# Boardroom Cyber Watch Survey

## 2014 | Report

**Cyber security is no longer sufficient**

to ensure business sustainability.

**Cyber resilience** should become the new

**boardroom priority**.


™ IT Governance Ltd is the single-source provider of books, tools, training and consultancy for IT governance, risk management and compliance. It is a leading authority on data security and IT governance for business and the public sector. IT Governance is 'non-geek', approaching IT issues from a non-technology background and talking to management in its own language. Its customer base spans Europe, the Americas, the Middle East and Asia.

More information is available at **www.itgovernance.co.uk.**

# Introduction

As we are halfway through 2014 it is evident that cyber security alone is no longer sufficient to ensure business sustainability. Daily, we read reports about organisations' defences being breached leading to the theft of confidential and personal data, causing vendors considerable financial losses and reputational damage among other implications.

While organisations need to defend themselves against potential attack, they must also accept that some attacks will inevitably succeed. Therefore **an organisation's cyber resilience is now the critical survival factor** – its ability to recover quickly once an attack has taken place.

Business continuity is unequivocally a boardroom responsibility, so directors will have to increase the attention and resources they devote to information security and resilience. For example, spending just 10% of the IT budget on security is no longer adequate to keep your organisation in business.

IT Governance's mission is to engage with business leaders and IT professionals about developing and implementing their cyber resilience strategy while ensuring they meet strict regulatory and compliance requirements, enabling businesses to compete effectively in the global information economy.

The '2014 Boardroom Cyber Watch Survey' is the second annual survey we have undertaken specifically targeting chief executives, board directors and IT professionals. It demonstrates the issues organisations are facing in the constantly changing cyber threat landscape and how the boardroom's and IT function's perception of cyber risks is shifting.

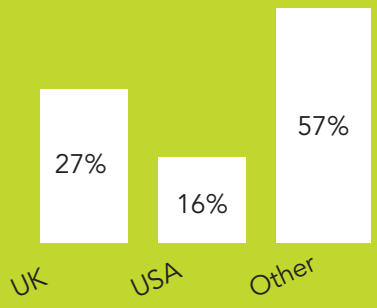
We are delighted that 240 respondents have taken part in the survey, representing a wide variety of industry sectors. The sample is truly international: while the majority are from organisations based in the UK and United States, respondents from South America, Central Europe, Africa, the Middle East, Asia, Australia and New Zealand have also contributed.

It gives me great pleasure to share our report on the survey. This document summarises the key findings and provides practical guidance on how both board directors and senior IT managers can address relevant challenges.

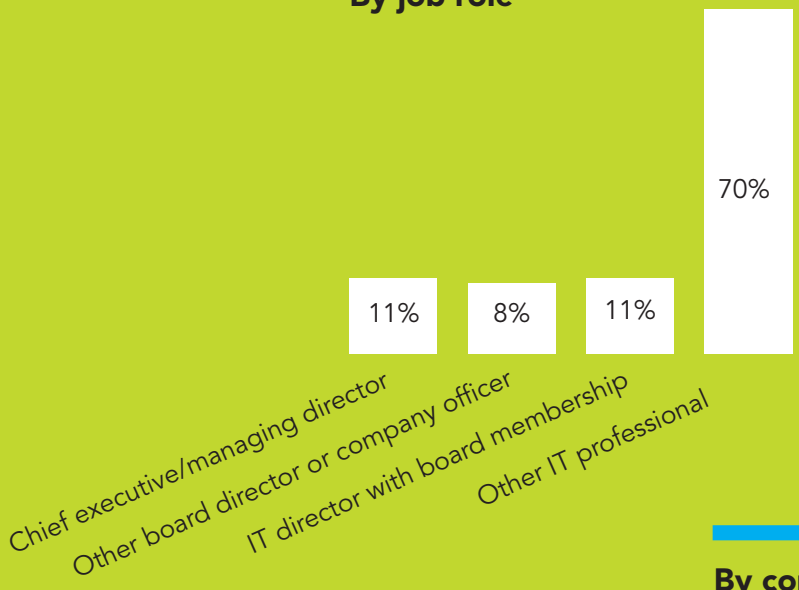
**Alan Calder**
Founder and Executive Chairman of IT Governance

# Survey Participants

## By country



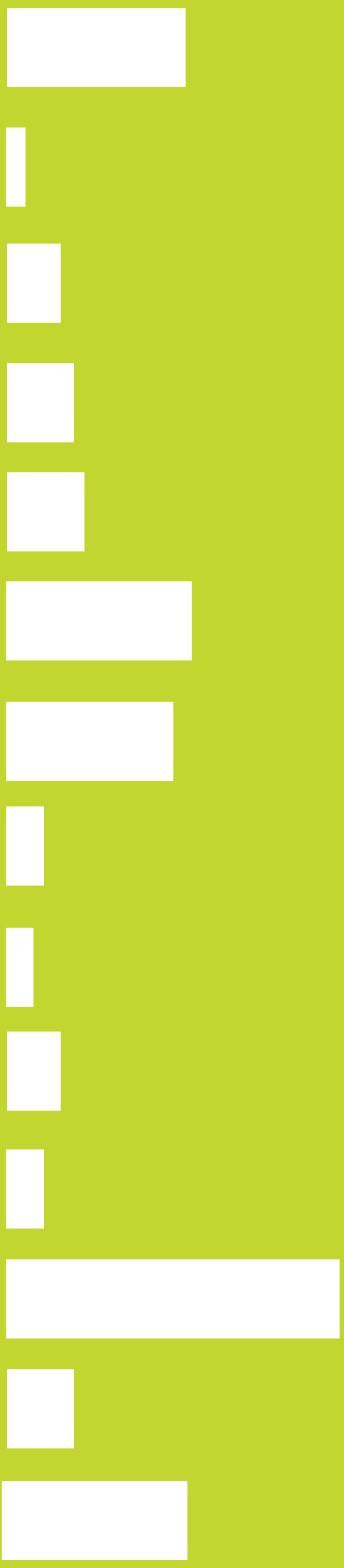

## By job role




## By company revenue

## By industry sector

| | |
|---|---|
| Business services | 14% |
| Charities & voluntary organisations | 1% |
| Education | 6% |
| Energy & utilities | 2% |
| Engineering | 3% |
| Financial services | 14% |
| Government / local authorities | 11% |
| Healthcare | 3% |
| Law | 2% |
| Manufacturing | 4% |
| Retail | 3% |
| Technology | 20% |
| Telecommunications | 5% |
| Other | 12% |



# Key Findings At A Glance

## Organisations remain complacent about the risks

The fact that 73% of our respondents believe they are capable of repelling cyber attacks demonstrates that organisations remain complacent about the risks they face. This complacency may be based on an underestimation of the current cyber threat landscape and/or an overestimation of their existing cyber security measures.

## Cyber security breaches can go undetected

Partly contradicting the above confidence, almost 36% of respondents believe their company was probably subject to undetected cyber attack in the past year, while almost 21% did not know.

## The IT function and the board don't communicate

A large proportion of boards are still in the dark about the current state of their companies' cyber defences: 32.5% of respondents say their boards receive no regular reports on this topic.

The quality of those reports is also a concern: 21% of respondents believe their companies' board reports fail to provide the information necessary for them to make decisions, and more than 28% are unsure if this information is provided at all.

Worryingly, almost a third of respondents (29%) believe that fear of retribution might be discouraging the IT department from fully disclosing details of cyber breaches to top management.

## Lack of cyber security knowledge in the boardroom

Many boards still lack the necessary knowledge to oversee cyber security effectively. 30% of respondents say that their boards lack the knowledge and qualifications to exercise effective governance in this area and 19% don't know.

## Cyber resilience is replacing cyber security

51% of those surveyed now accept the inevitability that some attacks will be successful and are more pragmatic, stating their objective as 'cyber resilience' - the ability to minimise successful attacks and to recover quickly when breaches are suffered.

## Growing customer demands for assurance

55% of respondents say that their customers enquired about their information security credentials in the past 12 months. This represents an increase from 50% in our 2013 study, and indicates a rising level of demand for best-practice standards such as ISO/IEC 27001.

The role governments play in pushing businesses to demonstrate assurance is also worth stressing. In the UK, the government's Cyber Essentials Scheme was officially launched in 2014. It aims to help businesses address cyber security and demonstrate assurance through certification. In the US, there are numerous state laws and industry-specific regulations against which organisations can demonstrate compliance.

# Finding 1

**A surprisingly high percentage of respondents (73%) believe that their current information security defences are effective at repelling cyber attacks, a figure at odds with all available evidence about the daily escalation of online threats. Only 14% think their defences are inadequate.**

Recent high-profile security breaches demonstrate that even large organisations with robust security procedures can - and do - suffer attacks. As recently as May 2014, retail company eBay and music streaming service Spotify reported that their networks had been hacked. If organisations of that size are affected, what chance is there for smaller enterprises?

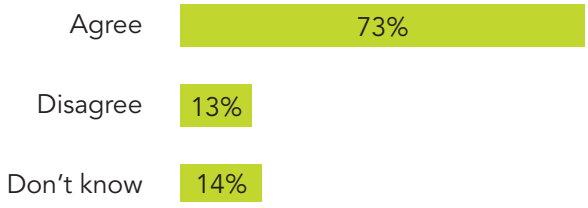
The fact that 73% of our respondents believe they are capable of repelling cyber attacks demonstrates that organisations remain complacent about the risks they face. This might be based on an underestimation of the current cyber threat landscape and/or an overestimation of their existing cyber security measures.

This complacency could also be based on the nature of undetected threats: respondents might believe their defences to be adequate because of the absence of any evidence of cyber attack. While this attitude is understandable, the false logic is surely obvious: ignorance of an event's occurrence doesn't mean it didn't happen. See also Finding 2 (next page).

**Tip:** Regular penetration testing will allow you to evaluate the effectiveness of your cyber security posture by simulating a malicious attack on your networks and systems. A penetration test, or 'pen test', is the easiest way of ensuring exploitable vulnerabilities are identified and addressed with appropriate security controls.

More information is available at:
www.itgovernance.co.uk/penetration-testing.aspx

My company's current defences are effective at repelling cyber attacks.



# Finding 2

**Despite the fact that 73% of respondents believe their current defences are effective enough, an element of doubt creeps in: only 44% thought it impossible for their organisation to have suffered an undetected cyber security breach in the last year.**

To an extent this contradicts the confidence shown in Finding 1 (see previous page), but it is fair to say that however confident people are about the effectiveness of their cyber security posture, a degree of caution will always be advisable. It is, after all, impossible to quantify data breaches till they are detected.

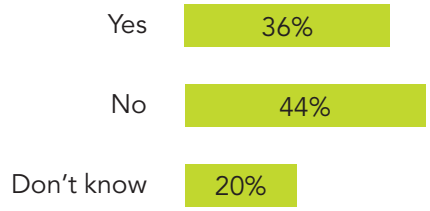
36% of respondents believe that their company could have suffered an undetected cyber attack in the past year and almost 20% didn't know – a vagueness that amounts to much the same attitude. This gives a total of more than 56% of respondents who thought it possible for their company to have suffered a breach without it being detected.

It is a given that most companies that suffer a breach will not realise it immediately. The Mandiant M-Trends® Report 2014 found that the average number of days that attackers were present on a victim's network before being discovered was 229 - more than seven months. This explains why many IT professionals wrongly believe their defences to be working satisfactorily even when they have been breached. They just don't know.

**Tip:** Cyber criminals are indiscriminate, and all Internet-facing organisations are potential victims. Businesses need to understand the threats they face and safeguard against them by maintaining their cyber security systems.

More information is available at:
www.itgovernance.co.uk/what-is-cybersecurity.aspx

Do you believe your company could have suffered a cyber security breach within the past year of which you are unaware?



# Finding 3

**A large proportion of boards are still in the dark about the current state of their companies' cyber defences: 32.5% of respondents say their boards receive no regular reports on this topic.**

Of the 55% that do receive regular reports, 19% of boards only receive reports annually and 18% of boards receive reports even less often than that. There are signs of progress, however: 62% of respondents say their boards receive reports at least monthly, whereas in our 2013 Boardroom Cyber Watch Survey only 48% said this was the case.

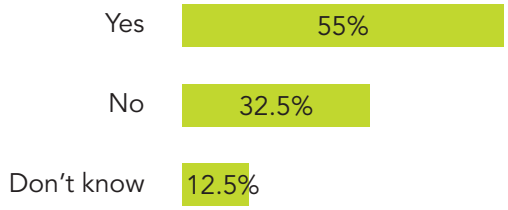
Cyber security is a business-critical concern that affects almost every business process, and whose success or failure at any level can cause the success or failure of the business. Given its importance, board members ought to receive regular and frequent reports from their CIOs and CISOs on the state of their organisations' cyber security.

Without board-level involvement in cyber security the consequences for an organisation can be disastrous, from financial penalty and loss of income to irreparable reputational damage. In cases of severe data breaches many companies collapse.

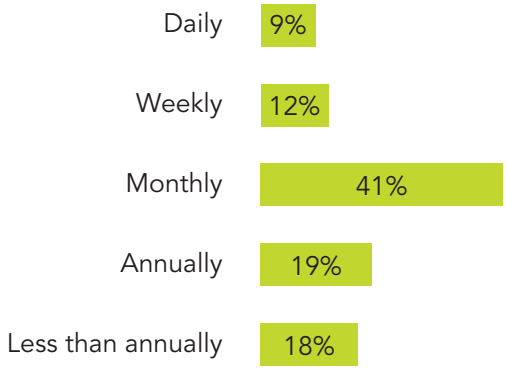
**Tip:** The international cyber security Standard ISO/IEC 27001 sets out the best-practice requirements of an Information Security Management System (ISMS), a holistic approach to cyber security that encompasses the whole organisation. Implementing an ISMS will allow you to win and retain business, protect and enhance your reputation, demonstrate regulatory compliance and satisfy audit requirements, and improve your organisation's efficiency.

More information is available at:
www.itgovernance.co.uk/iso27001.aspx

Does your board of directors receive regular reports on the state of your company's cyber-security defences?




If yes, how often does your board receive such reports?



# Finding 4

**The average quality of cyber security reporting to the board also requires improvement. Although nearly 63% of boards receive reports at least monthly, some 21% of respondents believe their companies' board reports fail to provide the information necessary for them to make decisions, and more than 28% are unsure if this information is provided at all.**

It seems that some companies are just going through the motions. They receive reports, but the reports themselves offer inadequate information.

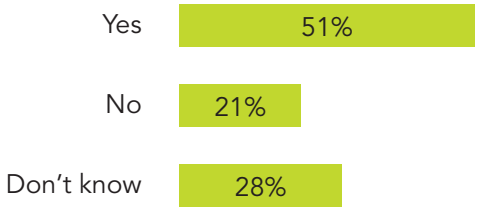
Cyber security depends on coordinated, integrated preparations for rebuffing, responding to, and recovering from a range of possible attacks throughout the entire organisation, and board-level understanding of cyber security issues, based on comprehensive reporting, is therefore vital.

Security threats are constantly evolving and increasing, and without proper knowledge of the status of their companies' IT security - and how it is able to respond to current threats - boards cannot make the informed decisions they need to safeguard their organisations and protect their information assets. Risk assessments provide the information that boards need. Asset-based risk assessments that identify the threat/vulnerability combinations likely to affect the confidentiality, availability or integrity of information assets enable expenditure on controls to be balanced against the business harm likely to result from security failures.

**Tip:** The international cyber security Standard ISO/IEC 27001 requires compliant organisations to carry out information security risk assessments. An Information Security Management System (ISMS) based on risk acceptance/rejection criteria allows the monitoring of external as well as internal service levels.

More information is available at: www.itgovernance.co.uk/iso27001-risk-assessment.aspx

Do cyber security reports presented to your board include the right information to provide the basis for action or improvements?



# Finding 5

**Another area of concern is the quality of communication between the IT function and the board. Almost a third of respondents (29%) believe that fear of retribution might be discouraging the IT department from fully disclosing details of cyber breaches to top management.**

The importance of board-level involvement in IT governance cannot be underestimated. Where it used to be the case that CIOs talked IT and board members talked business, the overlap between the two has now broadened considerably as IT and business needs have become ever more interwoven.

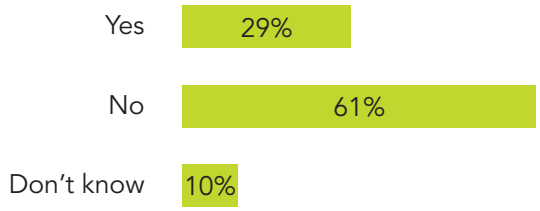
Communication, as in all business cases, is essential to ensure the effectiveness of an organisation's cyber security posture: CIOs need to understand business objectives as much as the board needs to understand IT governance issues.

IT governance is an essential part of corporate governance. Almost every modern business area involves IT in some capacity, so board-level involvement is essential to ensure the continuing success of the modern business. An IT governance framework ensures that an organisation's infrastructure supports its business goals, leading to the better alignment of IT with organisational decisions.

**Tip:** IT governance is a very broad term whose sub-domains include business continuity and disaster recovery, regulatory compliance, information security, IT service management, project governance and risk management. A number of IT governance frameworks exist, including COBIT®, ITIL® and Calder-Moir, and there are numerous applicable international standards, including the IT governance Standard ISO/IEC 38500, which provides principles for the use of IT.

More information is available at:
www.itgovernance.co.uk/it_governance.aspx

Do you believe fear of punishment could be discouraging your IT department from fully disclosing details of information security breaches to your company board?



# Finding 6

**Many boards still lack the necessary knowledge to oversee cyber security effectively. 30% of respondents say that their boards lack the knowledge and qualifications to exercise effective governance in this area and 19% don't know. Pressed further about whether their companies then had plans to prioritise cyber security governance training, 35% of respondents said no. Almost as many again said they didn't know.**

The fact that many companies still aren't considering training their boards despite acknowledging that they lack the necessary cyber security knowledge indicates that budgetary constraints may be a hindrance. Neglecting essential training in order to save money, however, is a false economy.

Cyber security breaches are expensive and often catastrophic. The average cost of a data breach runs into the tens of thousands of pounds for small businesses, and into the hundreds of thousands for large organisations. Many organisations fail to recover from a breach altogether.

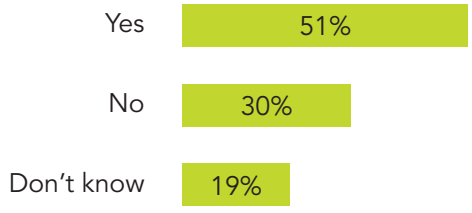
Boards fail to look far enough ahead when they reject training based on the time and expense that it demands. They are essentially burying their heads in the sand and hoping that they'll never need to call upon expertise that could save their company, and which they could easily gain with a relatively small outlay.

IT governance is a business-critical issue and therefore a board-level responsibility, and it is absolutely essential that board members are able to understand the challenges their organisations face in order to make appropriate business decisions.

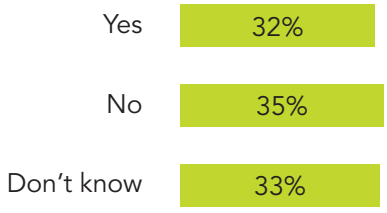
**Tip:** Suitable training - at any scale - needn't be the expense you fear. Education can come in many forms, from books and e-learning sessions to formal, classroom-based training courses. Having the cyber security knowledge to protect your organisation from attack will save you considerable expense and difficulty in the long run.

More information is available at:
www.itgovernance.co.uk/training.aspx

Does your board possess the necessary knowledge and qualifications to exercise effective governance in this area?




If not, are you planning to prioritise cyber security governance training for the most senior members in your company?



# Finding 7

**A lack of boardroom expertise may partly explain the reluctance of some companies to give up outdated cyber security goals. 38% of respondents say their objective is to prevent all cyber attacks. In contrast, 51% now accept the inevitability that some attacks will be successful and are more pragmatic, stating their objective as 'cyber resilience' - the ability to minimise successful attacks and to recover quickly when breaches are suffered.**

70% of respondents believe that cyber security – preventing all cyber breaches – remains a viable business goal. This, like Finding 1 (see page 8), indicates a degree of complacency based on an underestimation of the current cyber threat landscape and/or an overestimation of their existing cyber security measures.

56% of respondents say that board-level decision-making about information security matters involves directors who don't specialise in IT.

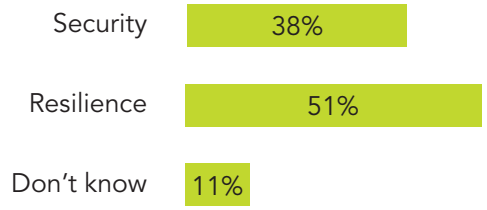
Considering this alongside Finding 6 (see page 13), which found that 30% of respondents said their boards lacked the necessary knowledge and qualifications, it is clear that boards' lack of technical expertise means they still aren't aware of the need for a robust cyber resilience policy.

Current cyber risks are such that a successful attack is inevitable. The only sensible response is to adopt a cyber resilience strategy that encompasses cyber security as well as business resilience, and aims not only to defend against potential attacks but also to ensure an organisation's survival following a successful attack.

**Tip:** Cyber resilience will ensure your cyber security is as effective as possible and also inaugurate robust business continuity plans so that you can resume normal operations after a successful attack.

More information is available at:
www.itgovernance.co.uk/cyber-resilience.aspx

Would you characterise your company's defensive objective as 'cyber security' or 'cyber resilience' (maintaining the best possible cyber defences but accepting the inevitability of some breaches and therefore putting emphasis upon cyber incident response)?



# Finding 8

**Despite technology being a fundamental enabler to most business functions, 31% of respondents say that their company fails to consider cyber security as part of the risk assessment for new business initiatives, and nearly 50% say that cyber security concerns have not deterred their company from undertaking new business initiatives.**

The fact that only 55% of respondents say that cyber security implications are considered as part of the risk assessment for new business initiatives and half of respondents say they have been undeterred by cyber security concerns shows reckless practices. The board has a duty - and often a legal obligation - to identify and manage risk. Unmanaged risk is the biggest threat to organisations, and the most common cause of project failures and business collapses.

Section C2 of the UK Corporate Governance Code (formerly the Combined Code) requires boards to 'maintain sound risk management and internal control systems'.

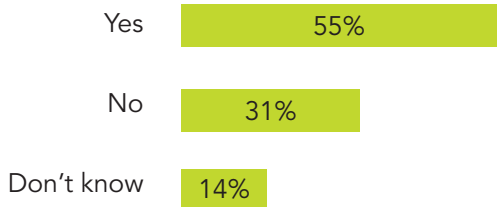
International industry-specific regulations (such as the Basel Accords) and US federal laws (such as SOX), require a risk management approach. Numerous international standards (such as ISO/IEC 27001) mandate risk management as an essential component of information security.

Risk management is an essential part of IT governance and cannot be neglected. It will enable you to manage your organisation's exposure to threats, comply with codes, standards and legislation, build customer confidence, and achieve optimum ROI.

**Tip:** Risk management depends on thorough and effective risk assessment across all business areas. There are a number of risk management frameworks, from the UK Cabinet Office's M_o_R® to the international Standard for risk management, ISO/IEC 31000, and the COSO Enterprise Risk Management Framework.

More information is available at:
www.itgovernance.co.uk/erm.aspx

Does your company's board routinely consider cyber security implications as part of the risk assessment for planned new business initiatives?



# Finding 9

**The study did find more positive signs of changing attitudes towards the management of cyber security: 35% of respondents say that their company employs, or is considering employing, a Chief Information Security Officer (CISO) in addition to a Chief Information Officer (CIO).**

The importance of experience and qualifications to senior-level posts is clear. 67% of CIOs have more than ten years' IT management experience, 70% of CIOs have business experience in areas other than IT, and only 22% don't have a business management qualification such as a degree or an MBA. What is also apparent is that the majority of CIOs, though clearly very experienced, have a business rather than an IT background.

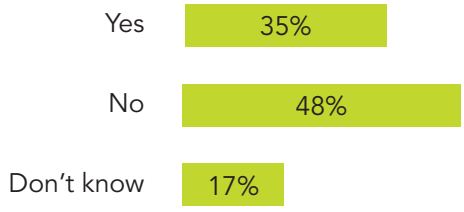
In the face of pervasive cyber threats the increasing importance of robust information security is reflected in the fact that having a dedicated senior professional in charge of information security - a CISO - is becoming increasingly normal. In industries where regulatory compliance is essential to daily operations in particular, it is imperative.

This increase in CISO positions demonstrates that as more organisations implement a standards-based approach to information security, so specific cyber security qualifications are increasing in value in the employment marketplace, and the demand for qualified information security professionals is growing.

**Tip:** Cyber security skills and qualifications are essential to any organisation committed to addressing cyber threats, and for information security professionals developing the requisite knowledge and skills in this area through certificated training is crucial to career development.

More information is available at:
www.itgovernance.co.uk/cybersecurity-training.aspx

Are you considering employing a chief information security officer (CISO)/ have you employed a CISO in addition to a CIO?



# Finding 10

**The importance of information security to customers was clearly highlighted in the study, with 55% of respondents saying that their customers had enquired about their information security credentials in the past 12 months. This represents an increase from 50% in our 2013 study, and indicates a rising level of demand for best-practice standards such as ISO/IEC 27001.**

Customers are understandably concerned about the safety of their personal information, and their apprehension is often exacerbated by frequent media coverage of large-scale data breaches. The easiest way to demonstrate that you are taking cyber threats seriously is to achieve accredited certification to the international cyber security Standard ISO/IEC 27001.

ISO27001 certification is a proof that you have implemented effective security processes based on international best practices, and regular auditing shows that you maintain the quality of your information security posture.

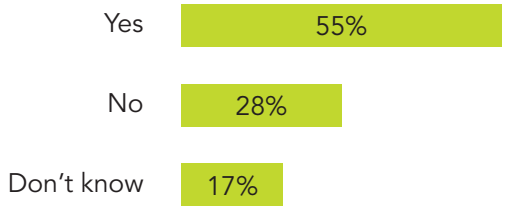
As well as increasing organisational efficiency, the assurance that accredited certification provides helps you gain new business and retain existing customers.

ISO27001 offers a holistic approach to information security that addresses people, process and technology, recognising that effective information security is an enterprise-wide concern. It is increasingly difficult to do business in an international market without ISO27001 certification as it is often a supply-chain requirement. In Japan and India it is a legal requirement.

**Tip:** ISO27001 is the only auditable international Standard that specifies the requirements for an Information Security Management System (ISMS), against which a company can be audited to demonstrate its adoption of best practices.

More information is available at:
www.itgovernance.co.uk/iso27001.aspx

Have any of your customers enquired about your company's IT security credentials in the past 12 months?



# Finding 11

**Asked if they believed that their country's government is taking cyber security seriously enough and providing sufficient support for companies to tackle this growing threat, about the same percentage of respondents – 42% – answered yes as no.**

Breaking the figures down further, it is interesting that there was a marked difference of opinion between the UK and the US. British respondents have more trust in their government's support to tackle cyber threats than their US counterparts do: approximately 51% of Britons answered yes, but only about 28% of Americans expressed similar confidence in their government.

In the UK, the government's Cyber Essentials Scheme was launched in 2014 to help businesses address cyber security. The scheme is a profile of controls based on the international Standard ISO/IEC 27001, implementation guidance, and test conditions for basic cyber hygiene, against which organisations can achieve certification.

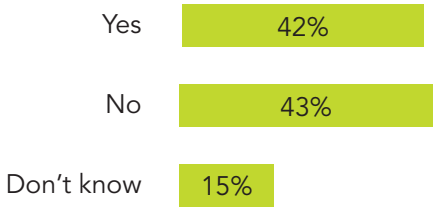
In the US, although there are numerous state laws and industry-specific regulations (for example CPPA, FISMA, GLBA, HIPAA and SOX), there is no federal law on cyber security. President Obama's proposed Cybersecurity Act of 2012 was defeated, and 2013's Executive Order: Improving Critical Infrastructure Cybersecurity is yet to be addressed by Congress. The National Strategy to Secure Cyberspace (2003) aims to engage and empower Americans to secure the portions of cyberspace that they own, operate, or control, or with which they interact, but is only an advisory strategy, not a federal law.

**Tip:** The UK's Cyber Essentials Scheme will enable companies to achieve – and demonstrate – a basic level of cyber security.

More information is available for the UK at: www.itgovernance.co.uk/cyber-essentials-scheme.aspx

More information is available for the US at: www.itgovernanceusa.com/cyber-security-regulations.aspx

Do you believe your country's federal government is taking cyber security seriously enough and providing sufficient support for companies to tackle this growing threat?



www.itgovernance.co.uk

**IT Governance Ltd**
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambs, CB7 4EA
United Kingdom

**T:** + 44 (0) 8450 701750
**E:** servicecentre@itgovernance.co.uk
**W:** www.itgovernance.co.uk


@ITGovernance


/it-governance


/ITGovernanceLtd

**Protect • Comply • Thrive**