ACCOUNTANCY EUROPE.

SME RISK MANAGEMENT
CYBER RISKS & RESILIENCE CHECKLIST

FACTSHEET **NOVEMBER 2022**

HIGHLIGHTS

Cyber incidents can have a significant impact on an SME's ability to do business and cause major financial loss. It is crucial that SMEs identify and mitigate those risks in a context where our economies are increasingly digitalised.

SMEs' accountants are their trusted advisors and can play a key role in mitigating SMEs' cyber risk. This paper – the latest in Accountancy Europe's 'SME risk management series' – provides a checklist for accountants to improve SMEs' cyber resilience. Accounting practices themselves can also use this tool to assess their own cyber resilience.

INTRODUCTION

Small and medium-sized enterprises (SMEs) face new risks that can significantly impact their business. These risks stem from global megatrends such as the climate crisis, digitalisation, global economic integration of COVID-19.

Accountancy Europe has launched a series on SMEs' risk management to inform SMEs and their accountants: sustainability (July 2020), SME sustainability checklist (2021), intellectual property (2022) and insolvency (2021).

This sixth paper focuses on cyber risks. It will explain why and how SMEs should consider and mitigate cyber risks and how the SME's accountant can best support them. The paper includes a checklist the accountant can use to help build their SME clients' cyber risk resilience.

The checklist can serve as a basis for a discussion or initial assessment of the client's cyber resilience. It can also support building cyber resilience and cyber risk awareness in the accounting practice itself. Accountants do not need to address each item on the checklist themselves, but they should be able to recognise when to refer their clients to relevant technical expertise.

WHICH CYBER RISKS ARE SMES FACING?

The World Economic Forum's (WEF) 2021 Global Risks Report identifies cybersecurity failure as the fourth highest clear and present risk with potential to cause a critical threat to the world. This places it just below other critical risks, such as climate disasters or infectious diseases.

Cyber risks emerge from increasingly digital economies and business models, for example, in business processes, payments, client and contact lists, or product and service designs. SMEs can benefit from improved efficiency, innovation, productivity and management that technology provides. But they also need to be aware of the risks that can come with these opportunities and mitigate them to fully tap into digital technology's potential.

Cyber threats are among the main risks linked to digitalisation. These could be categorised roughly into human mistakes and cyber attacks:

- Human mistakes result from unintentional errors by employees, managers or business partners with access to the business' digitalised workflows or databases. Examples include unwittingly publishing client lists or other sensitive data, forgetting passwords, deleting digital content or breaching legislation such as the EU's General Data Protection Regulation (GDPR)
- Cyber attacks consist of malignant parties – which can either be external, business partners, or the SME's own staff – intentionally damaging, destroying, spying on, sharing, publishing or otherwise misusing the company's digitalised content and processes (see below for specific examples).

An effective cyber risk mitigation strategy would address both these dimensions as they are inter-connected. Human mistakes can expose the business to cyber attacks, whilst cyber attacks create an opportune ground for human mistakes.

CYBER ATTACKS EXAMPLES

According to a 2021 EU Agency for Cybersecurity (ENISA) report, the most common cyber incidents faced by European SMEs were:

- 41% phishing
- 40% web-based attacks
- 39% general malware
- 19% malicious insider
- 12% denial of service
- 11% social engineering
- 7% compromised/stolen device

Pandemic's multiplier effect

Cyber risks are further exacerbated by recent trends – generated by the COVID-19 pandemic – pushing businesses to work more remotely and online. For example, the pandemic saw a 667% increase in the amount of phishing e-mails.

HOW CAN CYBER RISKS AFFECT SMES?

SMEs are an increasingly favoured target by cyber attackers. They are three times more likely to be targeted by cyber criminals than large businesses.
Examples of the cyber incident negative consequences on SMEs include the following:

- financial loss: cyber incidents often result in a substantial financial loss arising from:
  - theft of company information, financial information, e.g. bank details or payment card details, or money
  - trade disruption, e.g. inability to carry out transactions online, major disruption of production or other key IT-driven processes
  - repair costs for affected systems, networks and devices
- business loss: trust is an essential element of business relations. Cyber attacks can damage the SMEs' reputation and erode customers' and business partners' trust. This, in turn, can lead to losing customers, business partners and sales.
- legal consequences: data protection and privacy laws require businesses to manage the security of all personal data that they hold – whether on staff, customers or business partners. If this data is accidentally or deliberately compromised, and the SME has failed to deploy appropriate security measures, it may face fines and regulatory sanctions.

WHAT ARE THE MAIN OBSTACLES TO SMES' CYBER RESILIENCE?

Reinforcing cyber resilience is crucial for an SME to mitigate the cyber incidents risks and negative impacts outlined above. There are some obstacles that can hamper efforts in this area, as highlighted by ENISA.

LACK OF AWARENESS

A lack of awareness and management commitment are the most fundamental obstacles to mitigating cyber risks. In practice, this means allocating budget, resources and effective cybersecurity processes implementation.

Many SME owners are busy with the day-to-day running of their business and might not realise the scale of the risk that cyber security-related mistakes and attacks can pose for their business. Therefore, they may not prioritise taking pre-emptive measures to protect their business and only discovering the costs after a cyber risk has materialised.

Low cyber risk awareness among staff is also a problem. Each person in an SME with access to its information technology systems can unwittingly cause a cyber incident. Therefore, it is vital for all staff to be alert to potential cybersecurity issues.

WEAK PROTECTIONS FOR CRITICAL AND SENSITIVE INFORMATION

SMEs handle a variety of information such as personnel records, customer information, production and procurement details, financial data, policies, procedure etc. They are all essential to the company. Laws, regulations or agreements may also require the SME to protect them.

Absence of a specific backup up policy, up-to-date anti-malware solutions for all device types, or using obsolete or unpatched software could seriously jeopardise the company's critical and sensitive information. This would make the SME an easy target for the types of cyberattacks outlined above.
Insufficient budget

Cybersecurity efforts entail significant investments, including awareness training, cybersecurity controls implementation, engaging with external experts, and specialised education for staff members. Many SMEs view cybersecurity as a cost rather than an essential investment in their business. SMEs should, therefore, better understand the risks cybersecurity issues pose to their business and allocate appropriate budgets to invest in the required controls to protect their business' critical areas.

LACK OF EXPERTISE AND PERSONNEL

Managing cyber security within an SME is a big challenge. Cybersecurity is a topic requiring specialised knowledge. However, it is common within an SME that individuals multitask and may have multiple roles assigned to them. As a result, an employee within an SME may be responsible for cybersecurity and other internal processes.

Many cybersecurity solutions require specialised IT knowledge to implement and manage them properly. It is essential to recognise potential limitations of an employee responsible for cyber security and, for example, when additional expertise may temporarily be needed.

As an SME's business grows and changes, the technology they employ will change too. This means the cyber threat landscape will evolve. Therefore, SMEs will need to ensure that their efforts to manage cybersecurity are continuous and consistent. If the company does not directly employ a person with specialised information and computer technology (ICT) knowledge (which is typical for non-technical SMEs), there is a need to invest in external expert assistance.

LACK OF SUITABLE GUIDELINES

The availability and suitability of guidelines in the form of standards, whitepapers or similar is another major challenge. Such documents already exist, but ENISA argues that most of them either provide too generic information or are too complex for SMEs and would require them to seek specific IT expertise. Moreover, many SMEs are simply unaware of the existence of such guidelines, do not know which would best work for their business or do not even know where to begin.

WHY IS THE ACCOUNTANT WELL-PLACED TO HELP?

Professional accountants are well-placed to help SMEs overcome some of the obstacles outlined in the previous section. Most accountants are not IT experts. However, they are in a unique position to help building SMEs' cyber resilience because:

- they are SMEs' trusted advisors
- most SMEs in Europe already rely on accountants for services such as business planning, financial and cashflow management, tax and compliance, bookkeeping and financial advice. This means that they often have a detailed knowledge of their clients' IT systems, especially in respect of their financial systems
- SME owners meet with their accountants regularly, and they may be the first point of contact for SMEs
- SMEs rely on accountants to advise and challenge assumptions about running their business

Any individual accountant or accountancy firm may have hundreds of SME clients. They have thus gathered extensive experience in what works for businesses. Accountants thus understand the underlying fundamentals of the businesses they serve.

Specifically, on cyber security, accountants can help:

- raise awareness – among SME management and staff – about the need to mitigate cyber risks
- advise on which business operations or practices most likely raise cyber risks
- identify which parts of the business are 'most pertinent' for day-to-day operations and thus need particular attention and maximum protection. For example, bookkeeping systems should be backed up to ensure relatively minimal disruption, IT-driven production stoppage could have far more serious consequences for the SME and should be protected accordingly
- budget and plan the SME's cyber resilience investments, advising on the most critical measures to be taken and tailored for the specific business' features
- identify when and where specialist IT expertise will be required for introducing specific cyber resilience steps, and putting the SME in touch with relevant experts in the accountant's network
- inform the SME about relevant legislation, such as the GDPR, and support with compliance steps
- provide independent assurance on the SME's cyber resilience systems, as long as it is a different person and firm from the one that advised the SME for setting them up
- advise about developing contingency plans in the case of a cyber attack

The next section proposes a simple checklist for the accountant to support their work in building cyber risk resilience among SME clients.

CHECKLIST FOR ACCOUNTANTS

It is expensive for an SME to hire in-house IT expertise or refer to specialist IT experts. However, there are some basic steps that any SME can take to help build their cyber risk resilience

The SME's accountant can use this checklist to identify the SME's current 'standing' on cyber risks and help initiate action where necessary. The accountant should also be able to assess and advise when specialist IT expertise would be required.

LEARNING BY DOING

Not all accounting practices across Europe are on the same level when it comes to cyber skills, cyber risk awareness and related service provision. Any practice or practitioner interested in providing cyber resilience services to SME clients should start with their own practice. They should conduct a self-assessment of their practice – for example, using the below checklist as a support – and gradually build up their own cyber resilience.

This will help ensure the practice and its data are protected against cyber risks. Moreover, it will help build up cyber resilience experience and expertise, and develop a network of cyber experts that the accountant can eventually refer their clients.

STEP 1 – THE NETWORK

Accountants should start by building an ICT experts network they can rely on for additional insights and refer their SME clients to when needed.

The accountant can make the SME aware of cyber risks, convince them to take action and advise on some simple initial steps. However, most accountants would lack the ICT expertise to introduce more sophisticated solutions if these are needed. Accountants are also bound by professional requirements to ensure they do not take on work if they lack the necessary skills.

STEP 2 – THE ASSESSMENT GRID

This grid is based on a simple tool developed by SMESEC, aimed specifically at SMEs with limited resources, background and expertise in cyber security. Completing the grid and taking the initial steps for improvement should be easy and cost-effective for many SMEs. The accountant should use it as a basis for their conversation with SME clients on their cyber risk resilience.

The checklist can also be used to help build cyber resilience and awareness in the accounting practice itself. The accountant does not have to be able to directly address each of the checklist items but should be able to recognise when to refer their clients to relevant technical expertise.

	RISK TYPE	YES	NO	DO NOT KNOW
AWARENESS	Are the SME's clients aware of cyber risks and unlikely to expose the SME to cyber threats?			
	Does the SME's staff know how to identify and deal with suspicious or insecure e-mails, hyperlinks websites and hardware breaches, and act accordingly? *e.g., unsafe USB portable drives*			
	What about the suppliers?			
	Do the SME's employees receive regular cyber security training?			
	Has the SME established an information security policy distributed and explained among the employees?			
TASK & RESPONSIBILITIES	Has the SME defined a person responsible for cyber security? *i.e. trusted employee to whom report cyber breaches and mistakes; responsible for the 'post' cyber attack and improving staff awareness.*			
	Does that person have the knowledge of and skills to address the most prominent cyber attack types, as identified in this paper?			
	Does that person have the 'authority'/empowerment within the SME to undertake improvement actions?			
	Does the SME have a plan for mitigating negative economic impacts in the case of a successful cyber attack?			
DATA PROTECTION	Is sensitive and critical data stored by the SME encrypted, including data on mobile devices?			
	Does the SME handle personal and sensitive data in compliance with the EU GDPR?			
	Does the SME protect physical access to its computers, servers and network?			
	Outside shareholders			
	Ownership			
	Main sources of financing			
BACK-UPS	Does the SME have a recent backup of its data and systems?			
	Is a backup available offline, or at least in a different place and completely disconnected from their systems?			
	Has the SME tried to restore a data and/or system backup and seen that it works?			

	RISK TYPE	YES	NO	DO NOT KNOW
PASSWORD & USER ADMINISTRATION	Are accounts protected by means of multi-factor authentication (MFA)? *e.g., password combined with a pin-code or a security token*			
	Are the SME employees' passwords strong and specific for each user account and system, and are they periodically changed?			
	Can each employee only access the systems that they are supposed to access?			
	Are former employees robustly blocked from accessing the systems?			
	If an employee has been subject to a cyber attack, has that employee's password been changed?			
	Is a routine in place to restrict and protect the use of system administrative privileges?			
MALWARE PROTECTION	Is the SME's IT network protected by a firewall that protects their systems from outside attacks?			
	Are the SME's devices, systems and applications protected against malware (e.g. antivirus programs, ransomware protection, spam filters)?			
	Has the SME configured its malware protection to scan e-mail attachments, downloads, files received over networks, and connected storage media?			
UPDATES	Is all software on the SME's employees' devices regularly updated (e.g. applications and operating systems)?			
	Is the SME's malware protection regularly updated (e.g. antivirus programs, spam filters)?			
	Is all software on the SME owner's servers and devices regularly updated, including the firewall?			
SECURE COMMUNICATION	Is all software on the SME owner's servers and devices regularly updated, including the firewall?			
	Are the passwords and sent data encrypted between the clients and the server?			
	Is the SME owner's WLAN encrypted and protected, and do they require their employees at home to use a VPN to access the company's systems?			
EMERGENCY RESPONSE	Is the person responsible for cybersecurity able to end a cyber attack and limit its effects?			
	Do SME managers and employees know what to do in the event of a cyber incident? Are there procedures in place and clearly allocated roles?			
	If the SME's clients or vendors are attacked, would they inform the SME about the attack if it is affected?			
	Does the SME have an ICT expert contact who can support them in case of urgent need?			
	Does the SME have insurance in place to cover IT-related business disruptions, including cyber attacks, and their related business impacts?			
IN CASE OF SOFTWARE DEVELOPMENT	Is the WLAN for employees separated from the WLAN for guests?			
	Has the SME defined who is responsible for the security of each of their software products and services?			
	Did the SME perform code inspection, especially to detect vulnerabilities and security loopholes?			
	Did the SME do blackbox testing against common security threats?			
RESULTS				

STEP 3 – ANALYSE THE RESULTS AND TAKE APPROPRIATE ACTION

If you have a total number of **YES** between:

0 - 10	The SME is easy prey. Help the SME determine the easiest **NO** or **DO NOT KNOW** responses and turn them into a **YES**
11 - 24	The SME has a solid starting point, but more progress is needed. Design a change plan to help achieve a score of 24 or above within 6 months
25 - 30	The SME already does a lot on cybersecurity. Discuss together where more could be done
31 - 38	The SME is a point of reference and example to be followed by other

CONCLUSION

SMEs' business activities and survival can be severely impacted by cyber incidents – both intentional and due to human error. It is of utmost importance for SME owners and employees to be aware of potential cyber risks, work together to help mitigate them and act effectively if a cyber incident materialises.

The SME's accountant can help. They know SMEs and can advise on areas such as cyber risk mapping, mitigating steps, awareness raising and more. The checklist in this paper is designed to help the accountant have an initial cyber mapping conversation with their SME clients.

But despite all the best efforts to mitigate cyber risks, they can still materialise. SMEs and their accountants should set up effective procedures, backups and systems to ensure business continuity and system recovery when risks do materialise. The checklist can help here too.

ANNEX – DEFINITIONS AND TERMINOLOGY

Phising: a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure, like ransomware.

Denial Of Service: a DoS attack prevents users from accessing a service by overwhelming either its physical resources or network connections

Web-based attacks: when criminals exploit vulnerabilities in coding to gain access to a server or database, these types of cyber vandalism threats are known as application-layer attacks. Users trust that the sensitive personal information they divulge on your website will be kept private and safe.

Malware: is the collective name for malicious software variants, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically consists of code developed by cyberattackers, designed to cause extensive damage to data and systems or to gain unauthorised access to a network.

Malicious insider: also known as a Turncloak, someone who maliciously and intentionally abuses legitimate credentials, typically to steal information for financial or personal incentives.

Social engineering: is a manipulation technique that exploits human error to gain private information, access, or valuables.

Multi-factor authentication: MFA is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence.

Ransomware: is a type of malware that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid

System administrative privileges: are the ability to make major changes to a system, typically an operating system. It can also mean large software programs such as a database management system

Whitelist, allowlist, or passlist: is a mechanism which explicitly allows some identified entities to access a particular privilege, service, mobility, or recognition, i.e. it is a list of things allowed when everything is denied by default.

WLAN: Wireless area network.