RISK IN FOCUS 2021

Practical guidance on cybersecurity and data security

Focus on the human factor and good practices from your peers

ECIIA

EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING

DIIR

Deutsches Institut für Interne Revision e.V.

Risk in Focus 2021 has been published by a consortium of institutes of internal auditors that includes the Chartered Institute of Internal Auditors (UK & Ireland), Deutsche Institut für Interne Revision (Germany), IIA Belgium, IIA Nederland, IIA Luxembourg, IIA Austria, Instituto de Auditores Internos de España, IIA Sweden, Institut Français De L'audit Et Du Contrôle Interne (IFACI) and the Italian Association of Internal Auditors.

Contents

Introduction

This practical guidance is part of the Risk in Focus 2021 publication. It aims to provide a concise overview of key publications and existing tools developed by the 10 European institutes of internal auditors in Austria, Belgium, France, Germany, Italy, Luxembourg, the Netherlands, Spain, Sweden, the UK & Ireland and publications from IIA Global.

This guidance is developed to help internal auditors address some of the key risks identified in Risk in Focus 2021, with the aim of contributing to the reduction of their impacts on businesses and stakeholders. **Where the Risk in Focus report itself addresses the 'WHAT-could be important to audit', this guidance helps you address the 'HOW-to audit' this topic.**

For the 2021 edition, practical guidance will be available on the following three chosen topics from the report:

- Cybersecurity and data security
- Macroeconomic and geopolitical uncertainty
- Climate change and environmental sustainability

These topics have been selected due to their current and foreseen importance for most organisations and take into consideration the needs of Chief Audit Executives to strengthen or expand their knowledge and experience in auditing these three fast-developing risks.

Please keep in mind that we intentionally chose to dive into some specific components of these three risks. Whilst we have endeavored to explore what we think are the key focus areas of these risks, a thorough understanding of their application may require additional research on your part, but we aim to provide a selection of what would benefit the most to the profession in the current context.

All practical guidance is designed to firstly, help practitioners learn from experienced professionals (experts, operational teams or internal audit), and, secondly, offer practitioners useful reflections that we believe are of particular interest when auditing these topics and their associated risk management processes.[1]

Why should cybersecurity and data security risk be on your radar?

Cybersecurity and data security has been one of the top three priority risks identified in Risk in Focus over the past five editions. It is documented as the number one priority risk for 2021, and this trend is expected to continue for the next three years. As a result, a number of resources have been produced within the IIA network to support practitioners navigating this risk.

1. If you wish to know more on existing materials (non-exhaustive list available in appendix on pg.12) or support solutions developed by the contributing IIA affiliates, please contact your national institute or IIA Global.

The human factor in cybersecurity

An innovative way to tackle the risk and harness some opportunities (by Guy-Philippe Goldstein - researcher and lecturer at the Economic Warfare School of Paris, Advisor to PwC France).

Why should internal auditors look at the human factor?

Firstly, we must take into consideration that a majority of cyber-incidents may be human-enabled, and security breaches are mainly the result of human error. Thus, looking at the human component of the risk seems to be a pertinent approach for an organisation to resist most of the critical cyber threats and to develop its cyber-management culture. Secondly, the intangible and complex nature of the human factor requires the expertise and competences of an internal auditor to look at it. Indubitably, many other factors remain key to ensure proper controls and risk management protocols are in place, but the value here for internal audit is to analyse, measure and understand the soft component impacting the robustness of the cyber-management system.

Cybersecurity may appear as a very technical field, however, cyberspace can itself be construed as a man-made domain, composed of three pillars: hardware, software and "brainware". The human user manipulates data that is then reintegrated into cyberspace. Hackers have quickly seized this source of vulnerability: they have developed a whole field of expertise to target brainware, called social engineering.

The human user is also all the more important since cyber-conflicts are a range of activities called "critical infrastructure" – i.e. the private or public social organisations dedicated to run critical activities and composed of tangible and intangible assets. Among these intangible assets, protocols, culture or personality traits of the users are key elements to the decision system structure of the "critical infrastructure".

In that context, the importance of the human factor in cybersecurity must be examined from different angles.

The employee

At an individual level, the behavior of employees may constitute an important pathway for cybersecurity risks. Indeed, almost 90%[2] of all cyber-incidents may be human-enabled[3] - with human error accounting for 52% of the root cause of security breaches[4] including in industrial cybersecurity, as shown in recent surveys.[5] These errors are due to different types of mistakes, including: clicking on an infected attachment or unsafe URL; use of default usernames; easy-to-guess passwords; lost laptops or mobile devices; disclosure of confidential information via email error; system misconfiguration or poor patch management.

One reason for these mistakes is the smart exploitation of human weaknesses by cyber criminals. For example, during times of social upheavals or management crises, stress, confusion, and/or tiredness can constitute moments for exploitable weaknesses. We have seen a surge of such attacks during the coronavirus pandemic, for example an increase in phishing scams, from fake mask producers (PPE) to fake public authorities proposing economic aid.[6]

2. Almost 90% of Cyber Attacks are Caused by Human Error or Behavior | Chief Executive
3. IBM Security Services 2014 Cyber Security Intelligence Index
4. Surveys: Employees at fault in majority of breaches | CSO
5. Man-made disaster: half of cybersecurity incidents in industrial networks happen due to employee errors | Kaspersky
6. Hackers Exploit Coronavirus Pandemic in Latest Event-Based Email Attacks | Vade Secure

Another important reason that explains the importance of human errors is simply in circumventing established routine protocols. For example, in the UK a national survey has shown that 61% of respondents would frequently fail to delete confidential documents or would accidentally forward documents to individuals who had not been authorised to access them.[7] More recent surveys have shown an increase in the proportion of human errors causing cyber-breaches. In 2019 alone, that figure hit 90%.[8] Other surveys reveal that between 44%[9] and 66% of employees may be breaking established rules through harmless activities such as watching mainstream video services. Of that, around 20 to 25% of employees are said to have engaged in downloading pirated material onto work devices, visiting adult sites, or bypassing security measures to access blacklisted content. These do not constitute malicious activities per se, but breaches of established and routine protocols. Accordingly, and even in high security environments such as military activities, recent expert testimonies have highlighted that up to 90% of cyberattacks could be defeated by implementing "cyber hygiene" against such breaches of protocols.[10]

The culture of an organisation

The collective picture that emerges echoes what Chief Information Security Officers such as Jo De Vliegher from Norsk Hydro ASA said: the bulk of cybersecurity efforts reside in "maintaining the house in order".[11] However, the human user is also deeply influenced by the management and culture of the organisation they are part of.

Indeed, the human factor is also at play in different hierarchical ranks, as well as across departments. When US retail company Target was hit by a cyber-attack in December 2013, the slow response by the top executive committee became one of the main factors in the success of the operations by cyber criminals. Consequently, both the then CTO and the CEO were fired.[12] This new understanding that top non-IT executive managers and board members are held accountable for their actions (or lack thereof) regarding an entity's cybersecurity management is also reflected in the firing of US-based Imperva CEO in 2020.[13] A similar situation was noted in 2019, when the CEO and two directors of the publicly listed property valuation company Landmark White resigned as a result of a cybersecurity incident.[14] When US financial data company Equifax was breached in 2017, the ethically questionable decision to wait a long period of time before alerting customers, as well as the potential illegal lapses by some executives, may have contributed to the loss of trust and the severe valuation shock that the company endured.[15] The human factor consists here of negligence at the top executive level. It can be expressed simply by a lack of management's willingness to prepare for the worst: for example, in France, a survey found that 80% of companies haven't developed a cybersecurity incident response plan.[16] Corporate boards also have their role to play in overseeing executive committees' cybersecurity policies, or lack thereof.

The security culture must also be realistic. If security protocols are too complex, then in times of crisis they won't be used because the focus of management and staff will be on the immediate business requirements rather than the longer term risks associated with a security breach.[17]

However, the cybersecurity culture in an organisation may also have key detrimental impacts on the cyber-risks posed by its employees. The human risk factor may be amplified by very ambitious workloads[18], or aggressive/punitive management style, increasing the stress and leading to circumventing of critical security information. A punishing-type management may decrease productivity, increase anxiety levels, and in the long-term, decrease cybersecurity resilience.[19] On the contrary,

7. New report shows the staggering scale of breaches due to human error | Information Age
8. 90% of UK Data Breaches Due to Human Error in 2019 | Infosecurity Magazine
9. The human factor in IT security | Kaspersky
10. Fiscal Year 2019 Review and Assessment of DOD Budget for Cyber Operations and U.S. Cyber Command: Hearing Before House Armed Services Comm., Emerging Threats and Capabilities Subcommittee, 115th Cong. (Apr. 11, 2018) (statement of Kenneth P. Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security and Principal Cyber Advisor)
11. See good practices section on pg.10
12. Target CEO Fired - Can You Be Fired If Your Company Is Hacked? | Forbes
13. Imperva Taps Infor COO Pam Murphy As New CEO After Data Breach | CRN
14. Landmark White data disaster claims CEO scalp | Financial Review
15. FBI Looking Into Equifax Data Breach | The Wall Street Journal
16. 80% des entreprises françaises n'ont pas de plan de réponse aux incidents de cybersécurité | Informatique News
17. Human factors in cyber-security: nine facets of insider threat | I-CIO.com
18. Human factors in cyber-security: nine facets of insider threat | I-CIO.com
19. 4 in 10 organizations punish staff for cybersecurity errors | Help Net Security

examples of security environments developing non-punitive, empathetic cultures, such as the "Just culture" pioneered in airline security by the Nordic chapter of the International Civil Aviation Organization, which has been expanded to the whole of the European Union since 2015, does show the priority in documenting detailed information before and after an incident, over punishing employees.[20]

Towards cyber-management – and its auditing

The elements explained above do point to the fundamental importance of the human factor in cyber-risks, both at the individual and the organisational level. However, the fact that existing information security plans do not account sufficiently for human factors in risk management or auditing[21] demonstrate existing gaps in cyber-risk management. In particular, the importance of respect for transverse procedural and cultural principles, what may be termed as "cyber-management", applicable to the whole of the organisation, do point to an important role for internal auditors and internal controllers. By evaluating or questioning errors in the application of procedures or reviewing the development of certain cybersecurity cultural elements that mitigate the human error, internal auditors can contribute to the reduction of cyber-risks.

On **cyber hygiene** for human errors, internal auditors can provide assurance on good cybersecurity culture by auditing, at the very minimum, the following two essential elements:

- The design and implementation of policies for proper access, use and storage of software and data, including messages and key documents. The auditor should also assess how the communication, sensitisation and explanation of the protocols is shared with the staff.

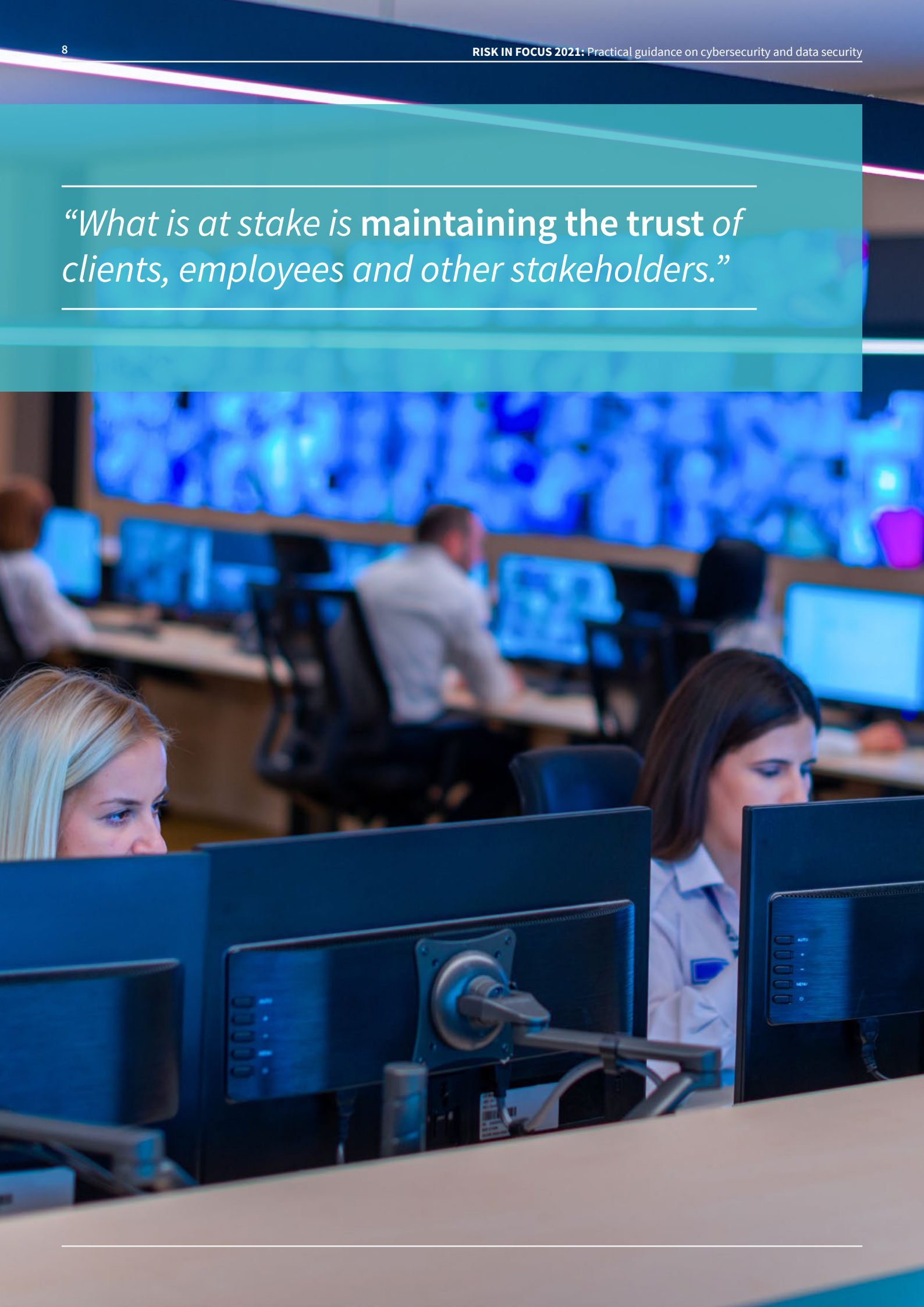
- The adherence of key employees with such protocols, including by auditing non-announced tests such as phishing campaigns. Based on the results of the tests, the auditor should assess the appropriateness of the remediation actions put in place.

With regards to the **security culture** and its realistic implementation, auditors should verify that there is a joint process so that any new cybersecurity measures are evaluated both in regard to the risk reduction effect and the usability for end users. This change in management culture has a major impact on cybersecurity. Thus, the auditor should remain vigilant to any significant change in management (including in mature organisations), and recommend unrehearsed cybersecurity tests or drills that should include members of the executive committee and be set up regularly.

Finally, in terms of top management and board members' involvement in cyber-risk management and cyberculture, internal auditors should verify that cyber-risks are properly identified in the corporate risk mapping, including the operational and ultimately financial consequences, and impacts on corporate value if such risks were to occur.[22]

20. Just culture can improve safety | Airlines
21. Calvin Nobles, "Botching Human Factors in Cybersecurity in Business Organizations", HOLISTICA Vol 9, Issue 3, 2018, pp. 71-88
22. See for example "Cyber-risques: Enjeux, appoches et gouvernance », IFACI, 2018, p.13

"What is at stake is **maintaining the trust** *of clients, employees and other stakeholders."*



Crisis is coming. Prepare for the worst

Lessons learned from a case study

Norsk Hydro ASA (the world's premier aluminum company) suffered a major ransomware attack in March 2019. The potential risk at the time of the alert was that the breach would affect all Norsk Hydro's employees across 40 countries (approximatively 35,000 people), resulting in missing employee records in thousands of servers and computers. The potential financial impact was estimated to approach $71 million.

This case is a paradigm shift in the cyber community. By handling this cyber-incident with transparency, the company has gained accolades from cyber experts.[23] It constitutes a set of best practices, tested "under fire", benefiting the protection of the company's most important asset, its stakeholders' trust.

Set up a disciplined crisis-management structure

Critical to this structure is the dedication of each member to one crisis-related task, and one task only. Consequently, the structure was defined into three groups of people:

1. A team that would focus only on "what happened in the past" – e.g. forensics, postmortem analyses.

2. A team that would focus on "the situation now", e.g. all the elements of current remediation during the crisis.

3. A team that would focus on the future organisation: the roadmap to progressively rebuild the IT department. This requires more of a gradual effort, starting with the creation of a new small domain totally void of the hackers' threat; then expanding to basic or critical services; and finally opening up to more support and administrative functions.

This crisis management should also include a war-room where both internal and external stakeholders (e.g. peer companies, experts or journalists) could exchange information. On this aspect, internal audit could assess the set-up of the war-rooms and the access restriction criteria for external stakeholders.

Communicate and share in a manner that is transparent, frequent, and tailored to different stakeholders

What is at stake is maintaining the trust of clients, employees and other stakeholders. With that goal in mind, Norsk Hydro was conscious that communication should be transparent, quick, and well organised – three characteristics that, combined, would also avoid various employees telling the media potentially conflicting stories. During the crisis, Norsk Hydro immediately setup a dedicated webpage as well as an overnight web-conference for both industrial clients and the general public (including investors and consumers). In the weeks that followed, a YouTube channel was created for Norsk Hydro's employees, so that collaborators could speak up and talk freely about their experience during the very height of the crisis. For financial stakeholders, an evaluation of the economic cost of the cyber-attack to the company was communicated after just six weeks. Through the crisis, other key partners or relevant peer companies would be invited to share thoughts, concerns and best practice. Even though initial reactions from external stakeholders may be of genuine concern and empathy for the breach – the sentiment could very well turn into loss of confidence as stakeholders grow more concerned about the impacts that the breach could have on them.

Actively prepare for when the defence fails

Norsk Hydro was confronted with a team of hackers who were likely to have planned their

23. Calvin Nobles, "Botching Human Factors in Cybersecurity in Business Organizations", HOLISTICA Vol 9, Issue 3, 2018, pp. 71-88

attack. This constitutes quite an investment and shows dedication. The lesson should be drawn for any company that constitutes a strategic interest for national security or is deemed as vital for national economic performance. It should also be made available for the smaller suppliers and partners of such companies, as they could become a pathway to the attack either via shared network infections or business interruptions. In that context, it is critical to invest in backups – either cold servers that can be put back online, or offline copies of critical information. For that same reason, Norsk Hydro could easily disregard the ransom demand, as well as quickly achieve a sense of confidence through their roadmap to business and IT recovery. It must also be stressed that these efforts do not necessarily require advanced technologies but rather a certain sense of organisational and individual discipline in order to frequently back-up data and conduct patch management. The organisation should regularly be tested from top to bottom to ensure that they are crisis-prepared should their defences fail, for example by utilising crisis scenario planning and testing ensuring that the scenario tests are relevant to the organisation and topical.

Good practices from your peers on penetration testing preparation

By consulting a few Chief Audit Executives from the private and public sectors, we identified the need for stronger, more frequent penetration testing. This appears to continue to be a priority for organisations. In fact, as previously mentioned, the human factor often offers an opportunity for malicious users to strike (personal gain, personal revenge against the organisation). If cyber hygiene and staff awareness is key, penetration testing remains a crucial mitigation measure for all organisations, regardless of their size, to stress the system in place. By preparing the processes and the individuals, the organisation accepts the potentiality of the risk but also actively works on the reduction of its impact and criticality and reinforces its resilience to the unprecedent scenarios.

Involvement of business managers in the penetration testing exercise is one of the most improved best practices. In a major French company with multiple European subsidiaries doing cash-pooling across entities, the results were shared and discussed with senior managers from the finance department. This helped to better understand the operational impacts from the exploitation of the identified vulnerabilities; better assess the business and financial implications; provide more support for such efforts; and better design mitigation and remediation solutions.

Similarly, a penetration testing exercise with a large global industrial company was developed by directly **asking the executive committee what the worst-case business scenarios could be.** The penetration tests did actually demonstrate the possibility for such worst-case scenarios to happen. Having developed these worst-case scenarios, members of the executive committee had not only a better sense of what was financially at risk, but also a greater understanding of what they needed to be prepared for.

The involvement of the whole of the IT department, in particular DevOps, is also required. In a large European media conglomerate, **penetration testing exercise helped confront a tolerant "start-up culture"** in digital development that did not emphasise enough security in its design. Faced with the exposed potential for vulnerabilities leading to business difficulties, the digital organisation created a dedicated position to overview and to help foster cybersecurity by design in all application development.

Employees and collaborators also need to be "stress-tested". When organised by CISOs, frequent phishing campaigns – mass mailing including messages with links that employees should not click on, but may nonetheless – can help to accelerate both an awareness of cybersecurity and application at the individual level of the routine actions to "maintain the house in order" as mentioned above. For example, in a European media conglomerate, such measures have helped to reduce the number of employees that were clicking on dangerous items from about 20% of the population to 5%.

To achieve the full "educational" effects and yield a sustainable change in individual behavior, it is important that individual learnings from actions can be offered to users. It is also required that some of the attack scenarios are validated by members of the executive committee to avoid unexpected disruption.

In this context, internal auditors should verify the following aspect of penetration testing frameworks:

- Promptness of testing, by evaluating if the tests are developed and implemented both for existing digital assets and new applications under development.
- Pertinence of the business scenarios, by verifying that all relevant contributors (from operational and support functions) are involved in the preparation process (joint team).
- Regularity of training programmes, by controlling that programmes such as phishing campaigns are set up, implemented with the right frequency and supported by a robust training assistance programmes for "failing" employees (as a mitigation measure).

Call to action

If you needed to be convinced of the importance of the human factor for organisations to manage cyber and data security risks effectively, we believe you should now be on board!

By collecting contributions from your peers, we realised how important is the need for internal auditors to better address this specific challenge. We were also alerted to the necessity for greater expertise and to reinforce the implication of the third line in dealing with this strategic and critical risk for all organisations.

If you wish to contribute to further work on this issue, please contact your local IIA institute.

Appendix

Other points of interest from existing sources of information

In this appendix, we present some relevant extracts from a selection of IIA publications (from IIA Global and contributing European institutes), focusing on some specific aspects of internal audit activity. We wish to provide internal audit teams with key points of interest which they should consider when providing assurance on cybersecurity and data security risks.

Defining the right audit coverage

From Auditing Cybersecurity within Insurance Firms – ECIIA (2019)

Culture:

- Cybercompetence
- Awareness programme
- Collaboration between internal and external stakeholders

Strategy:

Internal audit assurance work needs to focus on understanding the basis for an information security strategy of which cybersecurity is part, and its alignment to the business and IT strategy and how the strategy is further cascaded to the cybersecurity programme.

Governance:

- Definition and resourcing of the governance model
- Risk management
- Policies and standards

Ongoing risk management:

- Network architecture and controls
- Extended IT estate management
- Identity management and access control
- Data security
- Patch management
- Vulnerability management
- Malware protection
- Cyber threat intelligence
- Security over software development life cycle
- Security Operations Centre and event monitoring
- Incident management and response
- Resilience and recovery

About this publication: This position paper aims to set out the view from the ECIIA Insurance Committee with regards to the internal audit of cybersecurity. It provides an interesting view on how internal audit plays a vital role in the provision of assurance regarding the efficiency and effectiveness of the key cybersecurity processes and controls in insurance and reinsurance undertakings. Various lessons can be learned from a highly regulated sector such as insurance and can be easily extended to other sectors.

Looking at the Governance - 10 questions internal audit should consider

From GTAG (Global Technology Audit Guide) Assessing Cyber security Risk: Roles of the Three Lines of Defense - IIA Global (2016)

1. Are senior management and the board aware of key risks related to cybersecurity? Do cybersecurity 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 the first and second lines collaborating with their peers in the industry (e.g. conferences, networking forums and webcasts) to keep current with new/emerging risks, common weaknesses and cybersecurity breaches?
4. Are cybersecurity policies and procedures in place, do employees and contractors receive cybersecurity awareness training on a regular 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 cybersecurity programs?
7. Does management have an effective hotline or emergency procedure in place in the event of a cyber-attack 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 CAE 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 (e.g. IT providers, cloud storage providers, payment processors)? Has an independent cybersecurity examination engagement been conducted to assess the effectiveness of the service organisations controls as a part of their cybersecurity risk management program?
10. Has internal audit adequately identified common cyber threats facing the organisation (e.g. nation states, cyber criminals, hacktivists, networked systems, cloud providers, suppliers, social media systems, malware) and incorporated these into the internal audit risk assessment and planning processes?

About this publication: This guidance discusses the internal audit function's role in cybersecurity; explores emerging risks and common threats faced by all lines within the organisation; and presents a straightforward approach to assessing cybersecurity risks and controls.

Diving into the cybersecurity framework - basic questions internal audit can ask (based on the NIST Cybersecurity Framework)

From Cyber-Risk, Chartered IIA UK and Ireland (2019)

Identify

- Does the organisation know where its most precious information and data is and why it is important?
- Do employees know what is expected of them in terms of keeping data and information secure?
- Does the organisation have clear policies and procedures relating to cybersecurity?
- Are policies and procedures also communicated to and applied by the external partners the organisation depends upon?
- Is there clarity upon the ownership of the risks and controls?

Protect

- Where are the data and information kept? How is access controlled? And who actually has access to the data and information?
- Have risks associated with loss and theft be identified and assessed?
- Does risk mitigation maintain risks within agreed tolerance levels?
- Are third parties verified/checked prior to being given access to sensitive areas?
- Have outsourcing and supply chain risks associated with data been properly identified and evaluated?
- Do employees receive guidance, training and specific instructions?

Detect

- Do managers monitor, test and report upon risk mitigation?
- Are incidents and their impact reported to senior managers and the board?

Respond

- Do incidents, internal and external, prompt reassessment of risks?
- What would happen in the event of security breach – is there a response plan?
- Have these procedures been fully applied when needed with lessons learnt and corrective action?

Recover

- Is an IT disaster recovery plan put in place?
- Does the IT (DR) plan include key elements such as RTO (Recovery Time Objective), RPO (Recover Point Objective), key IT systems universe, detailed recovery procedures, etc.?
- How often is the IT DR plan being updated?
- Does the organisation have a Business Continuity Plan (BCP) plan?

About this publication: This document provides a quick overview on the cyber-risks (nature, impact, importance for the organisations, etc.) and aims to share some good practices collected amongst the network and recognised stakeholders. The NIST Cybersecurity Framework is an international standard broadly used as a reference for cybersecurity management.

Keeping the third party under the radar – 14 points to look out for during the cybersecurity audit of a third party

From: Data security in third party agreements; Chartered IIA UK and Ireland (2019)

1. Clear responsibility for data security at all levels of management in the organisation and in the third party. This might include designation of data guardians or champions.
2. A culture of security and control that involves training at induction and ongoing education in the organisation and the third party.
3. Residual risk levels on all aspects of data security. If residual risk levels are not set and compared to tolerance levels, and the organisations risk appetite there is scope for improvement.
4. Near misses and incidents are thoroughly investigated according to set procedures - the details of which are fed into the risk assessment process leading to improvement actions.
5. Where incidents have been identified, they are documented, reported and action taken as appropriate in line with GDPR requirements.
6. Specific monitoring and controls around the copying of data on removable media. In highly critical areas this may need to be prevented e.g. USB portal locked out of use thereby disabling downloading onto laptops and other devices.
7. Some or all data may need to be encrypted before any movement is allowed. Where this is electronical it should be by trusted secure networks.
8. The utilisation of secure couriers and appropriate tamper proof packaging in the transport of bulk data stored on removable media.
9. A formal detailed disaster recovery plan with acceptable restoration of service times and testing.
10. Continuous monitoring of data movement and activity. It is important that prompt action is taken to remove access privileges when people leave the organisation.
11. Evidence of vetting of personnel involved in data handling.
12. There are procedures and working instructions in place for the disposal or transfer of hardware and/or software to a different environment.
13. The level of insurance required is periodically reviewed along with the adequacy of liability triggers and liability caps.
14. Confirm that where personal data from the EU as a Privacy Shield certified entity has agreements that comply with the Privacy Shields onward transfer requirements.

About this publication: This guide aims to help practitioners look at data security in an organisation. It helps identify third parties accessing the data, and it also covers what managers and internal auditors can do to reduce the impact of risks in this area (for Chartered IIA UK and Ireland members only). If you wish to access the full document, please refer to your national institute.

Other IIA publications on cyber and data security risks

Guide des risques cyber 2.0
– IIA France (2019)

GTAG Auditing insider threat programs
– IIA Global (2018)

GTAG Auditing IT governance
– IIA Global (2017)

Ciberseguridad – una guia de supervision
– IIA Spain (2016)

Über das DIIR – Deutsches Institut für Interne Revision e.V.

Das DIIR – Deutsches Institut für Interne Revision e.V. wurde 1958 als gemeinnützige Organisation mit Sitz in Frankfurt am Main gegründet. Hauptanliegen ist der ständige nationale und internationale Erfahrungsaustausch und die Weiterentwicklung in allen Bereichen der Internen Revision. Heute zählt das Institut 3.000 Firmen und Einzelmitglieder aus allen Sektoren der Wirtschaft und aus der Verwaltung. Das DIIR unterstützt die in der Internen Revision tätigen Fach- bzw. Führungskräfte u. a. mit der Bereitstellung von Fachinformationen und durch um fassende Aus- und Weiterbildungsangebote. Weitere Ziele und Aufgaben sind die wissenschaftliche Forschung sowie die Weiterentwicklung von Grundsätzen und Methoden der Internen Revision.

DIIR - Deutsches Institut für Interne Revision e.V.
Theodor-Heuss-Allee 108
60486 Frankfurt am Main

email **info@diir.de**
www.diir.de

DIIR Deutsches Institut für Interne Revision e.V.