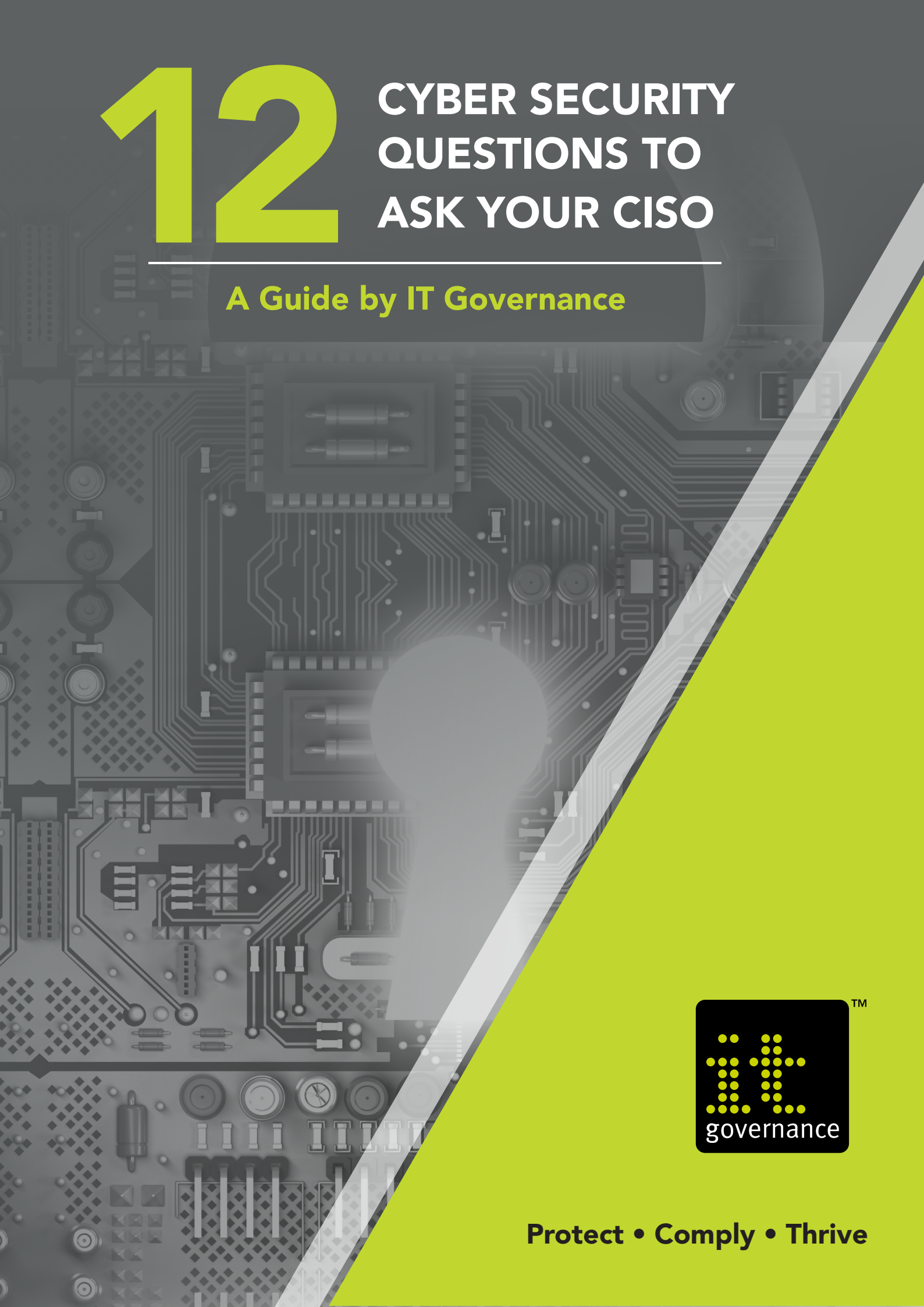
12 CYBER SECURITY QUESTIONS TO ASK YOUR CISO

A Guide by IT Governance



Protect • Comply • Thrive

Every director should have a general understanding of cybersecurity risk and what it means for their oversight responsibilities.

Regulatory pressures – most notably the EU General Data Protection Regulation (GDPR), the New York Department of Financial Services (NYDFS) Cybersecurity Regulation, and other federal and state data security laws and regulations – an increasing reliance on technology and big data, and the evolving threat environment each place significant obligations on organizations to reduce their cyber risks.

Cybersecurity is relevant to companies of all sizes in every sector. Threats are serious and evolving, and legal and regulatory requirements are growing. Regular communication between management and the board on cybersecurity is critical, to protect company interests and ensure accountability.

No longer a responsibility relegated solely to the CIO, cybersecurity has become a front and center concern in the boardroom.

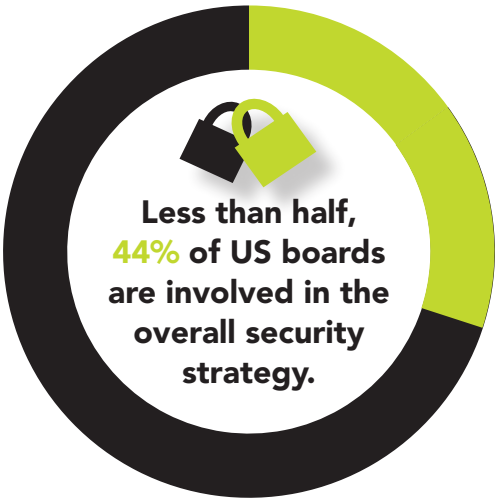
Despite this, The Global State of Information Security® Survey 2018 reveals that out of respondents surveyed, only 44% of corporate boards actively participate in their overall security strategy.

Although a board of directors and CEO may not need to know why a certain type of malware can penetrate a firewall, they do need to know what their organization is doing to address those threats.

Discussions at the board level should include identifying which risks to avoid, accept, mitigate or transfer (through cyber insurance), as well as reviewing specific plans associated with each approach.

The board must also ensure that the CISO is reporting at the appropriate levels within the organization. Sometimes the agenda of the CIO is in conflict with the CISO. As a result, some CISOs now report directly to the CEO, COO or CRO

Effective cybersecurity is an ongoing process. Armed with the right information, the board can play an essential role in preventing problems before they arise and rectifying data breach events.



Governance, compliance and data breach risks

It is evident that breaches can have enormous legal, financial and reputational consequences. The General Data Protection Regulation (GDPR) and NYDFS Cybersecurity Regulation will place even greater obligations on boards to address information governance and data privacy, or face staggering financial penalties.

Cybersecurity and compliance are ongoing processes that must regularly be tested, maintained and updated. Failure to implement and maintain essential security practices can significantly change to your organization's legal defensibility in the event of a data breach incident.

The value of achieving third-party compliance certifications

Obtaining certification to a recognized security standard provides an external, expert assessment of the effectiveness of the organization's security posture, and presents evidence that the organization has taken reasonable measures to mitigate data security risks.

Here is a list of 12 pertinent questions the board should be asking the CISO about cyber risk management.

12

1 What are the top risks our organization faces?

According to Gartner, by 2020 30% of Global 2000 companies will have been directly compromised by an independent group of cyber activists or cybercriminals.

Organizations need to prioritize the real risks by identifying security gaps and their impact on on business and ensure the budget to manage these risks is allocated accordingly.

The board should also be asking themselves whether they have a solid understanding of the impact of applicable (and emerging) legal, regulatory and contractual requirements related to cybersecurity.

2 Are we testing our systems before there's a problem?

There are many tests that can assess the vulnerability of systems, networks and applications.

An important element of any security regime should be regular penetration tests. Penetration tests are simulated attacks on a computer system with the intent of finding security weaknesses that could be exploited. They help establish whether critical processes—such as patching and configuration management.

Many companies fail to conduct regular penetration tests, falsely assuming the company is safe.

But new vulnerabilities and threats arise on a daily basis, requiring the company to continually test its defences against emerging threats.

3 Are we conducting comprehensive and regular information security risk assessments?

A risk assessment should provide the board with the assurance that all relevant risks have been taken into account, and that there is a commonly defined, understood means of communicating and acting on the results of the risk assessment.

Without determining the risk associated with vulnerabilities, organizations often misalign remediation efforts and resources. This approach not only wastes time and money, but also extends the window of opportunity for hackers to exploit critical vulnerabilities.

Since a threat (known or unknown) is the agent that exploits a vulnerability (such as outdated software), this relationship must be a key factor in the risk assessment process. Advanced security operations teams use threat intelligence to understand potential threat actors' capabilities, and current activities and plans; also, to anticipate current and future threats.

Information security or cybersecurity?

Information security and cybersecurity are closely related. Cybersecurity is defined as the protection of information from **cyber-attacks.** Information security on the other hand is a broader term that describes the **protection of information and information systems** from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide its **confidentiality, integrity, and availability** (CIA). Cybersecurity is usually seen as a sub-component of information security.

What is ISO 27001?

ISO/IEC 27001:2013 (ISO 27001) is the international standard that describes best practice for an ISMS (information security management system).

An ISMS is a system of processes, documents, technology and people that helps to manage, monitor, audit and improve your organization's information security – all in one place.

Achieving accredited certification to ISO 27001 demonstrates that your company is following information security best practice, and delivers an independent, expert assessment of whether your data is adequately protected.

ISO 27001 certification provides compelling evidence to stakeholders, clients and regulators that your organization has taken the necessary measures to protect itself from a data breach.

4 How do we demonstrate compliance with our cybersecurity controls?

An audit can support the board's need to understand the effectiveness of its cyber security controls. If the organization has chosen to comply with an information security standard such as ISO 27001, an independent review of the organization's information security controls can be conducted by a certification body. The audit can be used to provide evidence of the organization's commitment to information security.

The review, in turn, be used as a competitive advantage when bidding for new business, as is the case with companies certified to ISO 27001.

5 Do we have an effective information security awareness program?

According to the 2017 Cost of Data Breach Study, 25% of data breaches were due to negligent employees or contractors (human factor). Social engineeringremains a common tactic whereby criminals can break into a network through underhanded methods, by exploiting deceptive or deceitful employees (e.g. distributing malware through malicious links).

The critical importance of an effective staff awareness program cannot be emphasised enough. Research shows that traditional cybersecurity awareness measures can be greatly enhanced by a multi faceted security program that creates a total culture change and tackles persistent incorrect employee behaviors.

6 In the event of a data breach, what is our response plan?

Cybersecurity experts will agree that it is no longer a matter of 'if' but 'when' you will be breached. The critical difference between organizations that will survive a data breach and those that won't is the implementation of a cyber resilience strategy, which takes into account incident response planning, business continuity management (BCM) and disaster recovery strategies to bounce back from a cyber attack with minimal business disruption.

The board should also be aware of the laws governing its duties to disclose a data breach. The NYDFS Cybersecurity Regulation and GDPR are both examples of legislation that will introduce corporate breach notification obligations.

7 Are we adequately insured?

Recent reports reveal that cyber insurance is not adequate to protect companies from a full-scale cyber attack. Although it is difficult to quantify how expensive a data breach can be, information about other data breaches in your industry should provide an indication of the potential damages your organization might face.

The IBM Cost of Data Breaches Report 2017 shows that the global average cost of a data breach is $144 per record record, and the average overall cost to organizations was $3.62 million. Many organizations don't realize that they are liable for a data breach even if the data is stored in the Cloud, or if a third party with which it shares information is breached.

8 Do we comply with leading information security frameworks or standards?

Examples include the leading international information security management standard, ISO 27001, the Payment Card Industry Data Security Standard (PCI DSS) or the Cyber Essentials scheme (which provides basic cyber security protection against 80% of cyber attacks).

Certifying to leading international standards such as ISO 27001 is a strong indicator that the company employs proven best practice in cybersecurity, and presents a holistic approach to protecting not only information online, but also risks related to people and processes.
The organization may also opt for independent certification to verify that the controls it the implemented controls are working as intended.

9 Is our information security budget being spent appropriately?

Less than half of companies surveyed, 45%, say they have the board involved in setting security budgets, compared to a global average of 39%, according to the Global State of Information Security Survey.

Setting the information security budget is not just about having enough budget to buy more technology to patch cybersecurity holes.

The key is to take a strategic approach to budget allocation to make a real impact on the organization's information security posture. Increased security does not translate to increased technology. In fact, technology alone won't protect your business from the ever-present threat.

10 Do we have visibility into the network?

Poor network behavior visibility can wreak havoc in an organization. The IBM Cost of Data Breach Study 2017 revealed that the average time to detect a data breach is 191 days.

Many administrators do not have access to the network that is deep enough to paint an accurate picture of what's really going on inside the network. They also lack the tools that can quickly identify, interpret and act on threats.

11 Are supplier and supply chain risks part of our risk register?

Cyber threats may reach the organization through any number of vulnerable points along the supply chain. The cybersecurity of any one organization within the chain is potentially only as strong as that of the weakest link in the supply chain. It is often the smaller organizations within a supply chain that, due to more limited resources, have the weakest cybersecurity arrangement. Dealing with supplier risks requires a broad, inclusive approach that allows organizations to identify their place within the supply chain, and map their cybersecurity dependencies and vulnerabilities.

Organizations should implement a multi-stakeholder supply chain risk assessment process that engages as many members of the supply chain as possible.

12 When did we last test our recovery procedures?

Ponemon Institute's 2017 Cost of Data Breach Study: Impact of Business Continuity Management revealed that BCM programs significantly reduced the time to identify and contain data breaches.

Effective BCM helped save companies 43 days in the identifying a breach and 35 days in containing it. BCM and disaster recovery plans must be tested regularly to establish whether the business can recover rapidly following an attack. Some of the "what if" thinking should be devoted to establishing how vulnerable designated fallback options are to cyber attacks. For example, a malicious assault on your data may not be detected for some time and backup data may have been compromised.

About IT Governance

We advise global businesses on their most critical issues, presenting cost-saving and risk-reducing solutions, based on international best practice and frameworks. Our technical expertise and solid track record in international management system standards means we can project manage and deliver a complete solution from start to finish. We work shoulder to shoulder with our clients to help them protect and secure their intellectual capital, comply with relevant regulations, improve shoulder-to-shoulder defenses and deploy strategies that benefit the entire business.

For the past 15 years, we have developed and fine-tuned our ISO/IEC 27001 consultancy services with methodologies and tools, beginning when two of our directors led the world's first successful certification to BS 7799—the forerunner to ISO 27001.

We deliver a comprehensive range of solutions to help clients address their cyber security needs, including training courses, publications, staff awareness programs, policies and procedures toolkits, consultancy services and compliance software

For more information about ISO 27001, visit us at www.itgovernanceusa.com/iso27001

References

Gartner Security and Risk Management Scenario Planning, 2020

The "C" in today's C-suite: cybersecurity – Reactionsnet.com

Cyber Security: What the Board of Directors Need to Ask:

2017 Cost of Data Breach Study: Impact of Business Continuity Management

Cyber-security risks in the supply chain: CERT-UK

IBM Cost of Data Breaches Report 2017

Cybersecurity And The Board – Forbes

Cyber Security Breaches Survey 2017

Cybersecurity Ventures Report

Top 5 Cybersecurity Facts and Figures

How IT Governance can help your organization improve its cyber defences:

What we can do	How will you benefit	Solution
Determine your current information security processes and the Standard's requirements	The analysis will identify the resources and capabilities you need in order to close the gap.	Gap analysis
Deliver a **total security staff awareness solution** tailored to your organization's unique needs and culture.	With a multi-faceted security awareness program, we can help you create a total culture change and tackle persistent undesirable employee behaviors.	Security awareness program
Implement a **cybersecurity risk assessment** and management process.	Automating elements of the risk assessment process helps you save time, effort and expense with a quick and easy cybersecurity risk assessment tool.	vsRisk™ Risk Assessment Software
Assess your systems and networks for any potential weaknesses due to system configuration issues, hardware or software flaws, and operational weaknesses.	Accurately evaluate your organization's ability to protect its networks, applications, endpoints and users from determined attackers, get detailed information on actual, exploitable security threats, prioritize remediation, apply necessary security patches and allocate security resources.	Penetration Testing
Implement a **business continuity management process.**	Save hours of uncertainty, trial and error about how to go about implementing an effective business continuity management system that helps you to achieve cyber resilience.	Business Continuity Management /ISO 22301 Consultancy
Help you to implement an **information security management system (ISMS)** that protects all your organisation's information, not just digital information.	Achieve organization-wide protection, protect the confidentiality, availability and integrity of your data, reduce costs and improve your cyber resilience posture.	Information Security/ ISO 27001 Consultancy

Speak to an expert

IT Governance Ltd

Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park, Ely,
Cambs. CB7 4EA. United Kingdom.

t: 877 317 3454
e: servicecenter@itgovernanceusa.com
w: www.itgovernanceusa.com

/ITGovernanceLtd /ITGovernanceLtd /ITGovernanceLtd