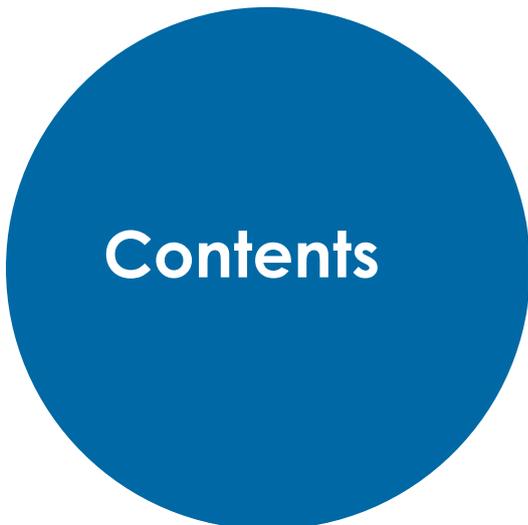


# The cyber-chasm: How the disconnect between the C-suite and security endangers the enterprise





# Contents

Executive summary	2
Research methodology	3
Findings of the survey	4
Conclusion	10
Appendix: survey results	12

## Executive summary

No company wants to be the next headline in the aftermath of a massive data breach, so you might think cyber-security strategies run like well-oiled machines. Not so, according to a new global survey by The Economist Intelligence Unit (EIU), sponsored by VMware. Instead, the research found a systematic disconnect between C-suite executives and senior technology leaders—a divide that can imperil the security of the firm.

- Corporate leadership and security executives do not share the same commitment to cyber-security—cyber-security ranks as the number one priority for security leaders, but only number nine for the C-suite.<sup>1</sup>
- The C-suite focuses on the strategic implications of cyber-security—primarily the impact of a cyber-attack on the firm's reputation or brand. The security function takes a tactical focus on assets—customer data, regulated information, apps, etc.
- The two segments are not in sync on the priority of assets for protection—a significant disconnect as many firms move to a flexible, priority-based defence system.
- Over 30% of security professionals expect a major and successful attack on the firm within 90 days, whereas only 12% of C-suite executives share that sense of urgency.

- This level of concern escalates—nearly 40% of security executives, and 25% of C-suite members, project a successful attack within three years.
- One area of agreement is on the origins of future threats; both segments worry about new technologies—such as cloud computing and BYOD (bring your own device)—that act as points of entry for unknown, unguarded-against threats.
- Security functions remain committed to traditional security solutions such as firewalls, identity management etc. Many are pursuing a “defend all” approach, making it difficult to prioritise defences.
- The C-suite, which makes budget decisions, is not likely to allocate the budgets that the security executives believe is necessary to protect the firm, or that match the expected escalation of threat levels.

This executive cyber-chasm creates imperatives for both segments. The C-suite needs to better understand the vulnerability of their business, and in particular how threats may escalate. The security/IT team needs to bring itself into alignment with the C-suite's more strategic view of cyber-security within the firm's operations. Finally, the security function must manage its expectations on the funding that will be provided to support cyber-defences, or adopt more flexible and lower-cost solutions.

<sup>1</sup> For the purposes of this survey, the Chief Information Officer was included in the security leadership segment. Please see Research methodology on the next page.

## Research methodology

In January-February 2016, the EIU, sponsored by VMware, surveyed 1,100 senior executives on data security practices within their firms. The survey's primary objective was to analyse the differences, if any, between the C-suite and senior IT executives on data security.

The survey sample was recruited from companies with between \$500 million and \$10 billion in revenues, and is equally representative of the Americas, Asia-Pacific and European regions. The panel came from 20 industries, with no single industry accounting for more than 14% of the total.

This was a survey of senior executives. The C-suite segment, sometimes referred to herein as senior management or corporate leadership, consisted exclusively of C-suite executives (eg CEOs, CFO, COOs). The security segment, sometimes referred to herein as the security executives, consisted of the CIO and those who identified themselves as Chief Data Officers or Chief Information Security Officers (CISOs).

Each panel was asked an identical set of 20 questions, and the results have been reviewed for insight and commentary by a panel of independent experts.

# Findings of the survey

## Mismatched perceptions of urgency and risk

Perhaps the most important decision a company can make about cyber-security is its importance. The C-suite and security leadership simply do not agree on the priority that it should be given.

By a large margin security executives rank cyber-security as the number one corporate initiative for their company. This is not surprising—after all, this group is directly responsible for corporate security strategies and their careers will be on the line if a serious

breach occurs.

The disconnect is that despite years of news reports about destructive data breaches at leading firms, security ranks near the bottom of the C-suite's priority list. Only 5% of C-suite executives consider it the highest priority corporate initiative—second to last on a list of ten major corporate initiatives. Instead, the C-suite focuses on growth issues such as acquiring customers and growing internationally.

Marc Goodman is the founder of the Future

**CHART 1 Which of the following corporate initiatives has the highest priority in your company?**

Select one.  
(% respondents)

### C-suite



### Security leadership



Source: Economist Intelligence Unit survey, 2016

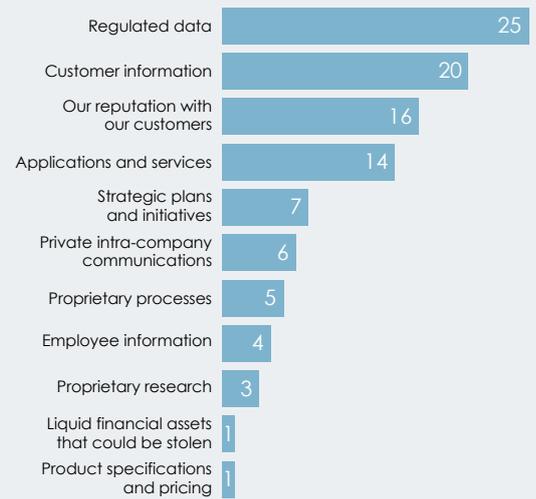
**CHART 2 What is the single most important asset in your company that needs to be protected from cyber-attacks?**

Select one.  
(% respondents)

**C-suite priorities**



**Security leadership priorities**



Source: Economist Intelligence Unit survey, 2016

Crimes Institute, and has consulted for international law enforcement agencies. He is not surprised by the C-suite attitudes. "Any good CEO focuses on making more money, while preventing losses is still seen as a necessary evil," he says. "Corporate risk management is something that needs to be managed, but it's not something that CEOs get up in the morning and feel excited about."

But while it may not be a surprise that cyber-security ranks below business growth on the C-suite agenda, it also trails other governance issues such as regulatory compliance and sustainability.

This may be an indication that executive boards are not giving security the attention it deserves. This lack of commitment can have direct implications for firms' security posture, by limiting funding and diminishing the impetus for organisational change.

Total information security is an impractical goal, so companies need to prioritise their more valuable or vulnerable assets. Unfortunately, this study reveals that the C-suite and security leadership are not in sync

on what needs to be protected the most.

The C-suite's priorities are clear—their primary single concern is to safeguard the reputation and brand of the firm. In contrast, security executives are focused on the data and the software—regulated data, customer information, applications, services, etc.

Industry research corroborates these findings. "Most institutions do not have enough insight into what information assets they need to protect with what priority," according to *Risk and Responsibility in a Hyperconnected World*, a report from the World Economic Forum and McKinsey & Company.<sup>2</sup> "Going forward, cybersecurity teams need to work with business leaders to understand business risks (for example, loss of proprietary information about a new manufacturing process) across the entire value chain and prioritize the underlying information assets accordingly."

This mismatch in priorities also speaks to a broader disconnect between management

<sup>2</sup> <http://www.mckinsey.com/business-functions/business-technology/our-insights/risk-and-responsibility-in-a-hyperconnected-world-implications-for-enterprises>

**CHART 3 Comparison of C-suite priorities and security implementation**

Select one.  
(% respondents)

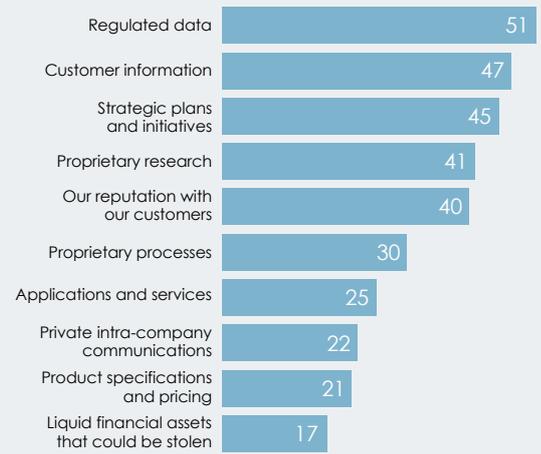
**C-suite**

Priority of assets to be protected



**Security leadership**

Assets—level of confidence in their protection



Source: Economist Intelligence Unit survey, 2016

and IT. The C-suite is thinking about the consequences of the breach—a strategic perspective. The security leadership remains heavily focused on information, data and applications—a tactical approach.

This is not just a difference of opinion—the divergence manifests itself in the structure of the firm's defences (see chart 3).

The security function's cyber-defence efforts appear to track the priorities of the security function—with less effort and resources directed to the priorities of the company's leadership. Accepting that the C-suite knows the broader interests of the firm, this implies that the most key assets are under-protected.

Another glaring mismatch between business and security leadership is in their relative perception of the risk of a security breach.

For example, almost a third (31%) of senior security executives believe that their company is either extremely or very vulnerable to a major cyber-attack within 90 days—an alarming number in its own right. But only 12% of C-suite members share this view and this urgency. This is a serious disconnect between those who lead their companies and those

who are charged with protecting it.

Similarly, 39% of security executives expect that their company will suffer a major breach within five years, versus just 27% of C-suite executives.

There is, however, broad agreement on the sources of cyber insecurity. Four out of ten C-suite respondents (40%), and a third of security leaders (34%), see cloud architecture

**CHART 4 A serious cyber-attack is one that succeeds in breaching your company's defences and causes harm to the business. How likely is it that your firm will experience such an attack within the following time frames?**  
(% respondents)

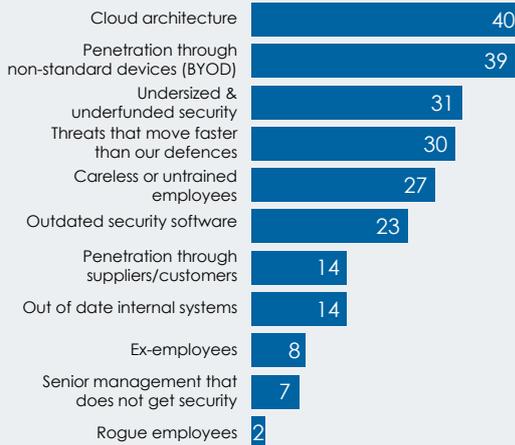


Source: Economist Intelligence Unit survey, 2016

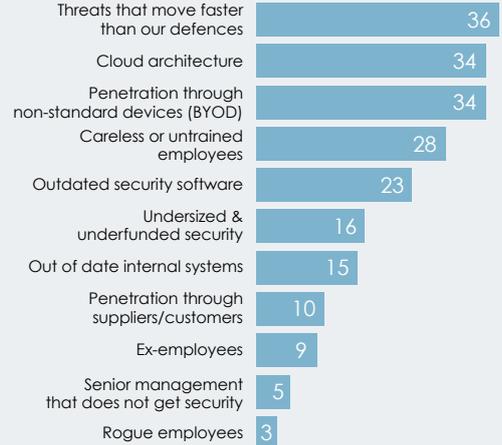
**CHART 5 What do you believe is the greatest risk or vulnerability of your firm to cyber-attack?**

Select one.

**C-suite**



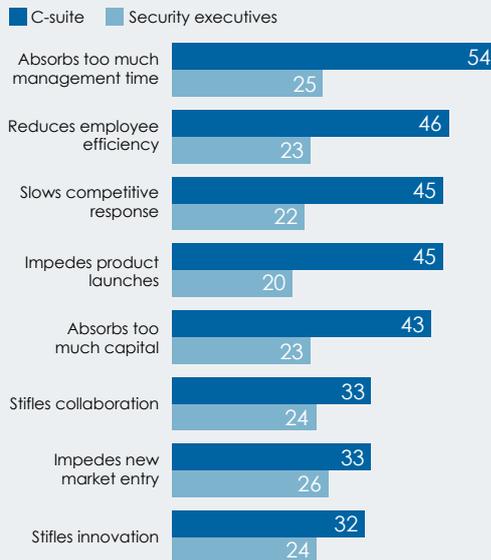
**Security leadership**



Source: Economist Intelligence Unit survey, 2016

**CHART 6 How has the threat of cyber-attacks, and the effort it takes to mitigate it (cyber-security), impacted the current operations of your company?**

(% respondents)



Source: Economist Intelligence Unit survey, 2016

as one of their company's greatest sources of security risk. There is similar agreement on penetration through non-standard devices (BYOD).

The C-suite clearly believes that cyber-security activity is taking a toll on critical functions—stifling innovation, slowing responses to competitors, delaying the launch of new products etc. Notably, they also see it as a major diversion of budgeted funds and, above all, a drain on management time and effort (including their own).

The IT leadership needs to understand the perspective of the C-suite—as important as cyber-security is, it is one of many contending corporate priorities. The C-suite is seeking to balance its constraint with an effective organisation. If the security executives are out of sync with this holistic thinking, the programmes they advance may be underfunded, rejected, or simply not acted upon by the larger organisation. This is another disconnect that can lead to vulnerabilities within the firm.

**CHART 7 Threats that move faster than our defences (selected as future threat to the business)**  
(% respondents)



Source: Economist Intelligence Unit survey, 2016

**The threats—perception of where future cyber-risk will come from**

One area where there is broad agreement between the C-suite and security executives is on the sources of future cyber-risk—the areas of greatest risk or vulnerability to the firm.

Both groups share the highest levels of concern around the growing adoption of cloud architecture, along with new vulnerabilities stemming from non-standard hardware related to employee BYOD policies.

These are not so much threats in themselves, but are instead the portals that future cyber-attackers can enter through. What both groups fear is the unknown—the potential to create threats that we don't know about yet. These are the threats that cannot be controlled.

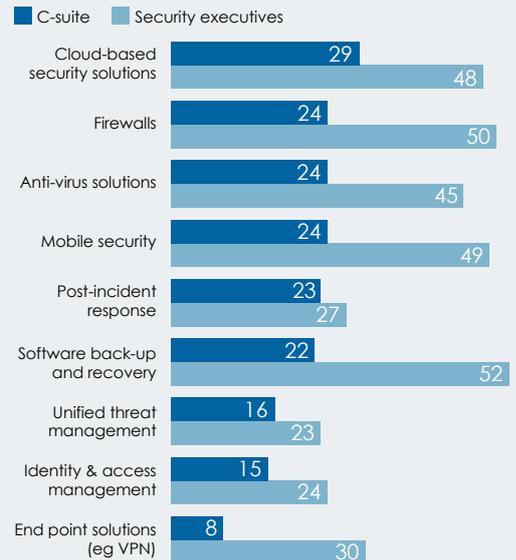
While there is general agreement on future threats, there is divergence on the "threats that move faster than our defences." Security leaders register a higher level of concern—36% versus 30% for C-suite members—in this critical category.

Again, this may indicate a dangerous lack of appreciation by the C-suite on the rapid mutation of the cyber-attack community.

**The nature of cyber-defences**

Security professionals understand they'll continue to play a cat-and-mouse game with hackers. Whenever a defence emerges to block the latest threat, sophisticated cyber-thieves quickly unveil a new and often more insidious exploit.

**CHART 8 Please indicate the importance of the following factors in your security strategy.**  
(% respondents)



Source: Economist Intelligence Unit survey, 2016

So it's not surprising the commitment CIOs and CISOs continue to hold for tactical responses, such as firewalls, anti-virus software and cloud-based security solutions. All of the solutions presented are deemed essential to security strategies by the security professional respondents.

However, the C-suite does not appear to share the same confidence in these approaches. Across all categories, the C-suite assigns significantly lower importance to these solutions—and they are the ones who write the cheques.

To be sure, most of these solutions will remain essential, like locks on the front door of a home. But in a world where the cyber-security stakes are so high, tactical solutions alone won't stop data breaches.

"The traditional approach holds that we are going to use anti-virus, firewalls and intrusion detection to create big moats so that when the barbarians attack, we'll see them coming and repel them," Mr Goodman says. "That's an outdated model of security for today. The new model acknowledges that the barbarians

aren't at the gate, they've overrun the gate and it's imperative for the CISO to actively hunt them down and get them off the network. It's about remediation and resilience because the bad guys are already here."

**Funding—paying for cyber-defences**

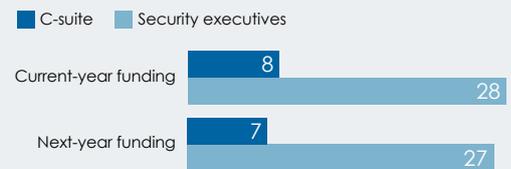
Funding presents a real challenge to a "defend everything" strategy. In every line of defence, the C-suite demonstrates a significantly lower commitment to fund these projects. On average, their level of commitment is less than half that of the security leadership.

**Threats grow more than budgets**

Having the C-suite and security staff on different pages about the urgency, trade-offs and nature of cyber-risks means they can't collectively do everything necessary to protect against current and future exploits. For example, the business leaders may not provide the financial support needed to stop sophisticated attacks. The survey illustrates this

**CHART 10 Respondents who foresee a large increase in cyber-security funding (more than 25%)**

(% of respondents who foresee a major increase in cyber-security funding)



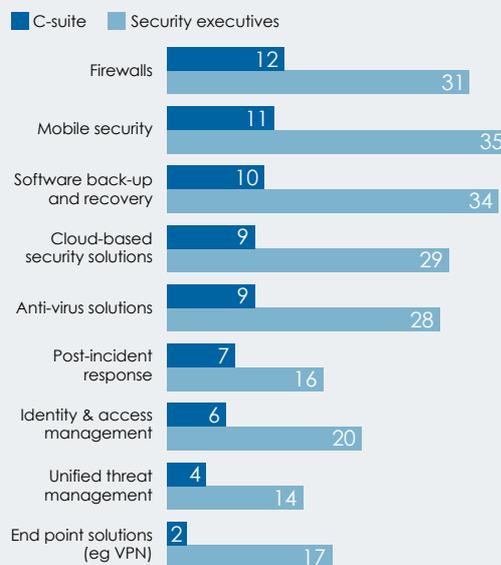
Source: Economist Intelligence Unit survey, 2016

with responses that show only modest funding increases in the months ahead.

Clearly, the security professionals would like to see additional financial resources to fight today's threats. In reality they may have to manage escalating security risk with much smaller budgets than they might like.

**CHART 9 Please indicate your firm's funding priority for the following cyber-security solutions.**

(% of respondents who designated the category a funding priority)



Source: Economist Intelligence Unit survey, 2016

# Conclusion

Why is there a disconnect over something as crucial as cyber-security?

One explanation lies in the different roles and responsibilities of each group. The C-suite sees the organisation holistically, as it tries to balance the full range of business, technology and operational matters. Historically, security staff have followed a more tactical path as they defend against highly organised, nation-state attackers, as well as opportunistic hackers and untrustworthy insiders.

But these differences alone don't tell the whole story. The research shows signs of wider problems, including missed opportunities for better communication between security staff and senior executives.

The implications are clear. Enterprises need a united front against the growing number and sophistication of attacks, and any disconnect between key stakeholders about cyber-vulnerabilities and the urgency of responses could result in company management not providing adequate resources and budgets for security officials to succeed. The challenge is particularly significant given the ambitious, multi-defence security programmes that security experts are advocating today. Potentially, this could delay responses to existing threats or keep organisations from proactively taking steps against emerging risks.

Fortunately, security professionals can foster closer alignment by building on their status as protectors of critical corporate assets. First, security personnel must redouble efforts to

inform the C-suite of the growing seriousness of cyber-threats. At the same time, security specialists must grasp the reality that they will likely have to depend on existing programs and relatively modest budget increases to effectively defend against a rising onslaught of more-sophisticated cyber-attacks.

CIOs and CISOs must incorporate the wider perspective of senior business executives into their security planning so they can demonstrate to the C-suite how cyber-security supports the firm's core strategic goals. "There's this major disconnect between people who want to build companies and those whose job it is to protect them because the protectors haven't done a good job in framing cyber-security as a key business enabler," says Mr Goodman. "Cyber-security shouldn't be seen as the thing that costs you money. It's something that will help you adopt new technologies so you can enhance corporate growth by delivering new products and services to your customers."

Security executives need to configure their cyber-defences to match the needs of the firm. "Current models for protecting institutions from cyber-attacks are becoming less and less effective," according to the World Economic Forum and McKinsey report. "They are technology-centric and compliance-driven. They do not effectively involve senior business leaders. They are highly manual and require specialized talent. As a result, they do not scale, given an increasing volume of attacks, and they place too high a burden on the

business. All too often security is the choke point for any innovative business initiative."

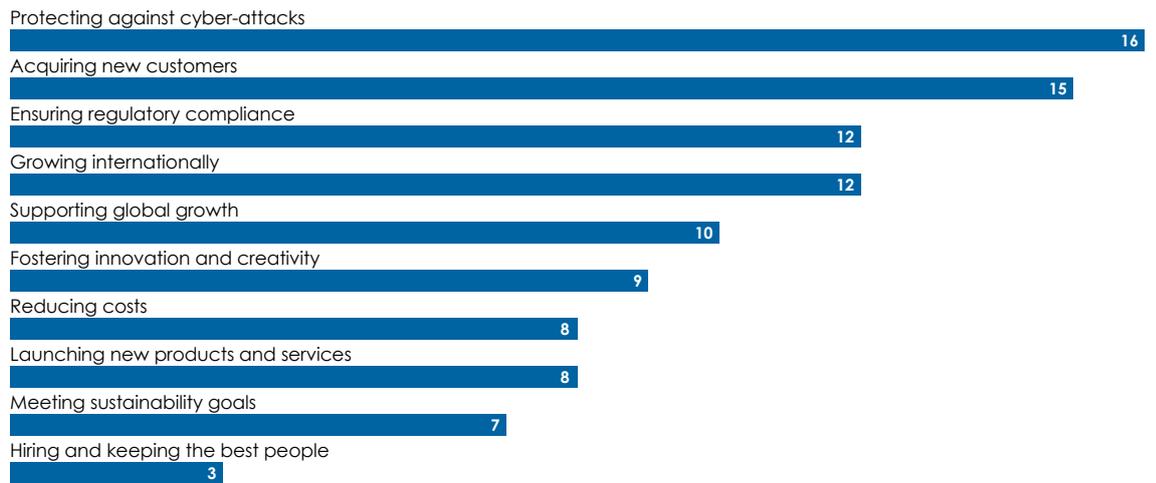
Finally, just as threats are escalating, so are the responses of firms. Effective cyber-defences are going to involve all personnel, cross siloes, and even extend to customers and suppliers. This absolutely requires the alignment and the commitment of the C-suite. This is a chasm that the security leadership will need to cross.

# Appendix: survey results

Percentages may not add to 100% owing to rounding or the ability of respondents to choose multiple responses.

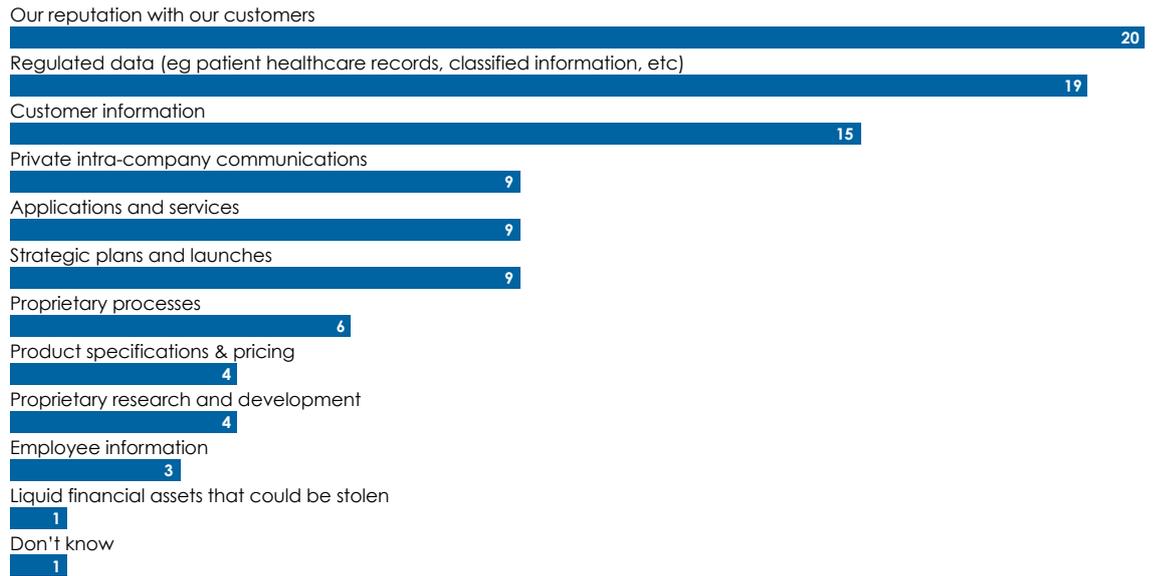
## Which one of the following corporate initiatives has the highest priority in your company?

Select one.  
(% respondents)



**What is the single most important asset in your company that needs to be protected from cyber-attacks?**

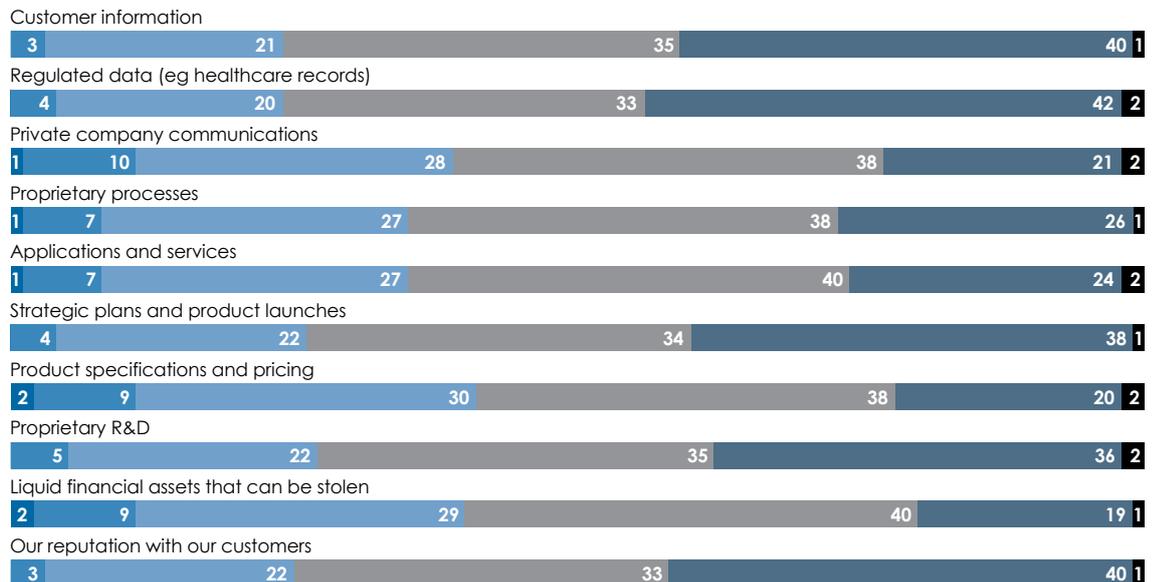
Select one.  
(% respondents)



**What is the single most important asset in your company that needs to be protected from cyber-attacks?**

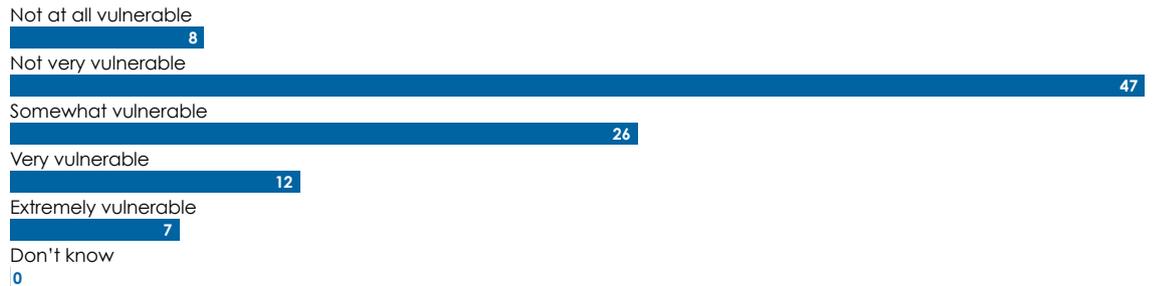
Select one.  
(% respondents)

■ Not confident at all  
 ■ Somewhat not confident  
 ■ Slightly confident  
 ■ Very confident  
 ■ Extremely confident  
 ■ Don't know



**What is your perceived level of risk facing your company from cyber-attack?**

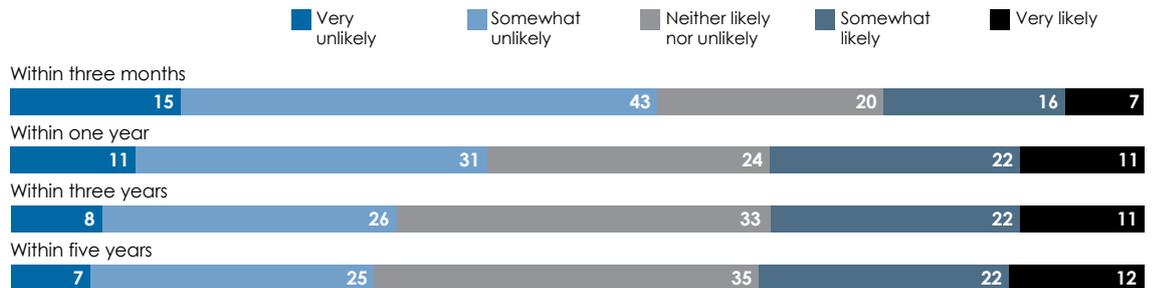
Select one.  
(% respondents)



**A serious cyber-attack is one that succeeds in breaching your company's defences, and causes significant harm to the business.**

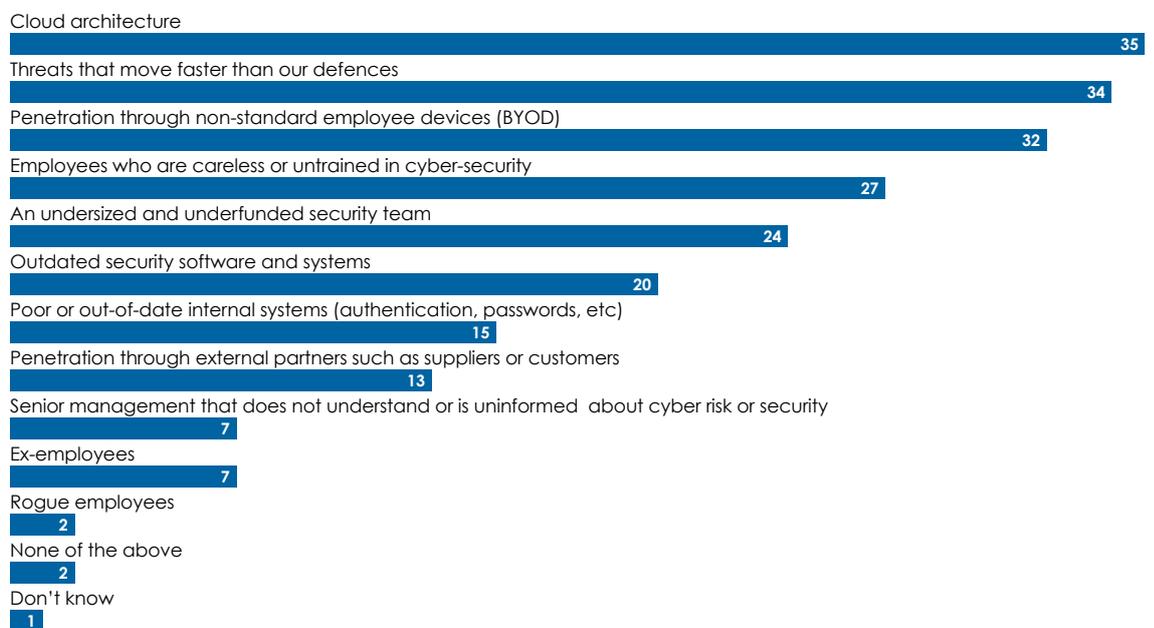
**How likely do you think your firm will experience such an attack in the following time frames?**

Select one for each row.  
(% respondents)



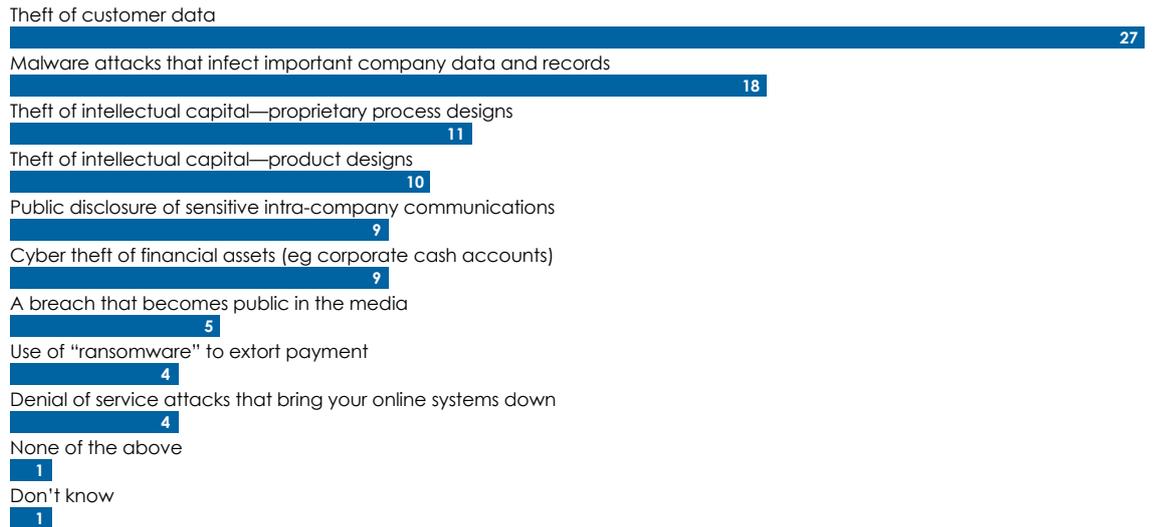
**What do you believe is the greatest risk or vulnerability of your firm to cyber-attack?**

Select the top three.  
(% respondents)



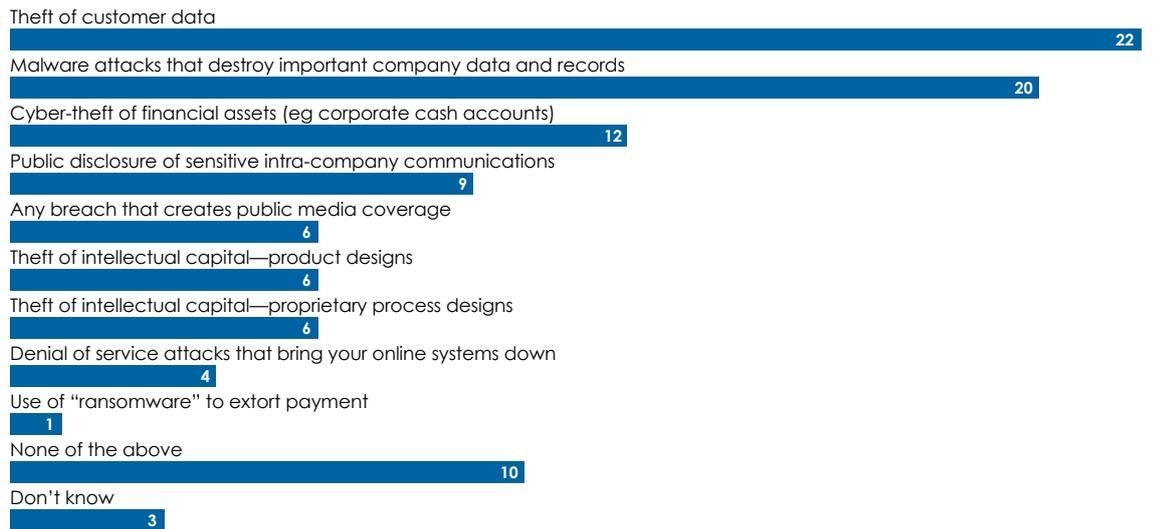
**Which one of the following types of attack, if successful, would cause the greatest harm to your company?**

Select one.  
(% respondents)



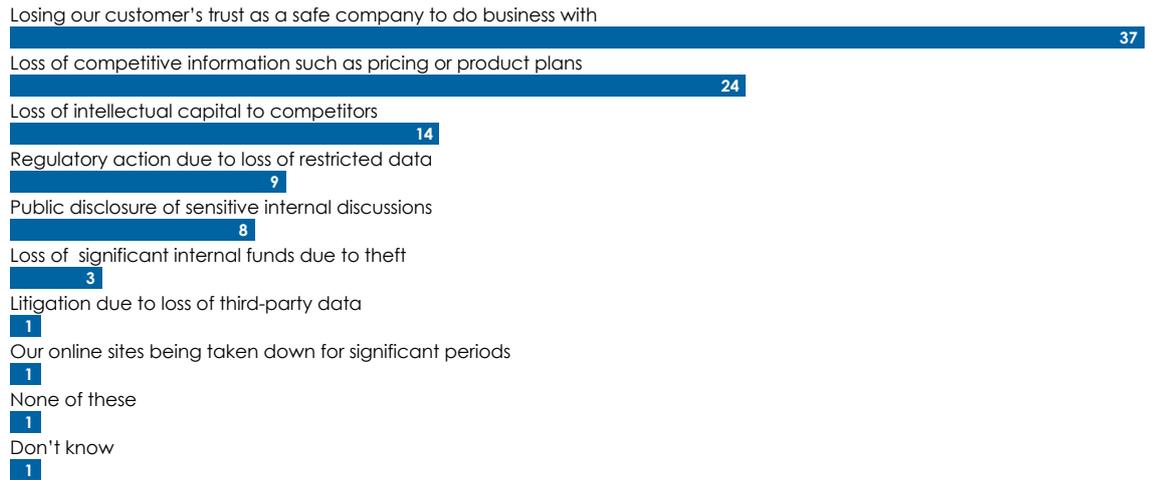
**Which one of the following do you think is the most likely to seriously attack your firm within the next year?**

Select one.  
(% respondents)



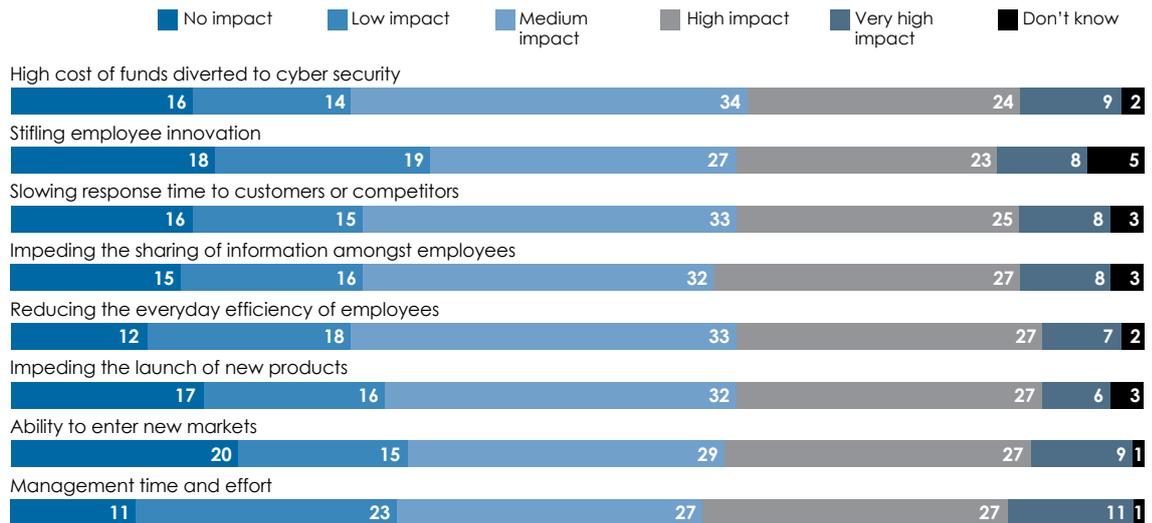
**Which of the following would cause the most damage to your company due to a successful cyber-attack?**

Select one.  
(% respondents)



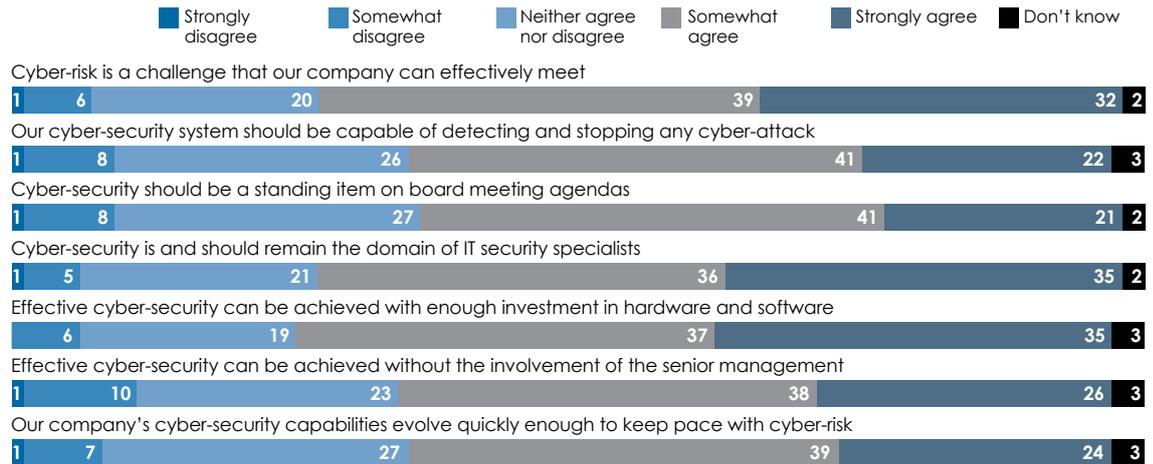
**How has the threat of cyber-attacks, and the effort it takes to mitigate it (cyber-security), impacted the current operations of your company?**

Select one in each row.  
(% respondents)



**To what extent do you agree with each of the following statements?**

Select one in each row.  
(% respondents)



**Please state your level of agreement with the following statement.**

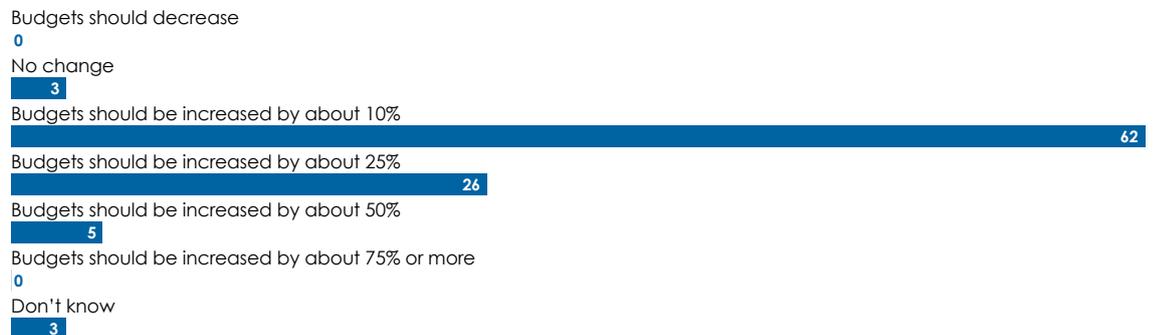
**"We now have enough resources (funding, people and technology) dedicated to cyber-security to meet the current cyber-risk challenge."**

Select one.  
(% respondents)



**How much, if at all, should your company's budget for cyber-security be increased in 2016?**

Select one.  
(% respondents)



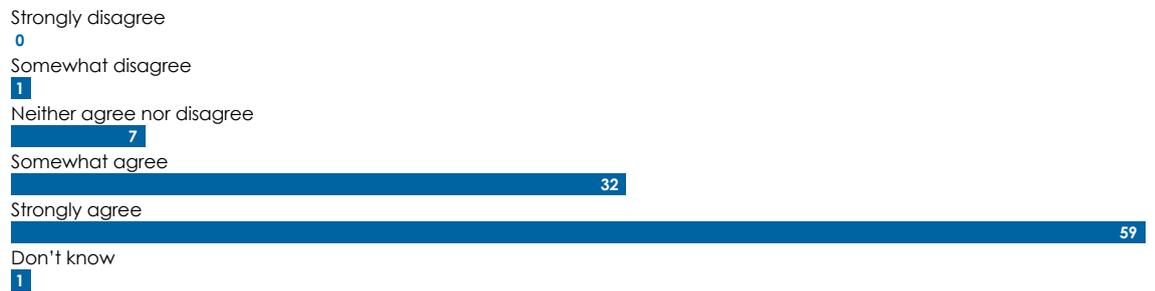
**To what extent do you agree with the following statements assessing your current security personnel needs?**

Select one in each row.  
(% respondents)



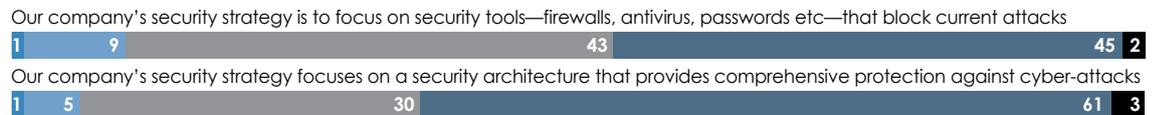
**To what extent do you agree your current security team and systems can meet the challenge of cyber-attacks?**

Select one.  
(% respondents)



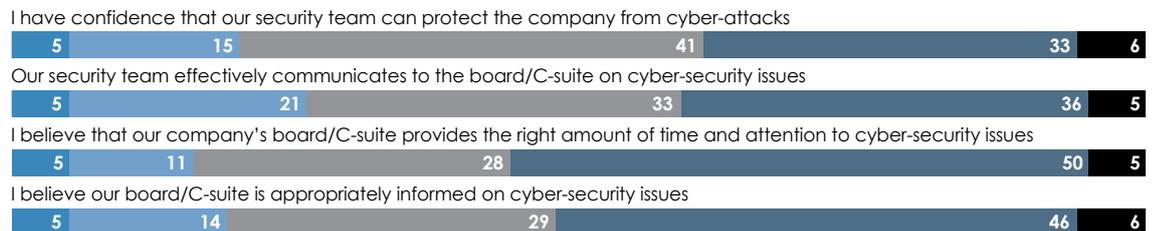
**Please provide your assessment of your company's security strategy by selecting one response for each statement.**

(% respondents)



**Please provide your assessment of your company's current cyber-security capabilities.**

Select one in each row.  
(% respondents)



**How important is fiduciary liability in board/C-suite decisions about cyber-security?**

Select one.

(% respondents)

Very unimportant

0

Somewhat unimportant

1

Neither important nor unimportant

13

Somewhat important

22

Very important

63

Don't know

1

**Please indicate the importance of the following factors in your security strategy.**

Select one in each row.

(% respondents)

Not a factor Not important Important Very important Critically important Don't know

Firewalls

4 24 32 39 1

Identity and access management

6 34 38 21 1

End point solutions (eg VPN)

1 6 31 38 24 1

Unified threat management

8 32 38 20 2

Cloud-based security solutions

3 24 32 38 2

Anti-virus solutions

5 24 34 35 3

Mobile security

1 6 22 32 38 1

Post-incident response

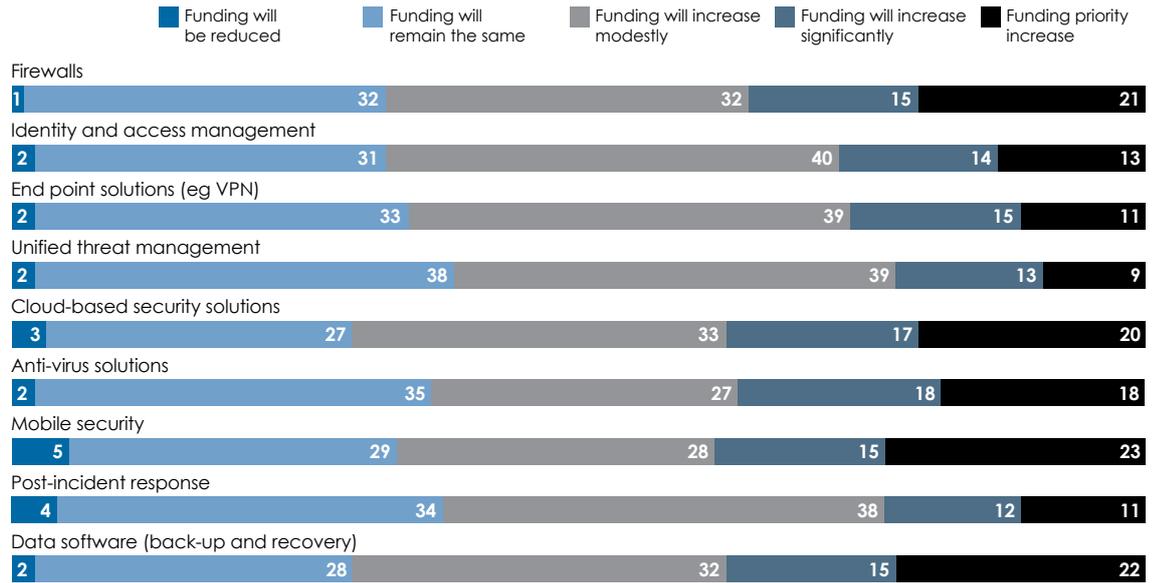
1 6 29 37 24 2

Data software (back-up and recovery)

3 25 31 39 2

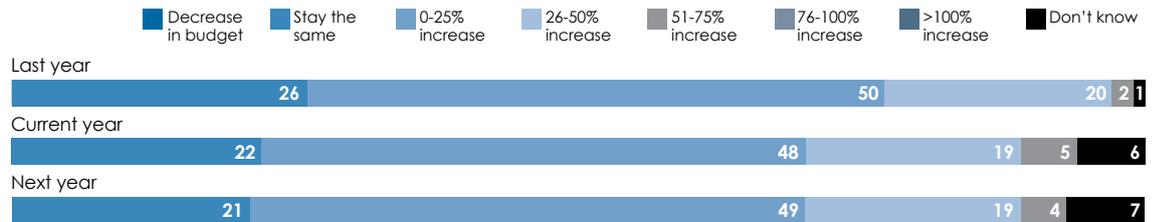
**Please indicate your firm's funding priority for the following cyber-security solutions by selecting one response for each solution.**

Select one in each row.  
(% respondents)



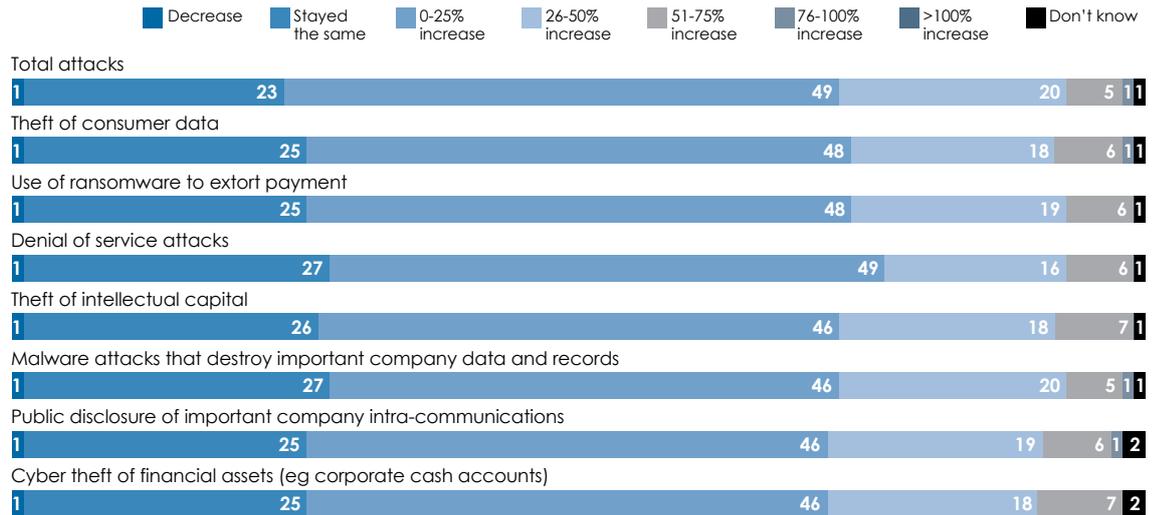
**Please provide an estimate of the change in your company's annual security budget in the past year, current year and next year.**

Select one in each row.  
(% respondents)



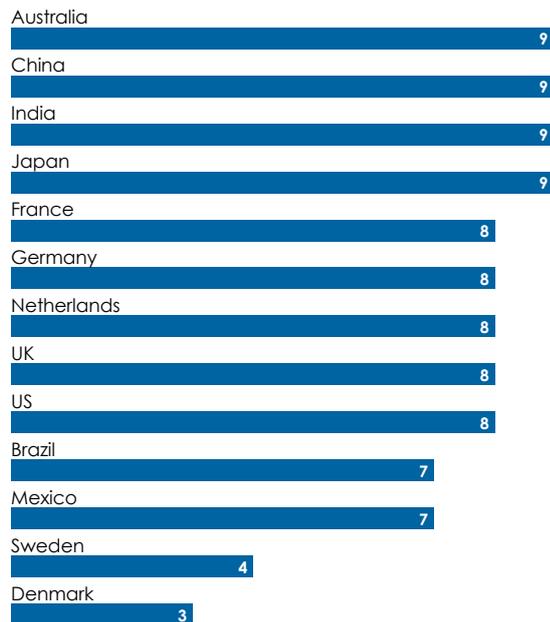
**Please provide an estimate of the change in cyber-attacks on your firm in the past year over the previous year.**

Select one in each row.



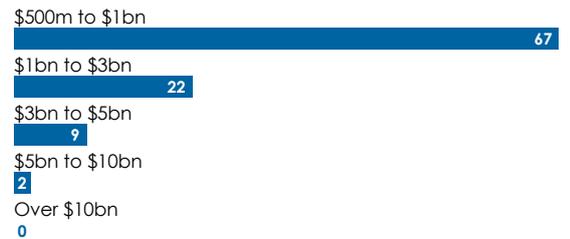
**In which country are you personally located?**

Select one.  
(% respondents)



**What are your organisation's global annual revenues in US dollars?**

Select one.  
(% respondents)



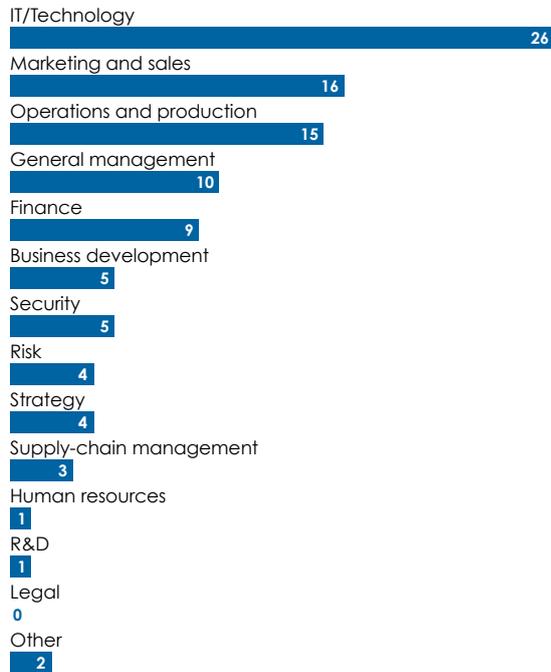
**Which of the following best describes your title?**

Select one.  
(% respondents)



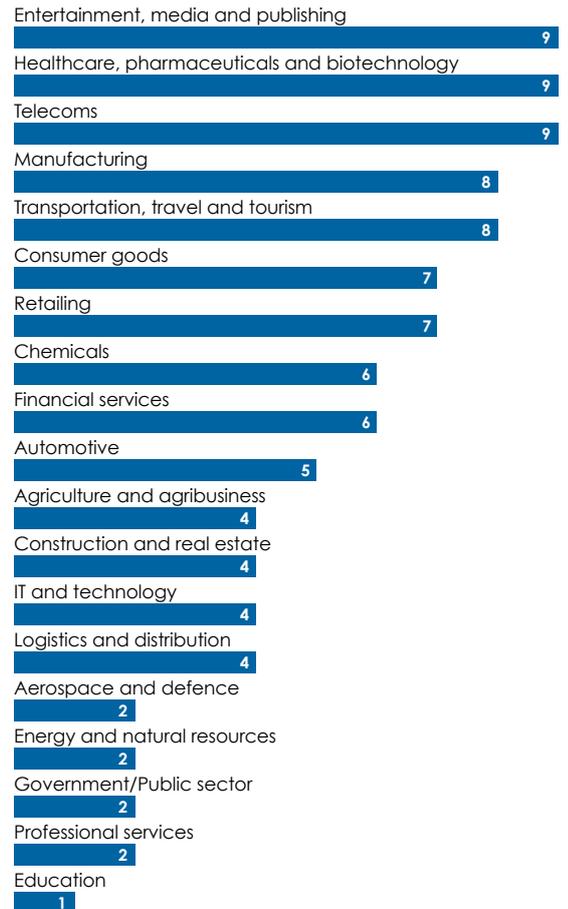
**What is your main functional role?**

Select one.  
(% respondents)



**What is your primary industry?**

Select one.  
(% respondents)



Whilst every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in the report.

**London**

20 Cabot Square  
London  
E14 4QW  
United Kingdom  
Tel: (44.20) 7576 8000  
Fax: (44.20) 7576 8476  
E-mail: london@eiu.com

**New York**

750 Third Avenue  
5th Floor  
New York, NY 10017  
United States  
Tel: (1.212) 554 0600  
Fax: (1.212) 586 0248  
E-mail: newyork@eiu.com

**Hong Kong**

6001, Central Plaza  
18 Harbour Road  
Wanchai  
Hong Kong  
Tel: (852) 2585 3888  
Fax: (852) 2802 7638  
E-mail: hongkong@eiu.com

**Geneva**

Boulevard des  
Tranchées 16  
1206 Geneva  
Switzerland  
Tel: (41) 22 566 2470  
Fax: (41) 22 346 93 47  
E-mail: geneva@eiu.com