CSO
FROM IDG

2018 U.S. State of Cybercrime

www.CSOonline.com

SURVEY GOAL

U.S. State of Cybercrime Survey is conducted annually to gain insight and evaluate trends in the frequency and impact of cybercrime incidents, cybersecurity threats, and information security spending. Additionally the study examines the risk of third-party business partners in private and public organizations.

TOTAL RESPONDENTS

515 executives at U.S. businesses, law enforcement services and government agencies.

COLLECTION METHOD

ONLINE QUESTIONNAIRE

60 QUESTIONS

AUDIENCE BASE

CSOonline.com

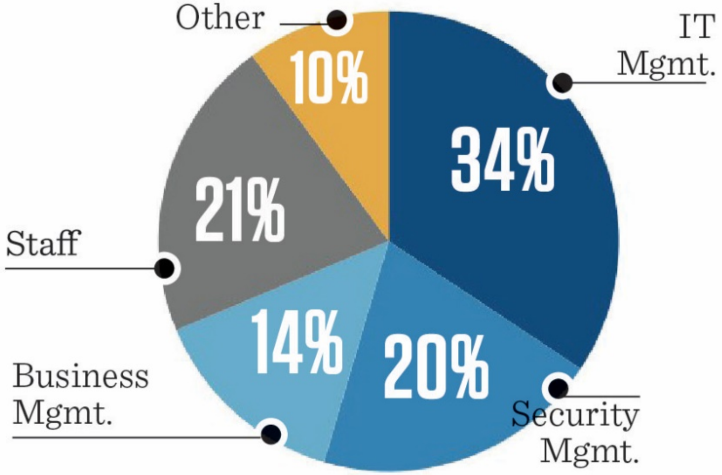
MARGIN OF ERROR

+/-4.3 percentage points

COMPANY SIZE

AVERAGE	ENTERPRISE	SMB
10,874	49%	51%

JOB TITLES



AVERAGE IT SECURITY BUDGET

$15M

TOP REPRESENTED INDUSTRIES

TOP REPRESENTED INDUSTRIES	
Technology	18%
Financial Services	15%
Manufacturing	12%
Education	11%
Government/Non-profit	10%
Services (legal, consulting, real estate)	8%
Healthcare	7%

Status of Cybersecurity Within Organizations

41%

report that the **frequency** of cybersecurity events **increased in 2017**

50% Enterprise; 34% SMB

66%

of organizations are **more concerned** about cybersecurity threats this year than they were in 2017

DOWN FROM 74% LAST YEAR

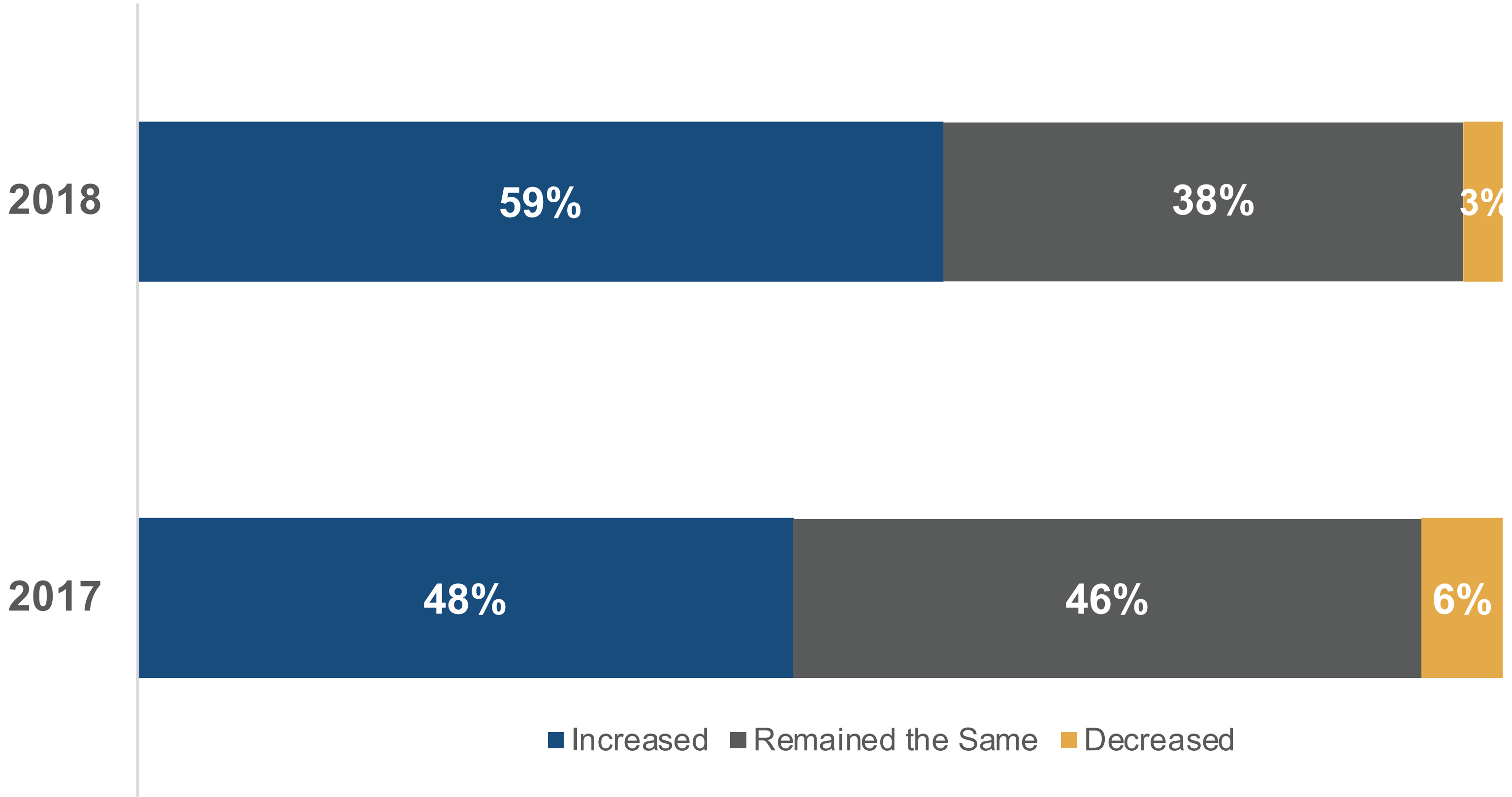
65%

of organizations have a formal incident response plan

44% test it at least once per year

Q. When compared with 2016, how did the frequency of cybersecurity events in your organization change in 2017? AND Are you more concerned or less concerned about cybersecurity threats to your organization in 2018 than you were in 2017? AND Does your organization have a formal incident response plan?

Security Budgets On the Rise



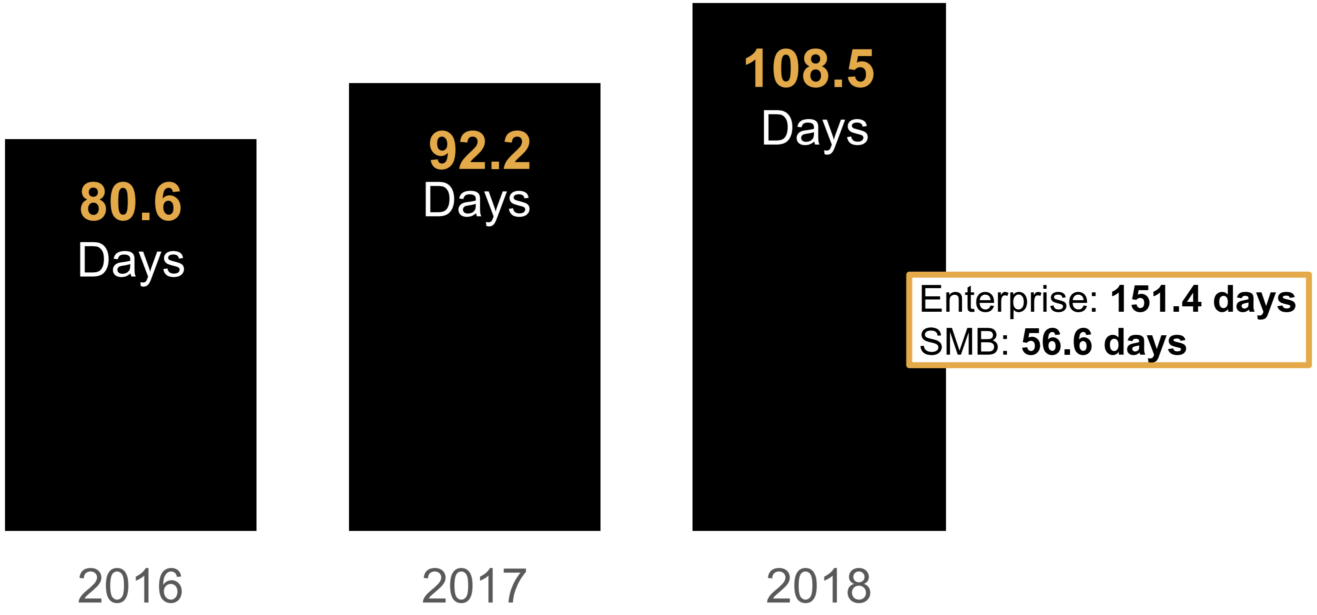
AVERAGE BUDGET CHANGE

9.5%

increase
from 2017

Q. Compared with the fiscal year 2017 security budget, how did your organization's fiscal year 2018 security budget change?

Sophisticated Hackers Delay Threat Detection



Enterprise: **151.4 days**
SMB: **56.6 days**

35%

indicate it takes longer than a month to identify intrusions on their network

UP FROM 28% LAST YEAR

Q. On average, how much time passed between the date you believe an intrusion began and the date it was discovered?

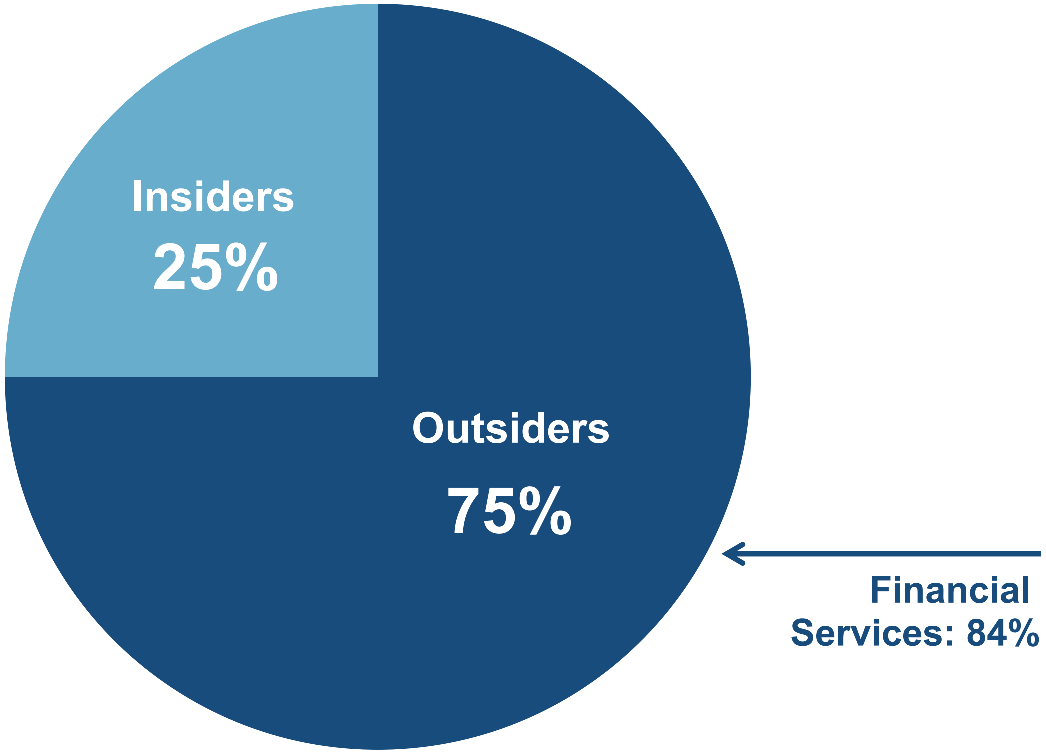
The 2018 U.S. State of Cybercrime Survey, in partnership with CSO, U.S. Secret Service, CERT Division of Software Engineering Institute at Carnegie Mellon University, and KnowBe4

CSO

FROM IDG

Various Sources of Cyber Events

Who's Causing these Cyberattacks?

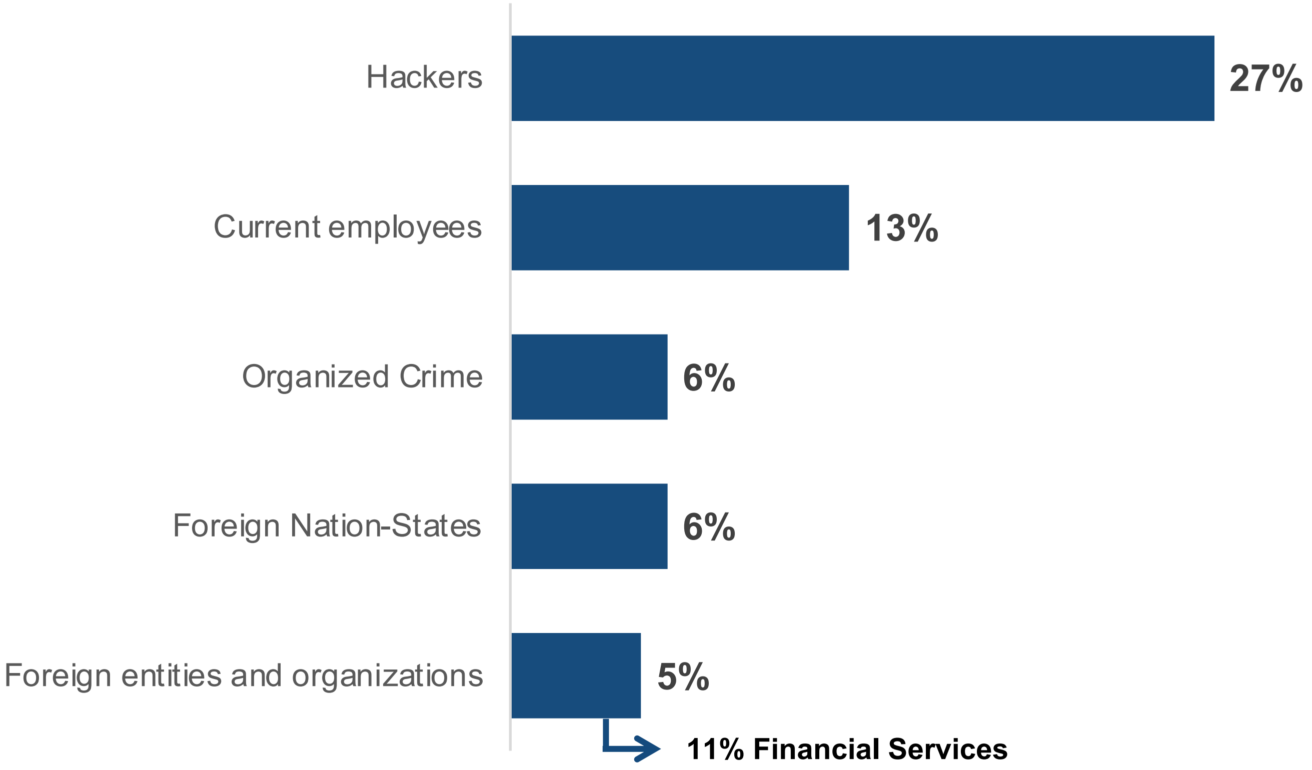


36%

of security attacks attributed to an **insider** are said to be **unintentional/ accidental**

Q. You indicated that your organization experienced at least one cyber security event the past 12 months. What percentage of these events are known or suspected to have been caused by: AND Of the security incidents you know you experienced and for which you were able to attribute to an insider, what do you believe was the motivation behind the attacks?

Hackers Prove to be the Greatest Cyberthreat Overall



39%

of respondents say that cybercrimes **caused by outsiders** were the **most costly** to their organization

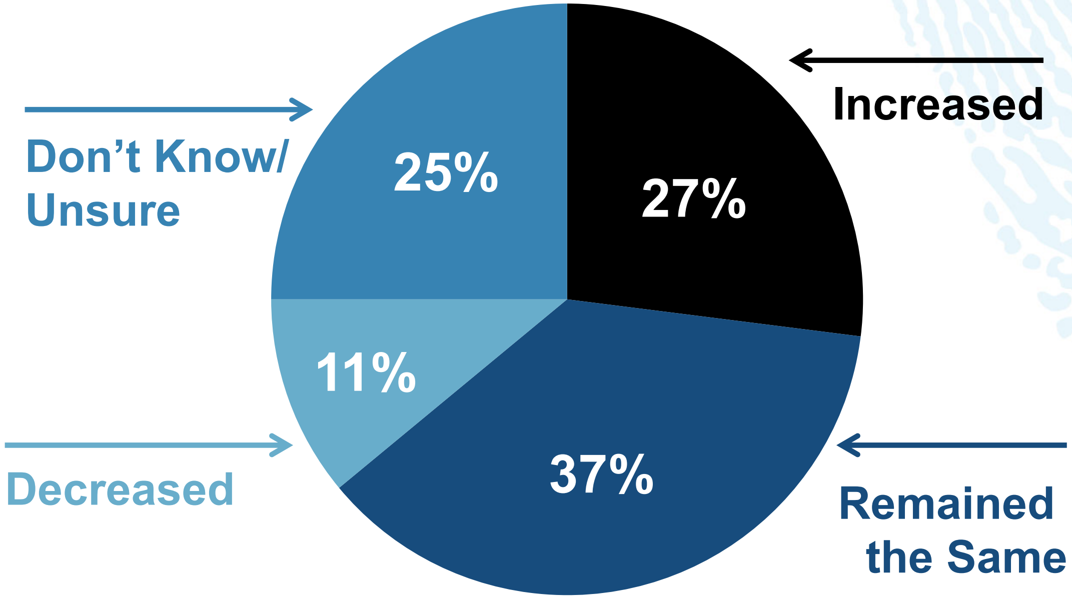
Q. Which of the following groups posed the greatest cyberthreat to your organization during the past 12 months? AND Q. In general, cybercrimes were more costly or damaging to your organization when caused by:

Financial Loss Occurring Due to Targeted Attacks

40%

of **financial loss** due to security events in the past 12 months was **caused by targeted attacks**

Monetary Losses from Targeted Attacks



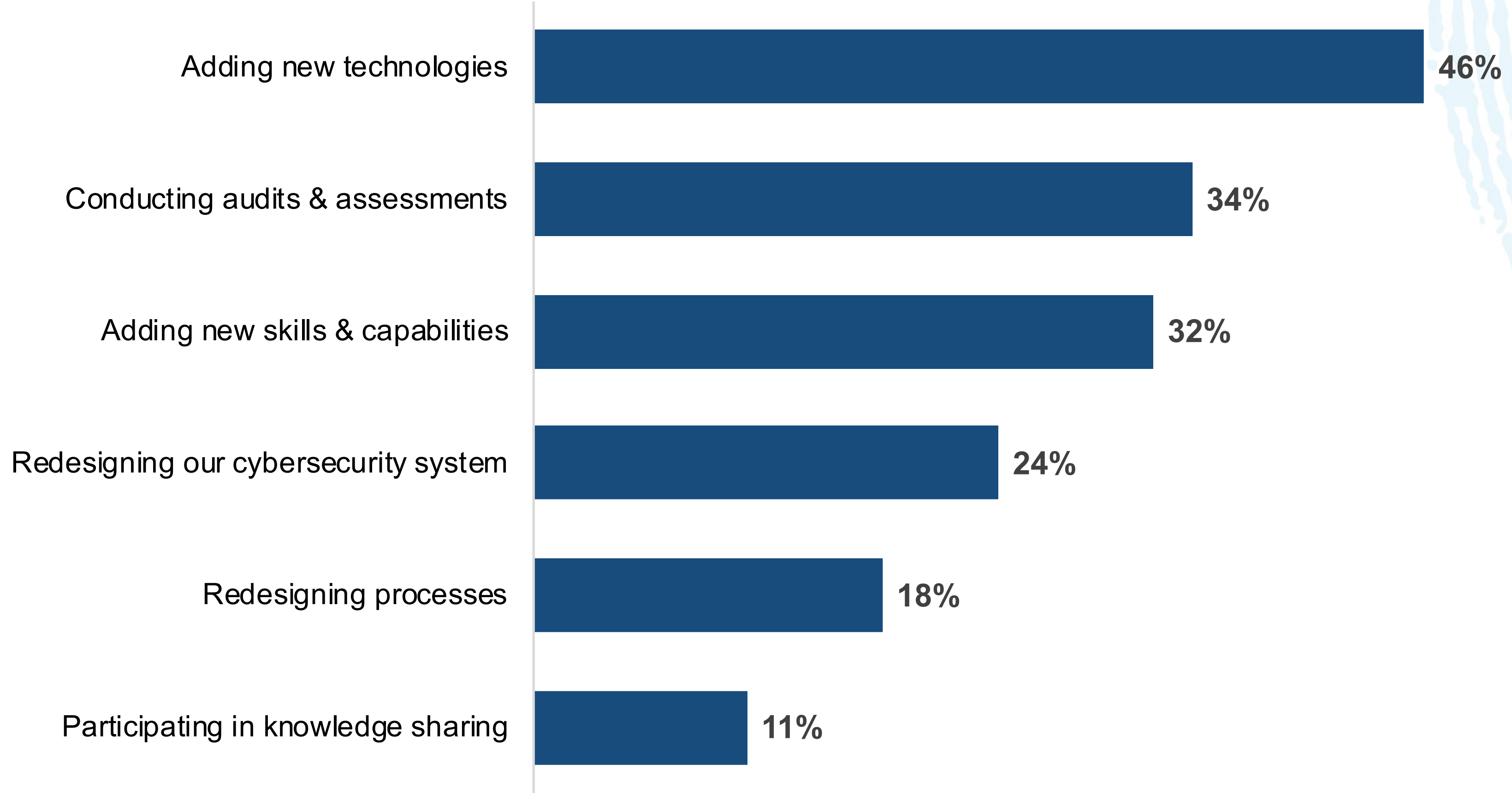
Q. When considering the financial losses or costs to your company from those targeted attacks, has the financial loss or cost increased or decreased when compared to the prior 12 months? AND Q. Of the security events your company experienced during the past 12 months that caused financial loss or cost, what percentage of these events were:

CSO

FROM IDG

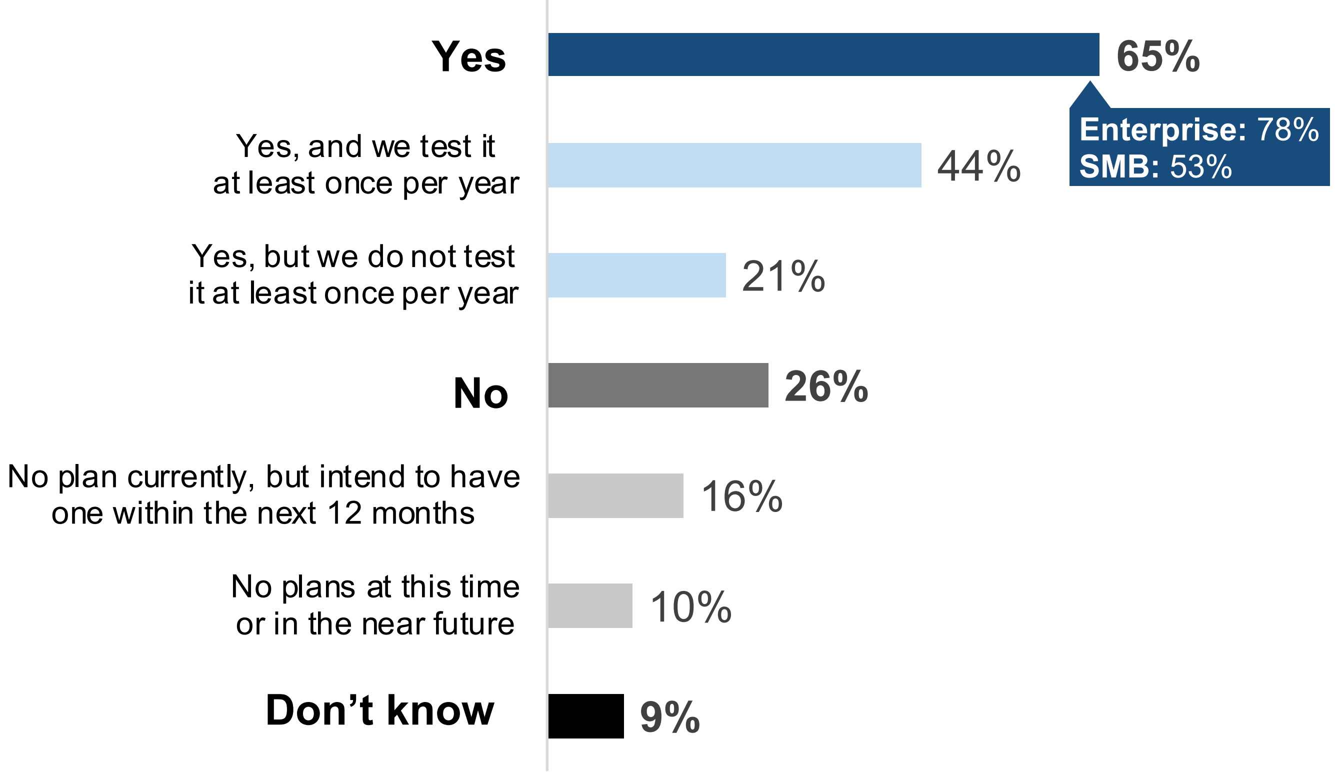
IT Investments & Strategies to Address Cyberthreats

Organizations Hope to Derail Attacks by…



Q. To address cyber-risks, are your investments and spend focused on:

Ability to Respond to a Security Incident



Enterprise: 78%
SMB: 53%

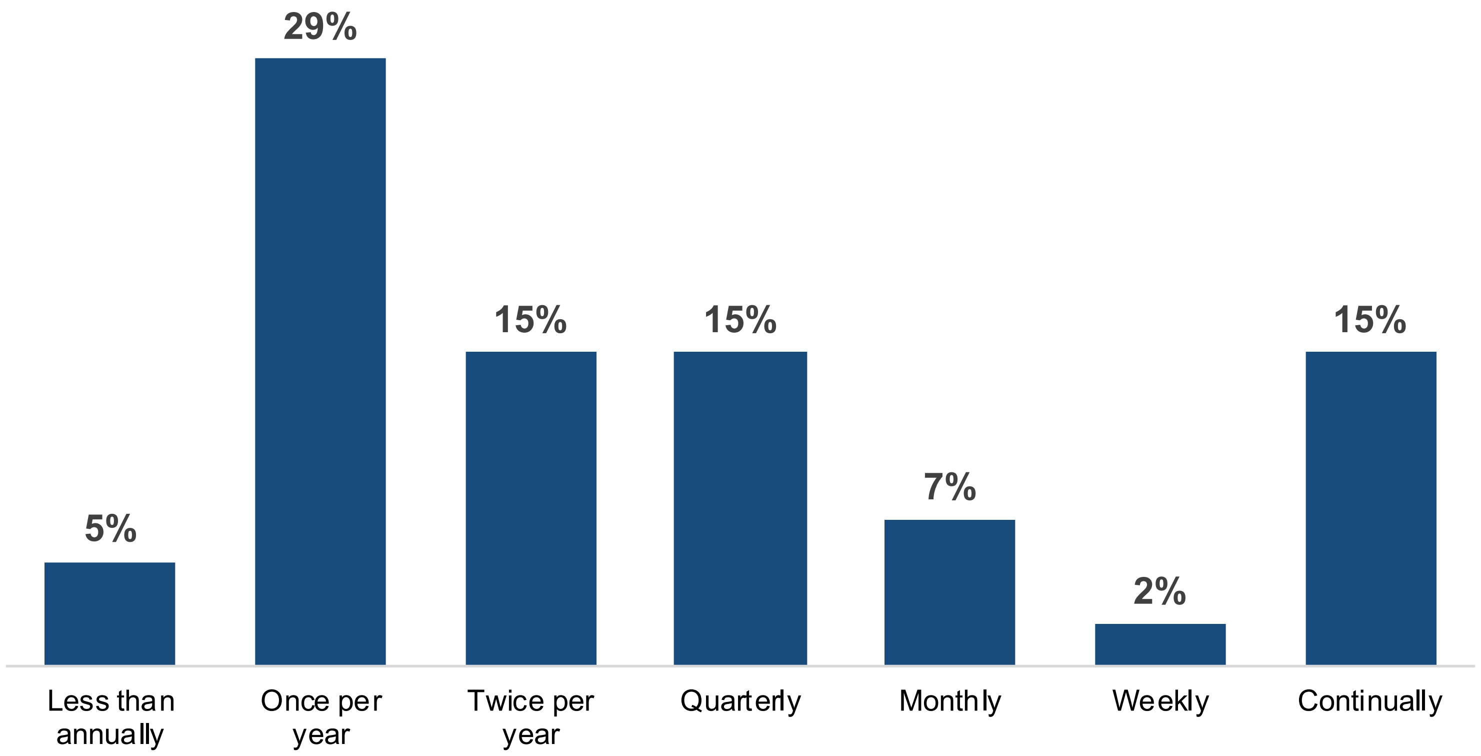
85%

of financial organizations have a formal incident response plan

69% test it at least once per year

Q. Does your organization have a formal incident response plan?

Majority of Employees Receive Security Training at Least Once a Year



6% of employees are only trained when hired

are **never trained**

Q. How frequently are your employees trained on security awareness?

CSO FROM IDG

The 2018 U.S. State of Cybercrime Survey, in partnership with CSO, U.S. Secret Service, CERT Division of Software Engineering Institute at Carnegie Mellon University, and KnowBe4

Conclusions

- Cyberthreats continue to be top of mind, as 66% report they are most concerned about cybersecurity threats this year than they were in 2017.
- The average number of cybersecurity events decreased this year to 107.2 – however this increased to 195.9 for enterprise organizations.
- The majority of attacks continue to come from outsiders, and these also prove to be the most costly for 39% of organizations.
- 66% of organizations have a methodology in place that helps you determine the effectiveness of your organization's security programs based on clear measures.
- Security awareness training should be a top priority, as 29% of security decision-makers report that their employees are only trained once a year.