# BAE Systems Cyber Security Survey Report

> Q1 2016



BAE SYSTEMS
INSPIRED WORK

# Table of Contents



BAE SYSTEMS
INSPIRED WORK

# Objectives and Methodology

- This report presents the findings of an online study conducted among a sample of 300 respondents who are managers for companies in the Financial Services, Insurance, or Tech/IT industries. This study was intended to:

  - Gauge concerns and attitudes of managers toward cyber defense
  - Determine what companies are doing to keep their information safe
  - Identify how companies are training employees on cyber security policies and practices

- Invitations to participate in the study were sent beginning on December 28, 2015 and data collection continued through January 4, 2016.

- Where applicable, red circles indicate a significant difference at the 95% confidence level.

BAE SYSTEMS
INSPIRED WORK

# Executive Summary

BAE SYSTEMS
INSPIRED WORK

# Executive Summary

**The research uncovered a gap between companies perception of their cyber security preparedness and their actual ability to defend themselves from cyber threats.**

- While managers paint a fairly positive picture of their organization's ability to protect its data and information security, the research raises concerns about the priority businesses place on cyber defense and how it is reflected through employee communication and training.

BAE SYSTEMS
INSPIRED WORK

# Executive Summary

- The **lack of awareness by executives on the state of their cyber security protocols and training** initiatives is alarming, and puts them at a serious disadvantage against cyber attackers.
- There is a **greater need for communication and deployment of cyber security best practices** across all industries surveyed.
- Companies need to make **a more concerted effort to deal with cyber security education and training**.

BAE SYSTEMS
INSPIRED WORK

# Key Findings

# Key Findings

## Respondents Recognize the Cyber Threat

Seven in ten (69%) respondents believe data and information systems breaches are a threat to their company

Almost seven out of ten (68%) respondents personally handle customer or client data as part of their day to day responsibilities

BAE SYSTEMS
INSPIRED WORK

# Key Findings

## Overconfidence in Current Systems

Almost all (**96%**) respondents rate their company's ability to protect its data and information security as good or excellent

BAE SYSTEMS
INSPIRED WORK

# Key Findings

## Noticeable Lack of Knowledge of Key Security Policies and Procedures

42% believe they are extremely or very knowledgeable about their company's information security policies and practices.

52% for the Tech/IT industry

36% for Financial Services firms

BAE SYSTEMS
INSPIRED WORK

# Key Findings

## Widespread use of Traditional Security Measures

Nearly all (98%) use any of the listed methods below to help prevent information systems breaches:

- Firewall (97%)
- Antivirus software (95%)
- Data encryption (87%)
- Employee training (80%)
- Intrusion detection system (73%)

BAE SYSTEMS
INSPIRED WORK

# Key Findings

## Formal Training in Cyber Security is Lagging

- **60%** of respondents report that their organization has a formal cyber security training program in place

- Nearly **70%** of surveyed companies that have cyber defense training programs only implement them on a semi-annual or annual basis, making their organizations vulnerable to attacks

BAE SYSTEMS
INSPIRED WORK

# Detailed Findings

BAE SYSTEMS
INSPIRED WORK

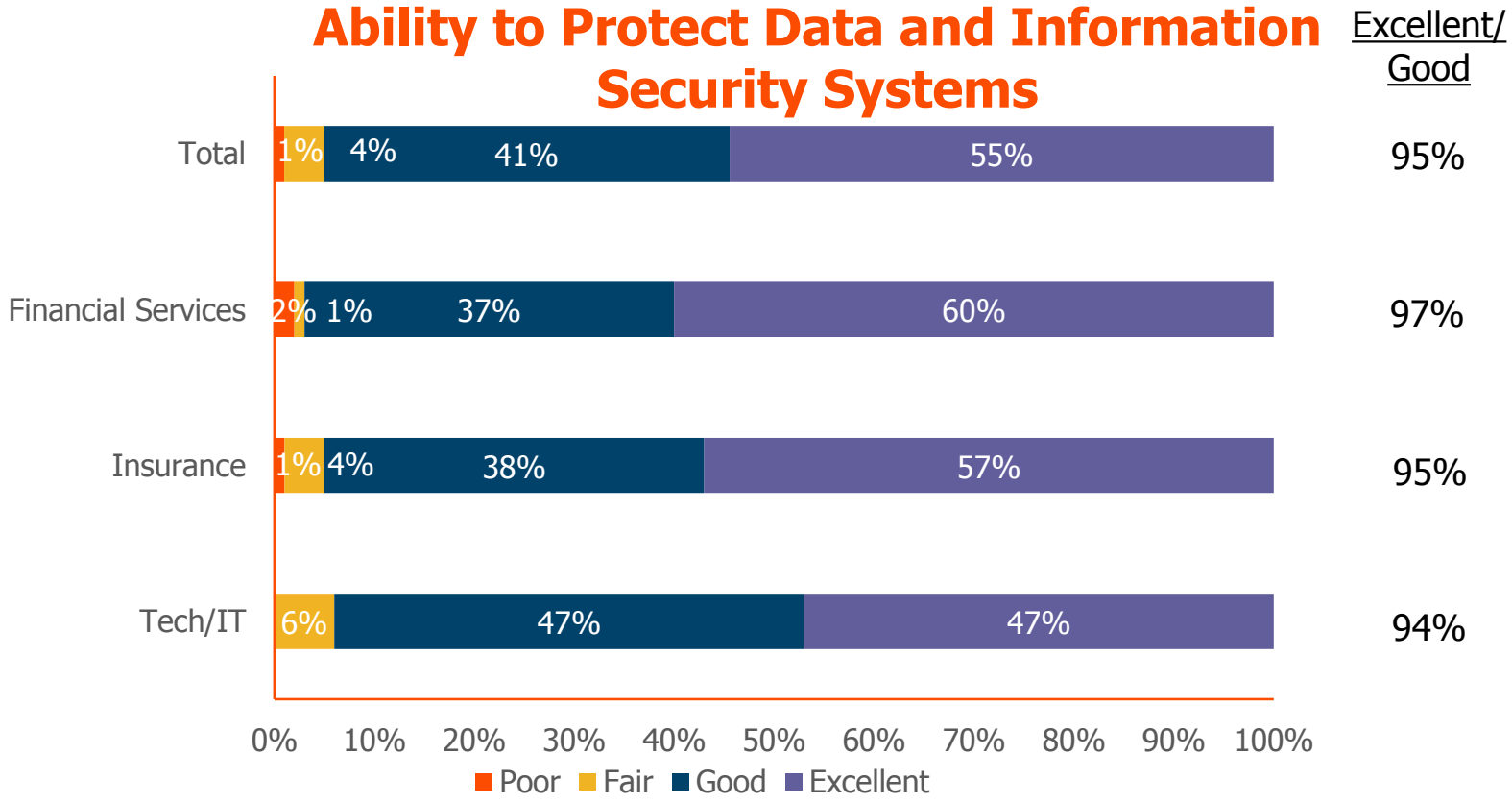
# Detailed Findings

Nearly all respondents (95%) rate their company's ability to protect data and information security systems as excellent or good. Slightly more than half (55%) saying it is excellent and 41% say it is good. Findings are similar for the three industries. Those in larger companies are more likely to rate their company's ability as 'excellent' (60% among those with more than 500 employees vs. 43% of those with 500 and under).

**Question 1**

How would you rate your company's ability to protect its data and information security systems?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)




 | 

BAE SYSTEMS
INSPIRED WORK

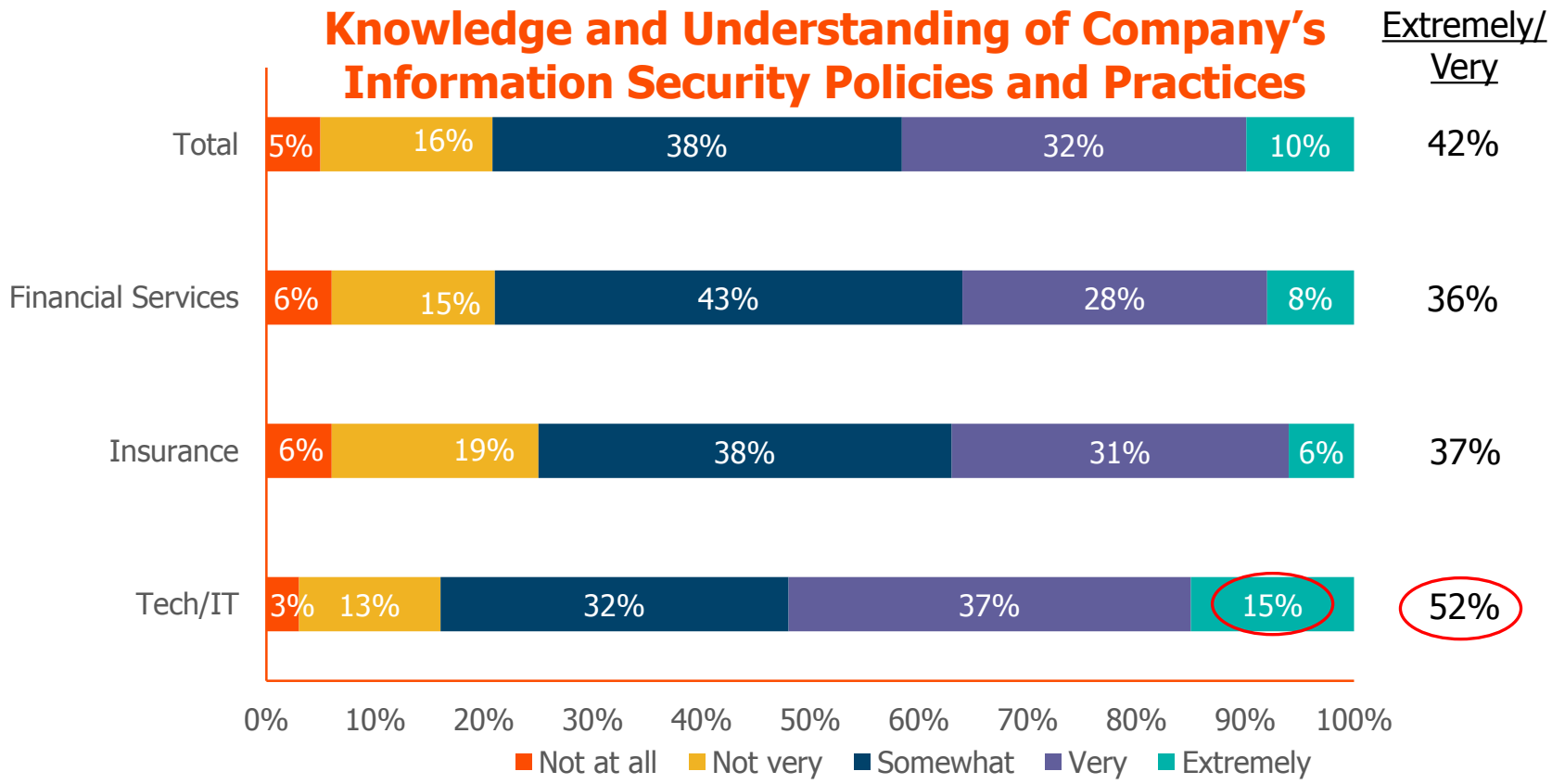
# Detailed Findings

Two out of five respondents (42%) believe they are extremely or very knowledgeable about their company's information security policies and practices. Significantly more of those in the Tech/IT industry (52%) than Financial Services (36%) and Insurance (37%) are extremely or very knowledgeable.

**Question 2**

And how would you rate your knowledge and understanding of your company's information security policies and practices – how the problems and potential problems are being acted upon and handled?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)




 | 

BAE SYSTEMS
INSPIRED WORK

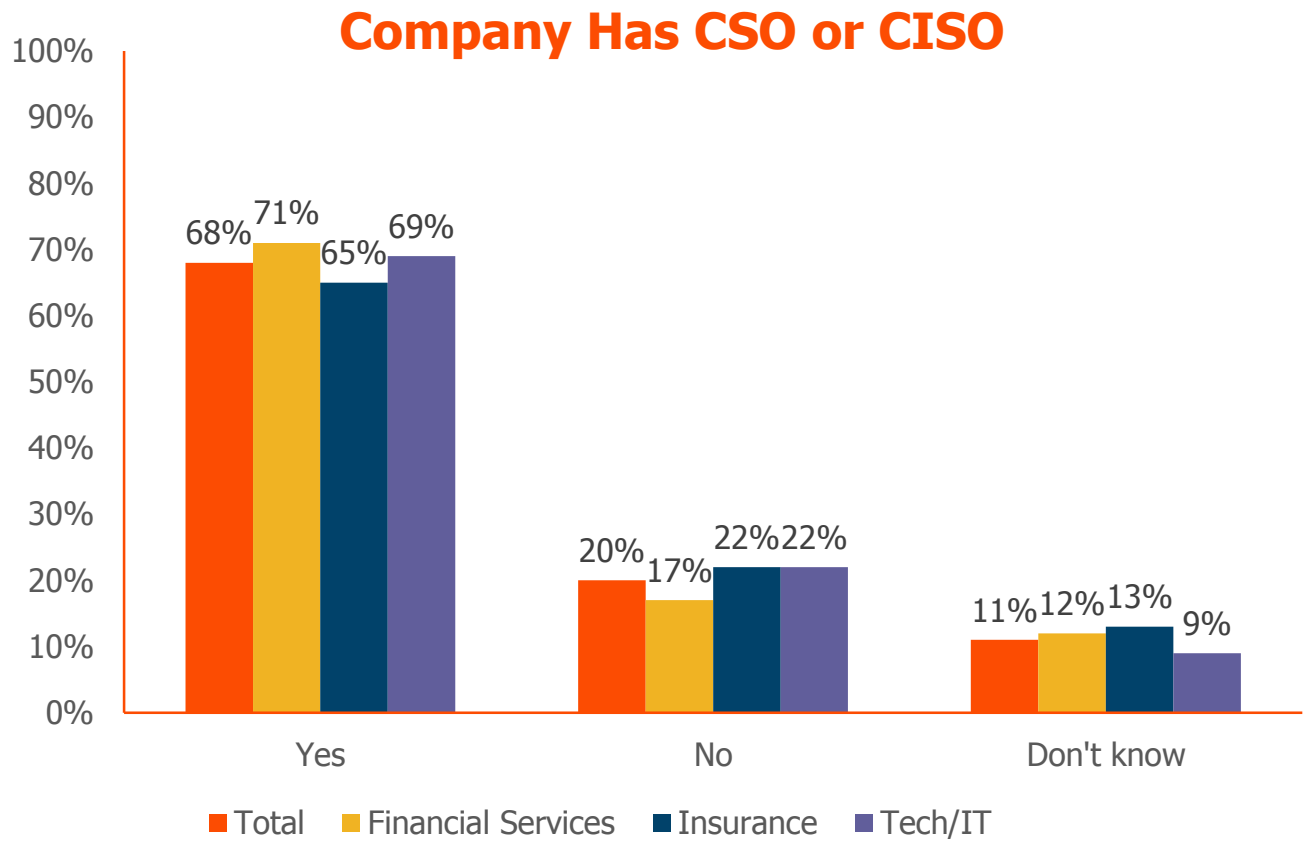
# Detailed Findings

Roughly two out of three (68%) respondents indicate their company has a CSO or CISO. Similar findings were found by industry. Larger companies (those with more than 500 employees) are more likely to have a CSO or CISO (73% vs. 57% only of those with 500 or fewer employees). Interestingly, about one out of ten (11%) did not know if there was a security officer in their company, regardless of the size of the company.

**Question 3**

Does your company have what some companies call a CSO (Chief Security Officer) or CISO (Chief Information Security Officer)? A CSO or CISO is responsible for the security of a company's communications and other business systems, especially those exposed to intrusion from outsiders on the Internet. He/she may also have a role in planning for and managing disaster recovery and is often involved in the business aspects of security as well as the purely technical aspects.

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)




 | 

BAE SYSTEMS
INSPIRED WORK

# Detailed Findings

Most CSO/CISO's (88%) are connected to the leadership team, with half (48%) being part of the leadership team and two in five (40%) report to the leadership team.  Findings are similar by industry.

**Question 4**

Is that person someone who…

(Base=Company has a CSO or CISO = 205; Financial services=71; Insurance=65; Tech/IT=69)


 | 

BAE SYSTEMS
INSPIRED WORK

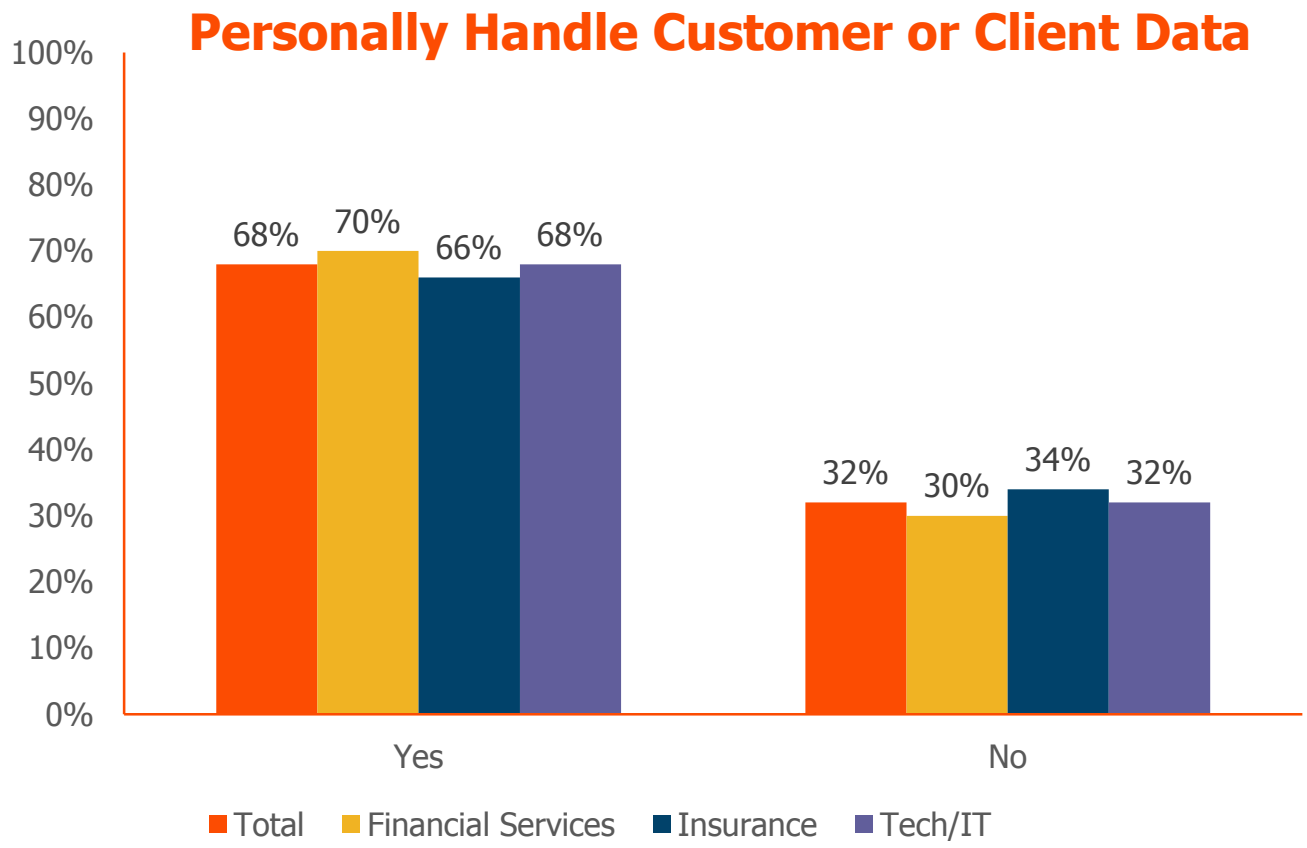
# Detailed Findings

Almost seven in ten (68%) respondents personally handle customer or client data as part of their day to day responsibilities.  Findings are similar across industry.

**Question 5**

Do you, personally, handle customer or client data as part of your day to day responsibilities?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)




 | 

BAE SYSTEMS
INSPIRED WORK

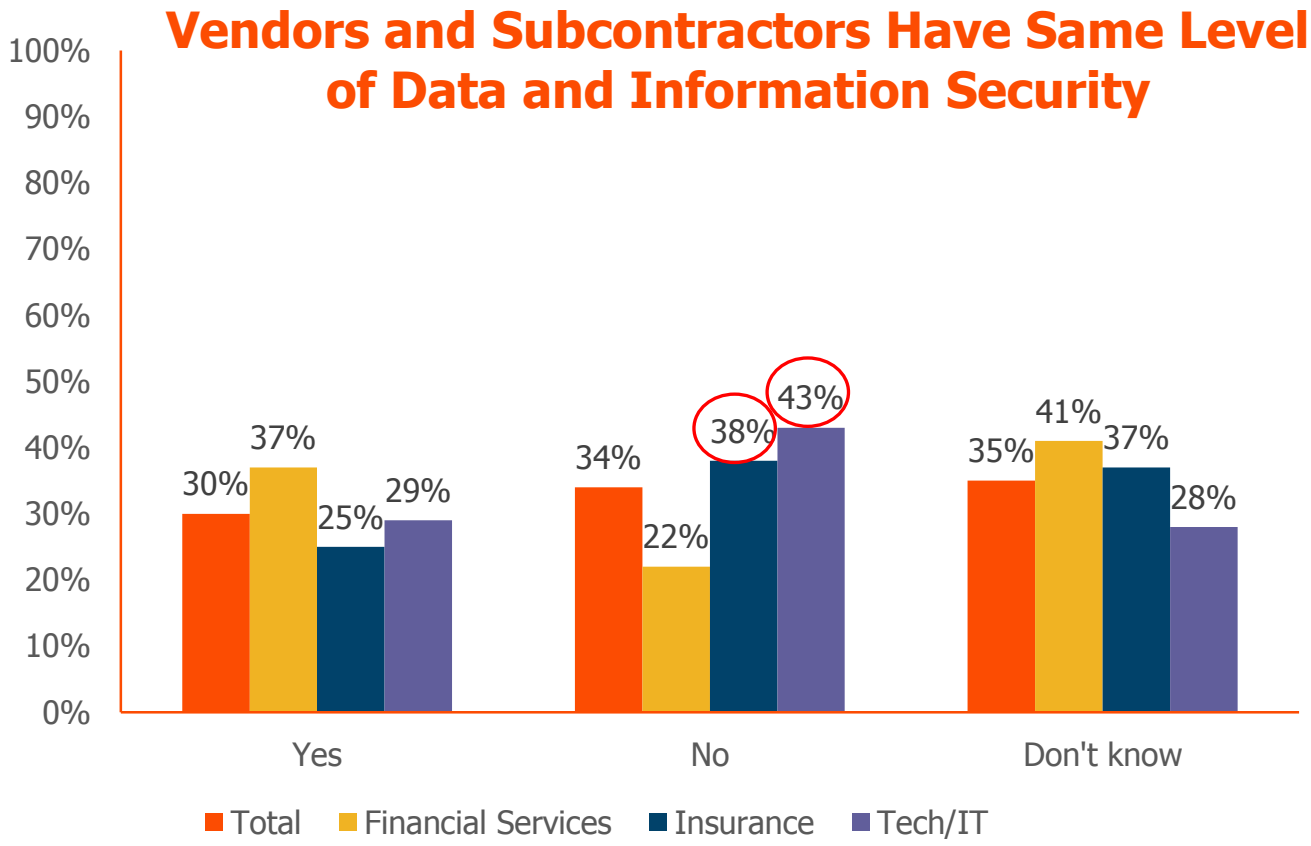
# Detailed Findings

When asked about their vendors and subcontractors, three in ten (30%) indicated that their vendors and subcontractors have the same level of data and information security as they do. One-third (34%) said they don't or are not sure (35%). Those in the Tech/IT (43%) and Insurance (38%) industries are more likely than those in Financial Services (22%) to indicate that their vendors and subcontractors do not have the same level of security.

**Question 6**

Do all of your vendors and subcontractors have the same level of data and information security that your company does?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)




 | 

BAE SYSTEMS
INSPIRED WORK

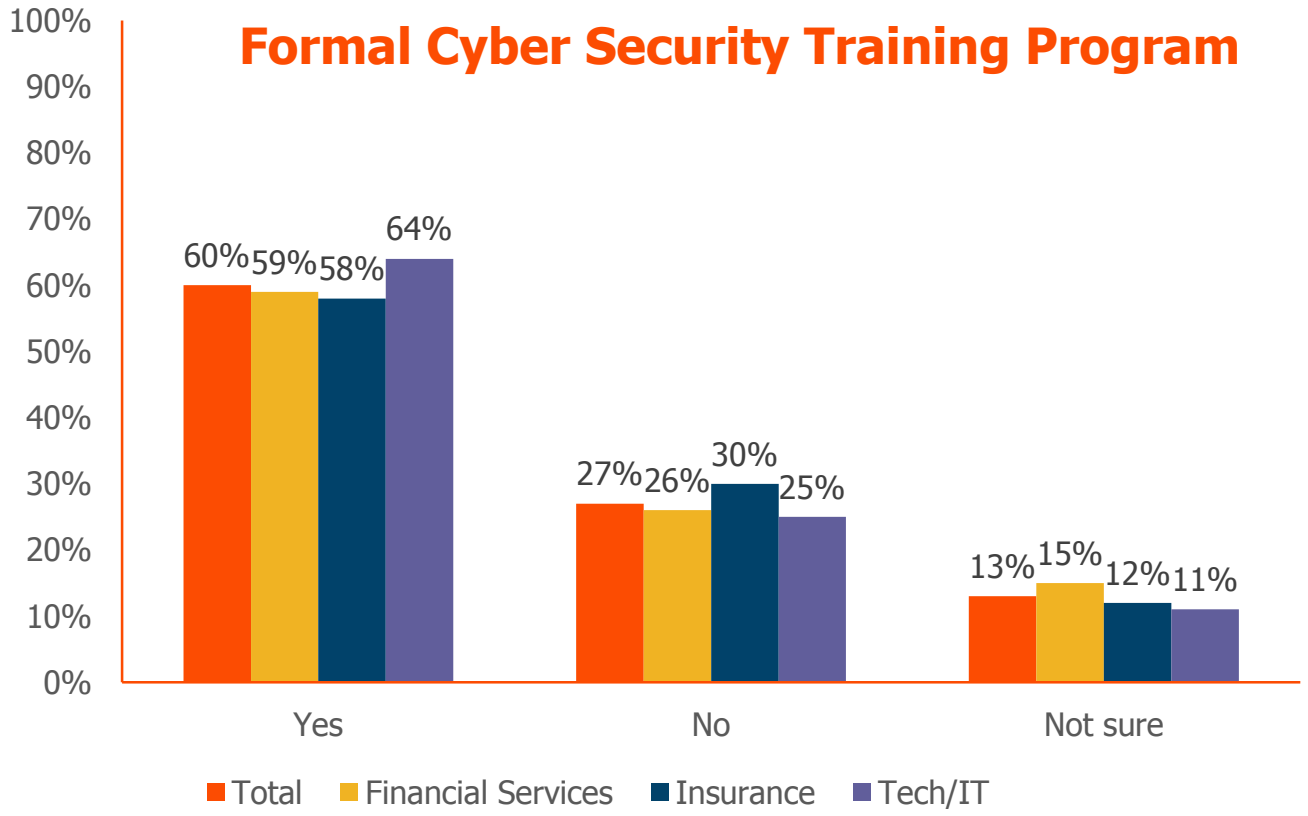
# Detailed Findings

Three in five (60%) respondents said their company has a formal cyber security training program. Regardless of industry, at least one out of four said that their company does not have a training program and more than one out of ten did not know. Those in larger companies are more likely to have a formal cyber security training program (67% among those with more than 500 employees vs. 44% of those with 500 or fewer).

**Question 7**

Does your company have a formal cyber security training program?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)




 | 

BAE SYSTEMS
INSPIRED WORK

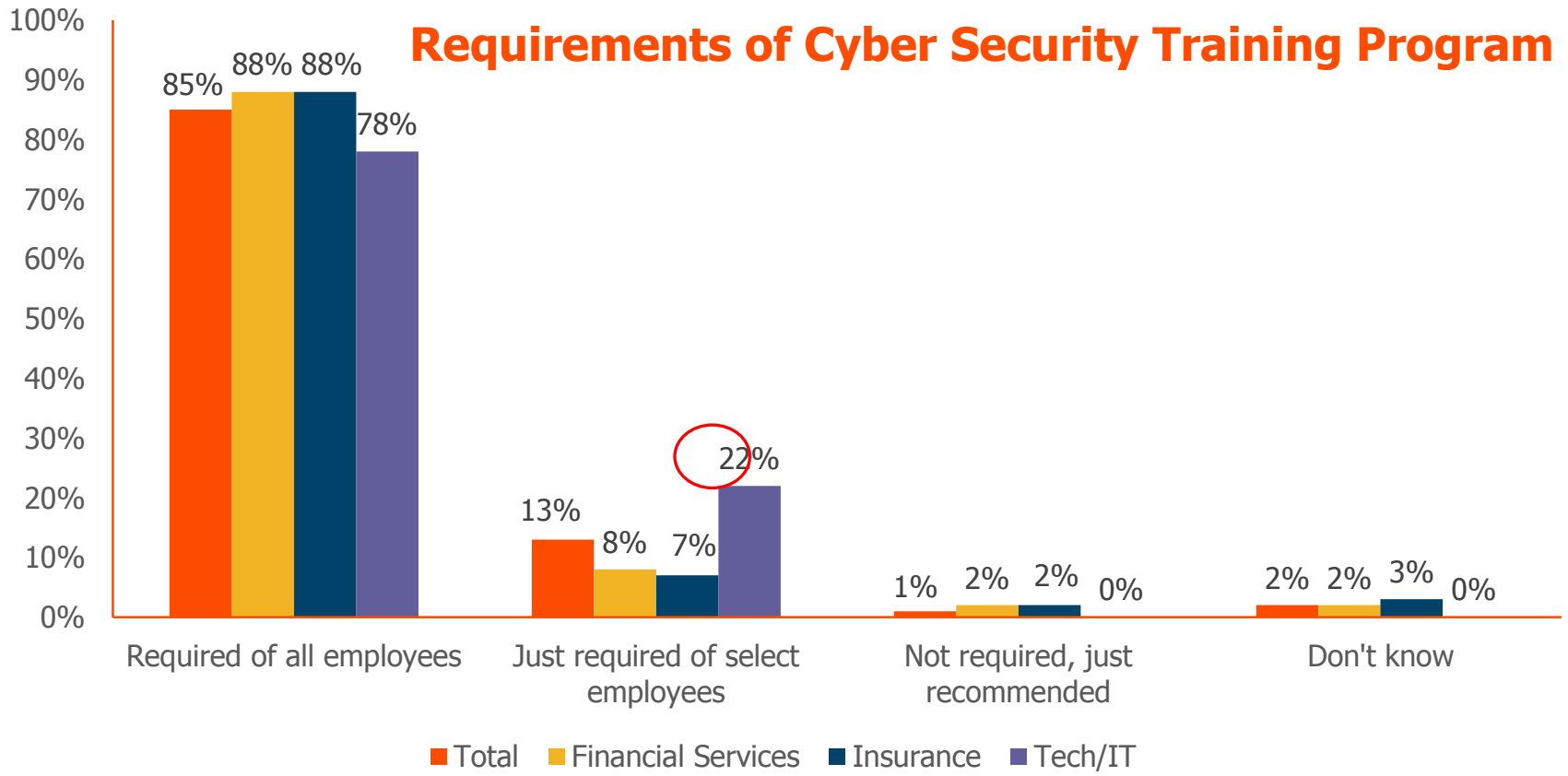
# Detailed Findings

Nearly nine in ten (85%) of those companies with a formal cyber security training program require all employees to take the training. Significantly more of those in the Tech/IT industry (22%) indicate the training is just required of select employees (vs. 8% of those in Financial Services and 7% of those in Insurance).

**Question 8**

Is the cyber security training…

(Base=Company has a formal cyber security training program = 181; Financial services=59; Insurance=58; Tech/IT=64)



BAE SYSTEMS
INSPIRED WORK

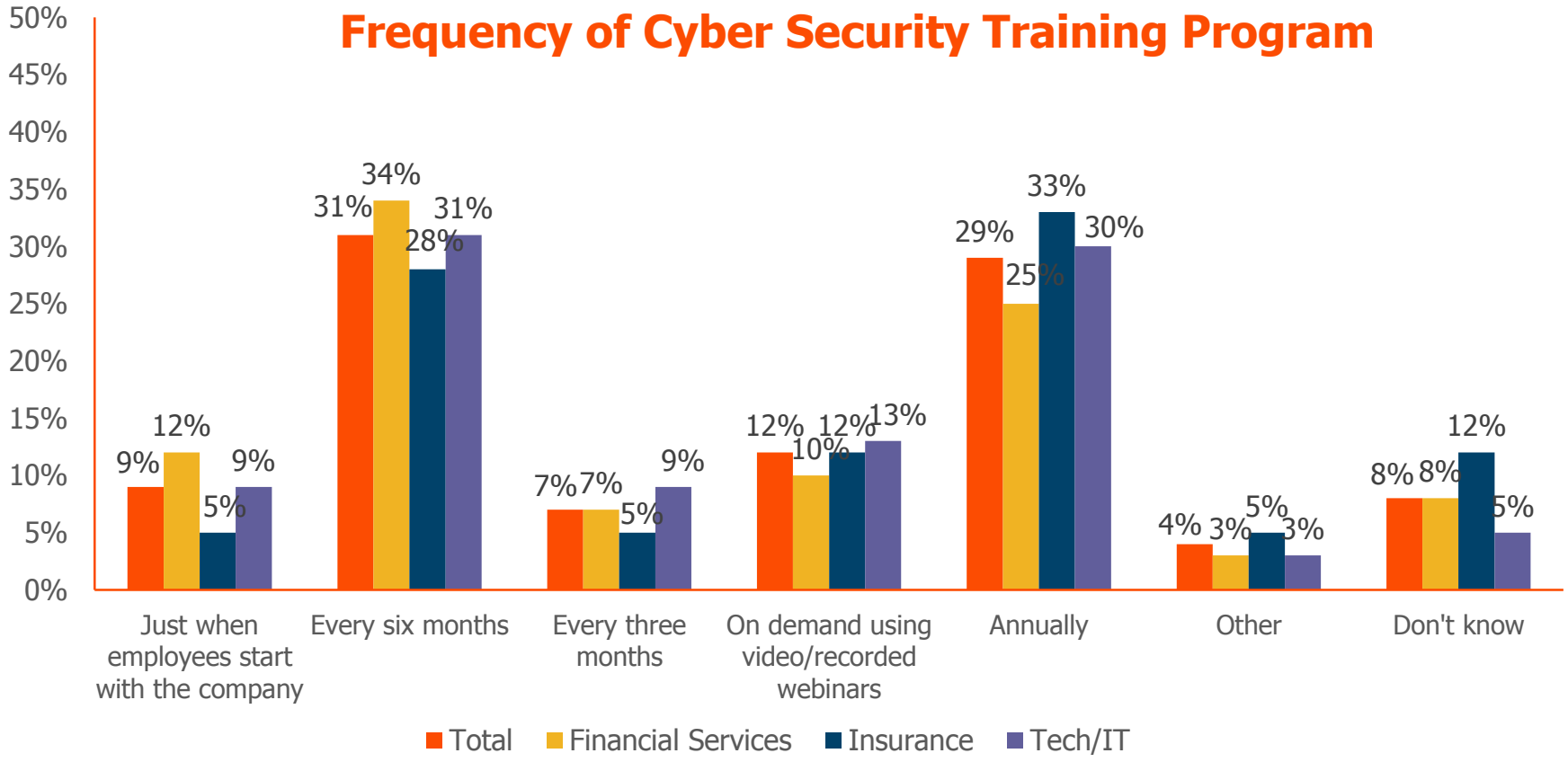
# Detailed Findings

Of those with a formal cyber security training program, two in five (38%) say the training is scheduled every three or six months. Three in ten (29%) said it's scheduled annually. Findings are similar across industry.

**Question 9**

How frequently is the cyber security training program scheduled?

(Base=Company has a formal cyber security training program = 181; Financial services=59; Insurance=58; Tech/IT=64)




 | 

BAE SYSTEMS
INSPIRED WORK

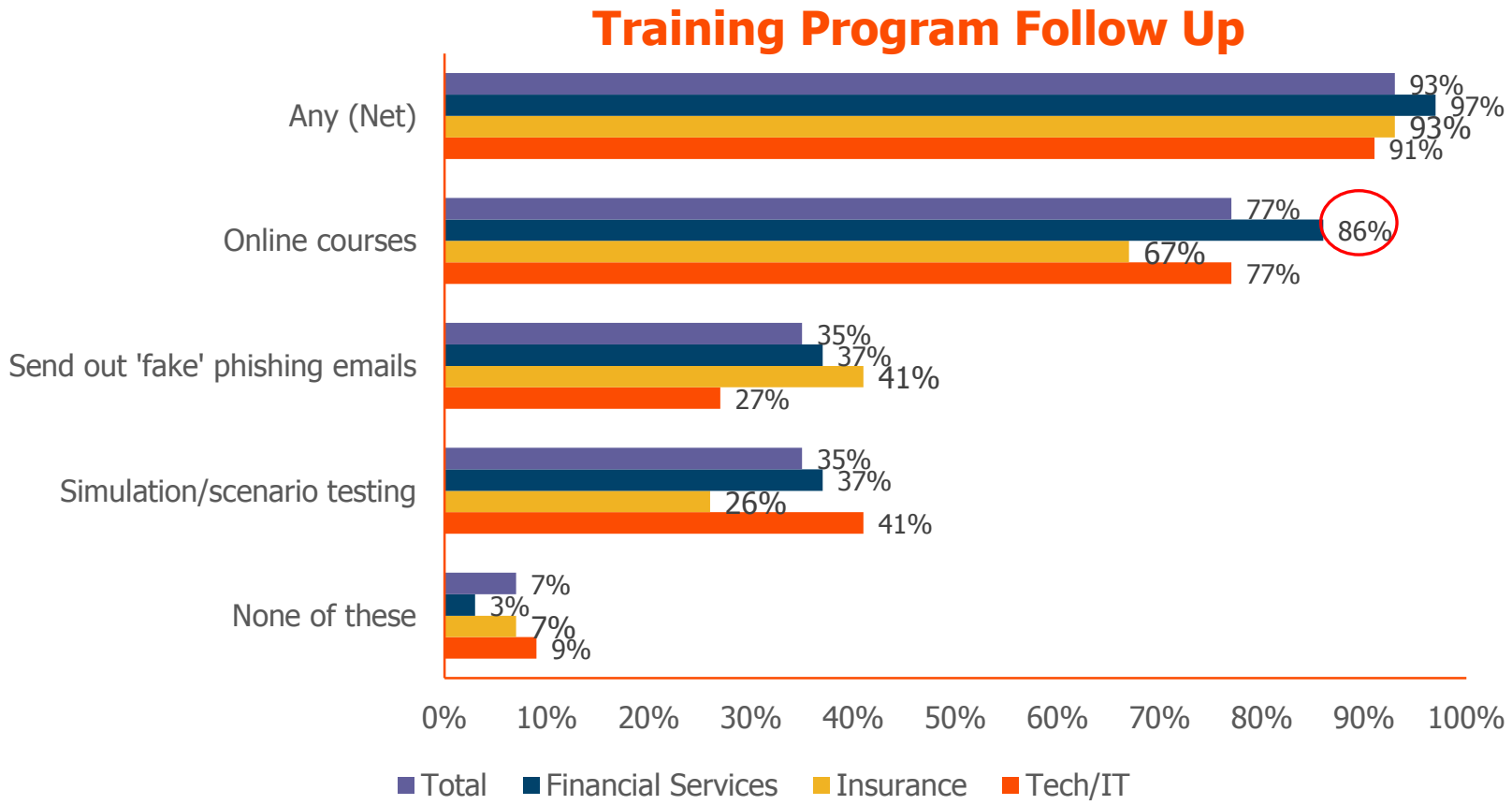
# Detailed Findings

Nine in ten (93%) of those who have a formal cyber security training program do any of the listed items as a follow up on the training program. Three-quarters (77%) use online courses, a third (35%) send out 'fake' phishing emails, and a third (35%) also use simulation/scenario testing. Those in the Financial Services industry are more likely than those in Insurance to use online courses as a follow up (86% vs. 67%). The same is true among larger companies (80% of those with more than 500 employees vs. 65% of those with 500 or fewer).

**Question 10**

Which of the following, if any, does your company use to follow up on the training program and ensure that everyone in the organization is up to speed on cyber security?

(Base=Company has a formal cyber security training program = 181; Financial services=59; Insurance=58; Tech/IT=64)




 | 

BAE SYSTEMS
INSPIRED WORK

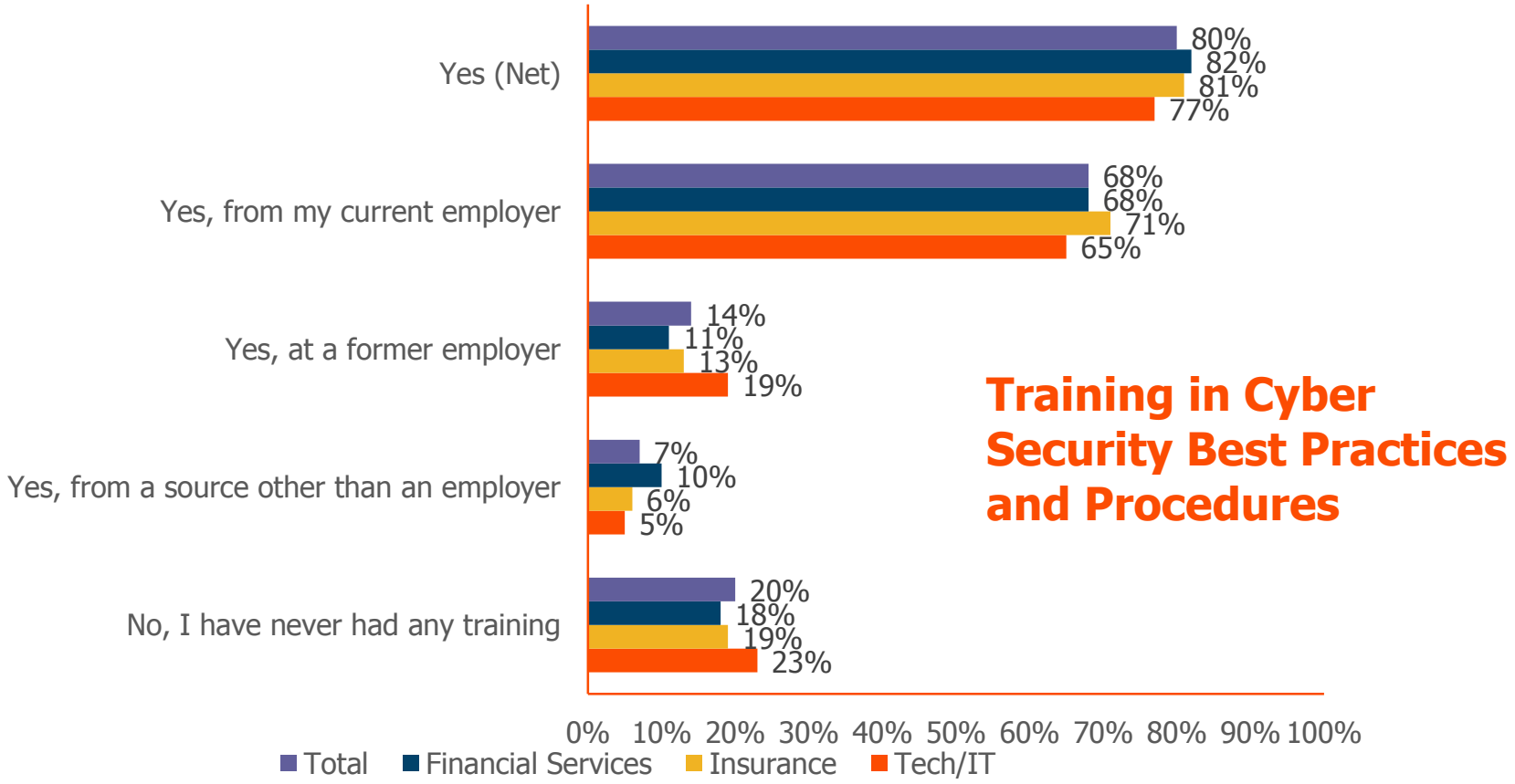
# Detailed Findings

Four in five (80%) respondents have personally had training in cyber security best practices and procedures. Two-thirds (68%) have received training from their current employer. Very few have received training from a former employer (14%) or a source other than an employer (7%). Findings were similar across industries. Those at larger companies are more likely to have personally had any training in cyber security best practices and procedures (83% among those with more than 500 employees vs. 72% of those with 500 or fewer).

**Question 11**

Have you personally had any training in cyber security best practices and procedures?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)




**Training in Cyber Security Best Practices and Procedures**

BAE SYSTEMS
INSPIRED WORK

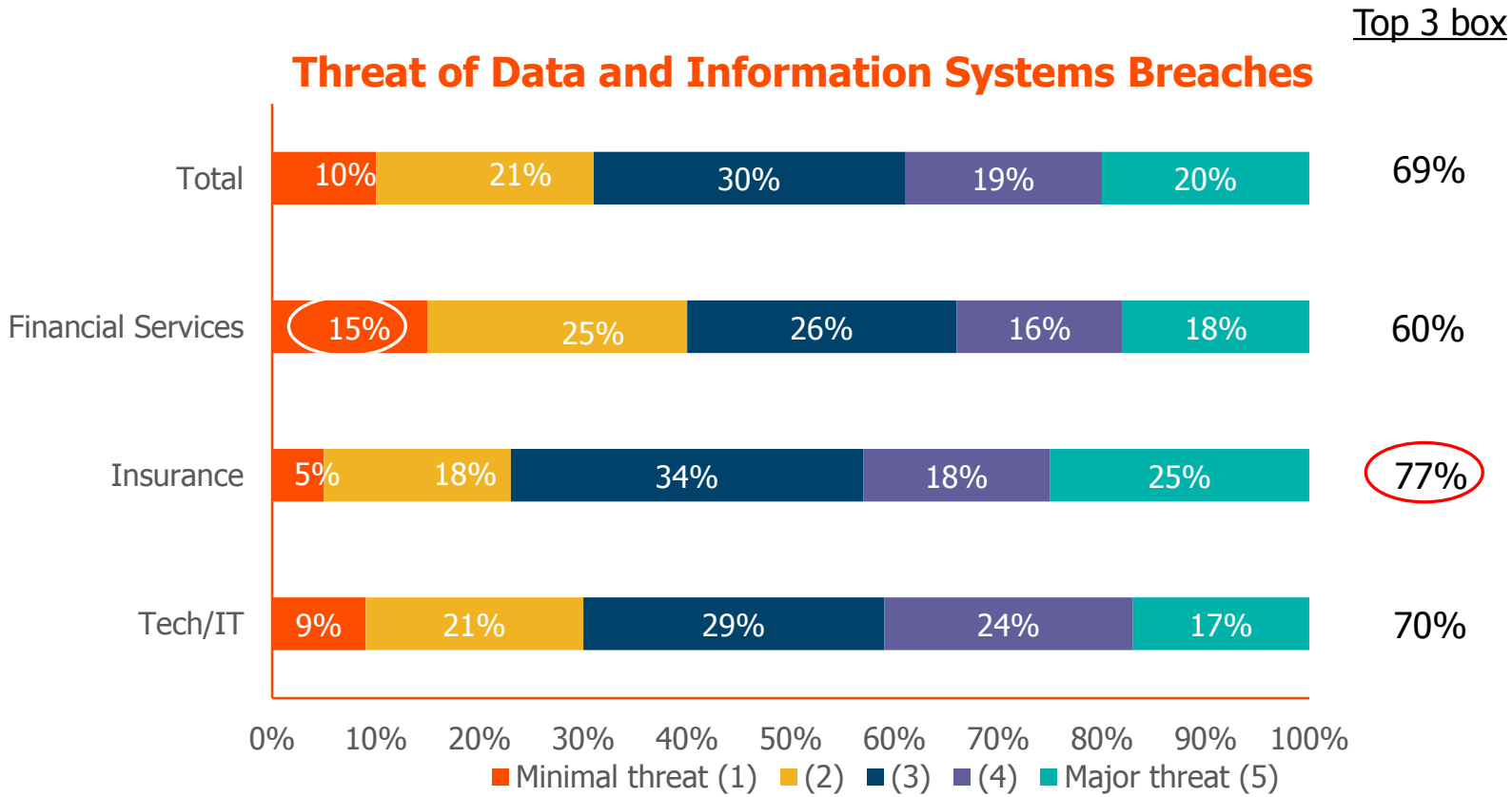
# Detailed Findings

Seven in ten (69%) respondents believe data and information systems breaches are a threat to their company, rating it a 3, 4, or 5. Those in the Insurance industry (77%) are more likely than those in the Financial Services industry (60%) to think these breaches are a threat. Those in larger companies are more likely to indicate that data and information systems breaches are a major threat (24% of those with more than 500 employees vs. 11% of those with 500 or fewer).

**Question 12**

How much of a threat do you think data and information systems breaches are to your company?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)




 | 

BAE SYSTEMS
INSPIRED WORK

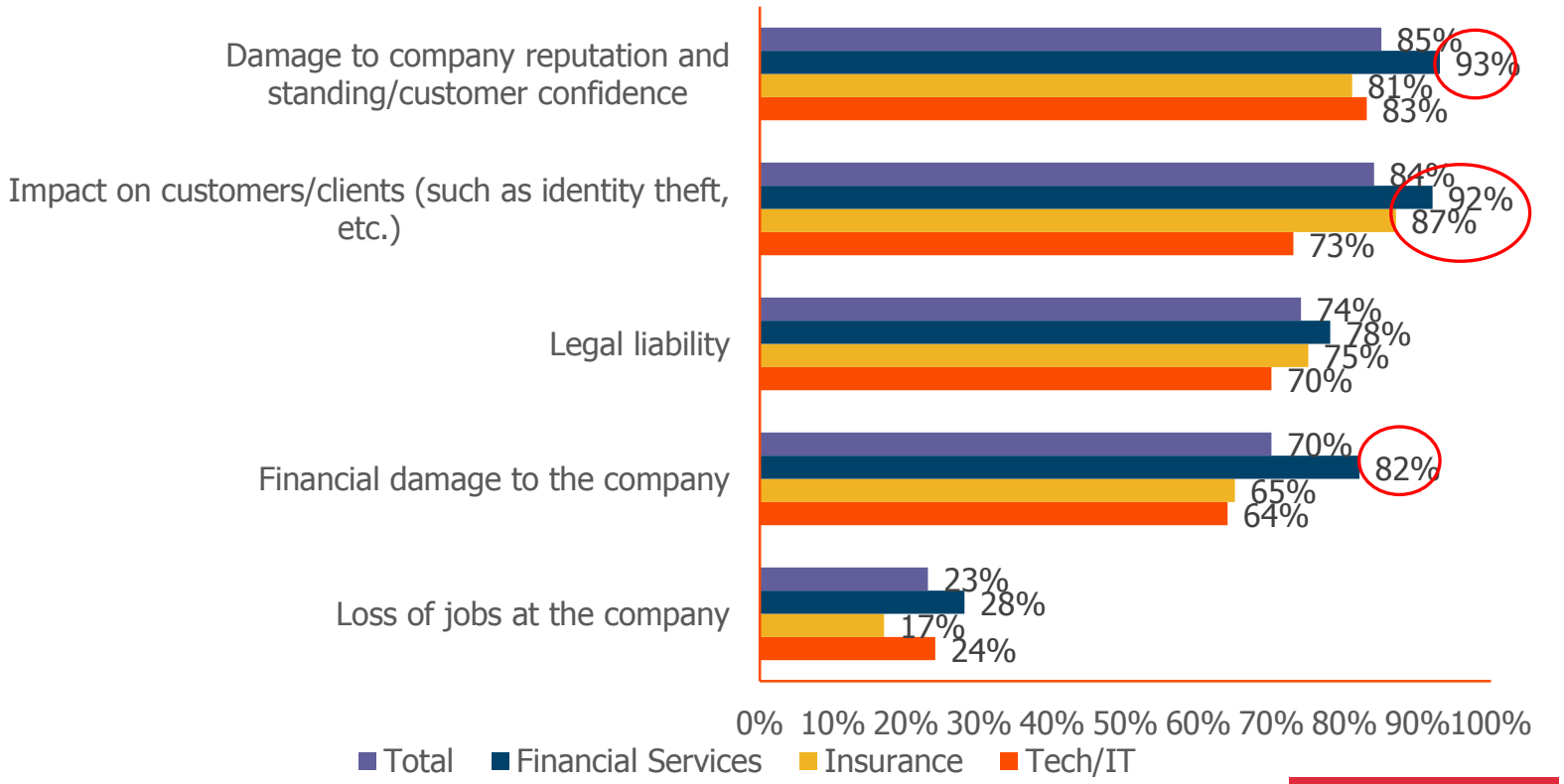
# Detailed Findings

Those who believe data and information systems breaches are a threat to their company were asked how these breaches are a threat. More than four in five (85%) indicated damage to their company's reputation and standing/customer confidence. A similar proportion (84%) said the impact on customers/clients. Three-quarters (74%) mentioned legal liability and seven in ten (70%) said financial damage to the company. Significantly fewer (23%) said loss of jobs at the company. Those in the Financial Services industry (93%) are more likely to cite damage to the company reputation than are those in Tech/IT (83%). Those in the Financial Services (92%) and Insurance (87%) industries are more likely to cite impact on customers/clients than are those in Tech/IT (73%). Those in Financial Services (82%) are more likely to cite financial damage to the company than are those in Insurance (65%) and Tech/IT (64%).

**Question 13**

In what way are they a threat?

(Base=Think data and information systems breaches are a threat to their company = 207; Financial services=60; Insurance=77; Tech/IT=70)




 | 

BAE SYSTEMS
INSPIRED WORK

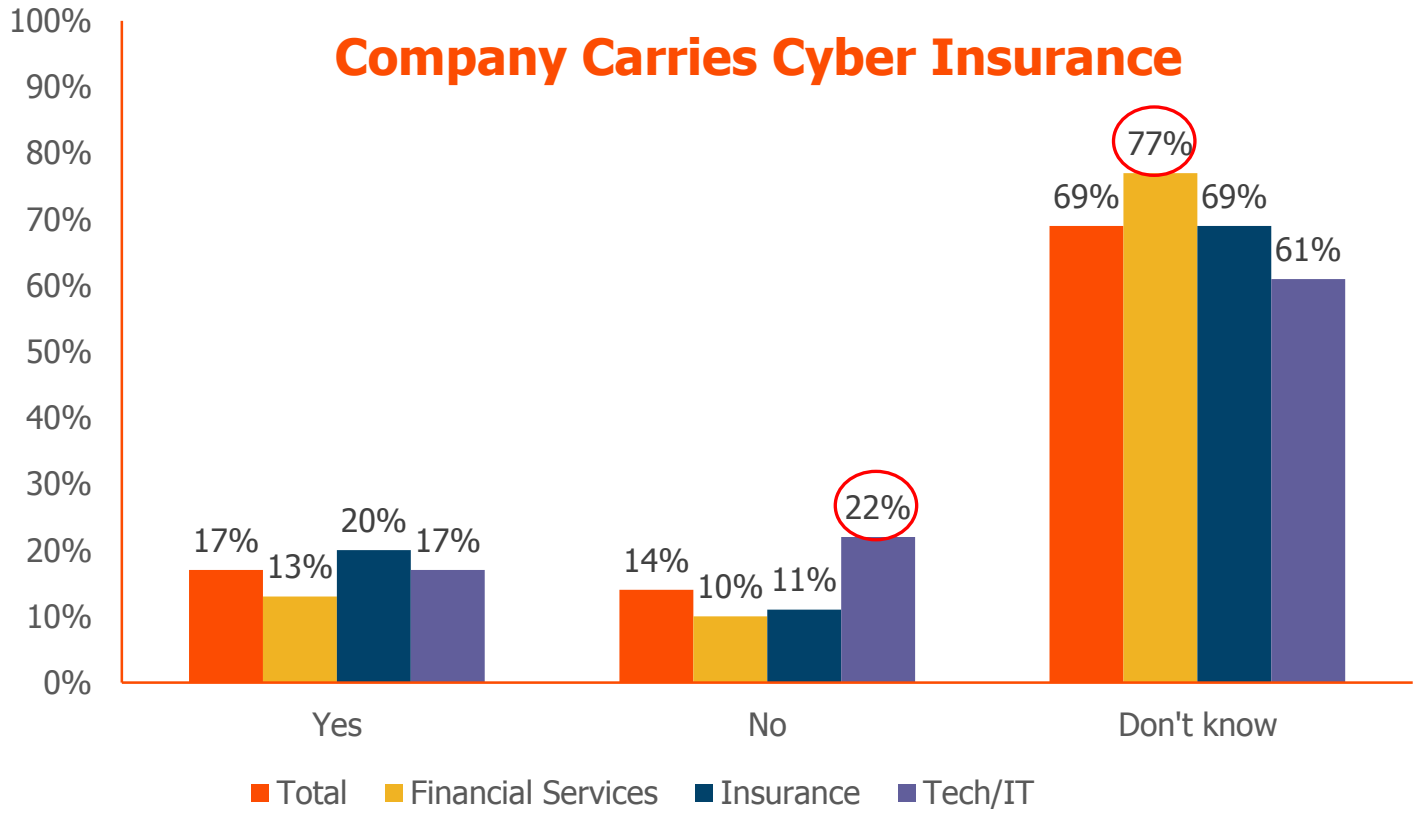
# Detailed Findings

Very few (17%) carry Cyber Insurance. The majority (69%) don't know if their company carries it. Those in the Tech/IT industry (22%) are more likely to say that their company does not carry Cyber Insurance (vs. 11% of those in Insurance and 10% of those in Financial Services). Those in Financial Services (77%) are more likely than those in Tech/IT (61%) to indicate that they don't know if their company carries Cyber Insurance. Those at smaller companies with 500 or fewer employees are more likely to know whether or not they carry Cyber Insurance (43% don't know vs. 80% of those with more than 500 employees).

**Question 14**

Does your company carry Cyber Insurance?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)




 | 

BAE SYSTEMS
INSPIRED WORK

# Detailed Findings

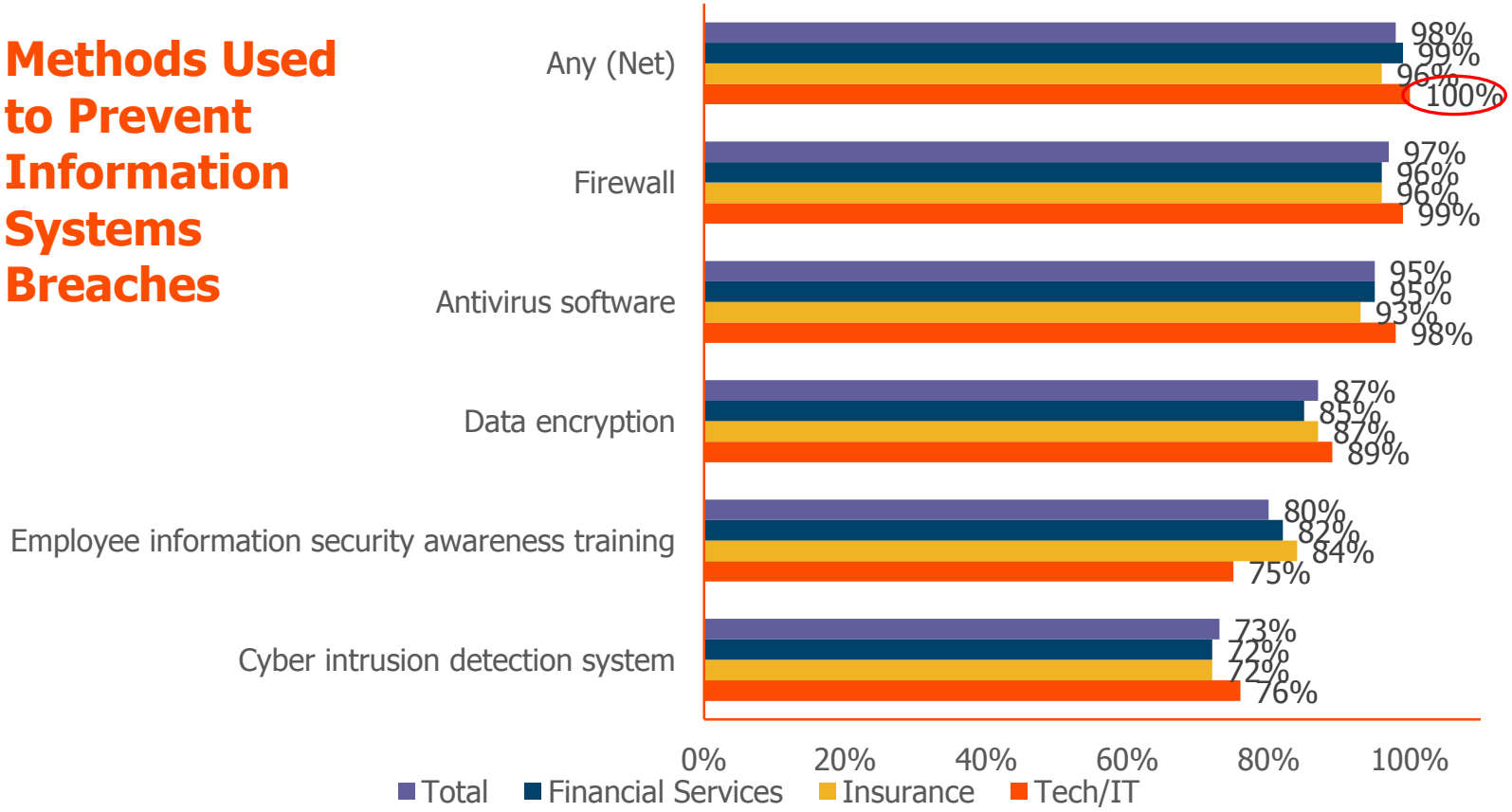
Nearly all (98%) use any of the listed methods to help prevent information systems breaches. Most used are a firewall (97%) and antivirus software (95%), followed by data encryption (87%). Four in five (80%) use employee information security awareness training, while three-quarters (73%) use a cyber intrusion detection system

**Question 15**

Which, if any, of the following methods does your company use to help prevent information systems breaches?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)

## Methods Used to Prevent Information Systems Breaches






BAE SYSTEMS
INSPIRED WORK

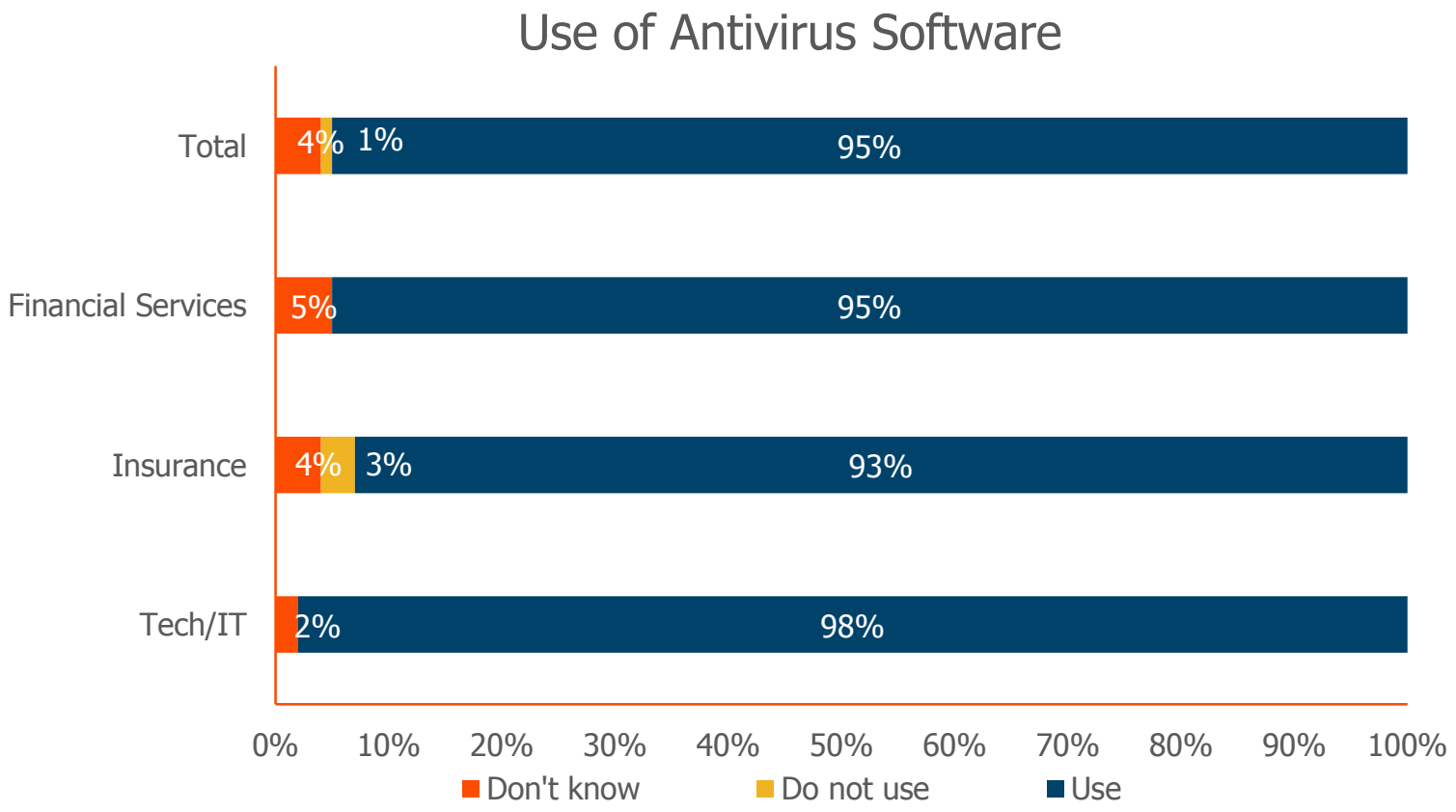
# Detailed Findings

Nearly all (95%) use antivirus software, regardless of industry.

**Question 15**

Which, if any, of the following methods does your company use to help prevent information systems breaches?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)



BAE SYSTEMS
INSPIRED WORK

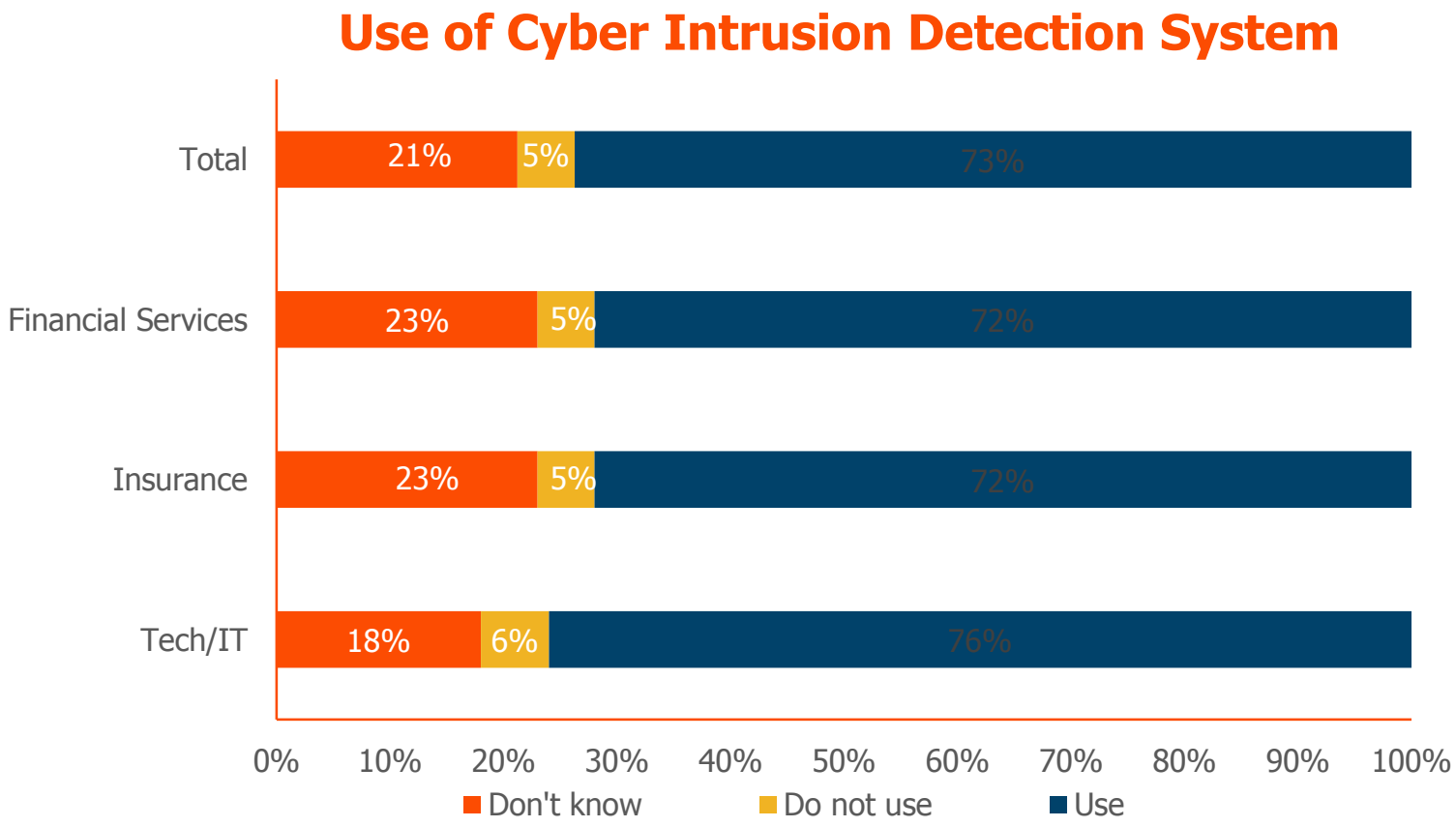
# Detailed Findings

Three-quarters (73%) use a cyber intrusion detection system, that is a hardware or software application that monitors network or system activities for malicious activities or policy violations.  Findings were similar among industry

**Question 15**

Which, if any, of the following methods does your company use to help prevent information systems breaches?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)



BAE SYSTEMS
INSPIRED WORK

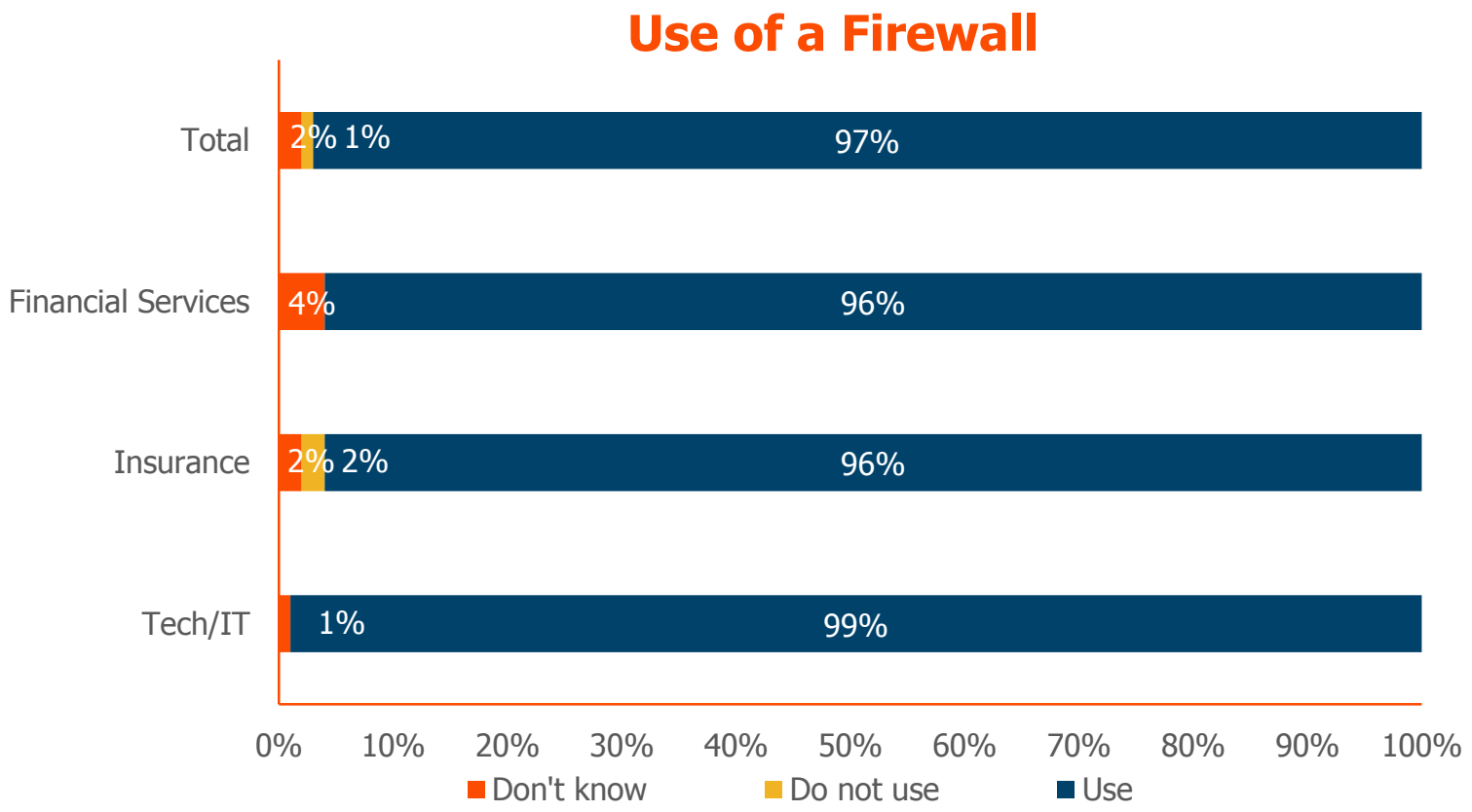
# Detailed Findings

Nearly all (97%) use a firewall, regardless of industry

**Question 15**

Which, if any, of the following methods does your company use to help prevent information systems breaches?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)



BAE SYSTEMS
INSPIRED WORK

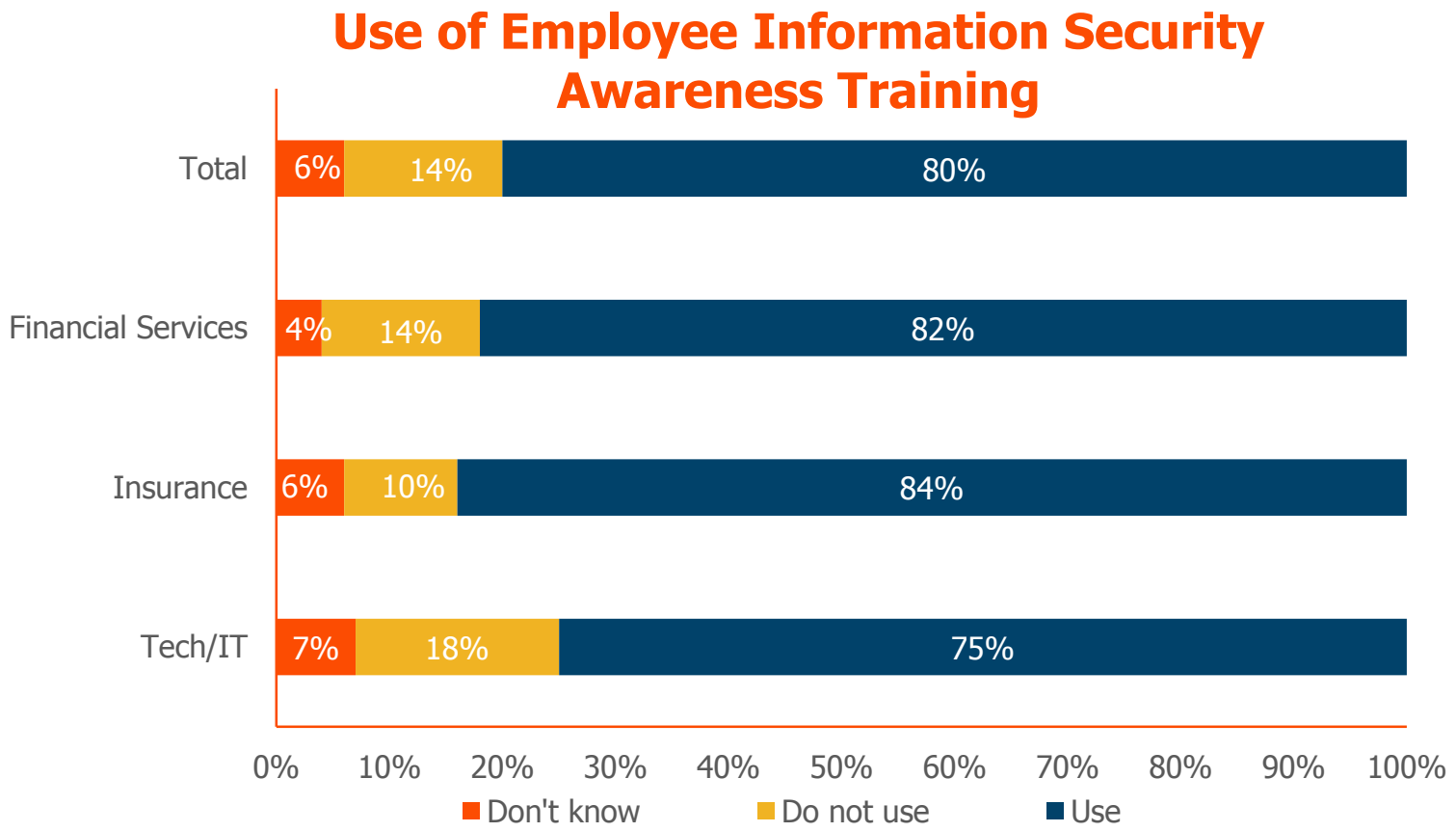
# Detailed Findings

Four in five (80%) use employee information security awareness training. Findings are similar across industry. Those at larger companies are more likely to use employee information security awareness training (89% of those with more than 500 employees vs. 61% of those with 500 or fewer).

**Question 15**

Which, if any, of the following methods does your company use to help prevent information systems breaches?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)



BAE SYSTEMS
INSPIRED WORK

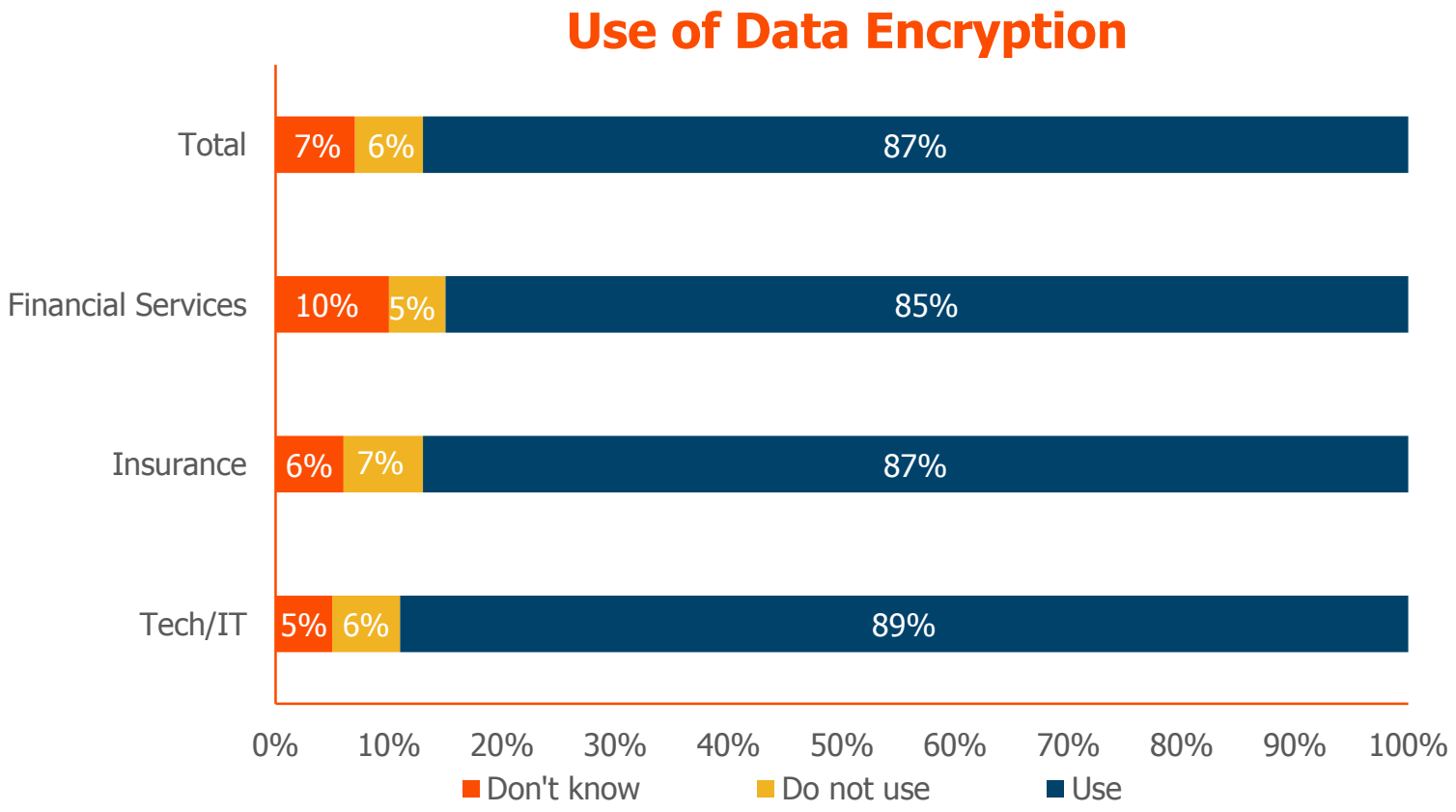
# Detailed Findings

Nine in ten (87%) use data encryption, regardless of industry. Significantly more larger companies use data encryption (91% of those with more than 500 employees vs. 77% of those with 500 or fewer).

**Question 15**

Which, if any, of the following methods does your company use to help prevent information systems breaches?

(Base=Total = 300; Financial services=100; Insurance=100; Tech/IT=100)



BAE SYSTEMS
INSPIRED WORK

# Demographic/Firmographic Profile

BAE SYSTEMS
INSPIRED WORK

# Demographic/Firmographic Profile

| | Total | Financial Services | Insurance | Tech/IT |
|---|---|---|---|---|
| | (n=300) | (n=100) | (n=100) | (n=100) |
| **Title/Role** | | (b) | (c) | (d) |
| **Manger** | 64% | 61% | 64% | 67% |
| **Director** | 23% | 15% | 26% | 28%b |
| **VP/SVP** | 13% | 24%cd | 10% | 5% |
| **Time with Company** | | | | |
| **5 years or less** | 33% | 31% | 30% | 39% |
| **6-10 years** | 22% | 30%d | 19% | 18% |
| **11-15 years** | 17% | 17% | 19% | 15% |
| **16-20 years** | 11% | 7% | 10% | 15% |
| **21-25 years** | 6% | 7% | 8% | 3% |
| **More than 25 years** | 11% | 8% | 14% | 10% |
| **Average** | 11.6 | 11.1 | 12.9 | 11.0 |

| | Total | Financial Services | Insurance | Tech/IT |
|---|---|---|---|---|
| | (n=300) | (n=100) | (n=100) | (n=100) |
| **Number of employees** | | (b) | (c) | (d) |
| **Under 250** | 22% | 27% | 20% | 19% |
| **250-500** | 8% | 10% | 7% | 7% |
| **More than 500** | 70% | 63% | 73% | 74% |
| **Gender** | | | | |
| **Male** | 51% | 48% | 42% | 64%bc |
| **Female** | 49% | 52%d | 58%d | 36% |
| **Age** | | | | |
| **18-49** | 56% | 64% | 51% | 52% |
| **50 or older** | 44% | 36% | 49% | 48% |
| **Average** | 47.1 | 45.3 | 48.5b | 47.4 |

BAE SYSTEMS
INSPIRED WORK

# Thank You

BAE SYSTEMS
INSPIRED WORK

**BAE SYSTEMS**
Surrey Research Park
Guildford
Surrey
GU2 7YP
United Kingdom

T: +44 (0)1483 816000
F: +44 (0)1483 816144