Decoding Cyber Risk

2017 Willis Towers Watson Cyber Risk Survey

US results

Willis Towers Watson

Executive summary

Cybersecurity is viewed as a fundamental challenge and a top priority for organizations.

Many companies feel they are on the right track in terms of data privacy and information security risk management.

But most recognize that this is a journey, and many are looking to create a culture of cybersecurity in their organization.

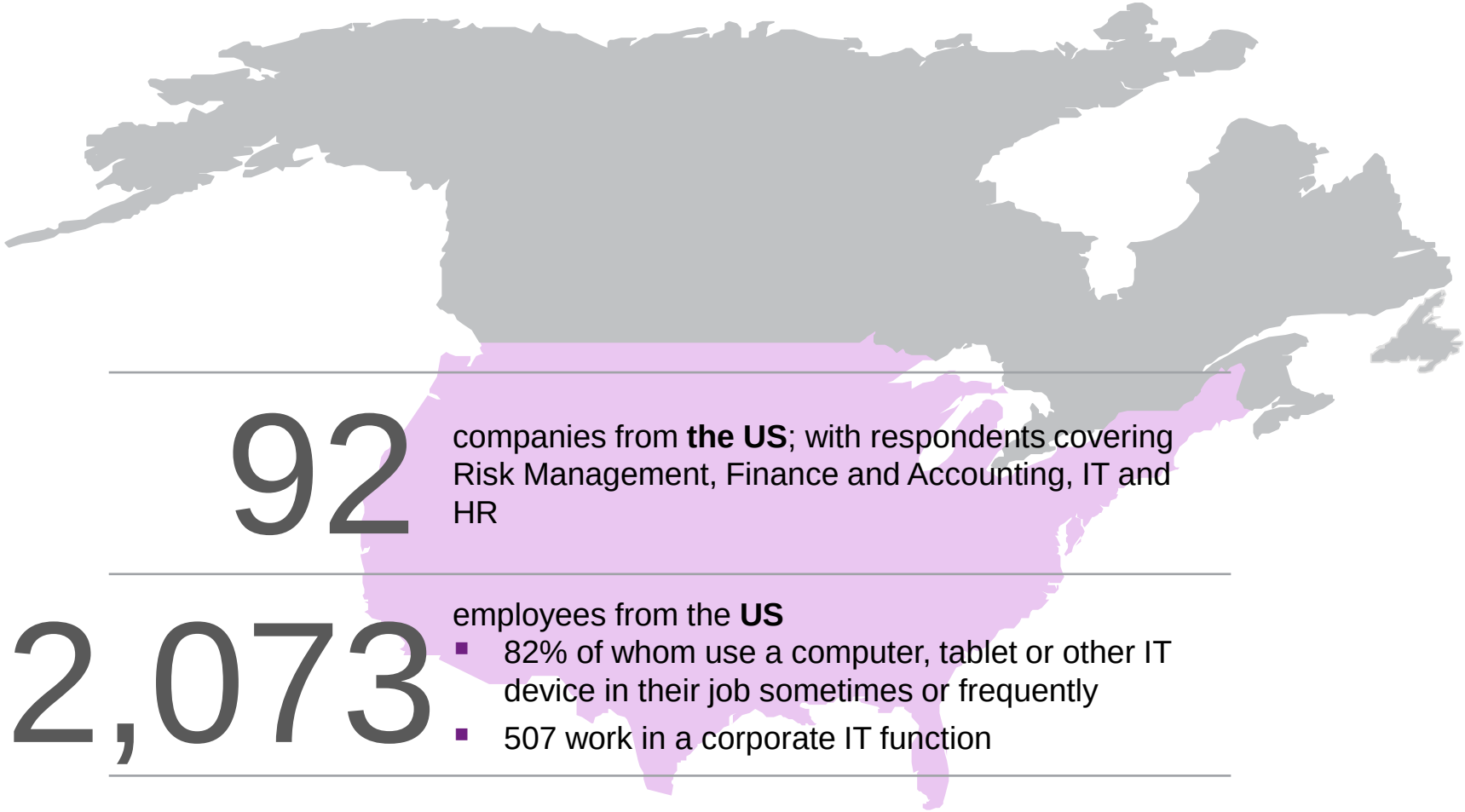
Many threats exist around employee behaviors, and the vulnerabilities they create will be a top priority over the next three years.

Immediate priorities are:

- Training for employees and contractors
- Reviewing the cyber insurance gap and adding coverage

About the survey

US responses



92 companies from **the US**; with respondents covering Risk Management, Finance and Accounting, IT and HR

2,073 employees from the **US**

- 82% of whom use a computer, tablet or other IT device in their job sometimes or frequently
- 507 work in a corporate IT function

Cyber risk

Developing a culture of cybersecurity

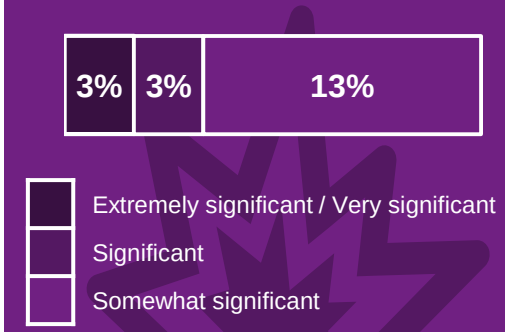
Cyber security is a fundamental challenge for US business

One in five companies have suffered a cyber breach in the last year

20%

reported that their organizations have been impacted by a **cyber breach** in the last year.

(Percentage of Somewhat significant/Significant/Very significant/Extremely significant)



16%

reported occasions when senior leaders have put **confidential information** at **risk** over the last three years.

(Percentage of Strongly agree or Agree)

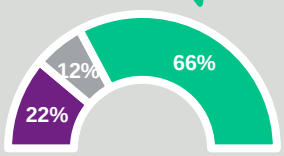
Note: May not sum to total due to rounding.
Source: 2017 WTW Cyber Risk Survey, US.

Cyber security is a fundamental challenge for US business

Two-thirds see cyber risk as a fundamental challenge to their business

66%

see cyber security as a **fundamental challenge** for their business.



ANOTHER RISK TO THE BUSINESS

NEUTRAL

FUNDAMENTAL CHALLENGE

85%

view cyber security as a **top priority** for their company.

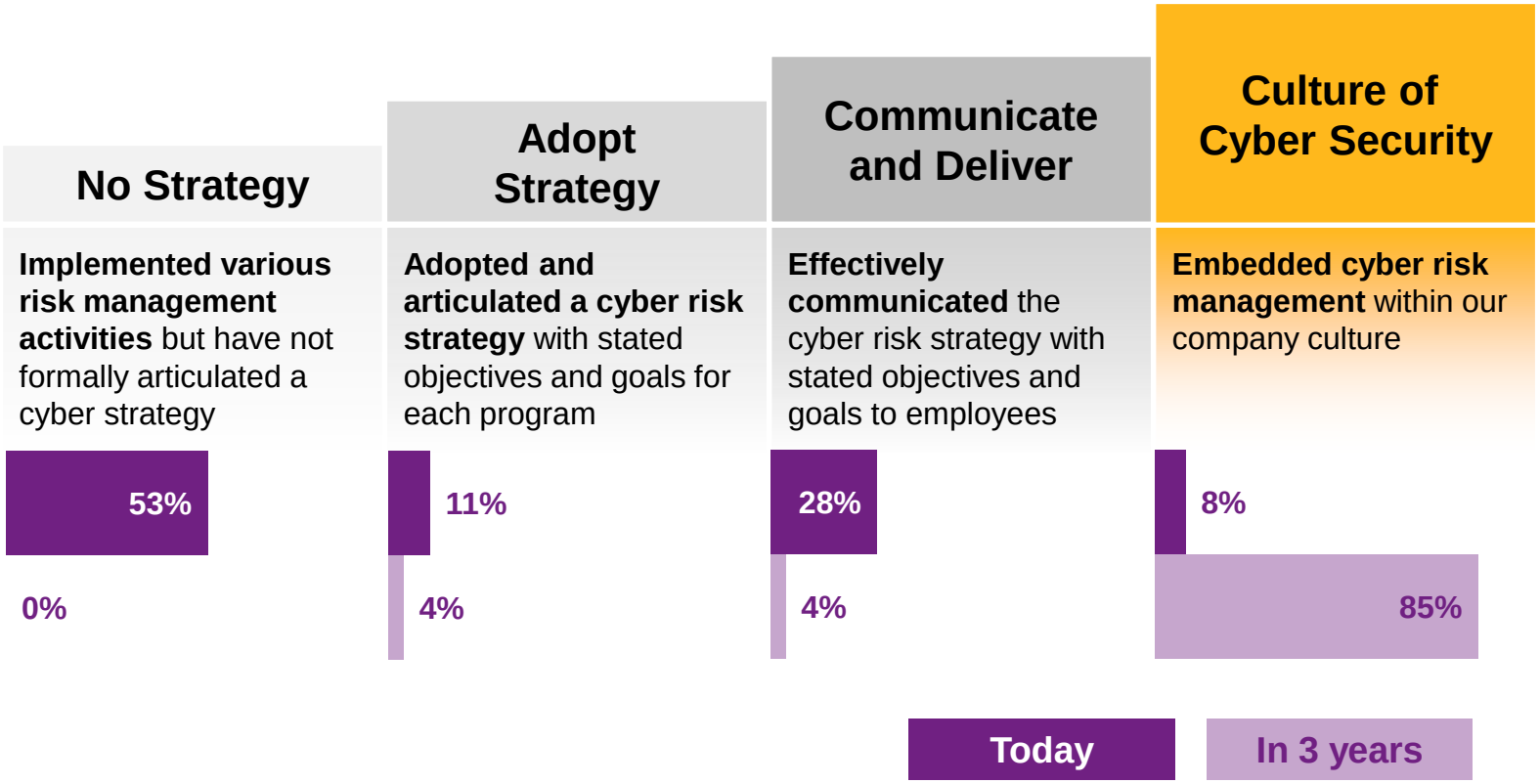
(Percentage of Strongly agree or Agree)

Source: 2017 WTW Cyber Risk Survey, employer survey, US.

Companies aspire to develop a culture of cyber security

Companies have adopted a wide range of cyber risk management activities, but few have embedded them into their company culture

Which of the following best describes what your organization has accomplished in your cyber risk strategy to date and what you expect to accomplish in the next three years?



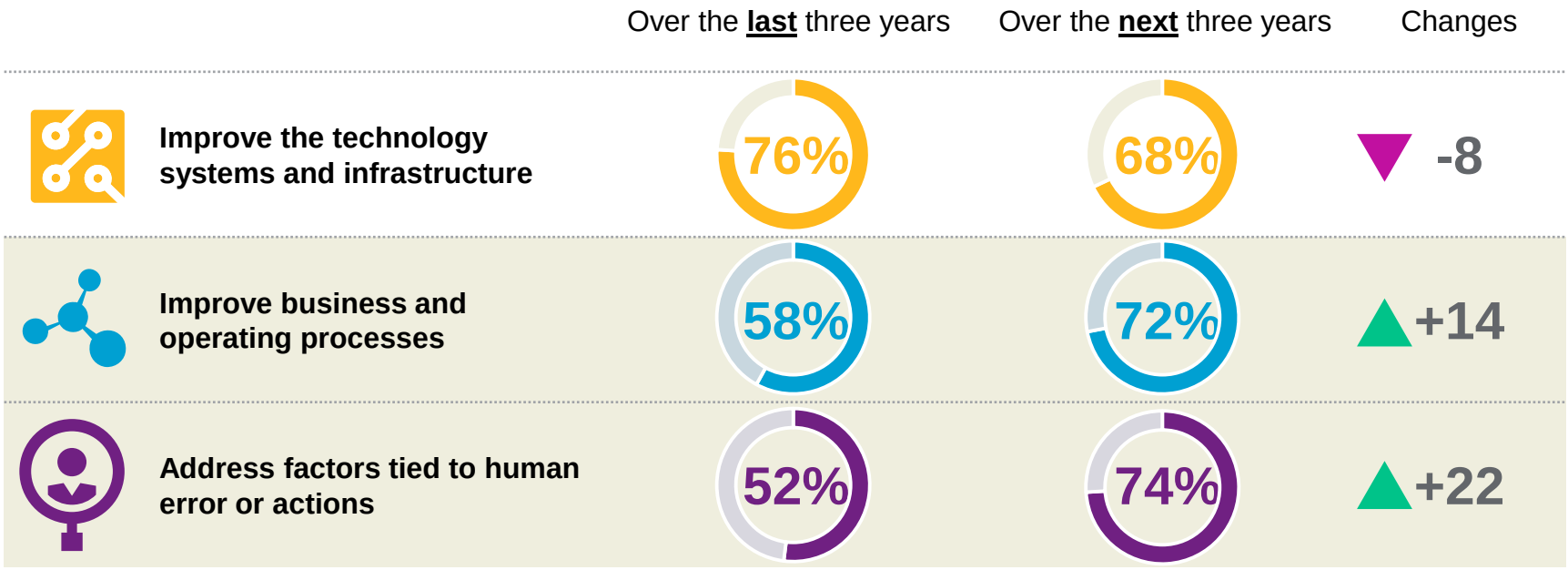
Source: 2017 WTW Cyber Risk Survey, employer survey, US.

Cyber risk

Actions, priorities and barriers

The initial focus was chiefly on technology, but increasingly this will shift to employee behavior and operating procedures

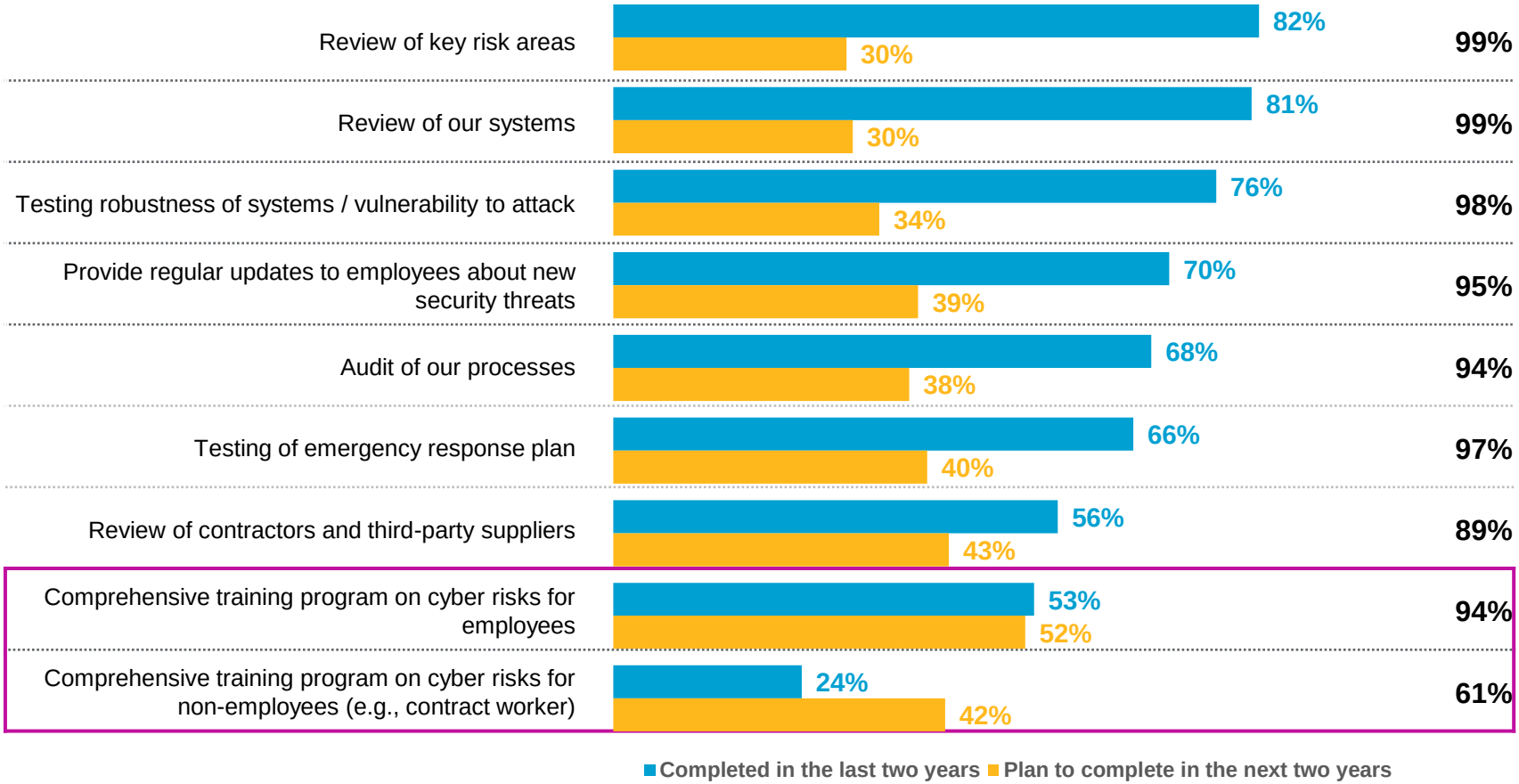
To what extent has your organization made progress in the following areas to mitigate vulnerability to a cyberattack over the last/next three years?



Note: Percentages indicate 'To a great extent' or 'To a very great extent'.
Source: 2017 WTW Cyber Risk Survey, employer survey, US.

The initial focus was chiefly on technology, but increasingly this will shift to employee behavior and operating procedures

Has your organization completed in the last two years, or does it plan to complete in the next two years, any of the following cyber risk related activities?



Source: 2017 WTW Cyber Risk Survey, employer survey, US.

Over nine in 10 companies have reviewed or will review their existing cyberinsurance, with eight in 10 looking to enhance coverage

Review and identify gaps in existing insurance coverage

94% Completed over last two years or plan to complete in next two years

66% Completed in last 2 years

37% Complete in next 2 years

9% do both

Add or enhance cyberinsurance coverage

81% Completed over last two years or plan to complete in next two years

54% Completed in last 2 years

36% Complete in next 2 years

9% do both

Source: 2017 WTW Cyber Risk Survey, employer survey, US.

Most organizations have centralized their approach to data privacy and information security

To what extent does your organization have a centralized or decentralized approach to data privacy and information security?

67%

Centralized

15%

Neutral

18%

Decentralized

Note: Centralized = respondents giving a 1 to 3 score; Decentralized = respondents giving a 5 to 7 score; Neutral = respondents giving a 4 score.

Source: 2017 WTW Cyber Risk Survey, employer survey, US.

Most companies feel they have appropriate levels of resources, clearly defined roles and responsibilities, and consistent policies

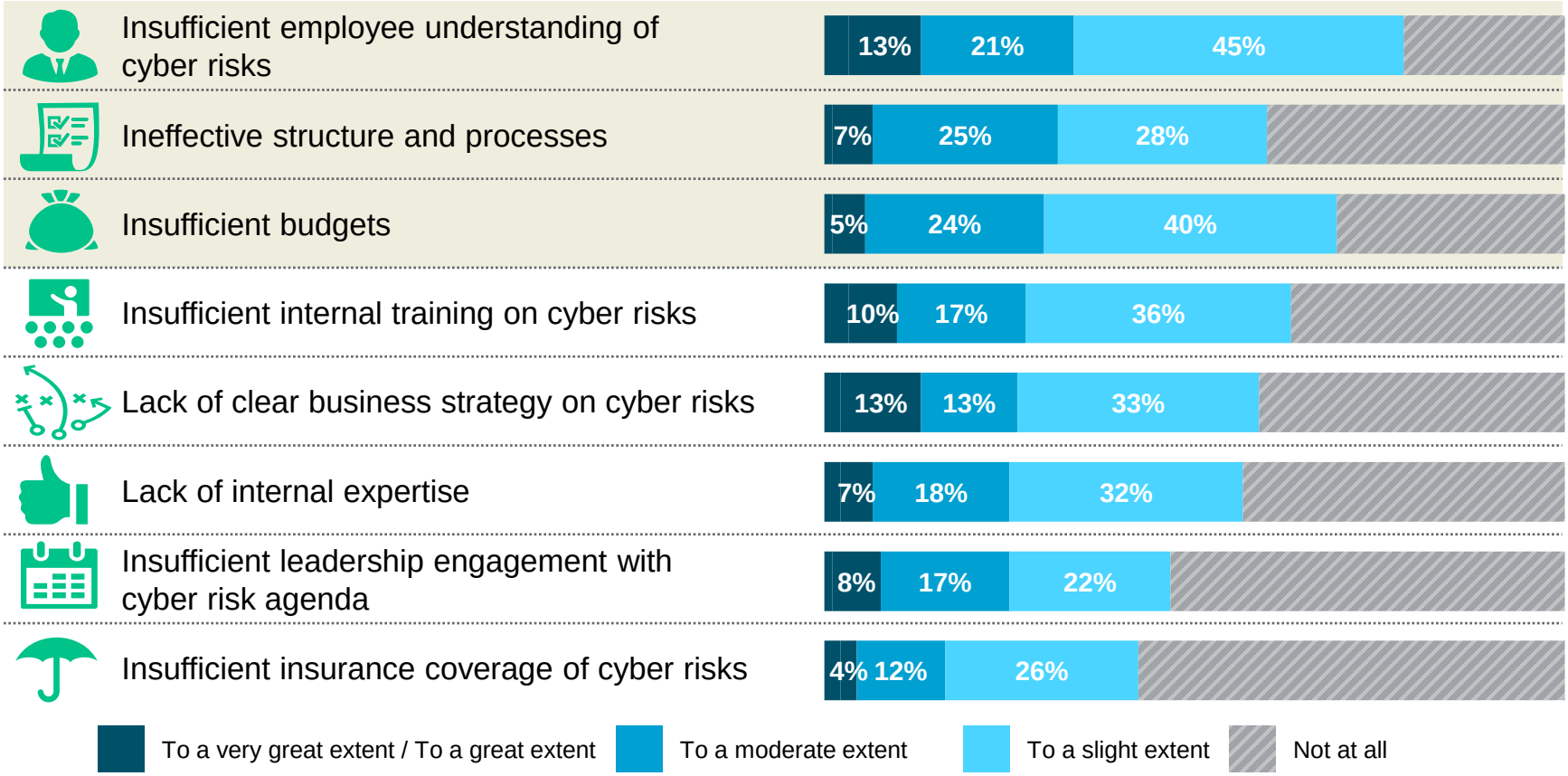
Our organization has an appropriate amount of support from centralized (corporate-level) resources	78%
It is clear which parts of the company are responsible for data privacy and information security	73%
Our organization does an effective job of finding the most qualified individuals to support our cyber risk operations	69%
Our organization has an appropriate amount of local-level support	65%
Our organization has consistent data management and information security policies across all aspects of the business	63%
Our organization has adequate budgets to meet all its cyber risk management needs	43%
The risk management and HR functions work closely together on cyber risk management	37%

But concerns exist about sufficient budgets and room for improvement in how risk management and HR work together

Note: Percentages indicate Agree or Strongly agree.
Source: 2017 WTW Cyber Risk Survey, employer survey, US.

A lack of employee awareness, ineffective processes and insufficient budgets are perceived as the key cyber risks

To what extent are the following barriers preventing your organization from effectively managing its cyber risks?



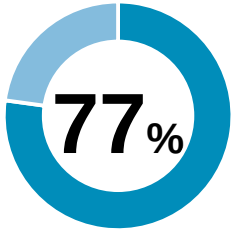
Source: 2017 WTW Cyber Risk Survey, employer survey, US.

Cyber risk

Does employee behavior match company policy?

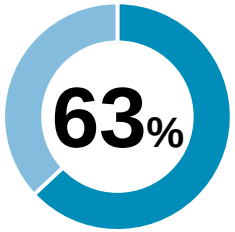
A large number of employees assume central IT is protecting them

Employer View



(% of 'Strongly agree' or 'Agree')

The organization communicates effectively to employees about data privacy and network best practices.



(% of 'Strongly agree' or 'Agree')

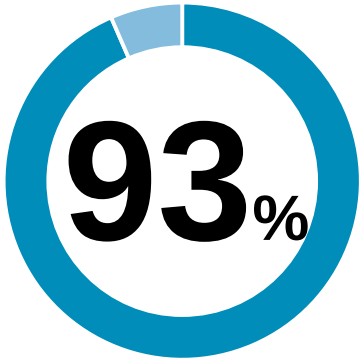
Our organization has consistent data management and information security policies across all aspects of the business.

Employee Behavior

Opening any email on my work computer is safe	46%	*(% of 'Strongly agree' or 'Agree')*
Discussed work-related topics in public places	41%	*(% of 'Frequently' or 'Sometimes')*
Shared network password with a work colleague	15%	*(% of 'Yes')*
Developed an issue with your work computer due to an action you took (e.g., surfing websites, downloading software)	15%	*(% of 'Yes')*

Source: 2017 WTW Cyber Risk Survey, employer survey and employee survey, US.

Are employees comfortable reporting incidents?



Employer View

believe that they have provided an environment in which employees are comfortable reporting about data privacy and data security.

Employee Behavior

80%

know the steps to take if they suspect sensitive information is at risk or has been stolen.

Received a suspicious email at work meant to trick you into opening a harmful link or attachment — **43%**

Among them, eight in 10 reported the suspicious email to IT department

Witnessed co-workers behaving in ways inconsistent with data privacy and information security policies — **34%**

Discussed information security risks with your immediate manager — **32%**

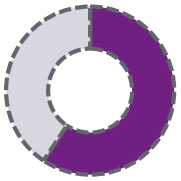
(% of 'Yes')

- **53%** Reported to manager or IT department
- **31%** Only spoke with those individuals
- **15%** Took no action

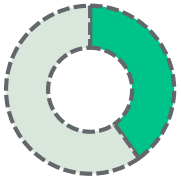
Source: 2017 WTW Cyber Risk Survey, employer survey & employee survey, US.

Over half of employers perceive data privacy threats by employees or contractors — but employees are less aware

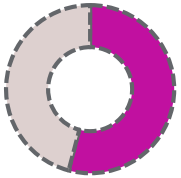
A disgruntled employee or contractor could deliberately compromise our systems or steal customer/client data?



59% Employers



40% All employees



56% IT professionals

Note: Percentages indicate ‘Agree’ or ‘Strongly agree’.
Source: 2017 WTW Cyber Risk Survey, employer survey & employee survey, US.

Does employee behavior match company policy?

Employer View

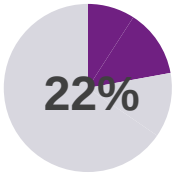
75%

of organizations have a strict policy regarding applications and software that can be downloaded by employees.

(% of 'Strongly agree' or 'Agree')

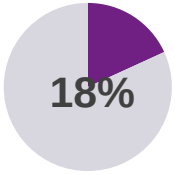
Employee Behavior

Use personal computing devices that have not been approved by your company's IT department to do work at home



(% of 'Frequently' or 'Sometimes')

Downloaded software onto your work computer that was not approved by your IT department



(% of 'Yes')

Employer View

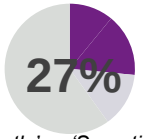
72%

of employers believe that they are doing enough to protect the integrity of customer/client data.

(% of 'Strongly agree' or 'Agree')

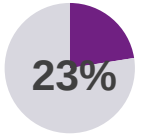
Employee Behavior

Remove paper files with confidential information from the office to do work at home



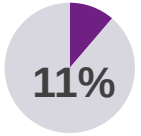
(% of 'Frequently' or 'Sometimes')

Sent or received an important or confidential work file via email without password protection



(% of 'Yes')

Sent a confidential work file via email to the wrong recipient



(% of 'Yes')

Source: 2017 WTW Cyber Risk Survey, employer survey & employee survey, US.

Awareness of social engineering risk among employees needs to be enhanced

Regarding how you use technology, do you…?

Protection from social engineering attacks

Disable features that let you auto-save passwords on your personal computing devices

Purchase a personal identity theft protection service

Vulnerabilities to social engineering attacks

Only change the password on my work computer when prompted

Share personal information (e.g., date of birth, employer name, job title) in profiles on social media sites

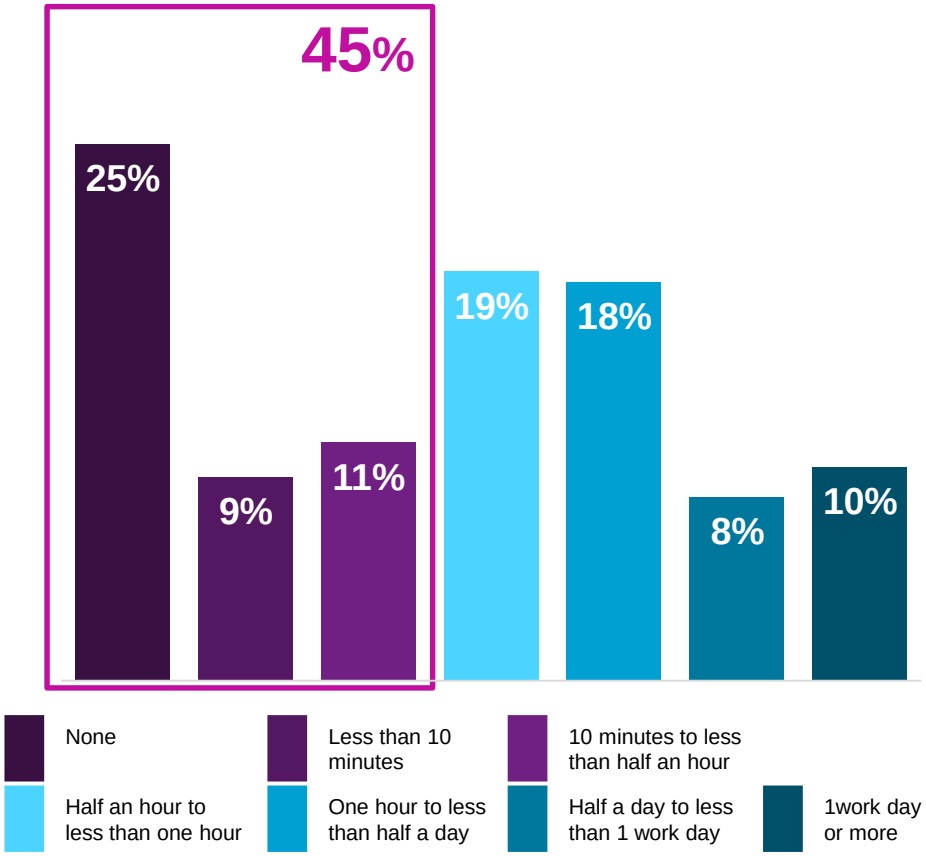
Use the same passwords across all your personal computing devices

Source: 2017 WTW Cyber Risk Survey, employee survey, US.

How engaged are employees with their company training programs?

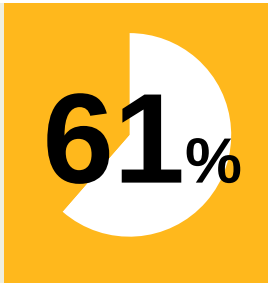
Nearly half of employees spent less than 30 minutes in training in the last year.

Over the past 12 months, how much time have you spent in training specific to data protection and information security at your company?



61% of employees completed the training only because it was required by their companies.

(% of 'Strongly agree/Agree')



Employees benefit from training

It improved my understanding of the steps I need to take to better protect confidential information	78%
It increased my sense of personal responsibility for data security at work	77%
It taught me something new about data and information security	71%
It motivated me to change how I manage my personal computing devices	63%

(% of 'Strongly agree/Agree')

Source: 2017 WTW Cyber Risk Survey, employee survey, US.

We define four types of employees according to how they use technology at work or at home

Alert

Employees who protect personal information in daily life and are aware of information security at work

37%

Comply

Employees who behave at work in compliance with data/information protection policies but are careless with personal behaviors

24%

Ignore

Employees who pay attention to the protection of personal information, but whose behaviors at work fall short

21%

Unconcerned

Employees whose behaviors of using technology both at work and at home may lead to potential cyber risks

18%

Based on the following questions:

PERSONAL BEHAVIORS

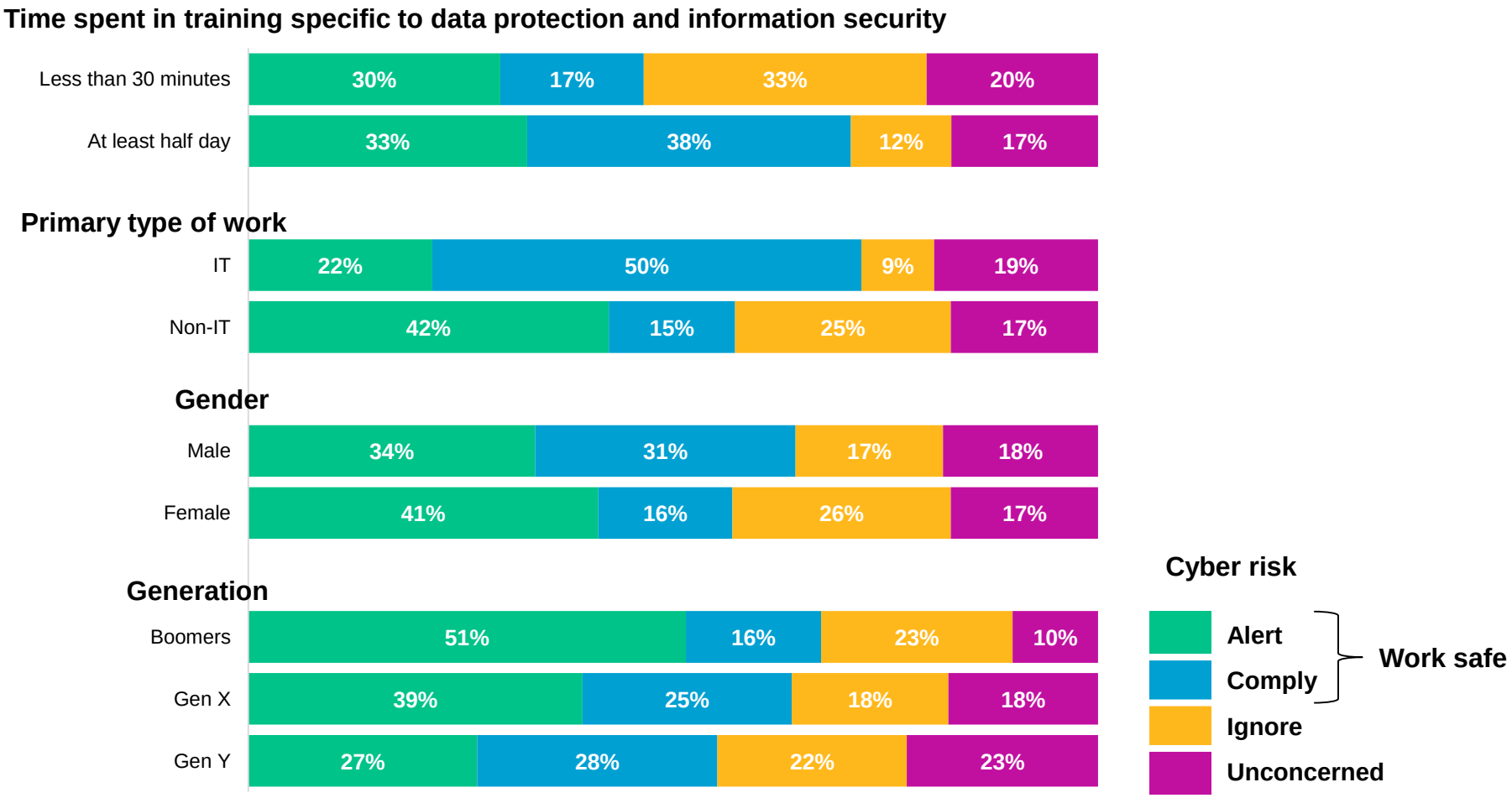
- Use the same passwords across all of personal computing devices
- Do not purchase a personal identity theft protection service
- Share personal information in profiles on social media sites
- Do not regularly update virus protection software on personal computing devices
- Do not change passwords for personal email and online accounts at least once every 3 months
- Do not disable features that auto-save passwords on personal computing devices

WORK BEHAVIORS

- Use personal computing devices that have not been approved by company's IT department to do work at home
- Remove paper files with confidential information from the office to do work at home
- Downloaded software onto work computer that was not approved by IT department
- Developed an issue with work computer due to an action employees took
- Shared network password with a work colleague
- Sent or received an important or confidential work file via email without password protection
- Lost a piece of work equipment
- Sent a confidential work file via email to the wrong recipient

Source: 2017 WTW Cyber Risk Survey, employee survey, US.

Behavior is strongly linked to training time, type of work and age



Source: 2017 WTW Cyber Risk Survey, employee survey, US.

Cyber risk

Key insights

Key insights

People risks are the next frontier in cyber risk management

1. **Many companies feel they are on the right track with their information security and infrastructure and operational policies**
2. **Large majority of companies have reviewed and enhanced their cyber insurance cover or plan to do so in next two years**
3. **Companies are shifting focus to tackle people risks and build a culture of risk management**

- There is a disconnect between company policy and employee behavior
- Employees are overly reliant on company IT to provide cyber security
- Employees need to move from complying to actively engaging in their training
- Social engineering creates additional vulnerabilities that need to be addressed

Key insights

Company actions

1. **Continuously evolve with the changing threats**
2. **Encourage employees to go beyond compliance**
3. **Train to win**
4. **Check your insurance policies**

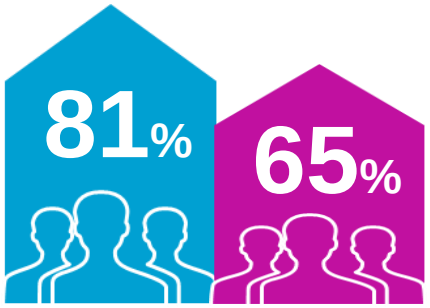
Cyber risk

Appendix: US - UK comparison

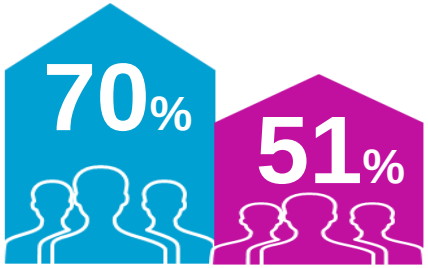
US employers take the lead in action

Over last two years:

- Completed reviewing their systems



- Provided regular updates to employees about new security threats



Employers say that:

	US	UK
They provide an environment in which employees are comfortable reporting concerns about data privacy and information security	93%	82%
They communicate effectively to employees about data privacy and network best practices	77%	68%
Managers set clear expectations regarding how employees need to handle confidential customer/client information	72%	63%
They are doing enough to protect the integrity of customer/client data	72%	63%
They have consistent data management and information security policies across all aspects of the business	63%	58%

(% of 'Strongly agree' or 'Agree')

Source: 2017 WTW Cyber Risk Survey, employer survey, US; 2017 WTW Cyber Risk Survey, employer survey, UK.

The percentage of US employers thinking that cyberinsurance coverage meets their needs is nearly twice of that of UK employers

Our cyber insurance coverage is comprehensive enough to meet our needs

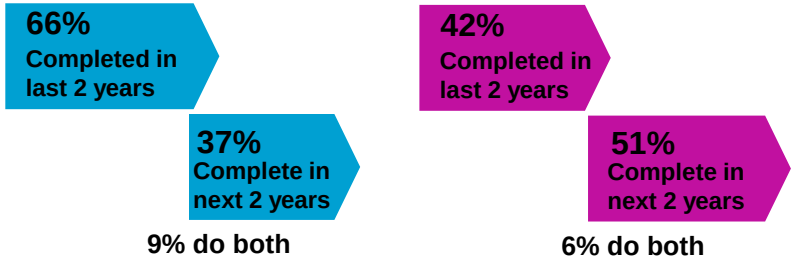
62% of US employers

38% of UK employers

Review and identify gaps in existing insurance coverage

94% of US employers **vs** **87%** of UK employers

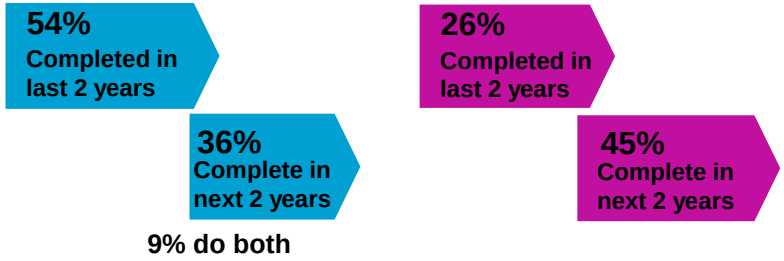
Completed over last two years or plan to complete in next two years



Add or enhance cyber-insurance coverage

81% of US employers **vs** **71%** of UK employers

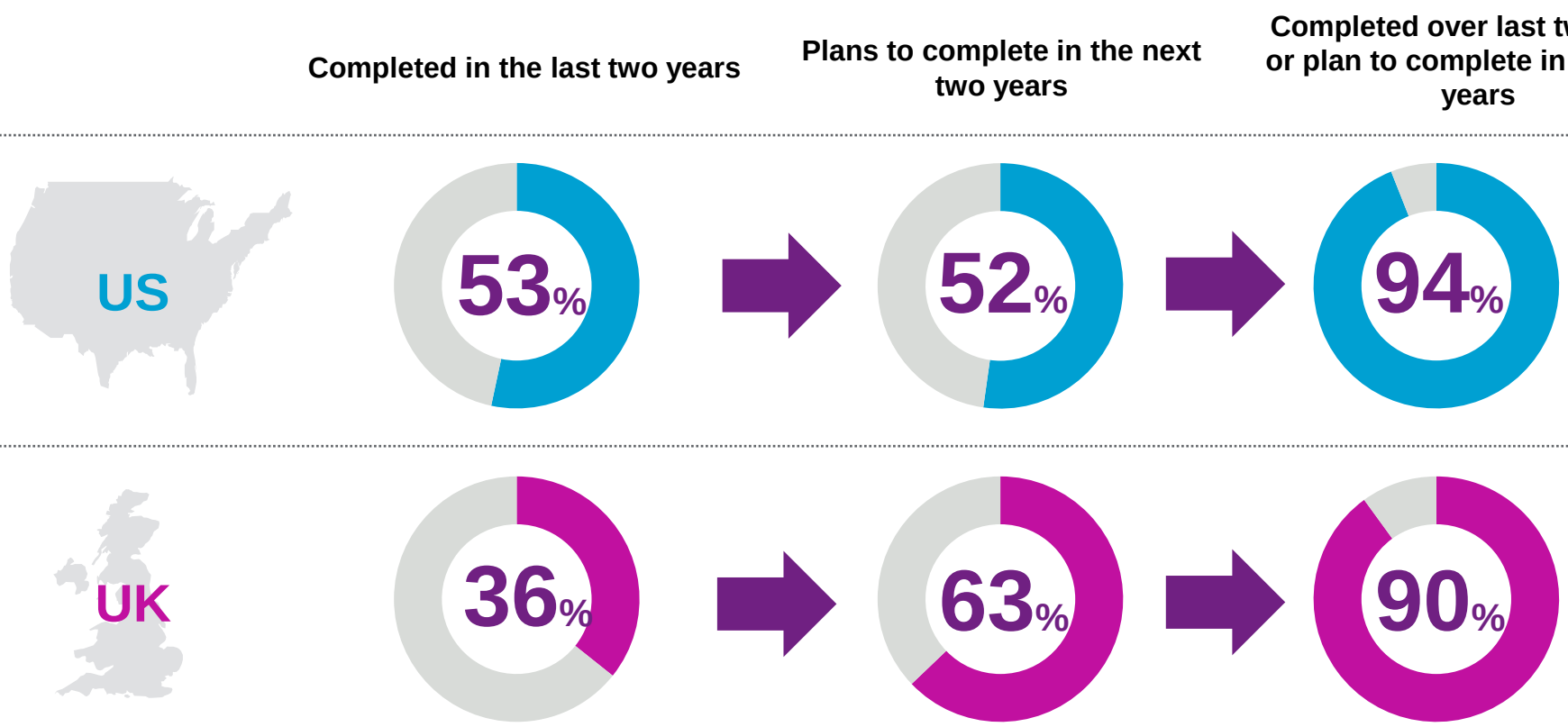
Completed over last two years or plan to complete in next two years



Source: 2017 WTW Cyber Risk Survey, employer survey, US; 2017 WTW Cyber Risk Survey, employer survey, UK.

Both US employers and UK employers see the importance of training

Has your organization completed in the last two years, or does it plan to complete in the next two years, a comprehensive training program on cyber risks for employees?



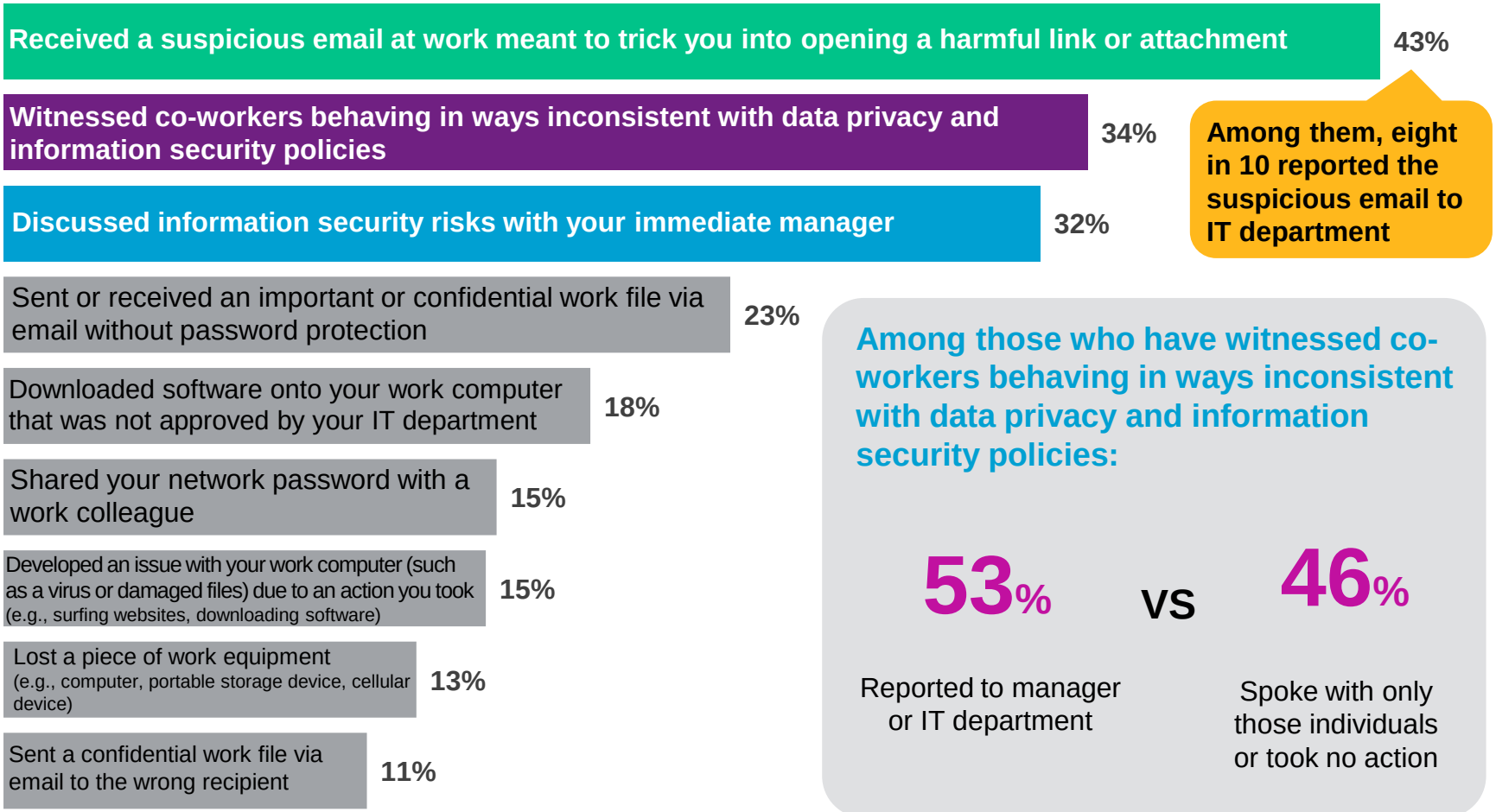
Source: 2017 WTW Cyber Risk Survey, employer survey, US; 2017 WTW Cyber Risk Survey, employer survey, UK.

Cyber risk

Appendix: Additional material

Many threats exist, especially around employee behaviors

For each of the following, have you ever…?



Source: 2017 WTW Cyber Risk Survey, employee survey, US.

About three-quarters of organizations feel their IT systems and cyber security strategy are fit for purpose

But there is a lack of confidence in cyber insurance coverage

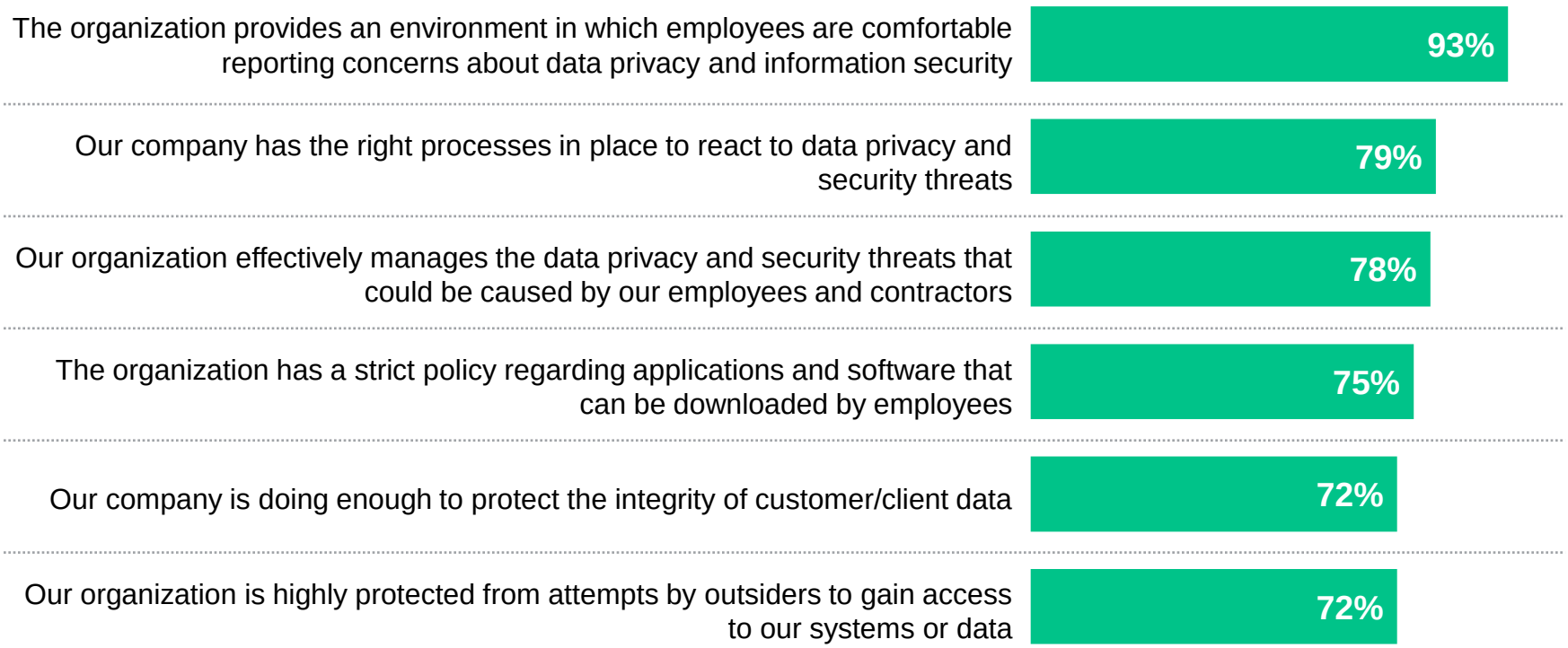
Do you agree or disagree with the following statements about how your organization manages cyber risk?

Note: Percentages indicate 'Agree' or 'Strongly agree'.
Source: 2017 WTW Cyber Risk Survey, employer survey, US.

Most employers have effective policies to manage data privacy threats by employees, manage software downloads and respond to security threats

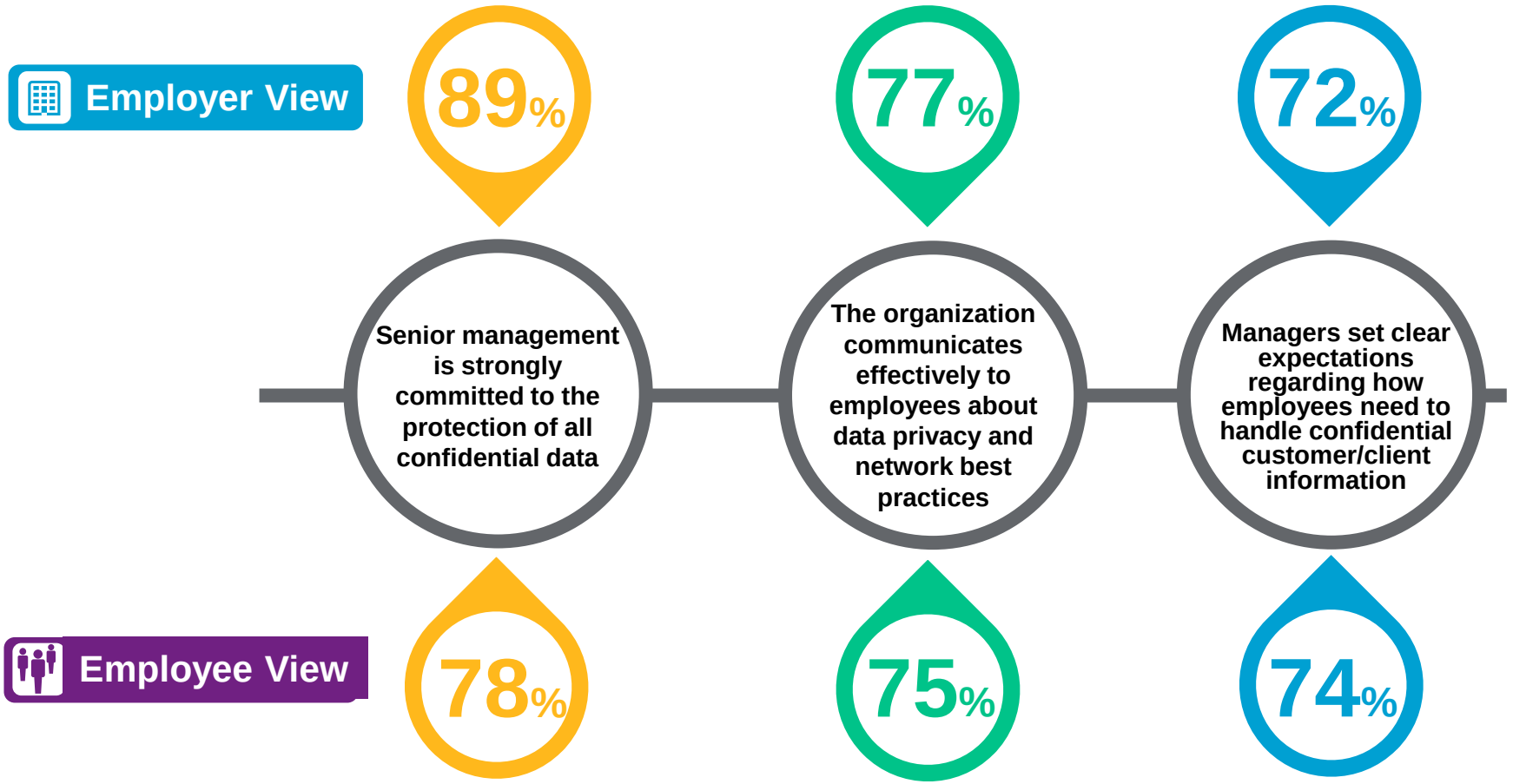
And nearly three-quarters feel they have done enough to protect client data, including against outsiders breaking into their systems

Do you agree or disagree with the following statements about how your organization manages data privacy and information security?



Note: Percentages indicate 'Agree' or 'Strongly agree'.
Source: 2017 WTW Cyber Risk Survey, employer survey, US.

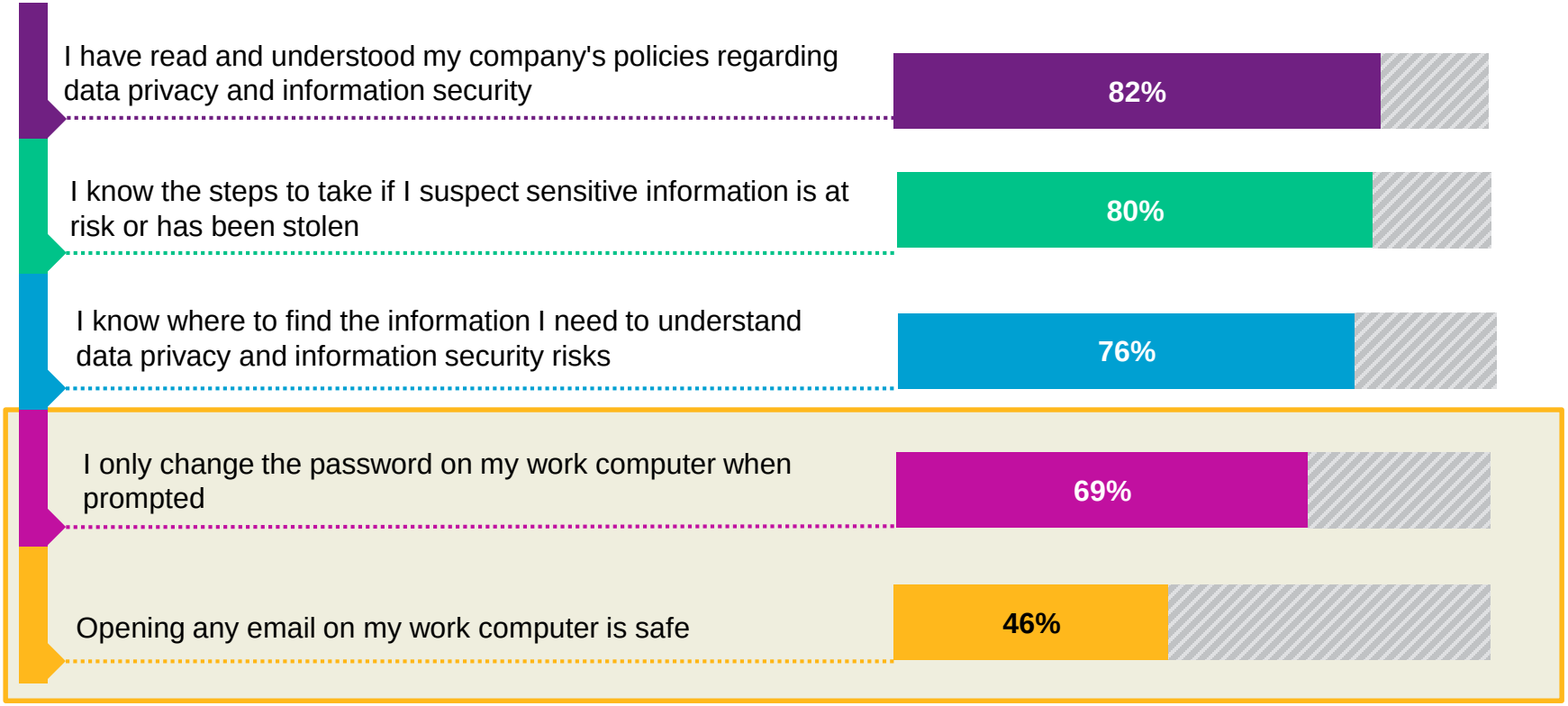
Nearly eight in 10 employers say that they have strong commitment from senior management, effective communication to employees and have set clear expectations to employees



Note: Percentages indicate 'Agree' or 'Strongly agree'.
Source: 2017 WTW Cyber Risk Survey, employer survey & employee survey, US.

Most employees feel they know how to manage data privacy and information security in their jobs

But still, two-thirds are pushed to change their password, and half are not aware of risks when opening emails on work computers



(% of 'Strongly agree' or 'Agree')

Source: 2017 WTW Cyber Risk Survey, employee survey, US.

Vulnerabilities around employee behaviors

How often do you do each of the following?

Use your work computer or cellular device to access confidential company information	41%
Discuss work-related topics in public places	41%
Log into your work computer or cellular device using an unsecured public network (Wi-Fi)	32%
Use your work computer in public settings (e.g., while commuting, on airplanes/trains, at cafes)	31%
Remove paper files with confidential information from the office to do work at home	27%
Use personal computing devices that have not been approved by your company's IT department to do work at home	22%

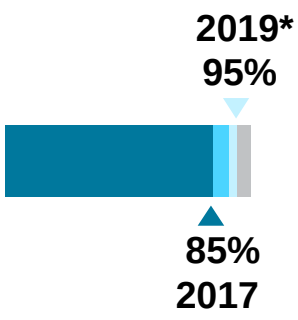
(% of 'frequently' or 'sometimes')

Source: 2017 WTW Cyber Risk Survey, employer survey, US.

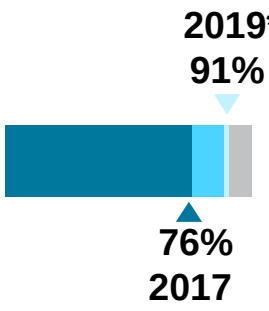
Policies to enhance cyber security

Which specific policies does your organization have in place or plan to have in the next few years?

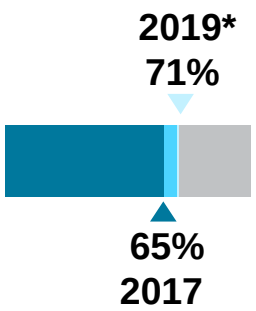
Require employees to create strong passwords (e.g., set minimum length, include upper and lower case letters, use numbers and symbols)



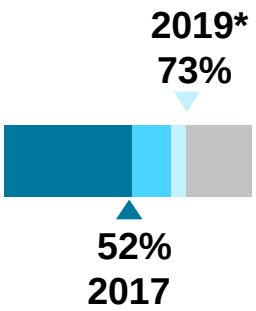
Require employees to change passwords at least every three months



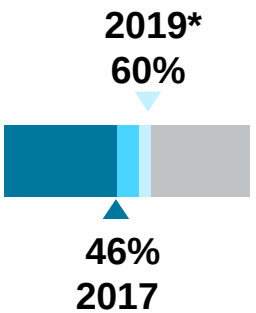
Have a disciplinary policy to enforce the data protection policy



Require portable storage devices used for company business to be encrypted at a standard set by the company



Prohibit the use of portable storage devices



*Includes companies indicating planned for 2018 or considering for 2019.
Source: 2017 WTW Cyber Risk Survey, employer survey, US.