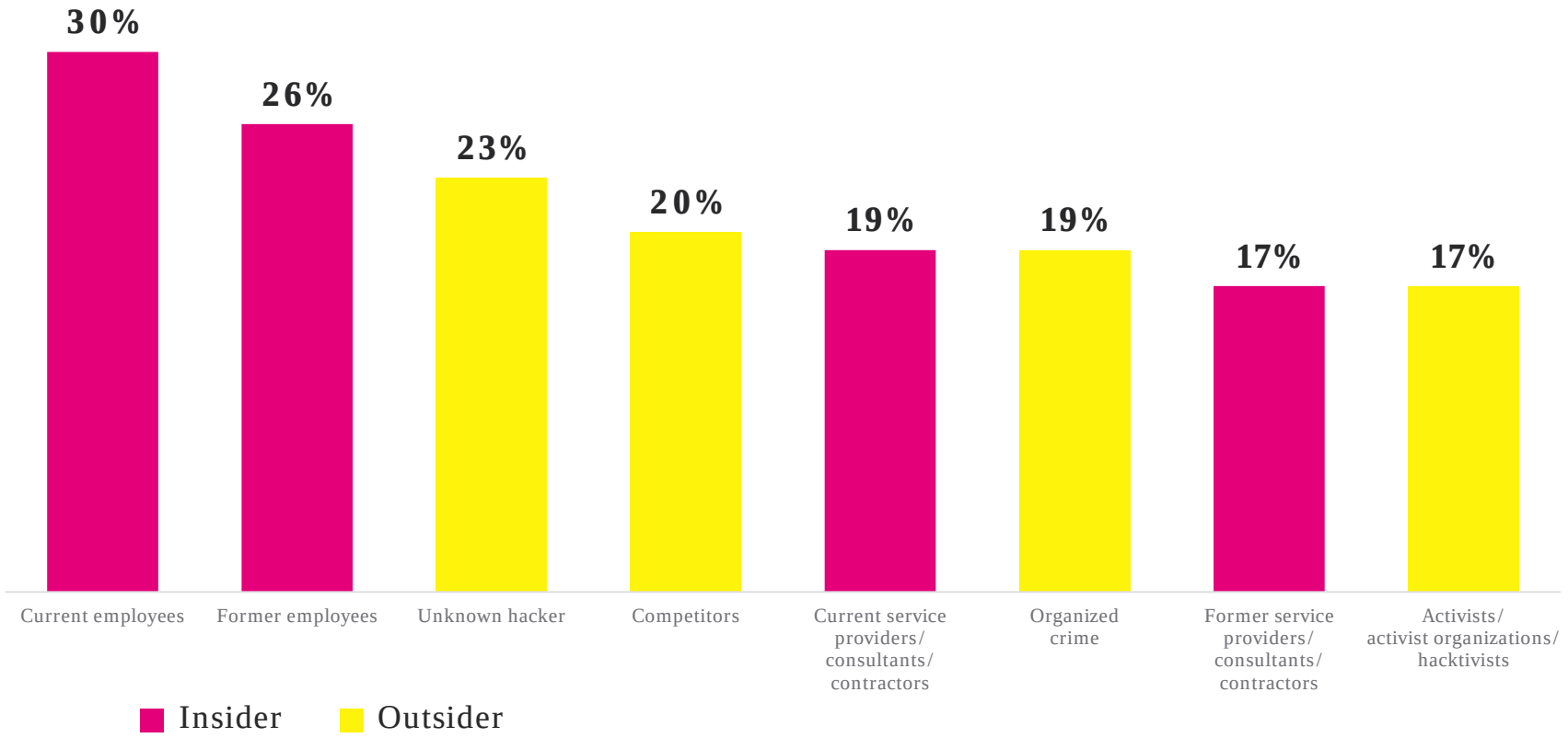
Q: Which safeguards does your organization currently have in place?

Managing Implications

SECURITY IMPERATIVES FOR THE HYPER-CONNECTED ENTERPRISE

- Leverage new technologies with best practices to apply controls and policies for data in a much more dynamic environment.
- Truly ensure that users are allowed to access to data they need in order to do their jobs...but not a byte more.
- Adopt concept of zero trust, where anything or anyone on the network is treated as potentially hostile.
- Revisit relationships with business partners. Today, less than half of all businesses conduct security evaluations on their potential business partners prior to conducting business with them.
- Among those who do...almost one-third of evaluations result in termination of contract because partners can't meet a minimum standard for security.

Current Employees – #1 Source of Security Incidents



Q. Estimated likely source of incidents (Not all factors shown.)

Evaluating Business Partners through the Lens of the Cybersecurity

47%

of enterprise organizations **evaluate** the cybersecurity of supply chain/business partners **prior to conducting** business with them

31%

say this has resulted in **termination of contracts** or relationships

58%

of enterprise organizations have Service-Level Agreements with their business partners to **specify minimum cybersecurity standards compared to 36% of SMBs**

Q. Do you conduct incident response planning/conduct table top exercises with your supply chain/business ecosystem partners? AND Q. Do you have Service-Level Agreement with your supply chain/business ecosystem partners that specifies minimum cybersecurity standards?

IDG

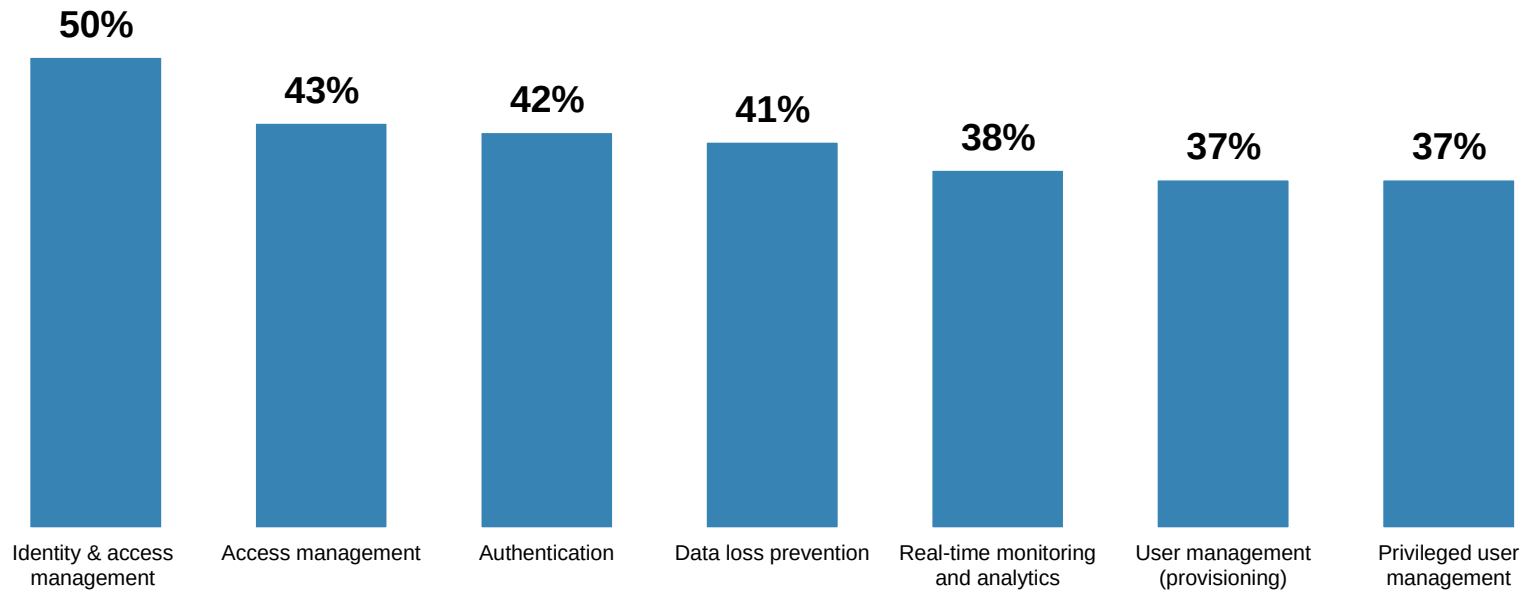
The 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

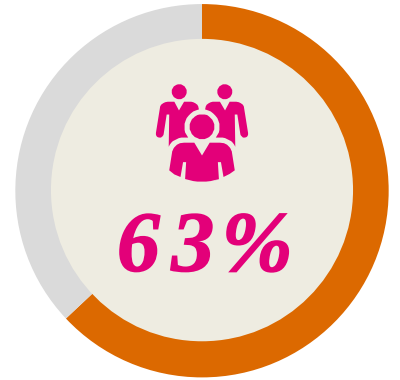
Current Landscape

KEY CHALLENGES:

- Most enterprise don't have enough security professionals on staff, and industry is not turning out enough of them fast enough to meet current and projected demands.
- Staffs often don't have the skill sets necessary to manage hyper-connected enterprises.
- As a result, enterprises look for technology management solutions that securely integrate existing environments and enable normalization of data across security systems.
- Many technology adoptions are driven by the businesses as opposed to IT…as a result security considerations are too often bolted-on afterthoughts.

Respondents Embrace Managed Security Services to Offset Talent Recruitment Challenges





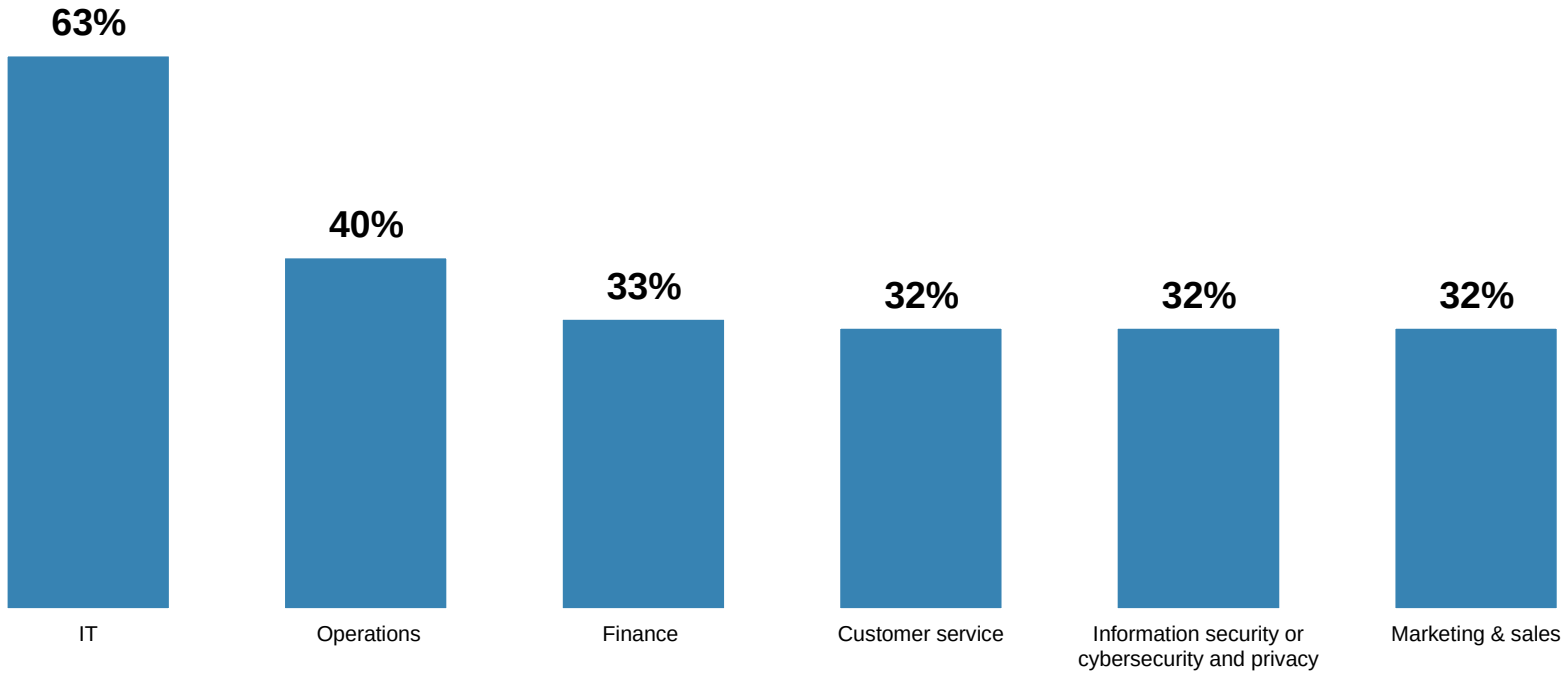
Use managed security services for cybersecurity & privacy

Q. Does your organization use managed security services in its cybersecurity and privacy programs? AND Which of the following managed security services does your organization use?

IDG

2018 Global State of Information Security Survey™ conducted by PwC, CSO and CIO.

Business Functions Run In a Cloud Environment – Majority Without a Security Strategy



47% of organizations currently have a **security strategy for cloud computing** in place

24% PLAN TO ACQUIRE WITHIN THE NEXT YEAR

Q. What business function areas does your organization run in a cloud environment? AND Currently, what percentage of your organization's IT services is delivered via cloud service providers?

IDG

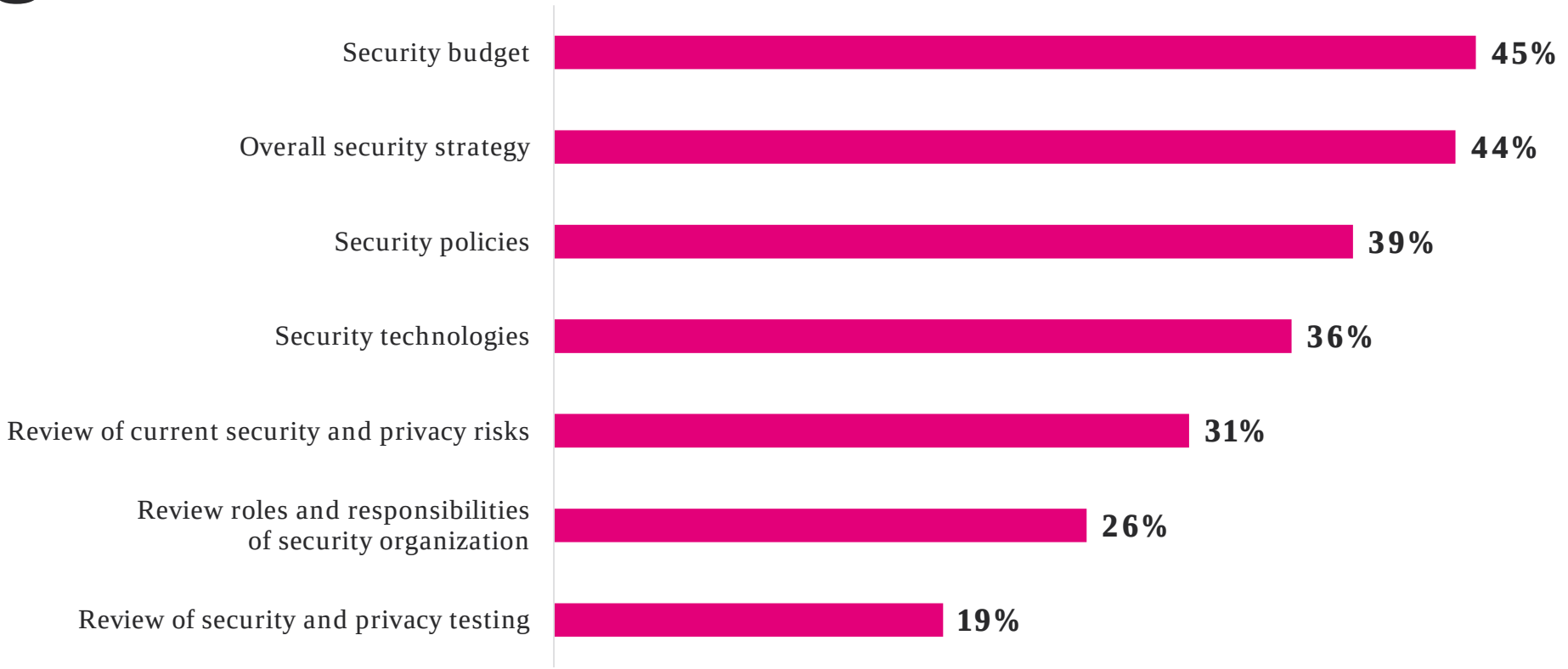
Toward a Risk Adjusted Hyper-connected Enterprise

ACTION ITEMS:COLLABORATION, TRANSPARENCY, RESILIANCE... ACCEPTANCE

- Business, security and technology teams really have to work much more closely together in developing new mobile-intensive and cloud-based processes.
- Transparency about technologies businesses want to use essential so that IT and security can do their jobs to enable their use in a secure manner.
- Resiliency is critical in a hyper-connected environment. Organizations must be able to take a punch...and recover...fast.
- Board level acceptance of risk tolerance an enterprise is willing to take...as new processes are enabled by new technologies.

IDG

Board Leadership Must Be Further Engaged



Q. In which of the following areas does your organization's Board of Directors actively participate?

CSO.com Advice for Businesses

- C-suites must lead the charge – and Boards must be engaged
- Pursue resilience as a path to rewards – not merely to avoid risk
- Purposefully collaborate and leverage lessons-learned
- Stress-test interdependencies in your digital business ecosystem
- Focus more on risks involving data manipulation and destruction