CSO
FROM IDG

# 2017 U.S. State of Cybercrime

www.CSOonline.com

# Purpose and Methodology

## SURVEY SAMPLE

| | |
|---|---|
| TOTAL RESPONDENTS | **510 executives at U.S. businesses, law enforcement services and government agencies** |
| MARGIN OF ERROR | **+/- 4.3%** |
| AUDIENCE BASE | **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, information security spending. Additionally, the study examines the risks of third-party business partners in private and public organizations.

## SURVEY METHOD

| | |
|---|---|
| COLLECTION | **Online Questionnaire** |
| TOTAL QUESTIONS | **61** |

# Respondent Profile

## TOTAL RESPONDENTS

510

## ORGANIZATION SIZE

| | |
|---|---|
| AVERAGE IT SECURITY BUDGET | $11.0M |
| AVERAGE NUMBER OF EMPLOYEES | 9,795 |

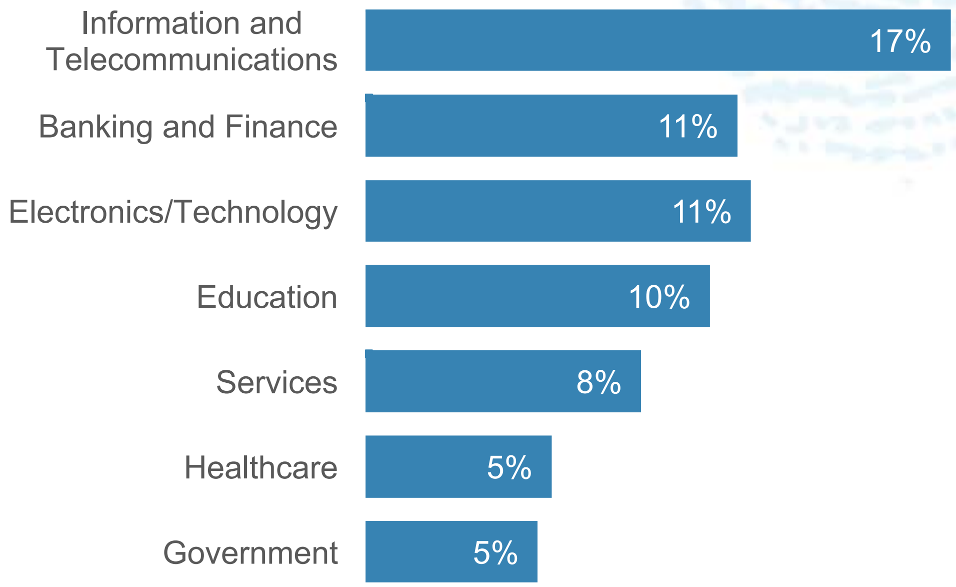
## JOB TITLE BREAKDOWN

| | |
|---|---|
| CORPORATE MANAGEMENT | 35% |
| DIRECTOR / MANAGER | 23% |
| EVP, SENIOR VP, VP | 10% |
| OTHER | 30% |

## COMPANY SIZE

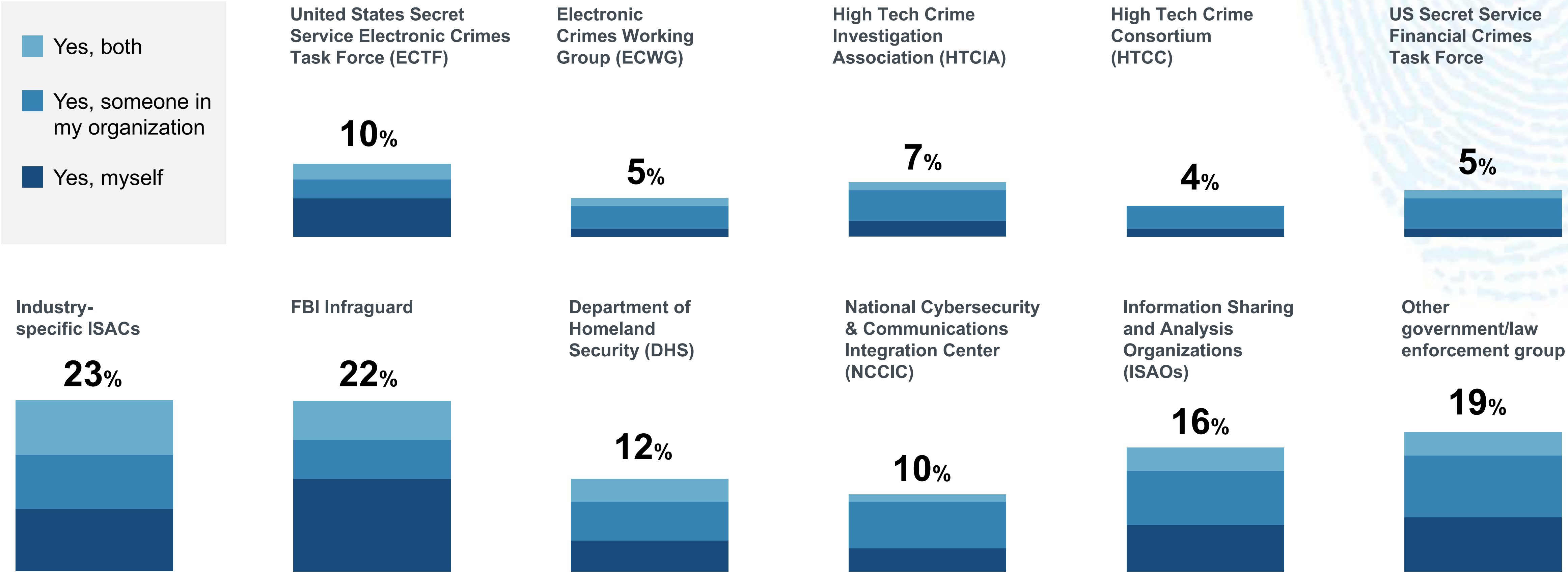
| | |
|---|---|
| 500+ EMPLOYEES | 41% |
| <500 EMPLOYEES | 59% |

## TOP REPRESENT INDUSTRIES



# Organizations rely on a number of information sharing organizations, but overall information sharing remains a challenge

**Q: Are you, your organization, or another individual at your organization currently a member of any of the following groups?**



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

# The Board is Playing a Greater Role – But the Reasons Vary By Organization

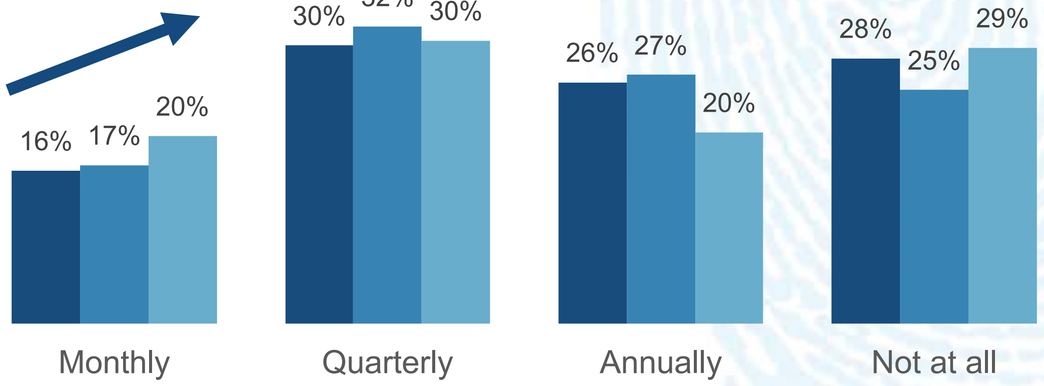
**Q1: How often does your CISO, CSO, or equivalent senior information security executive brief the Board of Directors on cyber risk?**

**Q2: How do you believe your Board of Directors views cyber risks?**

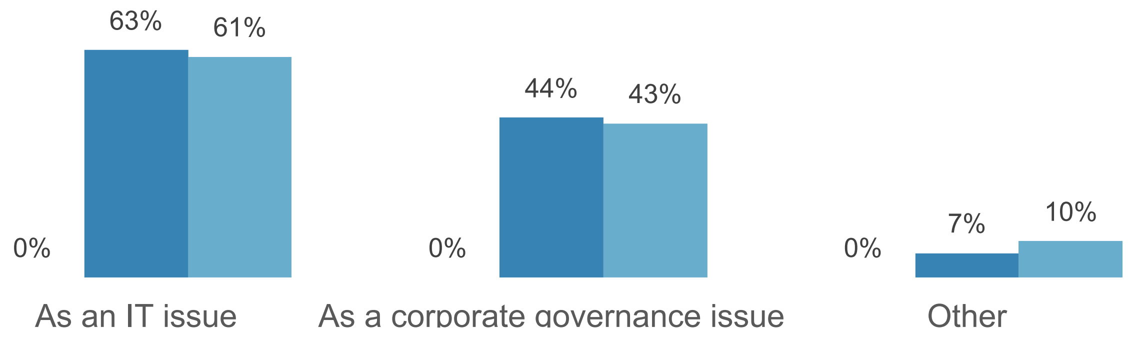
**Q3: Which Board Committee is responsible for cybersecurity risk management?**

■ 2015 ■ 2016 ■ 2017

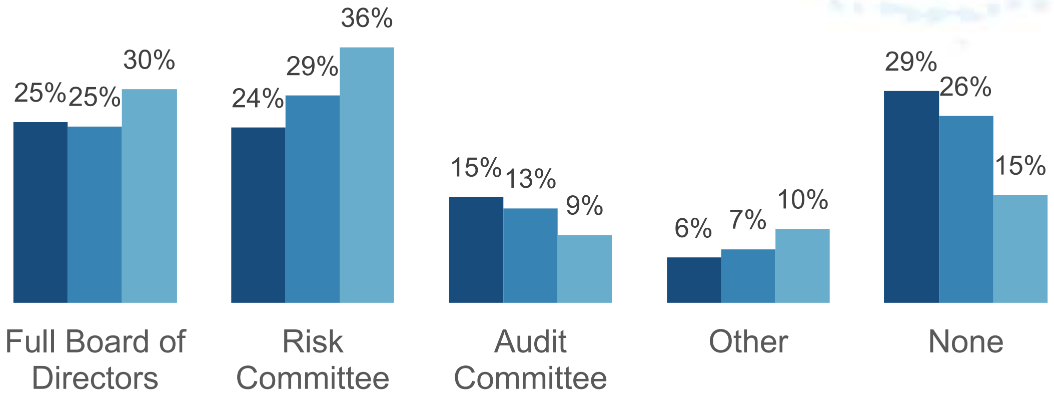
## CSOs/CISOs are reporting to the board more frequently



## 6 in 10 boards still only see cyber risks as an IT issue



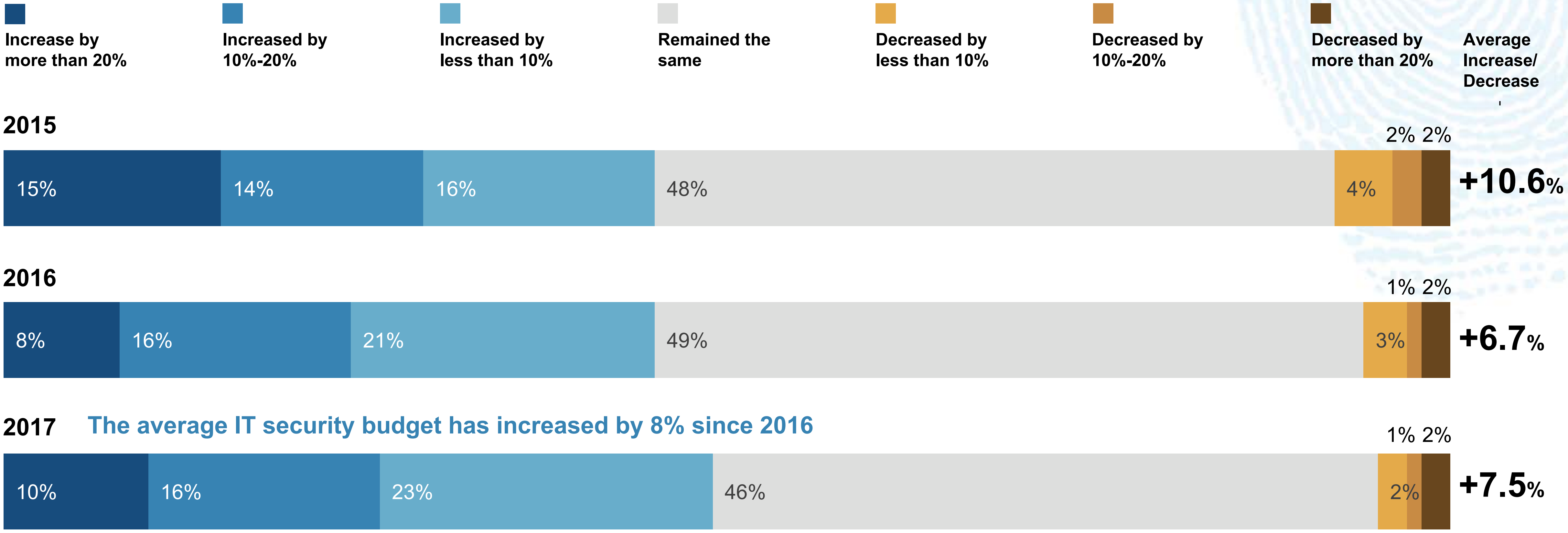
## Full boards and risk committees have increasing responsibility



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

# IT Security Budgets Continue to Increase YoY

**Q: Compared with the fiscal year 2016 security budget, how did your organization's fiscal year 2017 security budget change?**

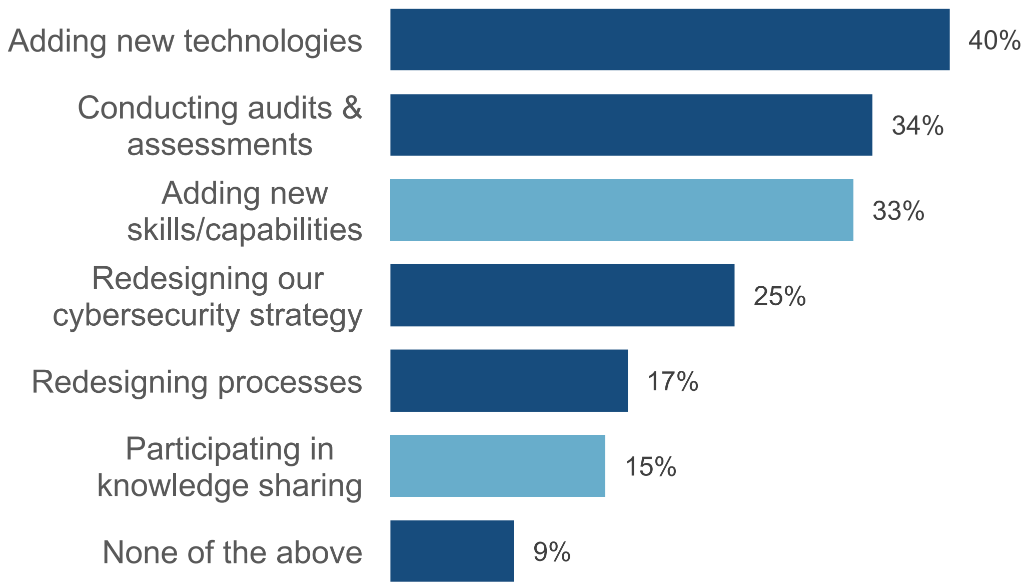


The average IT security budget has increased by 8% since 2016

# IT Security Investments Are Making An Impact

**Q: To address cyber-risks, are your investments and spending focused on**

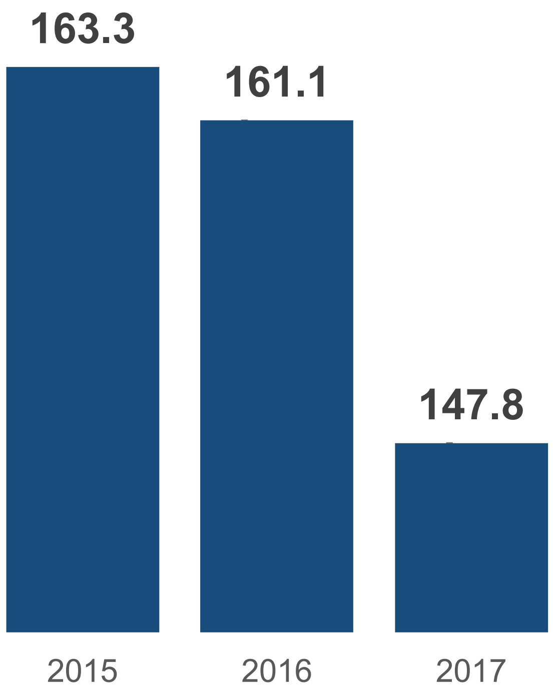
## Keeping skills fresh is key to addressing emerging threats



**Q: Please estimate the total number of cybersecurity events experienced by your organization during the past 12 months**

## Decline in Number of Security Events

from 2015 to 2017



↓ 8.2%

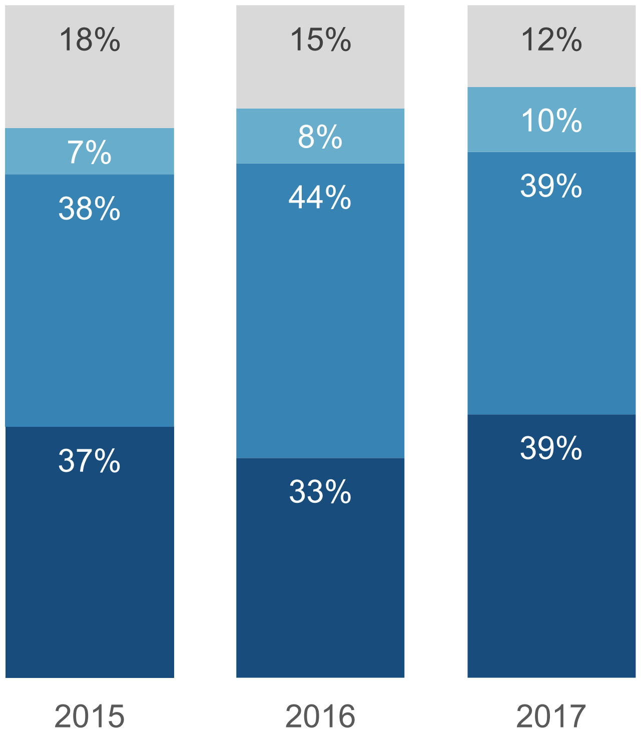
The 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

# Fewer Security Events, But No Less of An Impact

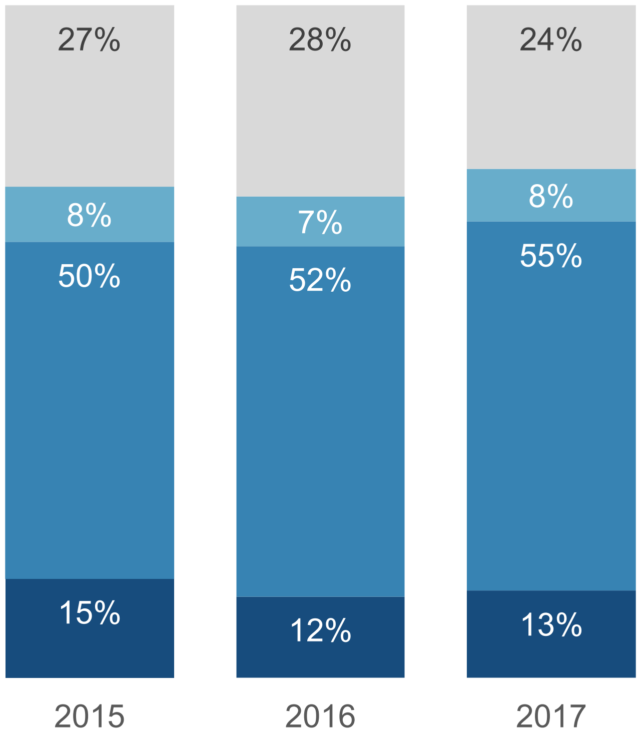
**Q: When compared with 2015, how did the frequency of cybersecurity events in your organization change in 2016?**

**Q: When compared with 2015, how did monetary losses as a result of cybersecurity events in your organization change in 2016?**

■ Increased ■ Remained the same ■ Decreased □ Don’t know/not sure



Uncertainty declining, a sign of increasing network visibility



Losses remain the same versus previous years

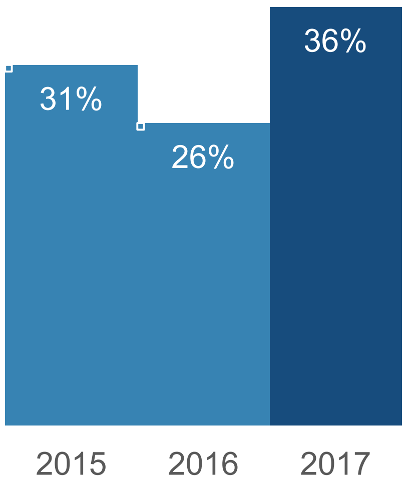
The 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

# Rising Severity Of Cybercrime Impacts

**Q: Which of the following types of impacts did your organization experience in 2016 as a result of cybercrime or cybersecurity events?**

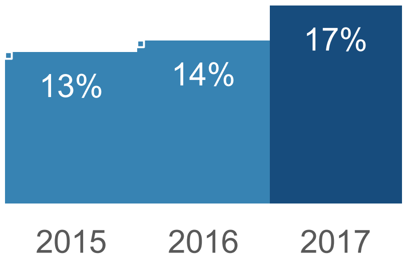
## 1

**Phishing**
**way up over 2016**



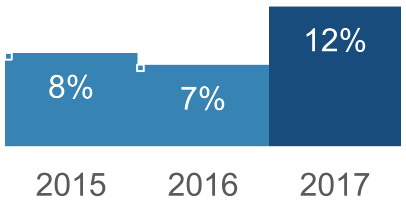
## 2

**Ransomware**
**growing steadily**



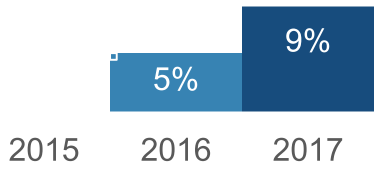
## 3

**Financial Fraud**
**jumped in 2015**



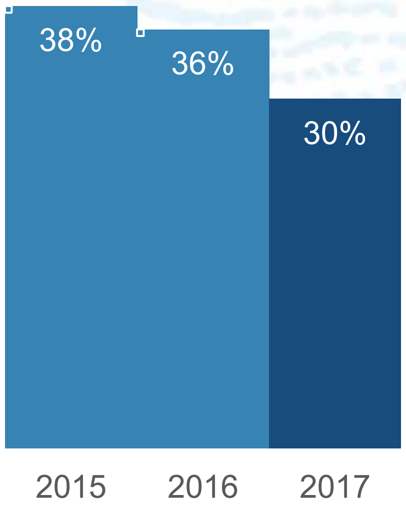
## 4

**Big spike in business being the victim of Business Email Compromise**



## 5

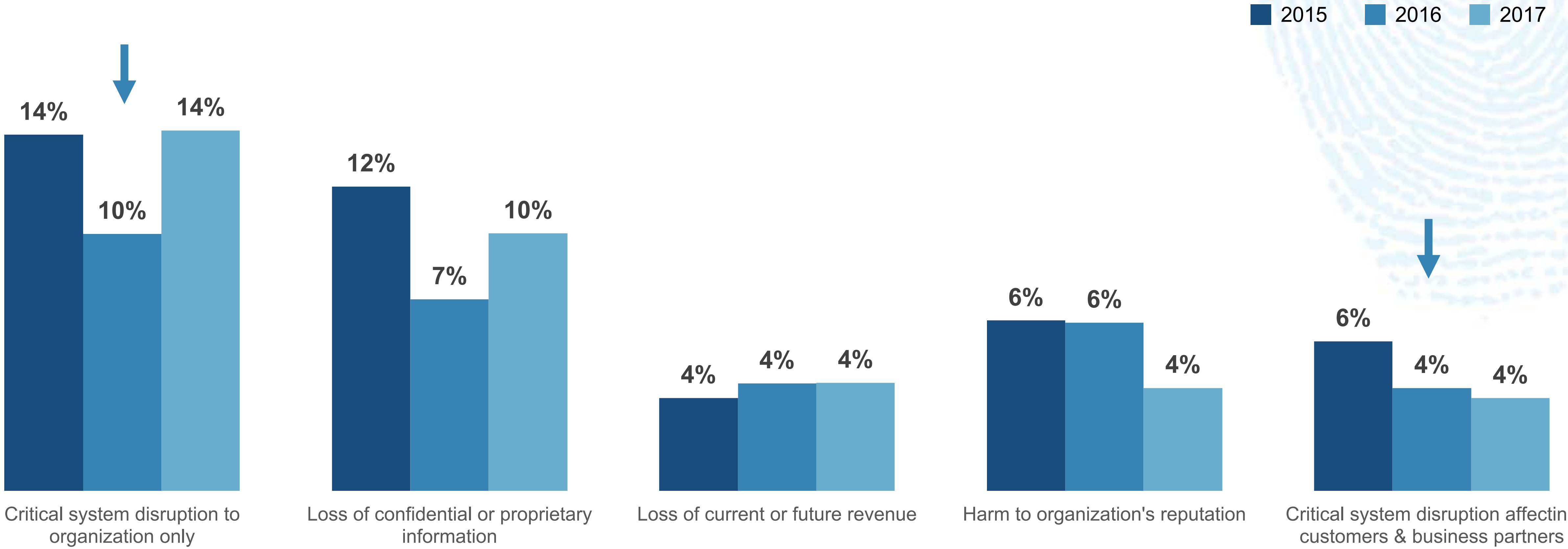
**Sharp decline in the number of businesses that experienced no losses**



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

# Nearly One-fifth Have Experienced Critical System Disruption as A Result Of Security Events.

**Q: With respect to your organization, what is the most adverse consequence that has occurred from a security event caused by an insider in the last 12 months?**



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

# Threats Are Becoming More Difficult to Detect

**Q: Which of the following types of impacts did your organization experience in 2016 as a result of cybercrime or cybersecurity events?**

## Uptick since 2015 in percentage that believe they've experienced:

↑ **+8pp**

**network slowdowns/ downtime**

↑ **+6pp**

**phishing**

↑ **+6pp**

**application alteration**

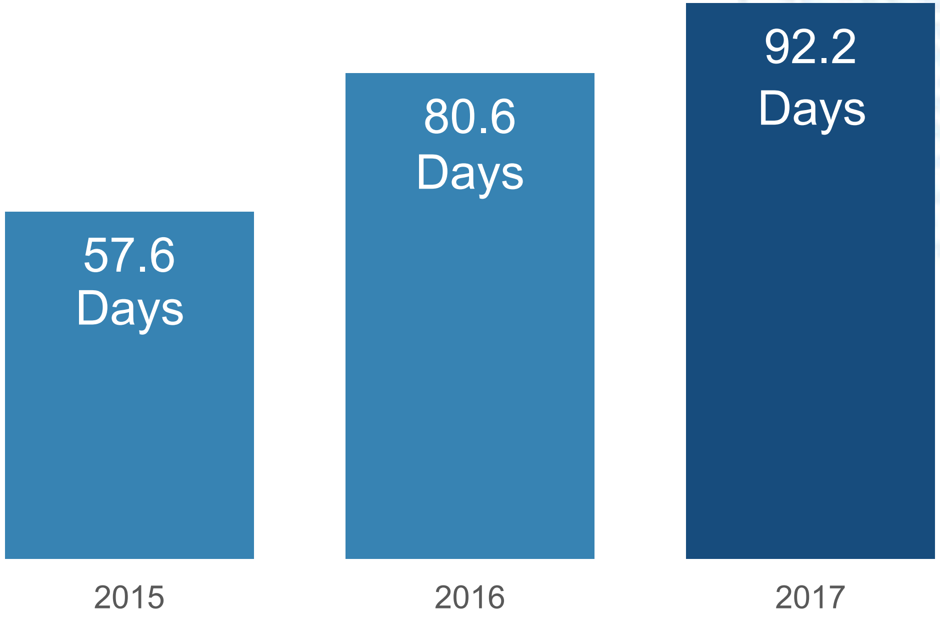
↑ **+7pp**

**card-not-present fraud**

*pp=percentage points*

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

## Average time to intrusion discovery has grown by more than one month since 2015

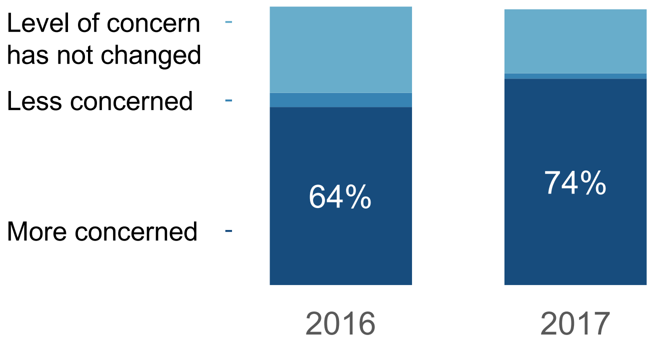


CSO FROM IDG

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

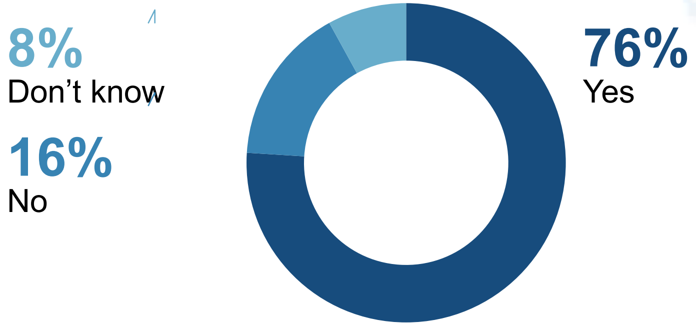
# Despite Confidence in Internal Expertise, Concern Level Rises

**Q: Are you more concerned or less concerned about cybersecurity threats to your organization in 2017 than you were in 2016?**



Big jump in concern about security threats

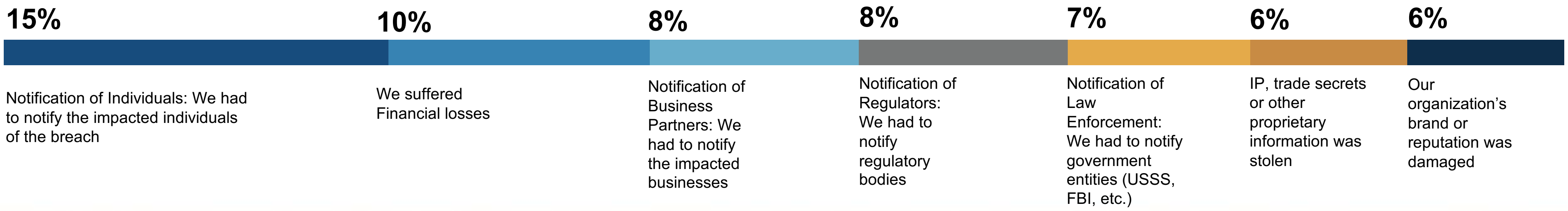
**Q: As new technologies or processes are introduced into your organization (cloud, mobile, social, data analytics, mobile payment systems, connected devices/IoT, etc.), does your organization have the expertise to address the cyber-risks associated with them?**



Business feel as though they have the expertise to address the risks associated with new technologies

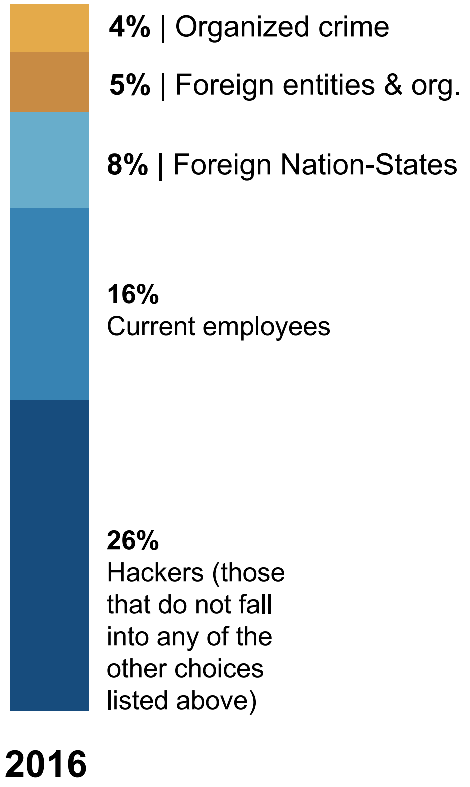
**Q: Please indicate which of the following resulted from the cybersecurity incidents your organization experienced in 2016.**

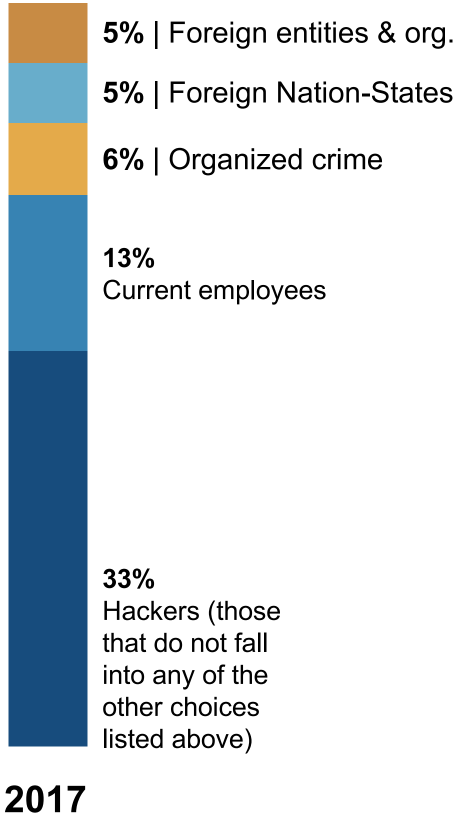
Top Impacts:



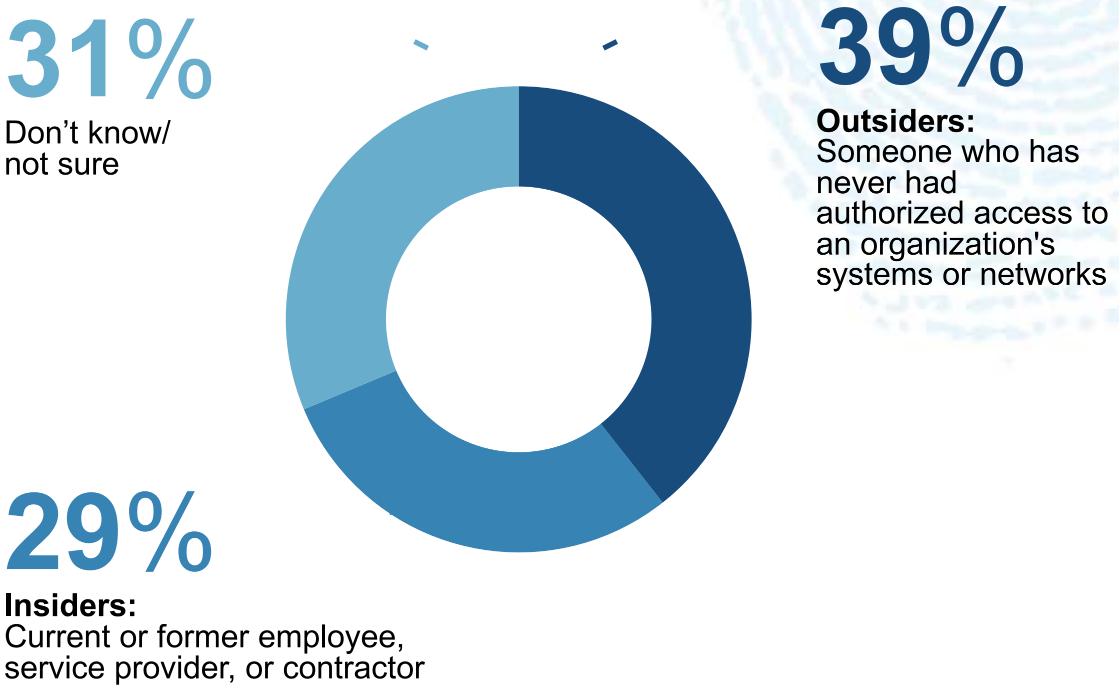
# Outsiders Are Generally Perceived as the Bigger Threat

**Q: Which of the following groups posed the greatest cyber threat to your organization during the past 12 months?**





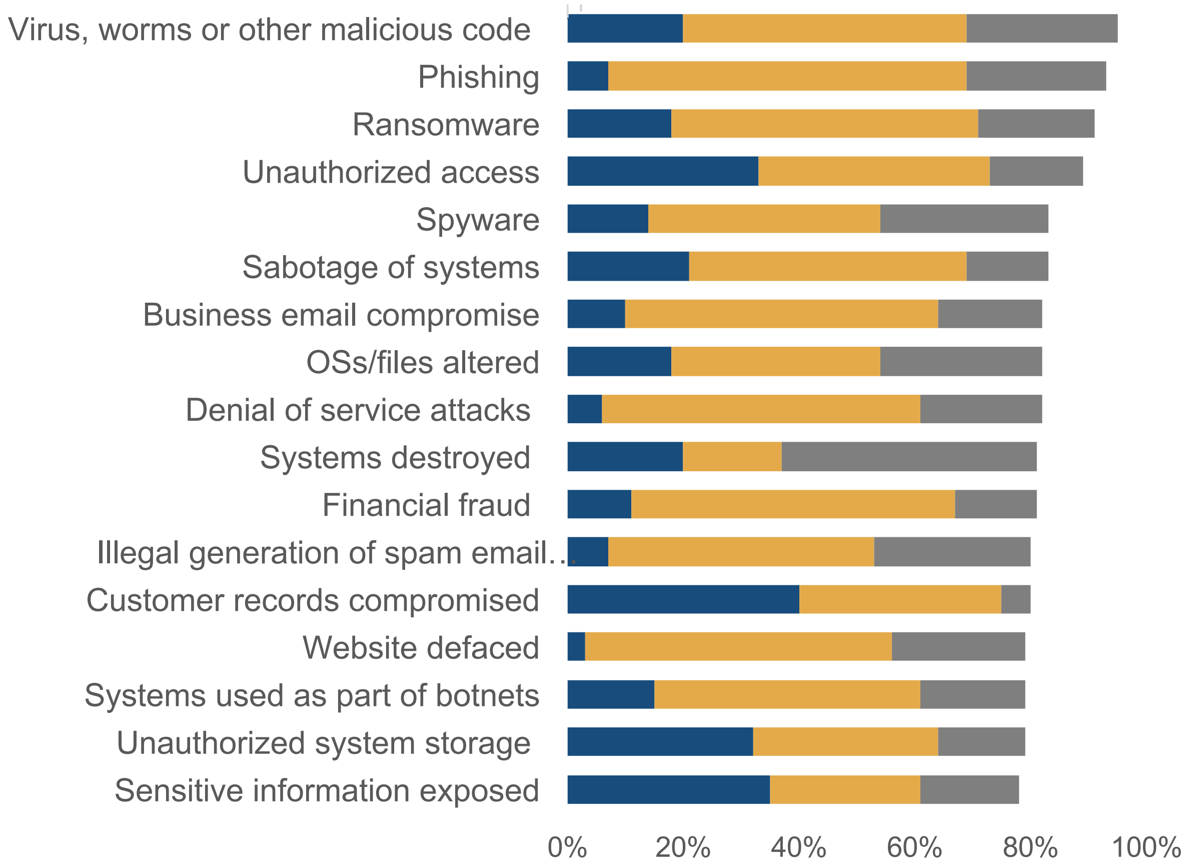
**Q: In general, cybercrimes were more costly or damaging to your organization when caused by:**

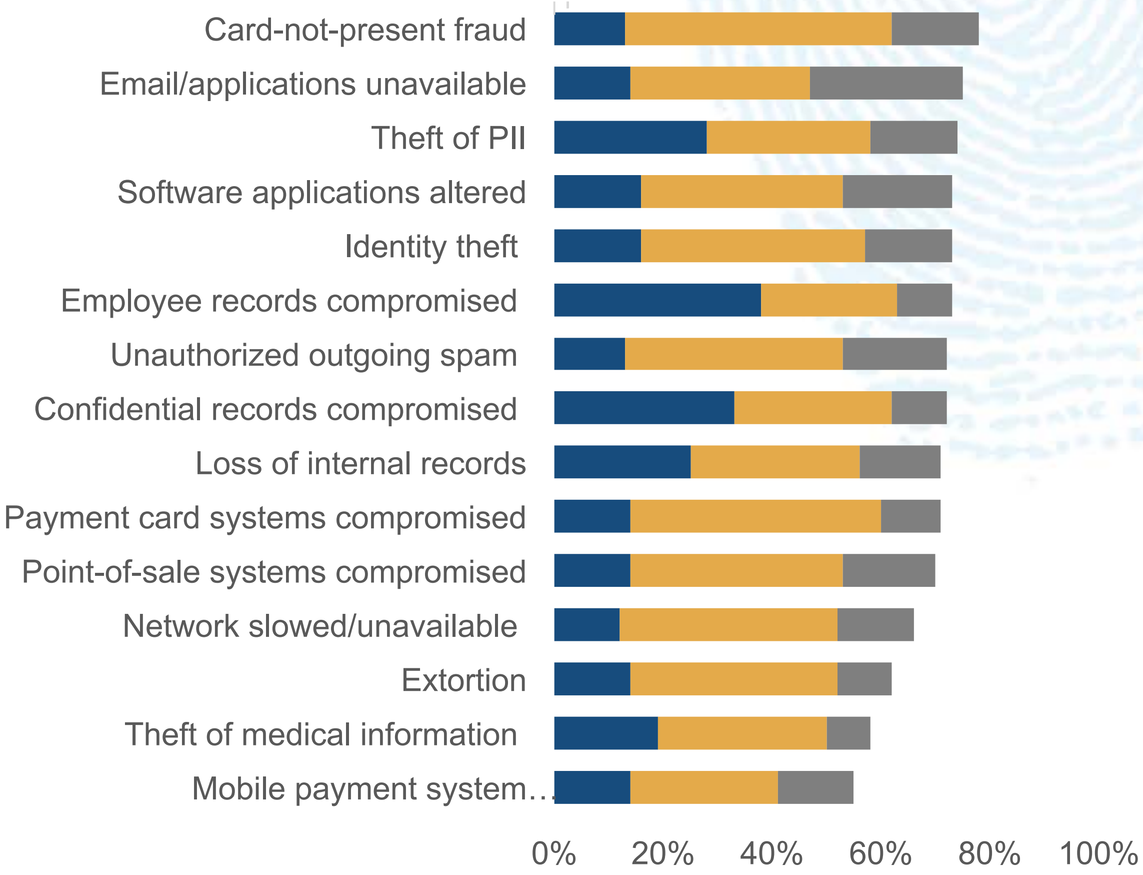


# Sources of Security Incidents

🟦 Insiders 🟧 Outsiders ⬛ Unknown

**Q: Please indicate the source(s) of these security incidents, to the best of your knowledge.**

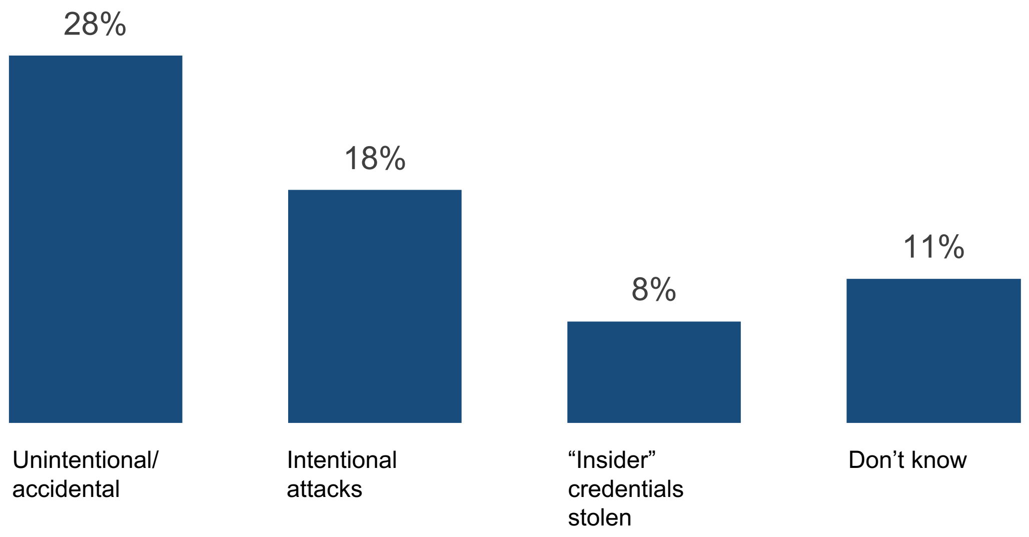




2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

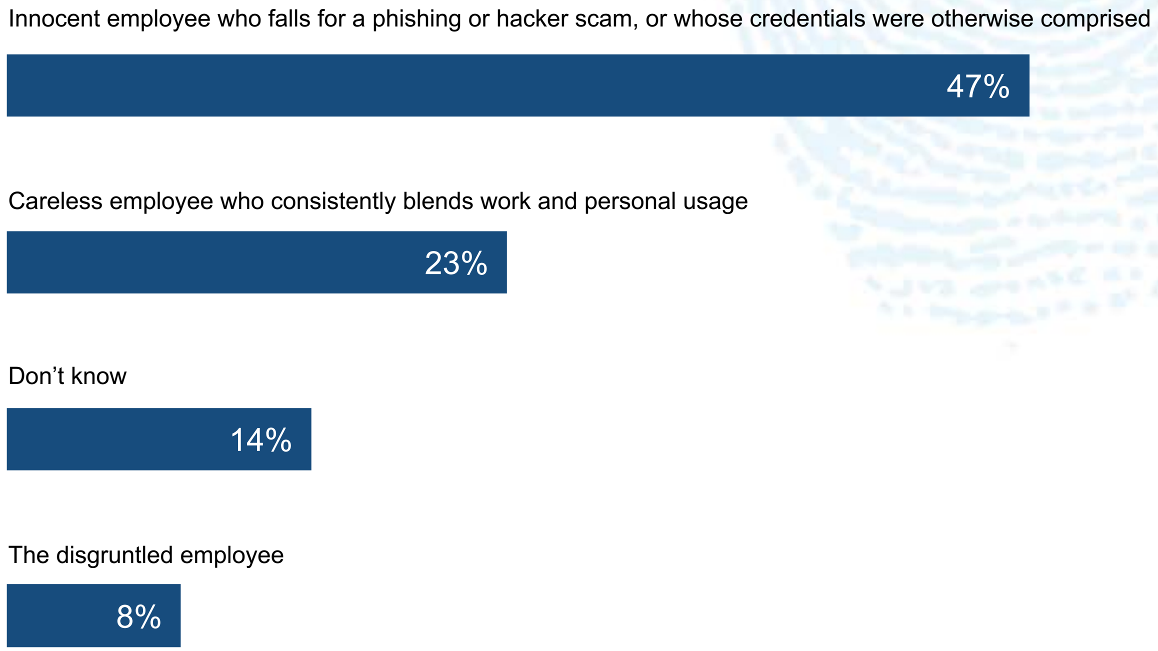
# Most Insider Security Events Are Caused By Employee Negligence, Highlighting The Need For Better Education Programs

**Q: Of the security incidents you know you experienced and for which you were able to attribute to an insider, what do you believe were the motivations behind the attacks?**



*Note: 45% report not applicable*

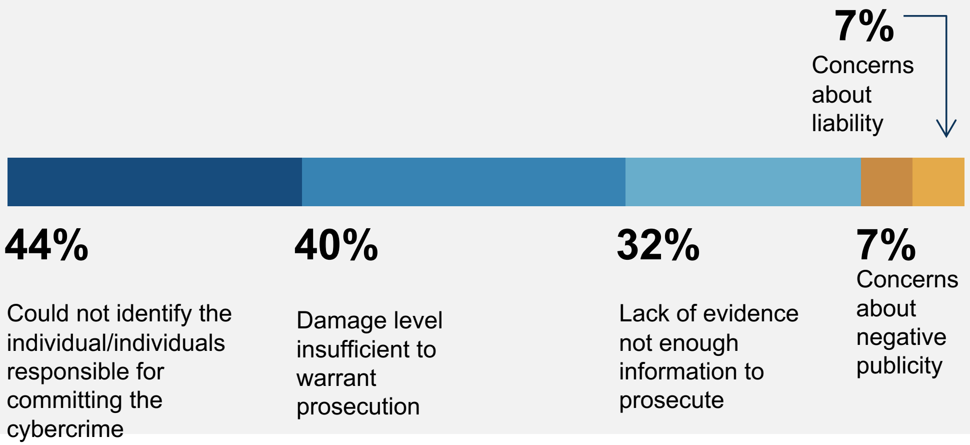
**Q: In your organization, which of these users pose the greatest risk for an Insider Threat incident?**



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

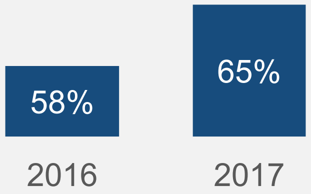
# Crime & Punishment: Increase in Targeted Attacks

**Q: If any cybersecurity events or cybercrimes were not referred for legal action, please indicate the reason(s) they were not referred.**



**Q: Please estimate the total monetary value of losses your organization sustained due to cybercrime and advanced persistent threats during the past 12 months, including those costs associated with resolving all issues associated with the incident.**

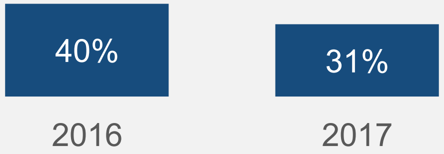
**Percentage of people answered "Don't know"**



Increasingly, businesses struggle to understand how much a security incident costs

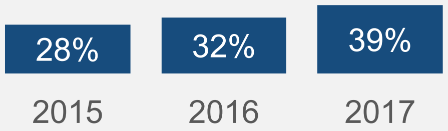
**Q: When considering the financial losses or costs to your company from those targeted attacks aimed at your company, has the financial loss or cost increased or decreased versus the previous year?**

**Percentage of people answered "Don't know"**

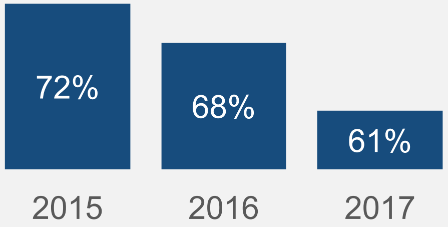


**Q: Of the security events your company experienced during the past 12 months, what percentage of these events were:**

- **Targeted attacks aimed at your company, your employees, your resources, or your customers**

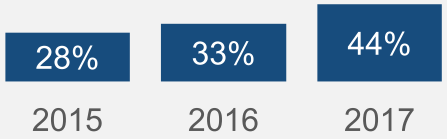


- **Non-specific or incidental attacks/malware that happened to impact your company, employees, resources, or customers**

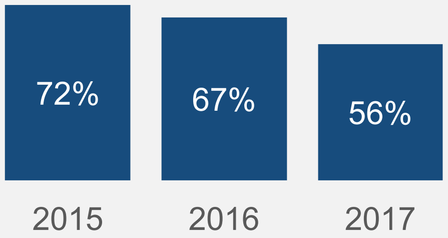


**Q: Of the security events your company experienced during the past 12 months that caused financial loss or cost, what percentage of these events were:**

- **Targeted attacks aimed at your company, your employees, your resources, or your customers**



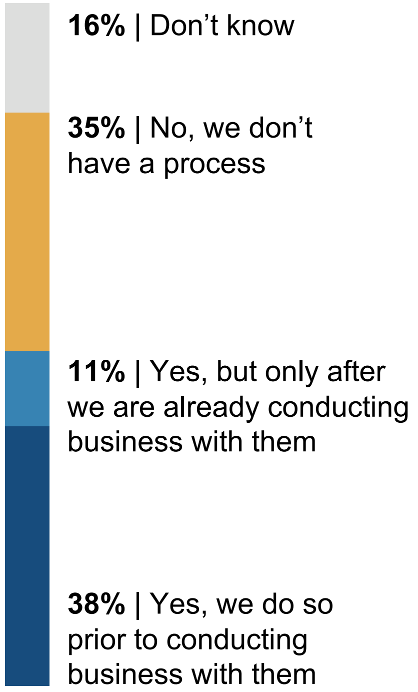
- **Non-specific or incidental attacks/malware that happened to impact your company, employees, resources, or customers**



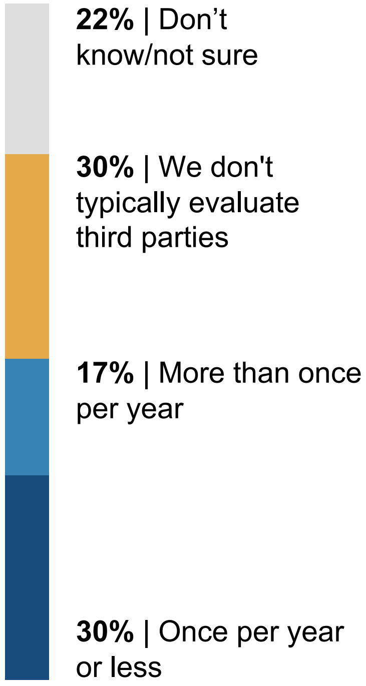
The 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

# Defending the Digital Business Ecosystem – Are Businesses Doing Enough?

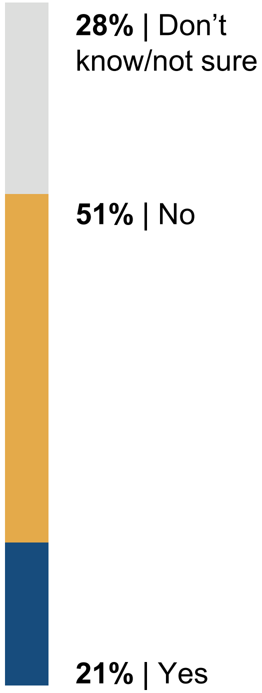
**Q: Do you have a process for evaluating the cybersecurity of supply chain/business ecosystem partners with whom you share data or network access (joint ventures, strategic partnerships, upstream or downstream supply chain, etc.)?**



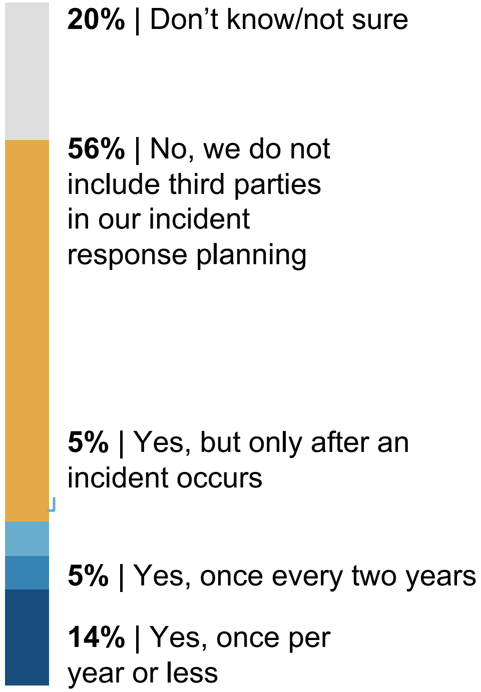
**Q: On average, how often do you evaluate the security of supply chain/business ecosystem partners with which you share data or network access?**



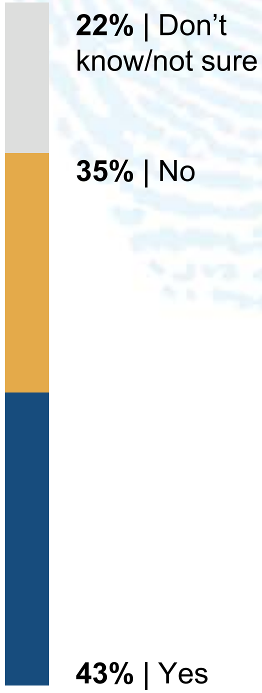
**Q: Has due diligence of supply chain/business ecosystem partners resulted in termination of a contract or business relationship?**



**Q: Do you conduct incident response planning/conduct table top exercises with your supply chain/business ecosystem partners?**



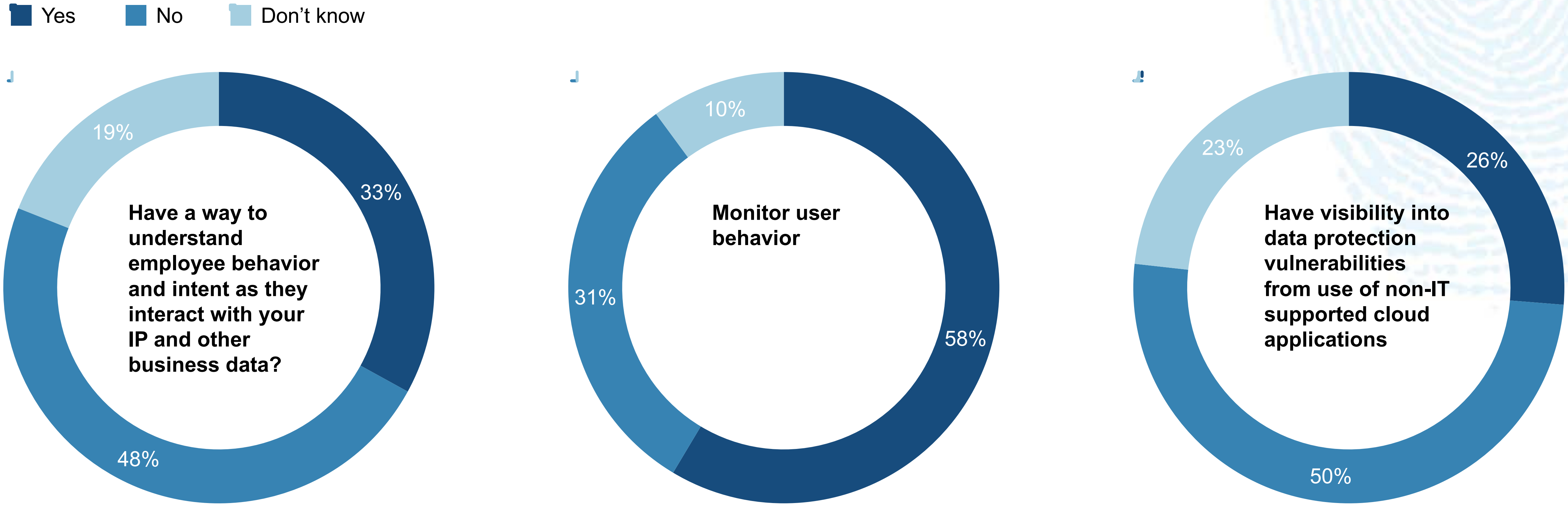
**Q: Do you have Service-Level Agreement with your supply chain/business ecosystem partners that specifies minimum cybersecurity standards?**



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

# Though Half of All Organizations Monitor User Behavior, Just One-third Have A Way To Interpret Intent

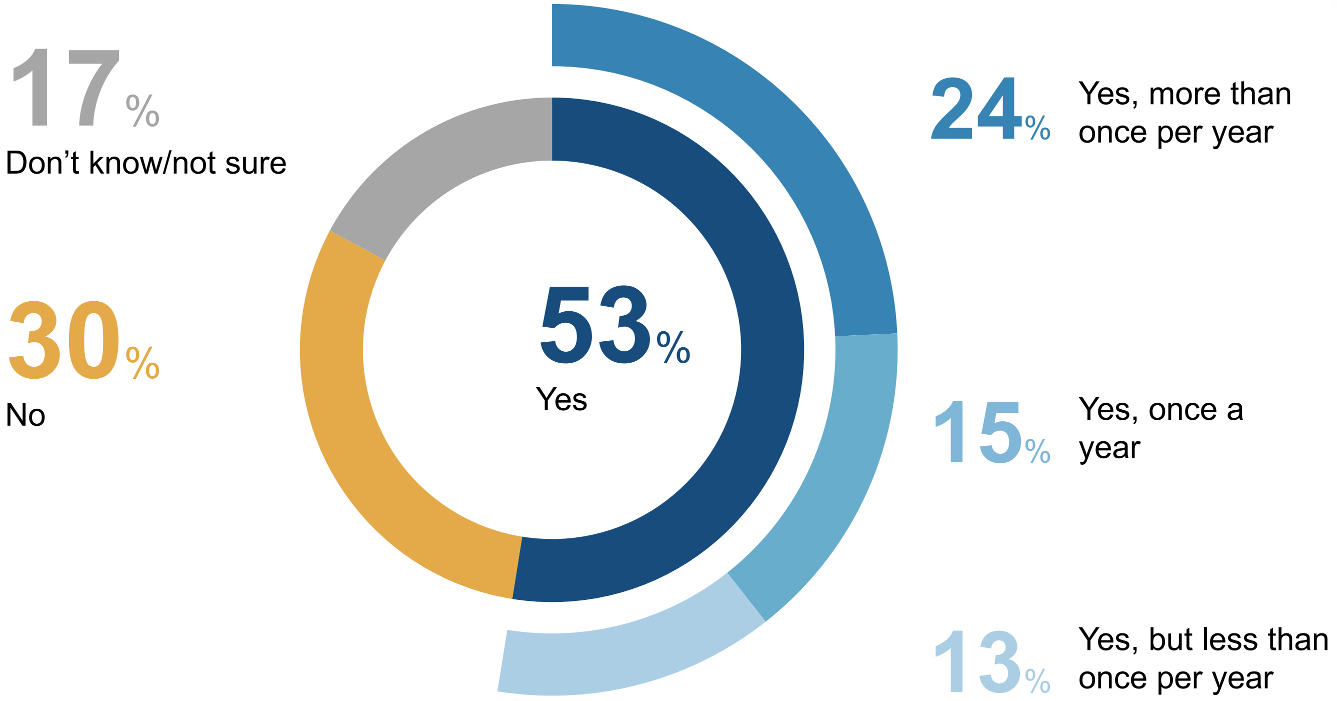
**Q: Does your organization currently:**



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

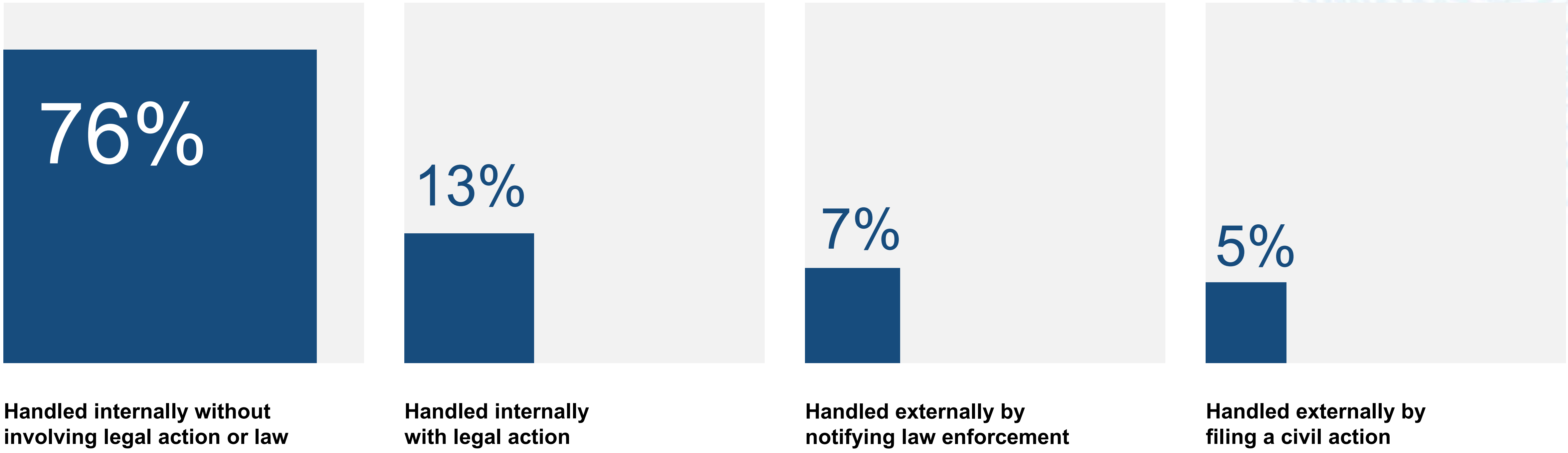
# Just One-third Are Measuring the Effectiveness of Security Programs Annually or More Often

**Q: Do you have a methodology that helps you determine the effectiveness of your organization's security programs based on clear measures?**



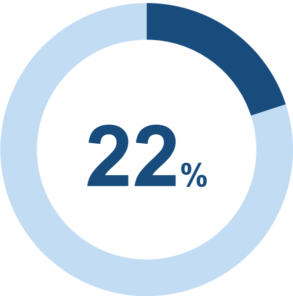
# In Most Cases, Cybercrimes Committed By Insiders Are Handled Internally

**Q: Please indicate the percentage of cybercrimes committed by insiders were:**

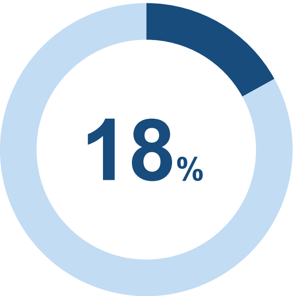


# Common Approaches to Insider Threat Funding Place Responsibility Squarely in IT's Hands

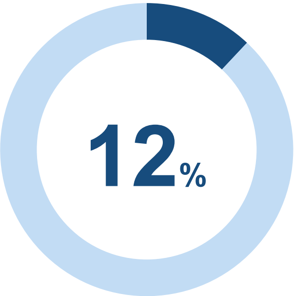
**Q: Describe your organization’s current approach to insider threat funding.**



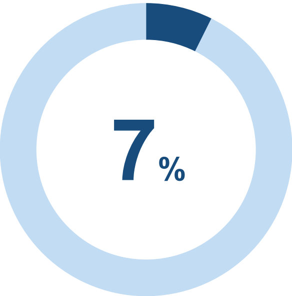
**IT initiative to upgrade security controls**



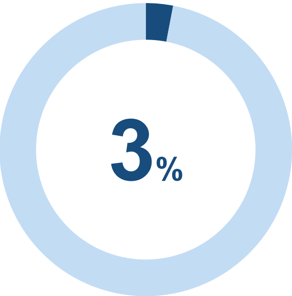
**IT budget is flexible if a solution is clearly superior and/or cost-cutting**



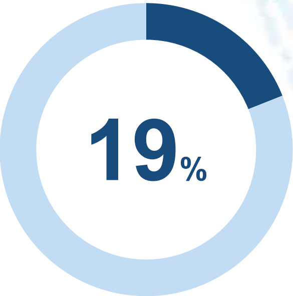
**Ongoing top-down company commitment and ample budget to stay ahead of the threats**



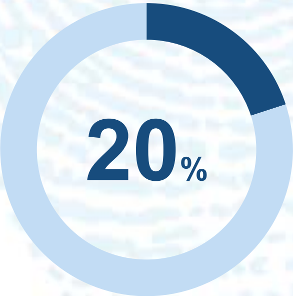
**Legal and compliance initiative to eliminate non-compliance fines or audit risks**



**HR organization initiative to observe user activity to protect both the employee and organization**



**Don’t know**



**Not applicable**

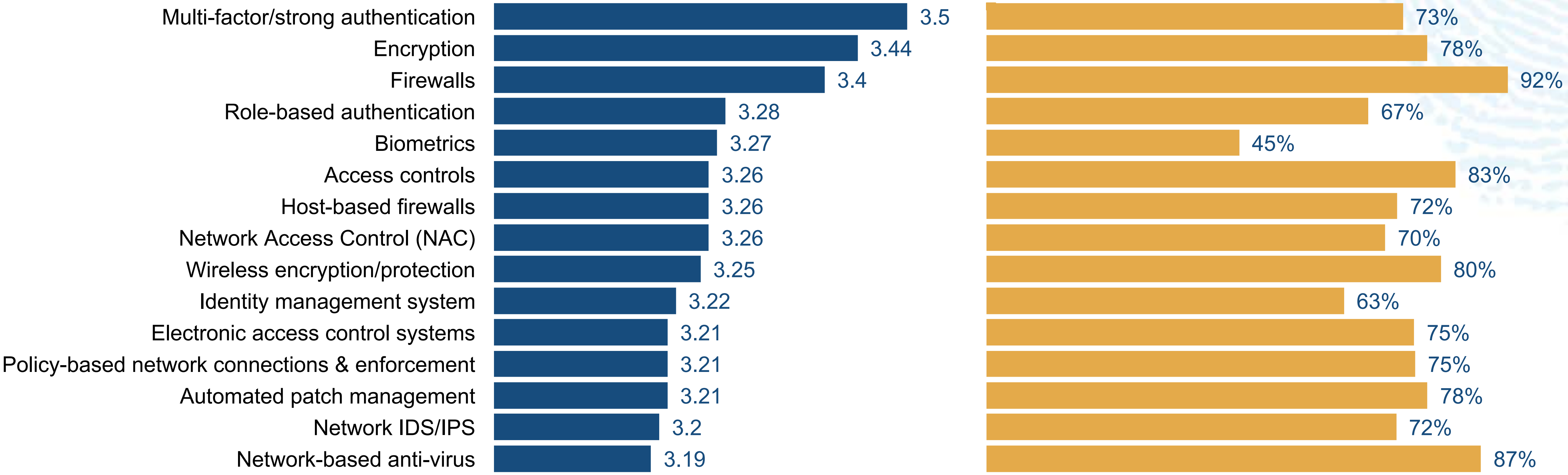
# Technology Usage and Effectiveness

**Q: How effective do you consider each of the following technologies in place at your organization in detecting and/or countering security events?**

Average Effectiveness – Top Ranked Technologies

*(1=Not at all effective; 5=Extremely effective)*

Percent with Each Technology in Use

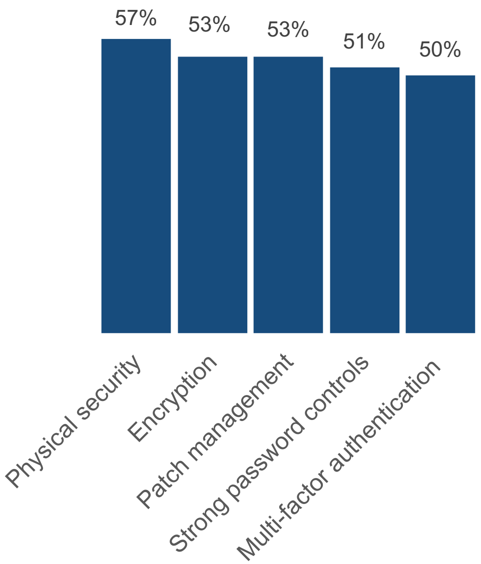


# So what do businesses tell us works?

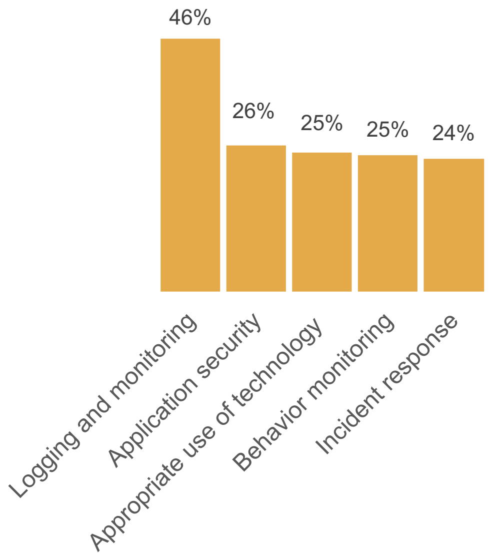
**Q: Have any of the following security policies and procedures at your organization supported or played a role in the following:**

Base: Organization uses security policies and procedures in an attempt to prevent or reduce security events (not ‘None of the above’, ‘Not applicable/no written policy in place’, or ‘Don't know’)

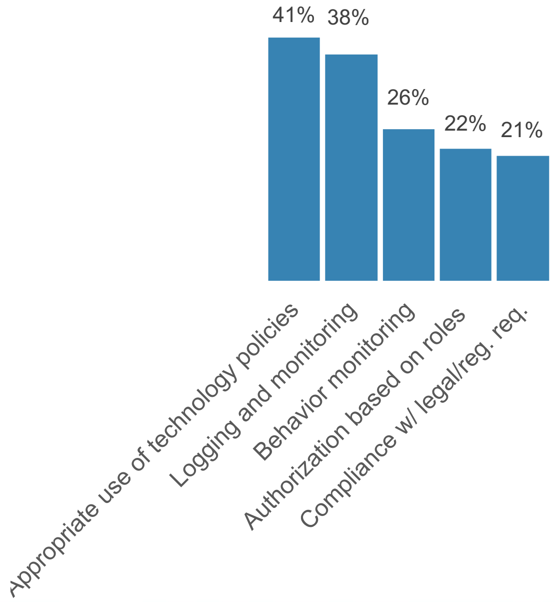
## Deterrence of a potential criminal



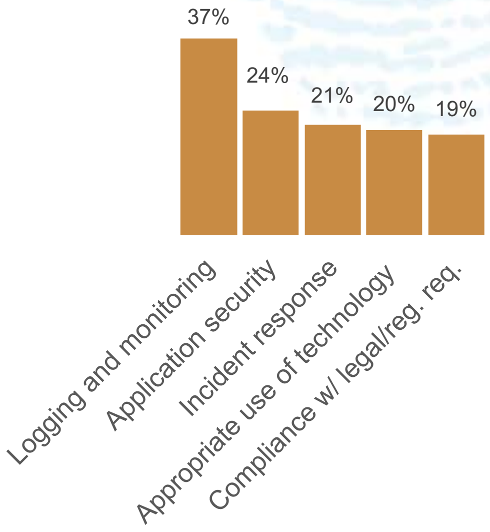
## Detection of a criminal



## Termination of an employee or contractor

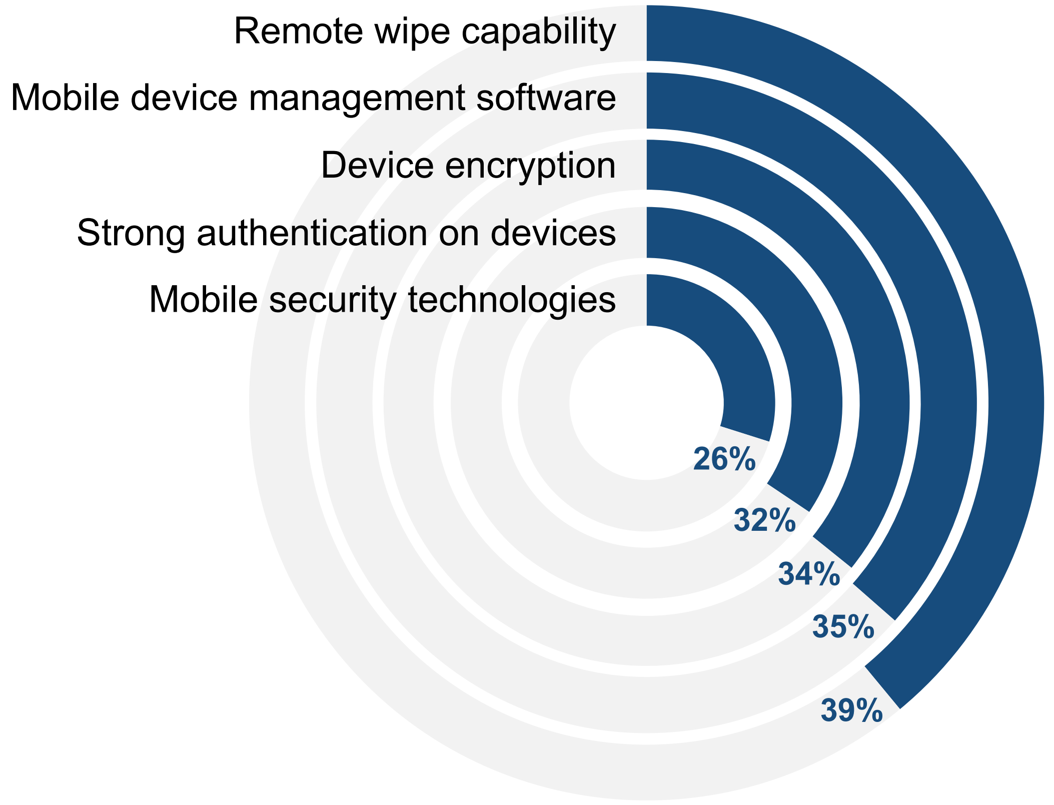


## Prosecution of an alleged criminal



# 26% Are Using Dedicated Mobile Security Technologies to Secure Devices

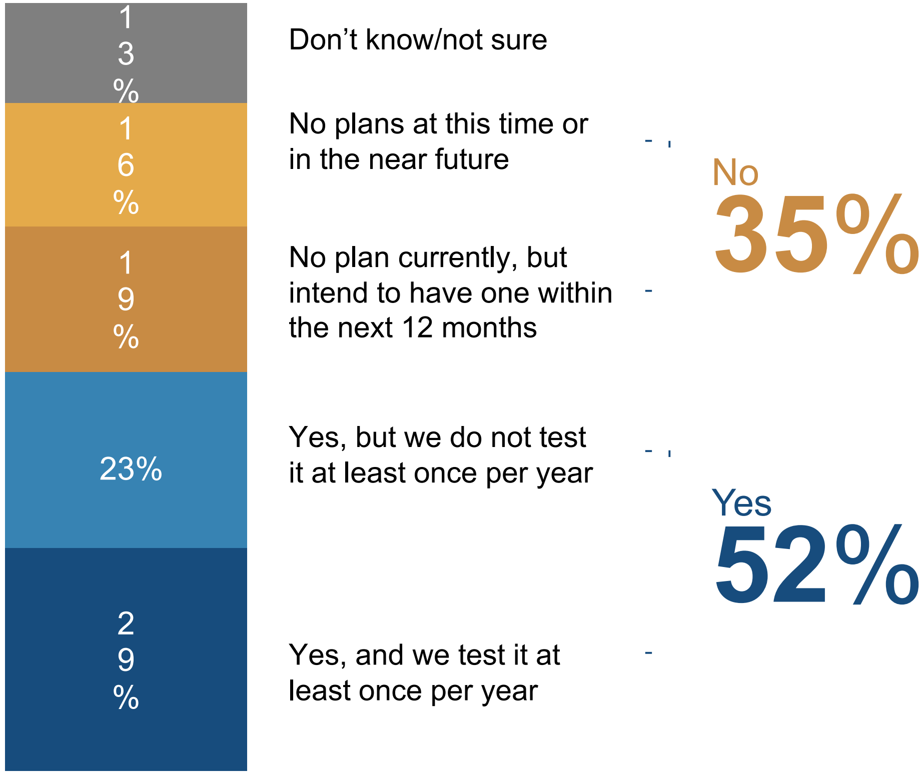
**Q: Which of the following does your company utilize to secure mobile devices (e.g., smartphones, tablets)?**



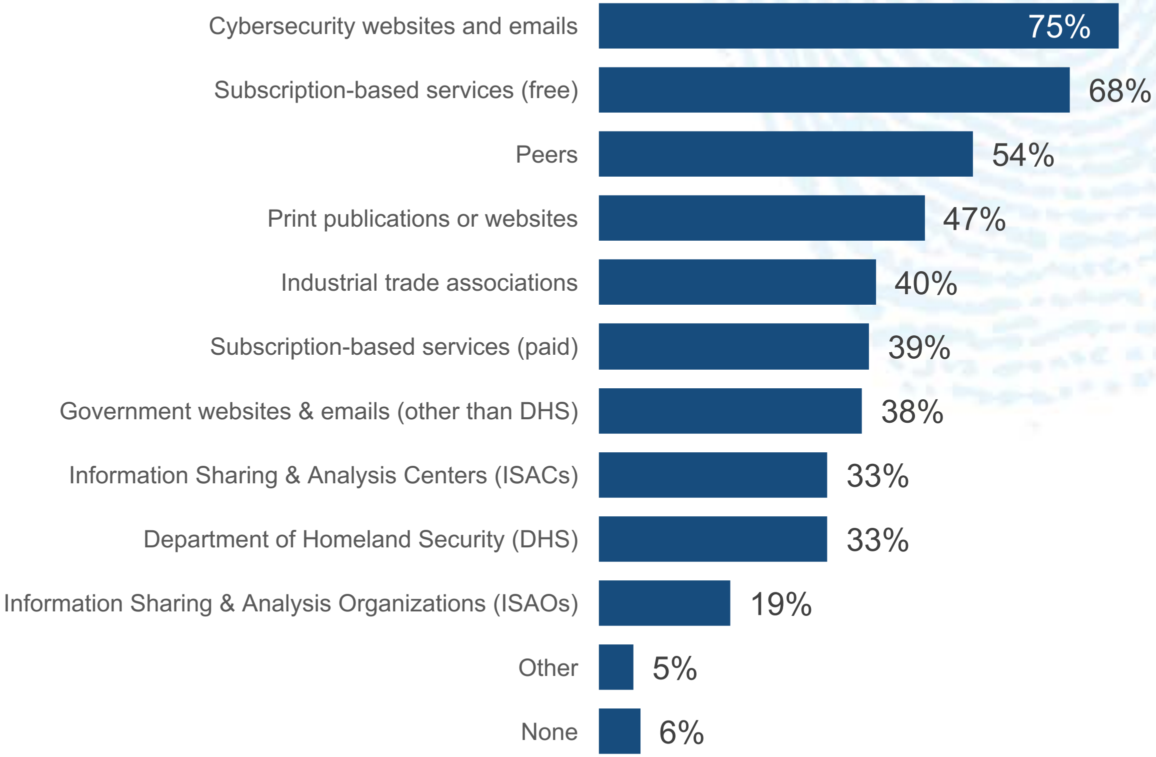
The 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

# Companies Monitor A Variety Of Sources to Keep Current on Threats, though Less Than One-third Update Cyber Response Plans Frequently

**Q: Does your organization have a formalized plan outlining policies and procedures for reporting and responding to cyber events committed against your organization?**



**Q: Please identify all sources you monitor to keep up with current trends, threats, vulnerabilities, technology, and warnings.**



# Conclusions

- Organizations rely on a number of information sharing organizations, but overall sharing remains a challenge
- The board of directors is playing a greater role – but the reasons vary by organization
- While IT security budgets continue to grow, and those investments are driving down the number of known security events, monetary losses haven’t really moved
- Successful phishing and ransomware attacks are climbing – and threats, overall, are becoming more difficult to detect
- Concerns about security threats took a significant jump this year
- Outsiders continue to be perceived as the greater threat and targeted attacks are becoming more prevalent. At the same time Insiders are falling for phishing scams and being careless, pointing to the need for better security & awareness training
- There remain significant holes in our digital business ecosystems
- While businesses collect lots of data, they struggle to identify intent in it – and only slightly more than half measure the effectiveness of their efforts
- Businesses still, overwhelmingly, handle the dirty laundry of insider attacks themselves without involving law enforcement
- Logging & Monitoring, as well as Encryption, continue to be perceived as highly effective in addressing cybercrime concerns

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