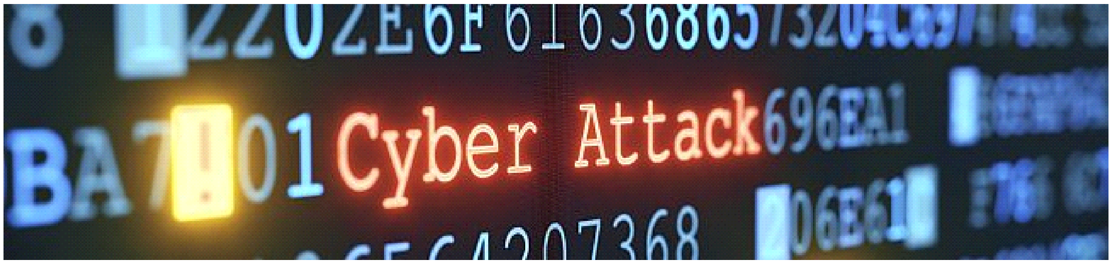
Chartered Institute of
Internal Auditors

01 February 2023

Cyber security

Chartered Institute of Internal Auditors



This guide provides an insight into regulatory developments in cyber security and the various roles that internal audit can play to support their organisation in seeking to manage cyber security risks and to mitigate them where appropriate.

Key points

1. A strong cyber awareness culture is one of the best defences against cyber-attacks. Internal audit has a crucial role to play in ensuring that this culture is understood and 'lived' by staff at all levels.

2. Forthcoming regulations will increase the burden on organisations to ensure they have effective cyber security strategies and culture in place, in addition to robust controls and policies to prevent and remediate attacks.

3. Cyber security starts with the board and senior management setting a clearly articulated strategy that supports and protects the organisation’s objectives.

4. The board and internal audit must work together to ensure that all of the organisation’s data assets, and the potential cyber threats that could jeopardise those assets, have been adequately mapped out. Assurances agreed in the audit plan should reflect the organisation’s cyber risk appetite.

Introduction

Technology and data now permeate practically all aspects of business and operations, from customer data to intellectual property to HR records, and their use is not just limited to technology and IT companies. The workplace is increasingly a digital environment. The cyber risks inherent in such widespread reliance on technology are profound.

Already there are serious financial and reputational implications for organisations that do not take cyber security seriously and are affected by successful cyberattacks, with Grant Thornton estimating that the total global cost of cyber attacks in 2015 was at least $315bn.

Organisations of all types, both in the public and private sectors, are becoming more vulnerable to the risks related to technology dependence. The risk is likely to continue to expand further in the future as innovations such as the internet of things (IoT) develop and mature (The ‘Internet of Things’ or ‘IoT’ has been taken to mean a system in which every day physical objects have network connectivity via the internet, allowing them to send and receive data), with Cisco estimating that machine-to-machine internet traffic will increase by 44% by 2020.

The European response to these trends, in the form of the Network and Information Security (NIS) Directive – adopted in August 2016 and due to be transposed by Member States by May 2018 – signals a sea change in European cyber security law.

Through its new information security and incident notification requirements for operators of essential services and digital service providers (DSPs), the Directive will impose legal obligations upon a host of organisations throughout the EU that may previously have lain beyond the scope of existing cyber security legislation.

A number of organisations deemed by Member States as ‘operators of essential servers’ will therefore, as laid out in Article 14 of the Directive, have to take ‘appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.’

Too often, organisations focus on implementing technical measures in response to cyber security risk over an organisational response. Internal audit can play a significant role in this organisational response to both the risks posed by cyber security and the stipulations of the NIS Directive.

Misha Glenny talks about cyber crime

Author Misha Glenny has spent years investigating cyber crime. He spoke at our annual conference in 2018.

Follow this link to view the video

Regulatory developments

NIS Directive

The adoption of the NIS Directive represents the most significant EU initiative in the area of cyber security in recent years. With Member States due to apply the law by May 2018, its application will have a significant impact on a number of organisations across Europe over the next few years.

Separately, the adoption of the General Data Protection Regulation (GDPR) in April 2016 signals a revolution in European data protection law, with the GDPR harmonising national laws and standards on data protection across the EU. Due to come into force in May 2018, the UK government has already indicated that it intends to comply with the GDPR whether or not the UK is still a member of the EU. Certain elements of the GDPR are also worth consideration briefly here.

Operators of essential services

One of the core elements of the NIS Directive is the obligation for Member States to identify critical sectors comprising operators of “essential services”. Organisations that fall within these designated sectors will then be subject to more stringent rules due to the importance of the services they provide and the potential societal and economic disruption caused by cyber attack.

Businesses and organisations can expect to be identified as an operator of an essential service if they:

1. Provide a service which is essential for the maintenance of critical societal and/or economic activities
2. If the provision of that service depends on network and information systems.
3. If an incident would have significant disruptive effects on the provision of that service.

Sectors most likely to be defined as such include banking, energy, transport, health, and elements of public administration.

Security requirements

For those organisations deemed to be an operator of an essential service, Article 14.1 requires that Member States ensure that they ‘take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems to which they use in their operations.’

The Directive recommends a risk-based approach, with Article 14.1 further stating that the measures adopted ‘shall ensure a level of security of network and information systems appropriate to the risk posed.’

Operators will also need to "take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services", for instance resilience and business continuity measures.

Incident notification

The NIS Directive also lays down a requirement for operators of essential services to report to the competent authorities – namely the Computer Security Incident Response Teams that each Member State is required to establish – any incidents that seriously compromise their networks and information systems and significantly affect the continuity of critical services and the supply of goods. In the UK, the competent authority will be the National Cyber Security Centre.

Digital service providers

Digital service providers will also have obligations similar to those outlined above to ensure the security of their network and information systems and minimise the impact of incidents affecting that security.

They will be subject to lighter-touch reactive requirements and cannot be subjected by member states to more onerous requirements than under the Directive, except for reasons of national security or law and order.

The General Data Protection Regulation

While the NIS Directive will have a significant impact on the profession of internal audit, the General Data Protection Regulation (GDPR) also contains some provisions that overlap with those laid down the NIS Directive.

While the GDPR is a broad Regulation, containing stipulations relating to the issues ranging from the processing and storage of personal data to use of personal data by research organisations, of particular relevance to cyber security are those articles contained in Section 2 on “Security of personal data.”

Articles 32, 33, and 34 lay down new rules on security of processing, notification of personal data breaches to authorities, and communication of data breaches to data subjects, respectively, each of which are closely related to the prevention and management of cyber security attacks and their consequences.

Impact

The immediate impact of the implementation of the NIS Directive by Member States over the coming two years will be to draw into regulatory scrutiny many organisations that may have previously lain beyond the scope of existing cyber security legislation.

A number of organisations that will be deemed as ‘operators of essential servers’ will therefore have to comply with the stipulations of the NIS Directive, mainly by taking ‘appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.’

Considering the NIS Directive’s references to giving due regard to ‘the state of the art’ in articles 14.1 and 16.1, the next section of this briefing will examine an example of best practice in the organisational management of risk developed by the IIA: the three lines of defence.

Management of cyber security risk: the three lines of defence

As explained in IIA Global's Global Perspectives and Insights: Internal Audit as Trusted Cyber Adviser, cyber security must be considered holistically and systemically, as the effects of failure can range from an inability to conduct basic operational processes, to loss of intellectual property, to potentially significant reputational damage. It is not solely a technology risk; it is a business risk and, as such, internal auditors have a critical role to play. In February 2016 a Hollywood hospital was subject to a cyber-attack with the hospitals computer system locked by ransomware. Procedures such as CT scans were unable to be carried out; employees were unable to gain access to important documents, patient data and emails. In this case the risk of harm was very real.

IIA Global lays out a best practice approach to improve the effectiveness and efficiency of risk and control functions within organisations in its position paper Three Lines of Defence in Effective Risk

Management and Control, published in January 2013. Ensuring that the three lines of defence in an organisation are properly segregated and operating effectively is a key method employed by many organisations to ensure that cyber security risk is properly managed and that ownership is clearly allocated.

Effective risk management is the product of multiple layers of risk defence. These layers should be in place and operating at a robust level to deal with any critical risk to the business, and can be equally applied to the management of cyber risk.

The board and executive management (sit above the three lines of defence)

Effectively acting as the primary stakeholders for the three lines and collectively have responsibility and accountability for setting the organisation's objectives, defining strategies to achieve these objectives, and establishing governance structures and processes to best manage the risks in accomplishing those objectives.

At executive level a chief technology officer (CTO) is typically responsible for providing knowledge and direction regarding the technologies available to drive the organisation's mission.

Organisations may also employ a chief security officer (CSO) or a chief information security officer (CISO). The CSO or the CISO typically generates and deploys the cyber security strategy and enforces security policy and procedures.

A chief information officer (CIO) may also be employed with responsibility for driving competitive advantage and strategic change throughout the organisation.

Taken together, the CTO, CSO, CISO, and/or CIO collaborate with the:

- chief executive officer and other members of senior management, such as the chief risk officer, in managing cyber security-related risk; and
- liaise with internal audit who would be able to contribute to the discussion in relation to the robustness of risk management and the effectiveness of the design of controls as well as how efficiently and effectively controls are being implemented.

The first line of defence - operational management

- Ownership, responsibility and accountability for data, processes, risks, and controls.
- This function often resides with system administrators and other charged with safeguarding the assets of the organisations.
- Administering security procedures, training and testing; maintaining secure device configurations and ensuring that software and security patches are up-to-date; and conducting penetration testing, amongst other tasks associated with the ownership and management of risks and controls.

The second line of defence - risk, security, control, and compliance oversight functions

- Ensuring that first line processes and controls exist and are effectively operating.
- These functions often comprise of IT risk management and IT compliance functions.
- Typically facilitate and monitor the implementation of effective risk management practices by management, and help risk owners in reporting adequate risk-related information up and down the

firm.

- Assessing the risks and exposures related to cyber security against their organisation's risk appetite and ensuring that they are properly aligned; monitoring current and emerging risks and changes to laws and regulations; and collaborating with the first line functions to ensure appropriate control design.
- Include designing cyber security policies, procedures, training, and testing; conducting cyber risk assessments, monitoring incidents, key risk indicators, and remediation; and assessing relationships with third parties and suppliers, amongst other things.

The third line of defence - internal audit function

- Ensuring that the first and second lines of defence are functioning as designed -provides independent and objective assurance to the board and executive management on how effectively the organisation assesses and manages its cyber risks.
- Providing independent ongoing evaluations of preventive and detective measures related to cyber security.
- Evaluating IT assets of users with privileged access for standard security configurations, problematic websites, malicious software, and data exfiltration.
- Tracking diligence of remediation.
- Conducting risk assessments of third parties and suppliers in line with the second line of defence's own work in this area.

Data breaches

In 2016 The Information Commissioner's Office had 2,168 data security incidents reported to them, broken down as follows:

Period	Total no.	Public sector	Private sector	Charities/ voluntary	Financial services
Jan - Mar	448	294	106	23	25
Apr - Jun	545	368	114	29	34
Jul - Sep	598	387	136	35	40
Oct - Dec	577	383	124	33	37
Total	**2168**	**1432**	**480**	**120**	**136**

Those incidents recorded as a cyber incident, e.g. exfiltration, key logging software, phishing are as follows:

Period	Total no.	Public sector	Private sector	Charities/ voluntary	Financial services
Jan -	0	0	0	0	0

Mar					
Apr - Jun	47	16	19	9	3
July - Sep	70	15	40	9	6
Oct - Dec	59	16	34	4	5
Total	176	**47**	93	**22**	**14**

In the UK, the most important piece of legislation organisations must worry about is the Data Protection Act and the possibility of fines by the information commissioner (ICO). Below are the seven most significant data breaches to hit the UK, not in all cases because they were particularly large but because of the type of attack or vulnerability involved or the sensitivity of the data compromised.

1. Sports Direct (2017): The retailer failed to tell its entire workforce that they might have had their personal credentials stolen in an internal security breach.

2. Three Mobile (2016): Hackers successfully accessed its customer upgrade database after using an employee login.

3. Sage (2016): There was unauthorised access to the software company's customer information using an internal login.

4. Tesco Bank (2016): Cyber criminals broke into the bank's computer system and stole £2.5 million from the current accounts of 9,000 customers.

5. Kiddicare (2016): A data breach at the online retailer exposed the names, addresses and telephone numbers of some of its customers. It said the data had been taken from a version of its website set up for testing purposes.

6. Talk Talk (2015): The company initially struggled to confirm how many of its four million customers were affected after hackers exploited a reported weakness in the firm's website. Shockingly, the incident was the second (and possibly third) data breach affecting the company in under a year.

7. Morrisons Supermarket (2014): An unusual example of the insider attack, the attacker published details of the firm's entire workforce database online, 100,000 employees in all. An employee was eventually arrested for the incident.

Data breaches go back at least 8+ years. However, the moment date breaches entered consciousness in the UK, related to the Nationwide Building Society (2006) incident involving an unencrypted laptop stolen from a company employee that put at risk the personal data of 11 million savers. The UK's poor disclosure rules made it difficult for outsiders to get information on what had occurred. The Financial Services Authority (FSA) eventually fined Nationwide £980,000, still the largest sum ever imposed for data loss in the UK, seen at the time as a warning shot for other firms that might have similar incidents. Not everyone noticed.

Some of the controls that IT specialists have suggested should be in place and that internal audit should check to ensure they are working effectively include:

- Biometrics, two factor and multi factor authentication enforced for every employee (eg entering password which is for example notified to your phone).
- Access levels are appropriate to the job role.
- Leavers are stripped of their IT access promptly and for those changing job roles access is updated to reflect the change in role promptly.
- Policies and procedures are in place for internal staff and external contractors supported by appropriate, training, audit and enforcement procedures.
- To have and implement a comprehensive data security plan that aligns IT, HR, legal and compliance among other functional areas.
- Staff training – to raise security awareness, evidence of staff training especially in the Financial Services world otherwise the Regulator will take the view that the training hasn’t occurred if it cannot be evidenced.
- Data leaving the organisation is encrypted at external end points.
- Encrypting the data that’s stored in the databases.
- Know where your data is and who has access.
- Making sure only some of the network is accessible through segregated access, masking certain stored information to ensure it’s not viewable in its entirety.
- Get visibility on how many records have been accessed and monitor what and why they have been accessing data.
- Ensure all manipulation of data is logged with logs being regularly audited. Ideally the logs should be automatically monitored by anomaly detection systems for inappropriate usage and unexpected patterns.
- Get exposure to communication streams to ensure you can spot exfiltration (the unauthorised transfer of data from a computer – either manual or carried out by someone with physical access to a computer or automated and carried out through malicious programming over a network).
- Proper detection mechanisms and incident responses processes in place.
- Have an effective cyber security strategy in place.
- Ensuring a data life cycle plan is in place.
- Ensure that the organisation is running fully updated software.
- Performance of regular security audits on website code.
- Running penetration tests on corporate infrastructure.

Perhaps one of the key factors for internal audit and your board and audit committee is to know what data your organisation holds and, based on a risk assessment, know what data it can afford to lose so that time and effort can be focused on preventing high risk data/information losses.

What can internal audit do?

While the board and senior management are primarily responsible for governance, the internal audit function plays a key role in assessing its application in practice. In particular, the internal audit function is well placed to assess whether the organisation’s information technology governance supports the organisation’s strategies and objectives.

Here are ten questions that Global IIA’s (GTAG) 'Assessing Cyber security Risk: Roles of the Three Lines of Defence' says the HIA should consider when evaluating the organisations governance related to cyber security:

1. Are senior management and the board aware of key risks related to cyber security? Do cyber security initiatives receive adequate support and priority?
2. Has management performed a risk assessment to identify assets susceptible to cyber threats or security breaches, and has the potential impact (financial and non-financial) been assessed?
3. Are first and second lines of defence collaborating with their peers in the industry (e.g. conferences, networking forums and webcasts) to keep current with new/emerging risks, common weaknesses and cyber security breaches associated with cyber security?
4. Are cyber security policies and procedures in place, and do employees and contractors receive cyber security awareness training on a periodic basis, and can such training be evidenced?
5. Are IT processes designed and operating to detect cyber threats? Does management have sufficient monitoring controls in place?
6. Are feedback mechanisms operating to give senior management and the board insight into the status of the organisation’s cyber security programmes?
7. Does management have an effective hotline or emergency procedure in place in the event of a cyberattack or threat? Have these been communicated to employees, contractors and service providers?
8. Is the internal audit activity capable of assessing processes and controls to mitigate cyber threats, or does the HIA need to consider additional resources with cyber security expertise?
9. Does the organisation maintain a list of third party service providers that have system access, including those that store data externally (eg IT providers, cloud storage providers, payment processors)? Has an independent cyber security examination engagement been conducted to assess the effectiveness of the service organisations controls as a part of their cyber security risk management programme?
10. Has internal audit adequately identified common cyber threats facing the organisation (e.g. nation states, cybercriminals, hacktivists, networked systems, cloud providers, suppliers, social media systems, malware) and incorporated these into the internal audit risk assessment and planning processes?

It is the HIA’s role to interpret preliminary responses from these initial questions and begin the process of identifying areas under threat based on a disciplined risk based approach.

The authors of IIA Global's CBOK report Navigating Technology’s Top 10 Risks: Internal Audit’s Role recommended seven key questions for internal audit to ask about cyber security preparedness. The questions are:

1. Is the organisation able to monitor suspicious network intrusion?
2. Is the organisation able to identify whether an attack is occurring?
3. Can the organisation isolate the attach and restrict potential damage?
4. Is the organisation able to know whether confidential data is leaving the organisation?
5. If an incident does occur, is a written crisis management plan in place that has been tested and is in line with organisational risk?
6. If an incident does occur, does the organisation have access to forensic skills to assist with the incident?
7. Is the incident team in place and do they know their roles and responsibilities?

Internal audit can also play a key role in coordinating assurance efforts. The IIA’s International Standards state that ‘the chief audit executive (CAE) should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimise duplication of efforts'. Giving priority to the most important information, the internal audit activity should work with relevant data owners, evaluate the provisioning process and determine who has been granted access to the data in context with its important.

The internal audit activity should then work with operational management to identify the systems and technologies that enable access paths to view critical information (e.g. employee data, personally identifiable information, customer credit card numbers, vendor purchase history).

Working with operational management will also help ensure the relevant elements for cyber security vulnerabilities are monitored on an ongoing basis. Internal audit should consider sizing the scope of the cyber security audit based on who has access to critical information and access the technology related to their access path.

The following questions will facilitate the process of identifying critical information:

- What information is deemed critical and why?
- What is the value of the data (to fraudsters, competitors, etc.)?
- Where is the information accessed, processed, and stored
- How is information transmitted?
- What is the extent of rigor followed to grant and revoke access?
- Have access levels been determined by role and what roles have administrative access?
- How is access assigned, approved, monitored and removed?
- How well protected is the information to unauthorised access?
- What type of testing is performed (penetration, access, tracked changes, etc.)?
- How is cybersecurity risk monitored for those who have functional access to critical information?

Where the organisation has performed business impact analysis the HIA can utilise this to determine if the internal audit plan sufficiently covers systems that contain critical information. The HIA can then disclose to the audit committee the areas where assurance may or may not be currently provided and plan to provide coverage.

Furthermore, as laid out in the IIA GTAG, as the third line of defence the internal audit function can be consulted regarding:

- The relationship between cyber security and organisational risk;
- Prioritising response and control activities;
- Auditing for cyber security risk mitigation across all relevant facets of the organisation;
- Assurance in remediation activities;
- Raising risk awareness and coordinating with cyber security risk management, particularly in organisations lacking mature first and second lines of defence functions;
- Validating that cyber security provisions are included in the organisations’ business resilience plans and disaster recovery testing efforts.

Finally, internal audit can play a key role in anticipating future risks in relation to cyber security through the creation and maintenance of risk “watch lists”, ensuring that certain risks – often sector -specific – are recognised and that the organisation is ready to respond.

Further reading

The Security Intelligence Center, Next Steps: Beyond Response to Anticipation

The Internal Audit Foundation and Crowe Horwath

Cyber risk
Institute of Risk Management

Preparing for the General Data Protection Regulation (GDPR) – 12 steps to take now
Information Commissioner's Office