InformationWeek

CYBER RISK AND RESILIENCY

How CIOs Are Dueling Disaster in 2023

Cyberattacks and other threats to an organization's ability to do business remain a top concern across all industries. While ransomware continues to make headlines, there are many others from outside as well as inside the organization — both manufactured and organic.

InformationWeek surveyed IT executives, management, and cybersecurity professionals with questions centered on the challenges of maintaining IT resiliency and cybersecurity. The survey asked about their cyber resiliency strategy, budget, staffing, incident response testing, cyber insurance and claims, and cyberattacks that significantly disrupted business.

Here's a peek at how the cybersecurity budget dollars are allocated and why (read the full report for more detail):

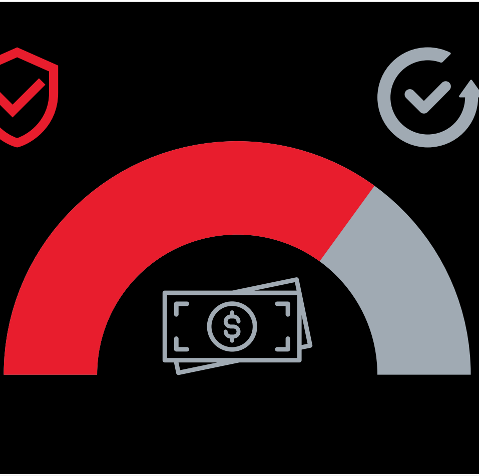
HOW ARE **CYBERSECURITY BUDGET DOLLARS** ALLOCATED?

Gartner predicts that spending on information security and risk management products and services will reach more than $188.3 billion this year. Budget dollars tend to be allocated for cybersecurity between two buckets:

70% Defense

Technologies and talent expenditures:

- End-user training
- Identity and access management (IAM)
- Encryption
- Physical security controls



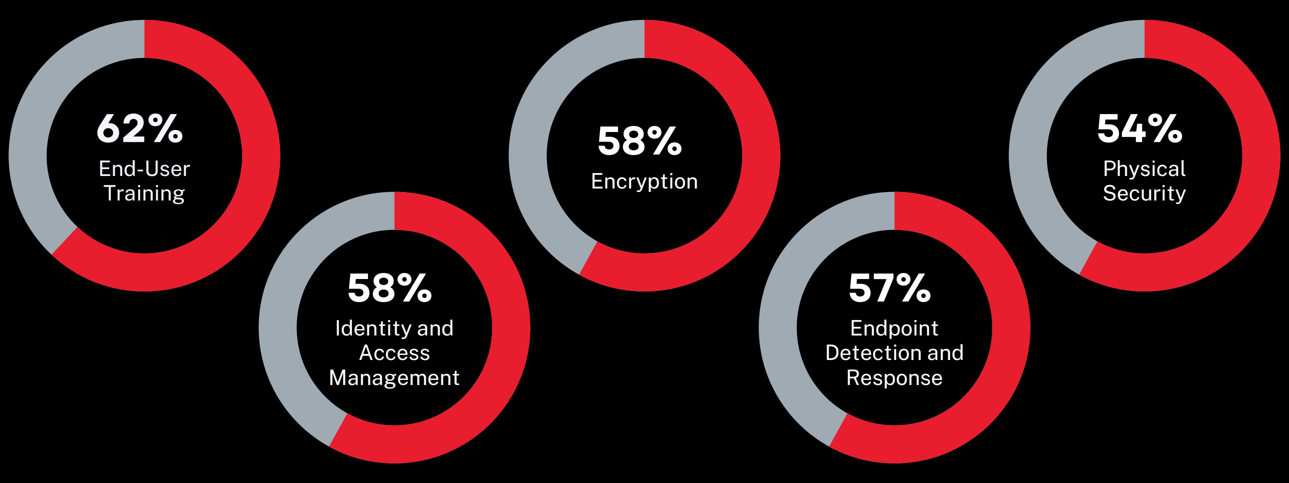
30% Response

Focused on business continuity (BC) and disaster recovery (DR):

- Data backups
- Cyber insurance
- Ransom money

WHICH **CYBER DEFENSE TOOLS AND PROCEDURES** ARE USED?

More than half (51%) of respondents said their companies did not experience a significant disruption of any kind. It's unclear what percentage of those may have just been lucky, and what percentage benefited from strong defense and resilience strategies, such as backups (69%) or these others:



HOW DO COMPANIES PREPARE FOR **REBOUND AND RECOVERY**?

A strong defense strategy may not be enough to hold the attackers back. When that happens, the company must rely on the strength of its rebound plan, which may include:

Incident Response

The best way to gauge the incident response effectiveness is to test it, yet nearly one quarter (23%) of companies surveyed have either never conducted tests or are unsure if their teams have tested with tabletop exercises or other measures.

Data Backups

It's no surprise that backups (69%) top the list of tools and procedures used. Half (50%) of respondents report they include misconfigurations in their cyber resilience plans as well as planning for severe weather events (43%).

Cyber Insurance

Nearly half (46%) of companies reported carrying cyber liability insurance either as a standalone policy or as a rider on a larger business insurance policy. Of those with cyber insurance, 84% believe the protection is worth the expense.

THE **BIGGEST CONCERNS** WITH CYBER-RELATED INCIDENTS

Ransomware is leading in media headlines and liability costs, but it's not the only thing threatening businesses. Even in a ransomware attack, the total cost is not measured solely in the ransom amount. These are the top concerns related to cyber incidents:

1. Lost Business
2. Closure of Business
3. Failure of Mission
4. Public Perception
5. Fines Due to Compliance Violations

LEARN MORE

Against this backdrop, how resilient are modern companies today? Are their cybersecurity champions burned out or enthusiastically rising to the challenges? And how is cyber insurance working out for policyholders now that there's sufficient time to weigh their effectiveness against the costs?

These burning questions, along with others are answered in our
2023 State of Cyber Risk and Resiliency Report
Download your copy of the report today!

As the world's most trusted business technology resource, InformationWeek offers independent insight and advice to help today's enterprise IT leaders navigate the fast-changing technology landscape and identify the best strategies and tools to drive their organizations forward. InformationWeek provides an unbiased environment for IT decision-makers to learn from experienced journalists, subject-matter experts, and their IT peers to explore new ideas, find answers to their business technology questions, and solve their most pressing problems.

Join us at InformationWeek.com

Copyright © 2023 Informa PLC Informa UK Limited is a company registered in England and Wales with company number 1072954 whose registered office is 5 Howick Place, London, SW1P 1WG.

informa tech