CORPORATE FINANCE FACULTY

CYBER SECURITY IN CORPORATE FINANCE

ICAEW

ACT TREASURY EXCELLENCE AS STANDARD

bvca Invested in a better future

Supported by The Law Society

LONDON STOCK EXCHANGE An LSEG Business

THE TAKEOVER PANEL

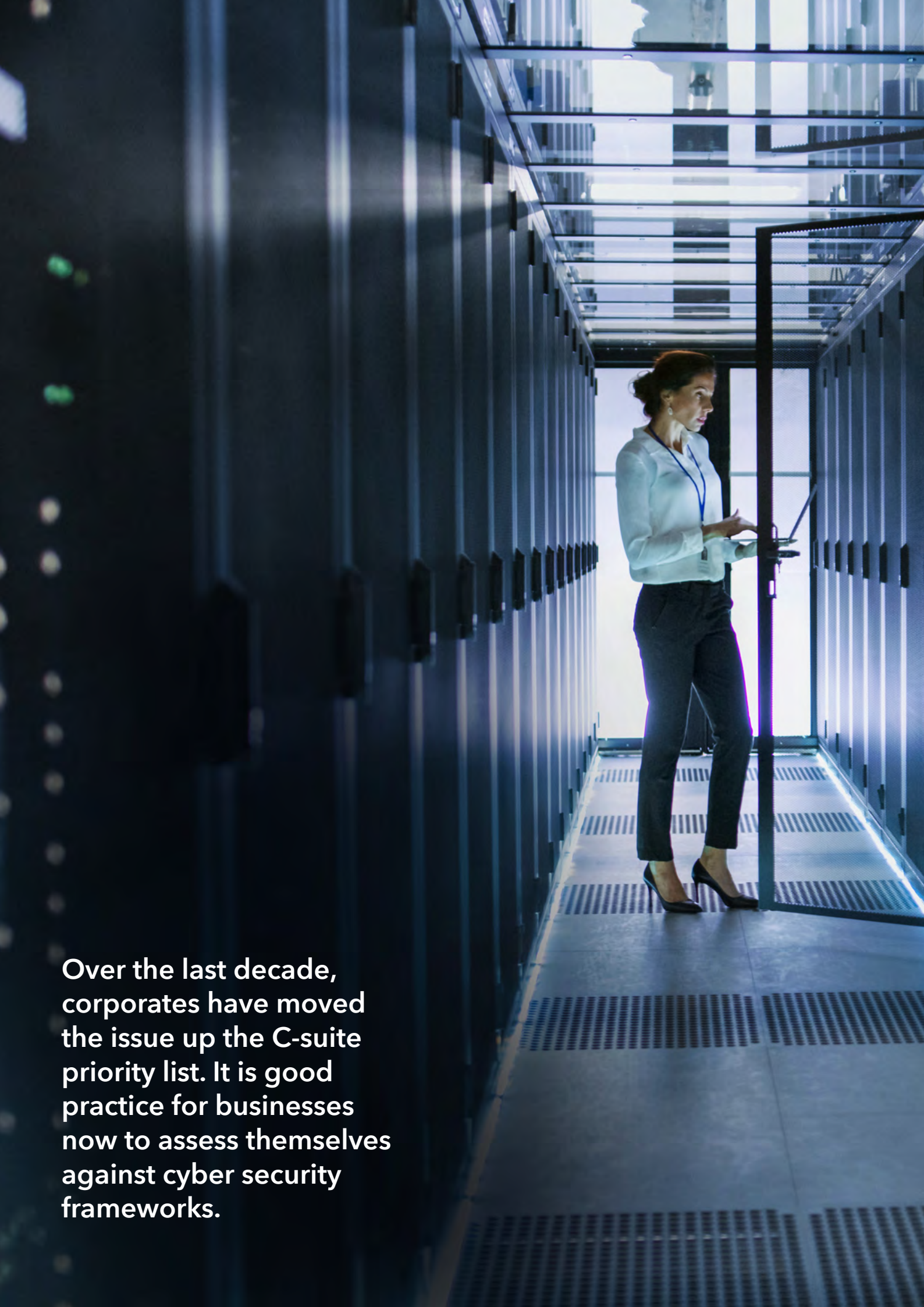
UK FINANCE

CORPORATE FINANCE COMMUNITY

For the purpose of this publication, corporate finance transactions are those where an organisation's capital structure may be changed to acquire or dispose of elements of that business, or invest and develop areas of the business. These include refinancing through to the introduction of new equity or debt.

Those involved in transactions – the corporate finance community – include advisers, company management, corporate treasurers, financial institutions and investors (for a list of possible participants see pages 8 to 9). Due diligence might be carried out by a team made up of external advisers and the acquirer's internal audit team.

CONTENTS



Over the last decade, corporates have moved the issue up the C-suite priority list. It is good practice for businesses now to assess themselves against cyber security frameworks.

FOREWORD

This second edition of *Cyber Security in Corporate Finance* is a reflection that, over the last decade, cyber security has developed to deal with new and increasingly sophisticated threats.

This publication aims to help businesses – with expertise from their advisers – tackle the risks when they are raising finance, undertaking mergers and acquisitions (M&A) or are involved in a restructuring.

Corporate finance transactions are a critical part of the economy. Investment through public or private markets enables businesses to innovate, or develop new sectors or geographies. M&A typically improves the competitiveness of a business and enhances its product or service offering.

Successful corporate finance transactions require the expertise of financial and legal advisers, financiers, and a range of other advisers. The flow of information and data during a deal leaves a business vulnerable to cyber security breaches. The National Cyber Security Centre (NCSC) has warned that the "potentially devastating impact" of cyber attacks means their risk should be the concern of boards and be prioritised to the same extent as financial or legal matters.

This publication provides information on the types of cyber risks, helpful best practice to guard against cyber attacks, and how to respond to cyber breaches during a deal process. It was written by an ICAEW-led taskforce comprising a broad range of parties involved in corporate finance transactions and cyber security.

The taskforce comprises the Association of Corporate Treasurers, the British Private Equity and Venture Capital Association, the London Stock Exchange, The Law Society, The Takeover Panel, UK Finance and professional services firms BDO, Deloitte, EY, Grant Thornton, KPMG and PwC. On behalf of ICAEW, I thank the taskforce and the NCSC for their help in developing this valuable guide for the corporate finance community.

David Petrie, Head of Corporate Finance
ICAEW

AIM OF THE GUIDE

Cyber Security in Corporate Finance aims to help businesses understand and manage cyber risks during a corporate finance transaction.

All businesses have an inherent cyber risk. Potential acquirers or investors face exposure to specific cyber risks including from:

- increased and complex access to company data during the transaction process, which could leave the business more vulnerable to cyber attack;
- increased interest from malicious hackers who see an opportunity from a transaction being underway, which might leave room for cyber security controls being missed;
- acquiring a business that has had a cyber breach it is unaware of and could affect the value put on that business; or
- sharing the consequences of a historical cyber breach following integration, such as reputational damage, technical contagion or legal consequences.

The guide highlights the questions a business should be asking of itself, and advisers should be asking the business, about cyber risk, and points readers towards further guidance. It sets out good practice and cyber security considerations businesses should address within the context of a corporate finance transaction. While not prescriptive, the considerations should be discussed at board level as they relate to a significant business risk.

There are specific regulations around reporting the impact of cyber attacks. However, there are no mandatory norms for managing cyber risk. In financial services sector businesses, there are operational resilience requirements, set out by the regulator, that cover various areas including cyber security. Many of the guide's suggestions are already being adopted by organisations as good information management practice.

INTRODUCTION

The cyber risks businesses face have grown and keep increasing. To protect against these growing threats to systems and data, organisations have needed to increase their investment in protective security measures. The consequences of weak cyber security can prove costlier than investment.

Over the last decade, corporates have moved the issue up the C-suite priority list. It is good practice for businesses now to assess themselves against cyber security frameworks, such as the NCSC's Cyber Assessment Framework. Companies are also increasingly seeking to recruit a chief information security officer (CISO), who will take ownership of cyber risk and report to the board.

A very small percentage of cyber crimes are actually solved, and it is therefore imperative that cyber security is taken seriously by all businesses to prevent an attack from occurring successfully. Even if a cyber attacker is caught, the cost to a company will most likely not be recovered. A business's operations could have been severely disrupted, or its reputation in the market severely damaged.

How a company responds to a cyber attack or data breach is just as important – non-reporting or non-disclosure may lead to reputational damage. Customers and suppliers buying from or selling to companies will be relying on the security around that interaction for their own business's cyber security. There are signs, globally, of best practice being regulated, which all businesses can consider even if they do not fall under the mandatory requirements.

When it comes to corporate finance transactions – public or private M&A, equity investment, or a debt raise – managing risk is a key part of the process. Cyber security falls within this business risk umbrella. Just as this has become a bigger proportion of the overall business risk day to day, so it is a bigger proportion of the risk in a corporate finance transaction.

Three aspects of cyber security apply to corporate finance transactions. These include the risk pre-deal, the risk during the period of the transaction, and the risk to the acquirer of the cyber security practices and controls (or lack thereof) that they are bringing into their business post-deal, or investing into.

A transaction can involve potential acquirers, their advisers and lenders all having access to sensitive data and information. The large number of people involved in the transaction is a risk in itself. The majority of parties will access data online and, if information is transferred onto their own systems, this will provide many more opportunities for cyber attackers. Public awareness of a transaction will also alert potential malicious attackers to a business going through significant change.

Corporate finance transactions can involve various types of information including personal data (for example, relating to employees, customers or suppliers), or non-personal but commercial (such as trade secrets), or even bid-specific information among the various counterparties in a transaction. This can be highly appealing to cyber criminals.

A corporate finance adviser's reputation relies upon trust and integrity. A cyber attack has the potential to devalue a firm's reputation, leading to possible loss of clients and/or financial loss, as well as potential disruption to its operations.

Because they will be holding large amounts of sensitive information about the activities, strategies and financial details of many companies, the corporate finance community is seen by those with malicious intent as a lucrative opportunity to access and exploit information.

Cyber security falls within the business risk umbrella. Just as this has become a bigger proportion of the overall business risk day to day, so it is a bigger proportion of the risk in a corporate finance transaction.

INSIDE THE DEAL BUBBLE

With any transaction, having control over who has access to data, and to what specific data, is critical to the process. The complexity of managing this will vary depending on the type of transaction. An off-market private deal agreed between two business owners with a minimal amount of due diligence involves far fewer people than would be typical in a public market cross-border acquisition, with an equity and debt raise, in a nationally strategic or sensitive sector.

As a transaction progresses, more people will have access to data, which should be tightly managed from a cyber security perspective.

There has been an increase in the number of outsourced parties involved in a transaction generally. Understanding the cyber security maturity of advisers and other parties to transactions, for example, reviewing third-party certifications such as Cyber Essentials Plus or ISO27001, is advisable to provide assurance that they have a certain level of data security.

The parties shown here may be involved in a transaction and, if so, should be considered for inclusion on an access to data list.

THE BUSINESS

- Senior management of the companies involved in the transaction
- Staff involved in roles critical to the transaction (finance, sales, IT)
- Other key staff
- In-house lawyers
- Internal audit team

STAKEHOLDERS

- Owners of the business
- Other minority shareholders in the business
- Private equity or venture capital (VC) investors in the company being sold
- The company's bankers and/or lenders

ADVISERS

- Corporate finance adviser
- Financial adviser
- Strategy consultants and advisers
- Legal adviser
- Cyber security adviser
- Tax adviser
- Financial due diligence provider
- Commercial due diligence provider
- Vendor due diligence provider
- Debt adviser
- Environmental, social and governance (ESG) adviser
- Public relations and investor relations advisers
- The company's external auditor and accountant
- Reporting accountants

OTHER SERVICE PROVIDERS

- Virtual data room (VDR) provider
- Financial printers
- Cloud services provider
- Ratings agencies
- Managed security service providers
- Underwriters/insurers

PUBLIC MARKET ADVISERS

- Brokers
- Sponsors and key advisers on the Main Market
- Nominated advisers on the Alternative Investment Market (AIM)
- Corporate advisers on other markets

REGULATORS AND GOVERNMENT

Other parties, regulators and government bodies may need to be given information during a transaction in specific circumstances.

These may include:

- Government departments, for instance, for notification as part of the National Security and Investment Act 2021 in the UK
- Industry regulators and market regulators
- International regulators on a cross-border deal
- Stock exchanges
- Cyber security authorities for a cyber security breach – the NCSC in the UK does not mandate businesses to report a breach to them, but does encourage them to do so
- Information Commissioner's Office (ICO) for a personal data breach in the UK

NATURE OF CYBER ATTACKS

The type of cyber attack deployed by different actors is continually evolving. A non-exhaustive list of attacks is described here. A broad range of malicious activities can compromise computer systems and networks, and cyber criminals may combine various techniques to create more sophisticated attacks. Businesses should remain vigilant and individuals responsible for cyber security should keep abreast of developments. Any cyber attack can affect a business's value, or be used to target businesses or their advisers during the transaction process.

Many, if not most, attacks involve an element of social engineering. The tell-tale signs include where a message arrives unexpectedly, with a question that is out of the ordinary, requesting an action that is potentially harmful, or where there is an unusual file attachment or, possibly, a sense of urgency about the message. A business should review the use of any communications channels that have been breached and look at alternative options.

Advanced persistent threats (APTs) are long-term targeted attacks that use multiple attack types. The attacker, most likely a state-backed actor, but possibly a well-funded and organised criminal group, remains within the network for an extended period with the aim of gathering as much information as possible.

MALWARE

Malicious software – including viruses, worms, Trojans, ransomware, spyware and adware – which, if able to run, can cause harm in many ways. This includes causing a device to become locked or unusable, stealing, deleting or taking control of data, or taking control of devices to attack other organisations.

RANSOMWARE

A specific type of malware that prevents access to a device and the data stored on it, usually by encrypting files. The perpetrator will then demand a ransom in exchange for decryption.

PHISHING

Untargeted, deceptive mass emails that ask recipients for sensitive information (such as bank details) or encourage them to visit a fake website. Phishing is used to persuade individuals to reveal sensitive information such as passwords or personal details. Whaling is a highly targeted phishing attack aimed at senior executives. Spear-phishing is a more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts. Smishing (SMS phishing) is a social engineering attack that uses fake mobile text messages to trick people into downloading malware or sharing sensitive information.

DENIAL OF SERVICE

Attacks that overwhelm a system, network or website with a high volume of requests, making it inaccessible to legitimate users. A distributed denial of service (DDOS) attack involves multiple compromised systems.

MAN-IN-THE-MIDDLE ATTACK

An attacker intercepts and alters communication between two parties without their knowledge, possibly between a company and its advisers, which can lead to data theft or compromise.

CREDENTIAL STUFFING

Attackers use previously stolen usernames and passwords to gain unauthorised access to accounts on other platforms. Shared passwords, or poor practice in creating new passwords, can leave businesses and advisers susceptible to credential stuffing during a deal.

DOMAIN NAME SPOOFING (DNS)

Also known as DNS cache poisoning, this is where entries on a DNS server redirect a targeted user to a malicious website, which is under the control of a cyber attacker.

MALICIOUS ADVERTISING

Cyber criminals use malicious advertisements to spread malware or redirect users to fraudulent websites.

WATERING HOLE ATTACKS

Setting up a fake website, or compromising a real one, to exploit users.

EXTORTION ATTACKS

An attacker chooses the approach that they believe is most likely to yield payment, for example, 'ransomware as a service'. This will involve extortion through a threat of exposing data, or threats to individuals or their families.

WHO AND WHY?

Cyber threats come from an ever-increasing range of sources. There is more data and information than ever before, and perpetrators of an attack can be motivated by a variety of factors, including financial gain, espionage, hacktivism or to seek political influence.

STATE-SPONSORED ACTORS

Often well-funded, backed by nation states and with advanced technical capabilities, these actors can target international transactions for geopolitical, economic or strategic reasons. They may target deals involving industries deemed of national importance by the government sponsoring the cyber attack. The aim will be to protect or give an advantage to local businesses engaged in that industry. State-sponsored actors may also use criminal proxies to direct attacks.

ORGANISED CRIMINAL GANGS

Motivated by financial gain, criminal hackers, aware of a potential transaction, may steal financial information before a transaction is announced, or carry out ransomware attacks, potentially at a critical point in a transaction process.

HACKTIVISTS

Carrying out cyber attacks for social, political or environmental causes, hacktivists target companies, or seek to disrupt particular deals or transactions. They either wish to raise awareness for their cause, or completely sabotage a transaction. They may deface websites, leak sensitive information, or disrupt online services.

COMPETITOR BUSINESSES

Business rivals in a competitive M&A process could potentially use cyber espionage to steal financial information, pricing or customer data, or sensitive information (such as intellectual property or trade secrets) to gain an advantage in deal negotiations. Confidential information on a bid before it is made public may be the target of the hack.

AMATEUR HACKERS

'Script kiddies' or novice hackers might have less technical expertise and resources than other cyber attackers, but can effectively disrupt a business using pre-existing automated tools or scripts to launch attacks on computer systems or networks. Most difficult to predict, they are typically motivated by simple, personal reasons – to have fun, create chaos or seek attention.

INSIDERS

These may be employees or contractors who have authorised access to systems and data. They may misuse their access to steal information, sabotage systems, or leak confidential data. Misuse can be unintentional, or it may be a deliberate malicious act by an employee, either because they are disgruntled, or for financial gain. This can be carried out through a third party.

MANAGING CYBER SECURITY IN CORPORATE FINANCE

There are practical steps that businesses and other parties to corporate finance transactions can take to protect themselves from cyber risks.

For illustrative purposes, this section suggests specific steps that can be taken during the typical phases in the acquisition of a business.

PHASE 1 PREPARATION

Insightful preparation is key to a transaction's success, and cyber security considerations should be included from the early stages of the process. Before starting a transaction, management of the vendor should have a full understanding of the risks to the business. They should decide what information they are likely to make available to the various counterparties, then gather the information and data, to enable all counterparties to make informed decisions about whether to proceed with the deal or not. This information gathering will most likely involve senior management and key staff critical to the corporate finance process, as well as any incumbent strategic advisers to the business.

Information relevant to the transaction will be a combination of physical and digital.

At this stage it is worth considering whether agreements, such as non-disclosure agreements (NDAs) or data-sharing agreements, need to contain data protection and cyber security provisions.

Many business aspects – sales, operations, human resources – have become increasingly data rich. It is perhaps no surprise that M&A processes now involve a greater volume of data. The simple act of pulling data together might alert individuals beyond that transaction working group that a transaction is planned.

? QUESTIONS

- What information is being collated and where is it held?
- Who will have access to the information being collated?
- Are their roles clearly defined?
- Who will have access to unstructured data, and who will have access to structured data?
- Are there any vulnerabilities or weaknesses in the IT infrastructure of either company that need to be addressed before the merger?
- Are any third-party vendors, suppliers or service providers involved in the IT infrastructure of either company and, if so, what are their cyber security practices?
- What is the incident response plan and business continuity strategy in case of a cyber security incident during or after the investment or merger?
- What sensitive data and systems are present in both organisations and what measures are in place to protect them?
- Can a data classification strategy be applied where data is grouped into areas such as highly confidential, confidential, internal and public, and security measures focused on the most sensitive.
- Are non-disclosure agreements with IT service providers up to date, and do they reference security of any information held and shared by them?
- What are the key information risks in the transaction for the business?
- Which security measures are proportionate to the risks and unlikely to unnecessarily delay the transaction?
- Can data be shared anonymously or on an aggregated basis to reduce the risk of personal data being identified?
- Is the data stored in the cloud? Are those risks being managed appropriately?
- What information risks might prove difficult to manage?
- Has the person with the best understanding of the risks involved been brought into the deal to advise on security and potential threats?

CONSIDERATIONS

- The number of people involved in a deal should be carefully controlled. From a cyber security perspective, the more limited the better, and the level of access afforded to individuals should be clear, precise and in line with their responsibilities.
- The principle of least privilege is best practice. This is a security concept in which a user is given the minimum levels of access needed to perform their job.
- Senior executive management – the CEO and the CFO in particular – will be central to the formative stage of any deal. Certain incumbent or strategic advisers will also be involved. With regards to IT, data and cyber security, the chief technology officer (CTO), chief risk officer (CRO), CISO or the individual responsible for overseeing an organisation's cyber security will be on the inside. Less senior staff may be brought into the deal where necessary, possibly including individuals needed to pull together the data, or assisting in cyber security threat analysis.
- Businesses should have a communications strategy if there is a cyber breach during the transaction.
- Meetings should be confidentially planned – for example, shared diaries for senior staff should not be used.
- Every individual in the deal working group should be clear about their level of access to data and briefed about the importance of ensuring there are no information leaks throughout the deal process. This procedure should be documented so that it can be monitored.
- Business management should have a full understanding of where all their IT systems and their entry points are, as well as the nature of the data and information stored on each system. The business should already have these safeguards in place, and ideally have this information to hand, reviewing and updating it on a regular basis.
- Management should consider where the data for the deal should be stored and how access to it should be controlled.
- A vendor should decide what data will likely need to be disclosed to maximise sale value, while protecting commercially sensitive information. This will vary depending on the nature of the deal, and in terms of sensitivity.
- A potential acquirer will wish to work out what information will be needed to fully inform their bid. That may ultimately be a wish list – if there is a lot of interest in the business, the vendor will have more control over the information it discloses.
- Management should have an understanding of where the key information risks in the transaction are for their organisation. Poor business as usual IT security will likely prolong negotiations and impact buyers' decisions to buy or not, and at what price. Cyber security measures already in place need to be proportionate to managing the risks, but flexible enough to allow the transaction to progress smoothly. It is best to focus security measures on the most sensitive information.
- The IT resource required for the transaction should be carefully considered. Who from the company will be required and how will that affect operations? Additional independent IT resources, or additional resources from finance, HR or sales, might be required to manage the data being collated for the VDR.
- A business should have secure information management and IT processes, and staff should be well versed in the process for prompt cyber incident reporting. However, this is the time to ensure that this is the case in practice, and not just on paper, by ensuring that staff are fully aware of the process.

OUTSIDE-IN REVIEW FOR ACQUIRER

At the preparation stage, an acquirer or an investor will have no access, or extremely limited access, to the potential acquisition target.

To gather information at this very early stage, an outside-in cyber review, known as open-source intelligence (OSINT), can be carried out. This is not the same as a full due diligence process, but it will, for example, highlight any gaping holes in the target's online infrastructure. It might also be the only approach available.

If an online presence or use of technology is key to the target, security around that will ultimately go to the heart of the deal value. Again, it may be possible to use something like open-source intelligence monitoring.

There may be recent domain name registrations, which have the potential for domain name spoofing during the M&A process. These registrations can be searched for ahead of any process beginning in earnest.

Dark web searches, a review of information on the ICO's database, digital profiling and digital reconnaissance, and any public information that might be available will all be part of an outside-in review. It will involve checks for:

- breached credentials and passwords related to the high-level domain of the target, which may be found being traded on the dark web;
- whether key individuals' email addresses have been compromised;
- occurrences of data leaks in relation to the high-level domain, which may also be traded on the dark web;
- chatter on dark websites using agreed terms related to the target business; and
- publicly available data points.

An acquirer should ensure the target's existing privacy notices are up to date. The outside-in review will also include a review of the target's external footprint. This is an assessment of the online infrastructure of the business, with checks including strength of communication security, technical vulnerabilities, common open ports, firewall issues and insecure login portals.

The review should look at the people element of the cyber risk. Does the target have a CISO? How long have they been in post? What qualifications and experience do they have?

It is possible that the outside-in review may reveal significant cyber risks that constitute a red flag for the deal to proceed.

FURTHER INFORMATION

Identifying the critical assets in your organisation

www.ncsc.gov.uk/collection/board-toolkit/identifying-the-critical-assets-in-your-organisation

Planning your response to cyber incidents

www.ncsc.gov.uk/collection/board-toolkit/planning-your-response-to-cyber-incidents

PHASE 2 ENGAGING, SELECTING AND APPOINTING EXTERNAL ADVISERS

External advisers can be appointed at the point when a company decides to proceed with a transaction. Some advisers may have been involved in the strategic thinking leading to the transaction.

An IT or cyber security adviser may already be in place but, if not, now is the time to do this. This is an important role, as they can provide assistance on, among other things, the cyber security throughout the process.

Mandates can be formalised and information sharing can begin. Sensitive data will begin to flow from the business to advisers and controls should already be in place. When appointing an external adviser, a company should seek assurances regarding their cyber security maturity and consider if specific approaches are needed for management of data.

CONSIDERATIONS

- Information sharing needs to be carefully managed to ensure there is clarity about what is confidential, how it can be accessed and how it can be shared. All parties involved should consider who within their organisations should have access to shared information and on what basis.
- Formal agreements about how information is shared and used are recommended, and considered common.
- Specific individuals or a small team in each organisation should be given responsibility for overseeing the data and information exchange process.
- Considerations for selecting a VDR can be found on page 25.
- The VDR login system will record details of who has accessed information from the time they are appointed, as well as information uploaded to the VDR. However, some information might be shared before the VDR provider is appointed.
- The information being shared, and how it will be filtered at each stage of the process, should be carefully considered. How much detail is needed initially will be the first consideration, with an eye on what will ultimately be shared with a preferred bidder.
- The acquirer and its advisers need to establish how information security is being monitored, and whether monitoring systems are adequate.
- It is important to establish a procedure and agree a trigger for notifying all parties of a cyber attack. Often, parties will set up a shared forum for incident reporting.
- It might be appropriate to rely on the representations of companies, advisers and agents involved in a transaction that adequate and suitable security standards are adhered to. There may be relevant third-party reports on security standards that an acquirer should review.
- There might be a heightened cyber security risk in any given transaction. Senior management may be aware of specific attacks within their industry or country.
- All parties should have acceptable procedures around the use of personal devices or mobile devices owned by the company and used outside of their office. Up-to-date cyber security suites should be installed and used to exchange information. There should be restrictions on the use of personal emails or messaging apps for correspondence about the deal.
- The process for resolving cyber security concerns arising from due diligence should be agreed.

VENDOR DUE DILIGENCE AND CYBER SECURITY

Cyber security vendor due diligence (VDD) allows potential buyers to obtain reliable insights from a trusted third party in the form of a report, the focus of which is directed by the vendor. The vendor can take remedial action to address issues raised in the report.

The decision over whether a vendor commissions VDD is often driven by the nature of the business and whether a trade or private equity sale is envisaged. If the decision is taken to produce a VDD report, cyber should form a part of it.

The scope of work for VDD covers all matters that an acquirer would expect from a cyber and IT/tech due diligence exercise, so will essentially be the same as that which an acquirer would commission in a buyside due diligence report.

? QUESTIONS

- Is there a cyber insurance policy? If so, what does it cover? And if not, why not? What is the coverage limit of the policy? Has the business ever made a claim under its cyber insurance policy? If yes, what was the outcome?
- Can the vendor provide documentation and evidence of their cyber security practices, such as security policies, incident response plans, business continuity plans and disaster recovery plans?
- What security measures are in place to protect sensitive data and prevent unauthorised access?
- Has there been a cyber breach in the past and, if so, what was the business response, what was the impact and how was it reported? Did it impact the cyber insurance policy?
- Has an independent cyber security risk assessment been carried out?
- What data is key to the business? For example, is it in the sales process, the supply chain, the product or service development, the finance function or HR?
- How are the data and other critical assets such as the IP protected?
- Does the business own the IP related to its activities?
- Are there third-party providers that input coding to the business's IT system?
- How reliant is the business on third-party services?
- What are the risks around those third parties – cyber breaches or insolvency, for instance?
- What are the vendor's policies, training and culture around cyber security governance?
- What technology is business critical and how has its resilience been developed?
- Will some elements of IT and cyber security require capital expenditure to ensure continuous management of security?
- What is the potential direct financial impact of a breach, and the indirect financial impact of the reputational damage from a breach?

PHASE 3 INITIAL APPROACHES

Once a list of potential acquirers has been drawn up by a business and its corporate finance adviser, the next step is approaching the prospective buyers. From a cyber security perspective, the smaller that group the better, but that may not be the way to maximise value.

At this stage, the business being sold will likely have prepared for the due diligence process. The amount, nature and timing of access to be afforded to prospective bidders may be set out in the approach.

Some deals can be very tightly managed, with only a handful of individuals from the business inside the deal bubble. If a business is highly desirable, has sensitive IP or handles sensitive data, greater efforts may be required to maintain control over data.

More parties will start gaining access to information, and the nature of that information will become more commercially sensitive.

CONSIDERATIONS

- How and what information is provided to the businesses that are contacted should be carefully considered. The vendors need reassurance that information will be handled securely – protocols need to be agreed. Limit the number of people receiving information as far as is practicable, exercising the need-to-know or least privilege principle for confidentiality in general and cyber security, while seeking to maximise value by approaching all credible buyers.
- A VDR will provide control and an audit trail of who has accessed data – end-to-end encryption is standard procedure for a VDR now. Relevant approvals and signed confidentiality agreements covering access to the VDR should be received before disclosing confidential information to another party. These will include agreements about what information will be shared, with whom and how it will be used, as well as breach escalation principles. It should also cover cyber security practice. Only information necessary for the transaction should be shared.
- There should be specific controls in place in the rare instances where data is provided in paper format, to be viewed in a secure deal room.
- A balance should be struck between the need to provide adequate information and protecting sensitive data. Sharing specific sensitive data to final bidders only is common practice.
- For those handling confidential or sensitive data, best practice is to make sure the necessary agreements are in place with those parties.
- Some interested parties may be from different jurisdictions. The risk profile of the sector or country they are from should be considered. They may be more vulnerable to cyber attack. The sector may be one that is of particular local interest, such as natural resources or technology. The deal may involve assets that could be considered of strategic importance to a particular country.
- Local regulatory norms should be considered – are some of the usual security measures allowed in the jurisdictions of potential suitors? Certain jurisdictions have different laws about the use of encryption, for instance.

WORKING PRACTICES

In the wake of COVID-19 lockdowns, working from home (WFH) became a new normal for many more individuals. Following the pandemic, increased flexibility and convenience has led businesses (including advisory businesses) to continue WFH practices to different extents. While remote working that is not necessarily 'from home' is not new, the frequency and extent is far greater than before the pandemic.

There should be comprehensive security and awareness training for the staff involved in the transaction and the planning of communications.

Working remotely can raise concerns around cyber security and it is imperative that protocols around this are agreed between all parties on the deal. A virtual workspace can be more susceptible to a wider array of cyber threats, and remote employees may no longer be protected by the corporate network's security measures.

Mobile devices used during a deal should be the company's devices, controlled and managed by the company, or personal devices with appropriate, corporate-controlled mobile application management (MAM) solutions.

The typical minimum controls that are expected are encryption-at-rest, antivirus, centralised monitoring, multi-factor authentication, access controls and controls over data in transit.

There is possibly greater risk for anyone working in a coffee shop, or on a train or plane, using public WiFi. Security awareness training is crucial for all staff involved in the transaction.

Just as it is important not to take deal-related calls in front of any unauthorised individuals, deal-related documents should not be opened at a place where unauthorised individuals can see the document contents.

Administrators with privileged access to the services or systems being used for the deal will clearly also have access to deal information and should be aware of their working environment and the risks of working from home and remote working too.

KEY CYBER SECURITY CONTROLS FOR WORKING AWAY FROM THE OFFICE:

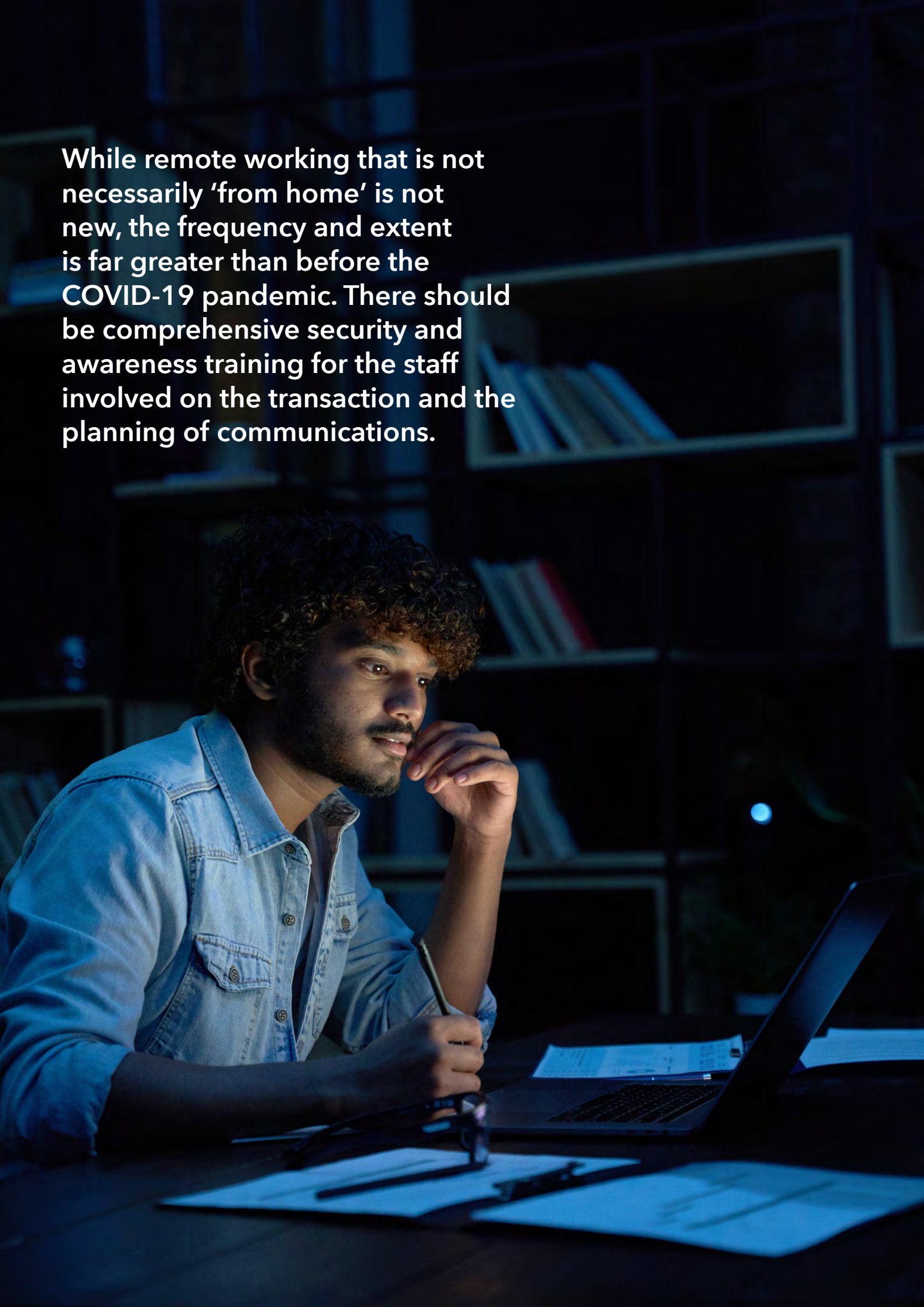
- **Secure virtual private networks (VPNs)** should be used to encrypt the data transmitted between remote devices and the corporate network.
- **Multi-factor authentication (MFA)** can prevent unauthorised access even if login credentials are compromised.
- **Endpoint security**, including antivirus, anti-malware and firewall programs, should all be regularly updated, with known vulnerabilities patched. Data leakage prevention and detection tools can be useful, particularly for insider threats.
- **Secure device usage** should be enforced so that work devices are solely used for professional tasks and not shared. These devices should lock automatically after a period of inactivity and require authentication for access.
- **Data encryption** is absolutely critical in deal situations. Encryption converts data into unreadable formats.
- **Secure file sharing and collaboration** provides a safe environment for remote teams to collaborate without exposing sensitive data to potential breaches.
- **Regular backups** safeguard against data loss due to cyber attacks, hardware failures or accidents, allowing for swift recovery.
- **Incident response plans** should clearly outline the steps to take in case of a cyber security breach while working from home.

FURTHER INFORMATION

Home working: preparing your organisation and staff

www.ncsc.gov.uk/guidance/home-working

While remote working that is not necessarily ‘from home’ is not new, the frequency and extent is far greater than before the COVID-19 pandemic. There should be comprehensive security and awareness training for the staff involved on the transaction and the planning of communications.



PHASE 4 COMPILING INFORMATION ABOUT THE BUSINESS

PREPARATION OF BUSINESS-RELATED INFORMATION

In a sale mandate, any number of potential acquirers will have been contacted by the business or its corporate finance adviser in relation to the transaction. The business owners, senior management or shareholders and the lead adviser will have agreed on the list of contacts. They will likely have had access to some sensitive information. Some potential acquirers may have begun their own review of the business using publicly available information, or proprietary information on the business held by third parties. They may also have carried out an outside-in review of the business's cyber security controls.

By now a large volume of information and data will be getting pulled together and is then shared with the largest number of participants that will be involved in the transaction at any point. This can include disclosure documents, information memoranda, prospectuses, vendor due diligence packs and information for relevant regulators. The risk of outsiders having knowledge about the transaction is substantial considering the involvement of numerous organisations. The risk of a cyber attack will escalate if the knowledge of the transaction becomes more widely accessible, as valuable and potentially sensitive data and information will be stored and circulated during the process.

Security breaches might also affect suppliers, customers or employees, not just the transaction. It might even affect markets, depending on the nature of the transaction and the information being shared.

QUESTIONS

- What documentation needs to be prepared to support the process and maximise sale value?
- What information and data needs to be included in the documentation? In particular, what sensitive information and data?
- Have there been any cyber incidents in the recent past? How were they dealt with? What changes to processes were made to protect against a repeat?
- Has an independent cyber security risk assessment been carried out?
- Are products and services provided by partners/suppliers documented?
- Are the critical assets storing that information known?
- What is required to meet relevant regulatory and legal requirements?
- What additional information and data will help support a higher valuation?
- Who will receive the documents – the potential bidders and their advisers?
- Where will the information be stored and access to it controlled? A VDR? Who will be in control of the VDR and the security around access and downloading of information? (See box on page 24)
- Can the information be tailored depending on the risk profile of each recipient, or type of recipient?
- Is specific authority required for disclosure of information or data in relation to customers, suppliers or employees? Does that increase the potential for a security breach?
- Are additional protections needed for any data being shared about customers or suppliers?

CONSIDERATIONS

- A business should consider whether information should be presented in a different format to different potential acquirers. Private equity and trade buyers are likely to have a subtly different focus when looking at an acquisition.
- Some parties might be attractive purchasers, but considered high risk when it comes to cyber security breaches (or any leak for that matter). Giving them access to the VDR and the data therein might not be safe. There may be alternative means of providing the information, such as inviting them to access information on a separate, monitored data store or in paper format in a physical data room.
- Is there a possibility of a private transaction being leaked to the public domain during the transaction process? If so, the business may be at a higher risk of cyber activity against them, and not just during the completion phase.
- Parties to a transaction should always be wary of the risks of over-disclosure. Only data or information that adds value, or specifically enables a buyer to come to a decision on whether and at what price to proceed, should be revealed. This is important generally, but is particularly pertinent in a cyber security context. One example is personal information, which may create data protection issues, but does not add any value to the sale price and is not generally required by the potential acquirers. Personal data is probably the key risk for many businesses.
- A business should create a post-deal IT integration plan, which also includes plans for cyber security and feeds into any transitional service agreements (TSAs) related to IT and cyber security. TSAs should identify what services will be offered by whom, to whom and timings.

DUE DILIGENCE ON CYBER SECURITY

An acquirer may have carried out an outside-in review (see page 16). If not, those areas and any further questions about the cyber security of the target should be asked as part of a due diligence exercise. Potential acquirers may be provided with a VDD report, which covers the scope of work that a typical acquirer would commission.

The VDD report will answer questions such as:

- When did the board last review cyber security?
- Who is ultimately responsible for managing cyber security in the company?
- Has the company audited itself against any cyber security frameworks, such as the US National Institute of Standards and Technology Cyber Security Framework (NIST CSF), or the NCSC's Cyber Assessment Framework or 10 Steps to Cyber Security principles?
- How confident is the company that its most valuable information is properly managed and is safe from cyber threats?
- When did the company last experience a cyber or information security breach?
- What were the costs of the breach – regulatory fine?
- What steps did the company take to mitigate the impact of this breach?

Due diligence will commonly provide information that can be used as leverage in negotiations. Various cyber security certification schemes (including the NCSC's Cyber Essentials and Cyber Essentials Plus) provide some assurance if in place. They ensure the business has at least the minimum level of security, and provide assurance to acquirers that the business takes cyber security seriously and is working to secure its IT. They do not, however, ensure the business has any GDPR-specific controls in place.

THE VIRTUAL DATA ROOM

Most businesses have much more data than they did a decade ago. Corporate finance transactions involve the wide sharing of data with ultimate and potential counterparties to a transaction, and their advisers. A business will have put together an enormous amount of data, which by the very nature of it being central to the buy/sell decision and pricing, will include sensitive information. It will be collated and shared with relevant participants from the first stage of a bid process.

Increasingly due diligence processes make use of VDRs. The information being shared will likely include data on pricing, costing, customers and suppliers, product design and specification data, and employee information of a personal and financial nature. Where a competitor is involved in the process, their access to sensitive data may be restricted or withheld until later in the process. As well as being commercially highly sensitive to the business, much of the information may be subject to data protection regulations. It is imperative that security remains high at this stage of the process.

There should be protocols around what individuals can download. All access to a VDR should be logged, along with what individuals are using the downloaded data for. Current industry best practice on data loss prevention should be followed – for instance, a download of a large amount of information should raise an alert.

Protocols will be managed by whoever is in charge of the data room in agreement with the vendor and their advisers. Getting the right balance between security and practicality is key. Security should be pragmatic and risk-based, so that the time available for working on the deal is not reduced. Ultimately, it's about detecting anomalous events. Some of the key cyber security concerns around the use of VDRs include risks of data breaches, and inadequate encryption.

Third-party confidentiality is another consideration. For example, some supplier or customer information or data, as well as reports for the business written by professional advisers, might be under a duty of confidentiality. If it is absolutely necessary to the transaction process, then consent from the relevant third party should be sought, in the knowledge that this request will alert the supplier or customer to an impending transaction.

VDRs have streamlined and brought increased efficiency to the data room process, and in many ways brought greater control of data that is shared, and to which parties are given access. But security is completely reliant on the controls put in place. Any weaknesses in the system or procedures could lead to breaches of security. It might be easier to identify where breaches have come from, but better still is when breaches simply do not happen.

VDR SECURITY

The security set up around access to the data room and use of information is key. Companies should appoint an employee or an adviser to actively monitor and manage this and provide a clear escalation process for reporting concerns.

Watermarking and dynamic watermarks

Watermarks will display the recipient's name, email address, or other identifying information. Dynamic watermarks are unique to each user, enabling traceability to the source of any leaked documents.

Data encryption

A VDR will typically use data encryption so it can only be read by the intended audience.

Activity tracking and audit logs

Comprehensive activity tracking and audit logs provide a detailed record of all user interactions within the VDR – document access, downloads, edits and sharing activities.

Multi-factor authentication (MFA)

MFA is increasingly applied to VDR access to address the issue of parties sharing common passwords and logins to data rooms. An audit of passwords and logins prior to access being granted should also be carried out to ensure that no logins are shared and passwords have been updated recently.

CHOOSING A VDR

To address cyber security concerns, companies should consider:

- choosing a reputable VDR provider with a strong track record of security;
- implementing robust access controls and user authentication mechanisms;
- encrypting data at rest and during transmission;
- regularly monitoring and auditing user activities within the VDR;
- conducting security assessments and penetration testing on the VDR or, more commonly, requesting information on this from the VDR provider;
- educating users about potential security risks and best practices;
- having strict agreements about data retention; and
- having a well-defined incident response plan in place.

Ultimately, a combination of technology, policies and user awareness is essential to mitigate the cyber security concerns associated with virtual data rooms.

Parties to a transaction should always be wary of the risks of over-disclosure. Only data or information that adds value, or that a buyer needs to come to a decision... should be revealed. This is important generally, but is particularly pertinent in a cyber security context.

PHASE 5 FINALISING TRANSACTION TERMS

The transaction will now be at an advanced stage. The final bidders will be looking to finalise the details of their offers. The level of detail will increase and the nature of the information being shared is again likely to be of a highly sensitive nature.

Participants such as bidders in a transaction will face risks. There have been incidents of bidders' highly sensitive information, such as bid prices and financing terms, being intercepted by rival bidders in a transaction even before details of their final bid has been submitted. This is clearly damaging to the bidder and the vendor, as it could put the transaction in jeopardy or impact value.

As part of the agreement, there should be a requirement that bidders will be unable to access data after dropping out of the process. Professional advisers, however, may need to maintain access to information for professional regulatory purposes. Most VDRs offer the ability to block data downloads, including through data encryption.

QUESTIONS

- How high is the risk of compromise or theft at this stage? Will it increase as the bids are finalised?
- If the transaction has been relatively low risk so far, and the approach has been that of a low-risk transaction, should cyber security measures be stepped up now by restricting access further?
- Do the questions raised around cyber security in earlier phases of the transaction need to be revisited?
- What are the consequences of a breach at this stage? What is the worst-case scenario?
- How can this be managed effectively and the effects of a breach be mitigated?

CONSIDERATIONS

- Non-disclosure and confidentiality agreements about the specifics of the financing might be appropriate.
- Some information could be kept offline. One example might be an auction, in which the final figure in a party's bid is kept offline and submitted by a senior member of the deal team at the meeting.
- Where information being requested is beyond standard market practice, vendors should consider carefully whether this should be disclosed.
- If acquiring a business, carrying out due diligence on its past record of dealing with cyber security breaches is important. Many businesses and other organisations will already have been targeted. Depending on the severity of attacks and how they were dealt with, this could have a material impact on the value of the business or even whether the transaction is worth proceeding with.
- Many companies may not yet be following practices that meet a buyer's expectations or requirements. If so, the risks of a past or future attack and what measures might be necessary to bring the company to a level that meets the acquirer's risk appetite should be considered.
- If an incident management plan has not been devised for the transaction so far, this may be the point where one should be drawn up, particularly if the deal is high profile, public or considered to be sensitive.
- Bidders should have a good estimate of any immediate or post-completion investment required. Having had full access to the target business, they will have confirmed any earlier findings and completed any gap analysis. What is the level of operating expenditure and capital expenditure for remediating any cyber security gaps identified in the due diligence process? Details of the issues to be addressed in taking over should feed into TSAs.

CASE STUDY: PUBLIC DEAL

A UK business fell victim to a cyber attack during the transaction process, just after it had been reported in the press. The business was vulnerable because it had not implemented effective security around devices, legacy IT and software. The deal did continue, but this lax security had a significant impact on costs, value and timelines. It also meant that serious investment and resources had to be earmarked for the post-acquisition period.

An incident management plan should be drawn up for the transaction. If a plan has not been devised so far, the point where this may be done is when terms are being finalised.

PHASE 6 COMPLETION

A transaction might only become public knowledge during or following completion. If this is the case, and the transaction is sensitive or of public interest for some reason, information risk might intensify at this stage.

There will also be heightened risk as funds are transferred to complete the transaction. Robust banking systems mitigate the risk of interception of funds being moved. However, there will also be additional employees involved in the transfer, adding to the number of internal people becoming aware of what is happening.

In addition, companies will have strategy documents detailing how they might benefit from the deal and their next steps on, for example, integrating a new business unit, separating a company from its parent, how it will enter new markets, and 100-day plans. Much of this information would be highly valuable to competitors and to countries looking to protect and enhance the interests of national companies.

CASE STUDY: REGULATED TELECOMS SECTOR BUSINESS

A private off-market acquisition in the telecommunications sector fell through during the period from signing to completion after an undisclosed breach was discovered in the due diligence process. The breach was reported, and the regulator Ofcom stepped in. However, the acquirer decided not to complete the deal. This showed the importance of thorough cyber due diligence on the part of the acquirer. It also showed the importance of a business and a vendor really being on top of cyber attacks, and ensuring full disclosure.

CASE STUDY: ONLINE CONSUMER BRAND

A consumer business with a significant online presence had not declared a previous breach. This was discovered prior to the deal being announced. The negative impact on the brand destroyed value as cyber security was key to their consumer business model.

On completion, TSAs should be in place covering IT and cyber security.

QUESTIONS

- Who will be involved in the transfer of funds and document signing?
- Are there parties or individuals that have not been involved so far?
- Have information risks been managed appropriately throughout the transaction?
- Is the transaction in the public domain?
- Is there now a greater risk to the information being shared and stored? What measures might be practicably put in place to protect it?
- What is the policy for storing sensitive information post-completion?
- How will any IT systems acquired as part of the transaction be updated and checked?
- Have acquired parties' systems been compromised? Are more detailed checks required at this stage?

CONSIDERATIONS

- There should be continued monitoring of access to documents relating to the transaction.
- Even post-transaction the risk of intrusion may remain, for example, from malware that has lain dormant on systems so far.
- The presence or otherwise of any weaknesses in the systems being used for the transfer and storage of funds should be established, especially if deal-specific accounts have been set up or payment limits have been increased above normal levels.
- There may be a need to review information management and security policies across the organisation.
- Post-transaction, the enlarged organisation may be at increased threat of cyber attack, so policies or procedures should be strengthened if appropriate.

PHASE 7 POST-COMPLETION INTEGRATION

A 100-day plan is usually a detailed plan that an acquirer has for the integration of its new asset to its existing business.

Due diligence findings can act as a foundation and guidance for any post-deal efforts related to cyber security. It is sensible to further break the integration plan into tactical and strategic efforts to ensure maximum protection at the early stages.

Integration will involve bringing together the IT systems, networks and data of two or more organisations, the extent of which very much depends on the strategy for combining the two businesses. This can give rise to issues.

If the acquired business will be a standalone subsidiary, only some elements of the finance function, for example, might be integrated. At the other extreme, it may require a full merger – all IT systems related to staff, operations, product design and development, sales and finance functions would need to be integrated. A takeover may involve anything between those two extremes.

There needs to be effective oversight from the parent entity regardless of whether the acquired business is integrated or is a standalone subsidiary. A governance/reporting structure for cyber security should involve leadership from both the parent and acquired entity.

The first action, which will have been addressed to some extent pre-completion, is to firm up the plan for integrating systems following a gap analysis. What systems will be integrated and to what extent? The next action is to put in place adequate resources to carry out the integrations, which may involve bringing in additional external IT resources to assist in the process.

The integration may involve dual running of systems for a period of time to ensure there are no issues, or that any arising issues can be resolved.

This will often be covered by a master services agreement, but that should incorporate any services that an acquired business is still purchasing, and how they may overlap with services purchased by the acquirer.

The acquired business may have better systems than the acquirer, so the acquirer's IT might be integrated onto those of the acquired business.

During this process, several cyber security concerns need to be addressed to ensure the security and integrity of both organisations' digital assets. This includes data breaches and data loss, mismatched security policies and controls, and vulnerability exposure.

CASE STUDY: IP

A business was acquired for the value of its IP. However, post-completion, it was discovered that a cyber actor had had access to the network for several years. The cyber attacker was selling the IP, which was being mimicked in another market to offer cheaper services. This could have been revealed by more thorough cyber due diligence, or possibly through commercial due diligence on that market.

POST-DEAL CYBER ISSUES

There are some specific cyber security concerns that can arise during the post-deal transformation process:

- **Data security and privacy**: During integration, data from both organisations may need to be migrated, shared or consolidated. This can lead to data exposure, unauthorised access, or mishandling of sensitive information if proper security measures are not in place. Data protection teams should be consulted on data transfers, particularly those cross-border, and ensure they are compliant with data protection regulation.
- **Network segmentation**: Integrating different IT networks can result in security gaps if network segmentation isn't appropriately managed. Failure to isolate critical systems can lead to the spread of attacks across the integrated network.
- **Access control and identity management**: Ensuring proper access controls for employees and systems becomes complex when merging two organisations. Inadequate access management can lead to unauthorised access, data breaches and insider threats.
- **Vulnerability management**: Combining IT systems from different businesses can introduce new vulnerabilities or exacerbate existing ones. Regular vulnerability assessments and patch management are crucial to prevent exploitation.
- **Cultural and policy alignment**: Different businesses will often have varying cyber security cultures and policies. Harmonising cultures and policies is important across the business operations as a whole, and specifically when it comes to IT, to maintain consistent cyber security practices across the integrated entity.
- **Third-party and supply chain risks:** The integration process might involve shared third-party vendors or suppliers including contractors. These external entities could introduce security risks if their cyber security standards aren't up to par.
- **Incident response planning**: An integrated entity needs a well-defined incident response plan that considers the increased complexity and potential for new types of attacks. Rapid response and recovery are essential to minimise damage.
- **Compliance and regulatory challenges**: Different industries and regions have distinct compliance requirements. Integrating businesses should ensure that their cyber security practices align with applicable regulations for jurisdictions and industries to avoid any legal and financial consequences.
- **Monitoring and detection**: Consolidating IT environments could include monitoring and detection capabilities to identify anomalous behaviour and potential security breaches across a larger attack area, with more points of entry for cyber attacks. The 100-day plan could also include a search for information in email or other IT systems for undisclosed legal claims against the acquired company or regulatory violations.
- **Secure communication**: Communication channels established during integration should be secure to prevent interception or manipulation of sensitive information.
- **Training and awareness**: Employees from both organisations need to be educated about any new security protocols, potential threats, and the importance of following cyber security best practices.
- **Shadow IT and unauthorised systems**: Integrating businesses might bring their own unauthorised or unmonitored systems, which can introduce security vulnerabilities and complicate risk management.
- **Use of social media**: Management of the use of social media needs to be reviewed to ensure that the acquired business does not introduce greater potential for phishing scams.
- **Asset management**: Keeping track of all IT assets and systems becomes more challenging after integration. Unmanaged or forgotten assets could become targets for attackers.
- **Business continuity and disaster recovery**: Management should ensure that the integrated entities have robust plans in place to maintain operations in the face of cyber incidents or disasters.

To mitigate these concerns effectively, it's crucial for organisations to conduct thorough risk assessments, develop a comprehensive cyber security strategy for integration, and involve cyber security experts and advisers to supplement internal resources where necessary. They should continuously monitor and adapt security measures as the integration progresses to ensure that the reality matches the theory.

CYBER AND DATA REGULATION

Creating a cohesive and universally accepted set of regulations for cyber security faces many challenges.

These include:

- diverse legal systems;
- rapid technological advancements;
- sovereignty and data privacy considerations;
- lack of consensus; and
- national protectionism.

The United Nations has several groups focusing on norms, rules and principles for responsible state cyber behaviour. The aim is to establish a stable and secure regulatory framework in the digital realm.

The Council of Europe's Convention on Cybercrime (also known as the Budapest Convention) aims to harmonise cybercrime laws across jurisdictions, and has been ratified by 70 countries.

NATO's Cyber Defence Policy aims to protect its networks and bolster its collective cyber security defence capabilities. At the 2023 NATO Summit, this was enhanced with the Virtual Cyber Incident Support Capability to support national responses to significant malicious cyber activities.

The International Organization for Standardization and the International Electrotechnical Commission have cyber security standards on industry best practices.

Regional agreements, such as the EU's General Data Protection Regulation (GDPR), enforces data protection and privacy rights in the EU. In the UK, GDPR is implemented by the Data Protection Act 2018. These are influencing global data protection standards.

Data-sharing considerations may become a priority when a merger or acquisition, or another change in the organisational structure, involves transferring data to a different organisation.

Acquirers should:

- ensure data sharing is considered as part of the due diligence;
- establish and follow the lawful basis for data sharing;
- establish what data is being transferred;
- identify the purposes for which the data was originally obtained;
- ensure data processing principles are complied with;
- document the data sharing;
- seek technical advice before sharing data where different systems are involved; and
- consider when and how data subjects will be informed about what is happening.

Being able to demonstrate to the ICO that compliance with the Data Protection Act 2018 is adequate should be a normal part of running any business.

The Network and Information Systems (NIS) regulations in the UK, and the NIS2 and the Digital Operational Review Act (DORA) in the EU, set out the frameworks for operational resilience for businesses.

There is growing consensus that international collaboration is essential to tackle cyber threats effectively. Countries adopting common frameworks for core cyber security principles, norms and standards is the ideal scenario. Timely and transparent sharing of threat intelligence among countries should be encouraged. Norms of responsible state behaviour and collaboration between governments and business are essential to address global cyber security challenges.

INCIDENT MANAGEMENT

Despite all the steps in this guide, the risk of a cyber attack cannot be eliminated. Cyber security incidents, such as a data breach or ransomware infection, can have a huge impact on an organisation in terms of cost, productivity, reputation and loss of customers. Being prepared to detect and quickly respond to incidents will prevent the attacker from inflicting further damage and can reduce the financial and operational impact.

Management should handle the incident effectively, which can be made more challenging if it is a public deal.

A business should have an incident response plan in place as it will minimise the impact of incidents, helping normal operations to be resumed as quickly as possible. It should be regularly reviewed and maintained to ensure that it continues to be relevant as roles and the structure of the organisation changes.

The incident response plan should include:

- how the severity of an incident is determined;
- delegation of authority for key decisions;
- responsibilities for contacting key individuals in the organisation (including board members), suppliers and regulators to share information about the incident; and
- clear roles, responsibilities and reporting requirements.

The quality of decision-making can be compromised in times of crisis, so it is vital that everyone has a clear understanding of their role and the organisational response in advance. Responding to an incident may require making major decisions, such as whether to take systems offline (for instance a website, or other operationally critical systems). Individuals should know what authority they have, especially if an incident happens outside of normal business hours.

Monitoring should be maintained at a high level.

QUESTIONS

- Does the business have an incident response plan in place that is regularly practiced? Board members must be involved, along with any cyber advisers and third-party suppliers where relevant.
- Does every board member understand what's required during an incident?
- If a significant cyber incident has occurred in the recent past, can the person responsible for cyber security report what improvements have been made?
- Are cyber incidents considered in the design of the business's disaster recovery and business continuity plans?
- Do the key people in the business know where to go for help with a cyber incident?
- Do all staff know who to contact in the event of a cyber incident?

CONSIDERATIONS

- The business should have prepared and agreed a cyber incident management plan well in advance of the attack. Cyber risks should have been reviewed, updated and board-level exercises undertaken.
- The cyber security operations team will have seen the first signs of the attack such as an increase in alerts indicative of a serious threat to systems.
- The immediate response should be containment of the attack on the networks and systems.
- Third-party experts should be contacted and used for help and advice. The NCSC has a list of experienced certificate incident response (CIR) companies that help their clients manage the complexities of a serious cyber incident. In addition to this, the Cyber Incident Signposting Service (CISS) should be used to inform the relevant authorities – such as law enforcement, the ICO and NCSC.
- To estimate the costs of rectifying the situation, as well as the third-party advice, businesses will need to consider payment to ransomware attackers versus the cost of ongoing operational disruption and reputational damage. The business should take advice on specific rectification costs. Recommended best practice is never to pay ransomware.

CYBER INCIDENT REPORTING

Businesses may be required to notify multiple organisations of cyber breaches as different organisations have different remits. If you're unsure who to report to, the UK government's Cyber Incident Signposting Service (CISS) provides guidance. It will navigate through several questions and identify the relevant organisation(s) that you'll need to inform and any time limits to notify breaches.

An incident can be reported directly to the NCSC using its 'Report a Cyber Incident' form and takes approximately 15 minutes. This should be used if the business is alerting the NCSC for information only, or requires technical assistance. A report should be made if the incident affects:

- data on employees, customers or suppliers;
- the organisation's computer firmware, software or hardware;
- personal data of the UK, Channel Islands or Isle of Man.

The report should detail the business, the basics of the incident and its impact, along with the attack identifiers. Cyber security incidents that are reported using this form are monitored 24/7 by a NCSC Defence Watch officer, who will endeavour to reply at the earliest opportunity.

Businesses will need to balance resources needed for information gathering and for stopping or containing a breach.

FURTHER INFORMATION

Developing your IR plan

www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes/developing-your-plan

Report a Cyber Incident

report.ncsc.gov.uk

INCIDENT RESPONSE

If a business suffers a cyber attack, it is crucial to respond swiftly and effectively to minimise damage and prevent further compromise. This applies in the normal course of business, and if it is in the midst of a transaction. Signs that a system is suffering a cyber attack include:

- computers running slowly;
- users being locked out of their accounts;
- users being unable to access documents;
- messages demanding a ransom for the release of files;
- people receiving strange emails from outside of their domain;
- redirected internet searches;
- requests for unauthorised payments; and
- unusual account activity.

Individuals witnessing any such activity should contact the relevant personnel and seek advice as to specific actions they should take.

KEY ACTIONS INCLUDE:

- **Isolate and contain**: As soon as an attack is detected the affected system should be isolated from the network to prevent the attacker from moving laterally and causing more damage.
- **Notify relevant personnel**: The IT team, security personnel and senior management should be informed about the attack. Clear lines of communication should be established for ongoing updates.
- **Engage the incident response team**: If there is an incident response team or a third-party cyber security firm, they should be engaged immediately. They can guide the business through the response process and help it make informed decisions.
- **Preserve evidence**: Any potential evidence related to the attack should be preserved. This might be crucial for identifying the attacker and for potential legal actions.
- **Assess the impact**: The extent of the attack and what data or systems have been compromised should be determined. This will guide the response efforts.
- **Notify law enforcement**: If sensitive data or customer information has been compromised, data protection regulators should be notified as appropriate.
- **Notify affected parties**: If customer data has been compromised, affected individuals may need to be notified. The requirement to notify may vary depending on the industry and jurisdiction.
- **Patch vulnerabilities**: The vulnerabilities that allowed the attack should be identified and patched. This could involve updating software, changing configurations, or implementing security patches.
- **Change credentials**: Passwords and access credentials for affected systems and accounts should be changed. This helps prevent further unauthorised access.
- **Monitor and analyse**: Systems should be continuously monitored for any signs of ongoing malicious activity. The attack should be analysed to understand the tactics, techniques and procedures used by the attacker.
- **Legal and regulatory compliance**: Ensure that the business complies with any legal and regulatory requirements related to data breaches and cyber attacks.
- **Implement remediation measures**: Based on analysis, necessary remediation measures should be implemented to close security gaps and prevent similar attacks in the future.
- **Improve security maturity**: The incident should be used as an opportunity to assess and improve the business's overall security maturity. This might involve re-evaluating security policies, employee training and technology infrastructure.
- **Update stakeholders**: The business should keep employees, customers, partners and stakeholders informed about the situation, its response efforts and any changes they might need to make at their end.
- **Communication strateg**y: A communication strategy should be developed to manage public relations and maintain trust with customers, partners and other parties to a deal.
- **Learn and adapt**: Once the incident is resolved, a thorough post-incident review should be conducted. What worked well and what could be improved should be identified and the lessons used to enhance the incident response plan.
- **Employee training**: Employees should be trained on cyber security best practices to prevent future attacks. Employees are often the first line of defence.

INSURANCE

WHAT IS COVERED?

Cyber insurance is important cover for most businesses now, and specifically during any deal process. It will typically cover direct losses resulting from damage to, or loss of information from, a business's IT systems and networks following a cyber attack. The losses might be direct financial theft, or the costs resulting from a theft of data, or damaged systems.

It may also cover liabilities and costs relating to third parties as a result of a cyber attack such as investigation and defence costs, civil damages and compensation payments to affected parties. Generally, it will cover much of the cost of assistance and recovery of systems after a cyber attack.

How can insurance help a business when it comes to cyber security?

Ahead of any incidents, insurers will usually offer businesses access to specialist advice to assist with cyber security risk management, which will reduce the chance of cyber incidents taking place.

What cyber insurance cover might be available?

A cyber insurance policy will usually cover the costs of dealing with any security breach, subject to terms and conditions. Costs may include notifying customers of the attack, hiring resources to deal with customer enquiries, public relations advice, IT forensics, legal fees or advice on responding to regulatory bodies.

Insurers will offer forensic or post-incident support. These specialists will assess IT systems, identify the source of any breach and suggest preventative measures. They will also advise on the legal and regulatory requirements, and how best to notify customers of any data breach.

Cyber extortion cover will protect a business in the event of a malicious attack, where the cyber attacker seeks a fee, having taken control of operational or personal data. It typically covers a reimbursement of the ransom amount and any consultant's fees related to the negotiation and transfer of funds. This cover is particularly relevant to businesses that operate online, and are vulnerable to ransomware. Before any ransom is paid, the incident should be reported to the police and discussed with the business's insurer so that any conditions of reimbursement are met, where possible.

NCSC recommends that ransoms are not paid. Businesses should consult with their advisers for the best approach to their particular circumstances and check the NCSC website for the latest guidance on dealing with ransoms.

Cyber insurance can also cover damage to digital assets. This is particularly important to businesses that rely on online sales or on automated manufacturing systems for instance.

Insurance for business interruption will cover lost profits during any interruption, which may be caused by the increased cost of conducting business after the incident, and before normal service is resumed.

What will cyber insurance not cover?

The policy will state which jurisdictions it covers and those that are excluded. It will often apply in the UK and EU, while North America is often excluded.

A policy is unlikely to cover claims from employees or contractors for the loss of their personal information following a data breach. It will not cover damage to physical property or bodily injury as a result of a cyber incident.

Losses because of the failure of critical national infrastructure, such as electricity, gas, water, satellite or telecommunications, will be excluded. Just as war and terrorism are excluded because the size of the risk is so much bigger than the capacity of any individual insurer, so too is cyber warfare now. Any policy will not cover criminal, civil or regulatory fines, penalties or sanctions. And finally, cyber insurance will not cover incompetence.

QUESTIONS

- Does the target have cyber insurance?
- If not, why not? Is it uninsurable for cyber? Why?
- If it is insured, what exactly does the policy cover and what is excluded? What jurisdictions are included?
- Does the policy include coverage for cyber incidents that may arise during the merger or acquisition process?
- How expensive is the cyber insurance cover?
- What is the renewal date?
- How is the policy affected by a change of ownership? What is the period for transition of the policy?

APPLYING FOR CYBER INSURANCE

Insurers will ask tailored questions pertinent to a particular business. A business should take care answering, and ensure the answers reflect the reality of the cyber security being practiced in the business as accurately as possible.

The insurer will provide an extensive list of requirements for best practice. It will detail the approach an organisation should already be taking for cyber security.

- Does the business carry out monitoring inspection?
- Is there a detailed cyber security policy?
- Are staff fully aware of that policy?
- Does the business regularly carry out staff awareness training around cyber?

The insurer's list of best practice requirements is intentionally extensive and exhaustive. Management should thoroughly review policy terms, coverage details and exclusions. Insurers are extremely explicit in what is covered and what is not. There will typically be a clause underpinning the policy stating that if they carry out an investigation and find the company is at fault or it didn't have sufficient compensating controls, the company will be held liable and the insurance will be void.

In practice, this is no different to any other insurance, and highlights the importance of senior management understanding and implementing cyber security protocols within their business.

FURTHER INFORMATION

Cyber insurance guidance

www.ncsc.gov.uk/guidance/cyber-insurance-guidance

WHAT PRICE COVER?

Despite a greater number of organisations taking out cyber insurance, the growth in demand along with the costs of remediation have outpaced the supply of insurance coverage and driven up premiums.

Cyber insurance as a product is relatively young, and the nature of cyber attacks and the potential financial impacts continue to evolve. Insurers are still gathering information to understand the issue. Increasing financial losses are a result of more sophisticated and frequent attacks, which are becoming more ambitious in scale. The greater complexity of cyber attacks has meant recovery costs have gone up. The costs of a cyber attack can also go beyond its obvious stakeholders.

The cost of cyber insurance depends on many factors, including the size and type of business, the sector it is in, how central technology is to the core activities of the business, the risk profile of the company and any third-party service providers, its claims history and the level of coverage required.

Private equity or trade?

For most large private equity firms looking to invest in a business, cyber insurance has become non-negotiable. That can prove challenging for some companies, because they may have self-insured for cyber previously, either because management assessed the cost as prohibitively expensive, or because the business was unable to get cover.

Private equity will certainly be nervous about investing in a business that does not have cyber insurance cover and will first want to test the water to see that the company is cyber insurable.

Because cyber insurance can prove expensive, many businesses are self-insuring, taking the money they would typically wish to be paying for a cyber insurance premium and putting it into a 'managed defence and response' plan – a proactive approach to defending against and detecting potential cyber attacks and compromises. For private equity to support such a self-insured approach, the business would need the level of cyber security control that would enable a third-party insurer to offer it a policy.

Trade buyers might take a similar approach, or seek to bring the acquired business into its own policy. However, the acquisition target will have to have the same level of cyber security controls as the acquirer or premiums could rise disproportionately.

Regulatory developments such as in the EU, the UK and the US, have increased the cost of compliance and size of potential fines, making a stronger business case for cyber insurance.

Of course, remedial cyber security actions can mitigate cyber risks and the cost of cyber insurance.

FURTHER INFORMATION

Five ways to recognise social engineering blog.knowbe4.com/five-signs-of-social-engineering

Cyber security: Practical tips for protecting your organisation online www.ncsc.gov.uk/files/NCSC_SME%20Cards.pdf

ICO Ransomware and data protection compliance ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/security/ransomware-and-data-protection-compliance/#scenario-7

OTHER LINKS

https://www.ncsc.gov.uk/section/products-services/cyber-essentials

https://www.ncsc.gov.uk/collection/risk-management

ACKNOWLEDGEMENTS

We are grateful to the following who generously contributed their and their organisations' time and insights to develop this guidance:

Adam Avards, UK Finance

Ankit Pandey, PwC

Carlton Lloyd Cristie, LSEG

Charlotte Devlin, Grant Thornton

Ciaran Harris, BVCA

David Petrie, ICAEW

Elizabeth Huthman, KPMG

Esther Mallowah, ICAEW

Ian Waterworth, AFME

James Arthur, Grant Thornton

James Rashleigh, PwC

Jamie Iles, Deloitte

Janis Wong, The Law Society

Jason Gottschalk, BDO

Josh M, NCSC

Katerina Joannou, ICAEW

Luke Hebbes, LSEG

Lyn Webb, EY

Marc Mullen, *Corporate Financier* magazine

Marcus Corry, AFME

Mark K1, NCSC

Martin Davies, The Law Society

Naresh Aggarwal, ACT

Ros Gray, The Takeover Panel

Sarah Boyce, ACT

Susan Sharawi, Deloitte

Yvette Allen, Deloitte

ABOUT ICAEW

Chartered accountants are talented, ethical and committed professionals. ICAEW represents more than 202,450 members and students around the world. All of the top 100 global brands employ ICAEW Chartered Accountants.*

Founded in 1880, ICAEW has a long history of serving the public interest and we continue to work with governments, regulators and business leaders globally. And, as a world-leading improvement regulator, we supervise and monitor around 12,000 firms, holding them, and all ICAEW members and students, to the highest standards of professional competency and conduct.

We promote inclusivity, diversity and fairness and we give talented professionals the skills and values they need to build resilient businesses, economies and societies, while ensuring our planet's resources are managed sustainably.

ICAEW is the first major professional body to be carbon neutral, demonstrating our commitment to tackle climate change and supporting UN Sustainable Development Goal 13.

ICAEW is a founding member of Chartered Accountants Worldwide (CAW), a global family that connects over 1.8m chartered accountants and students in more than 190 countries. Together, we support, develop and promote the role of chartered accountants as trusted business leaders, difference makers and advisers.

We believe that chartered accountancy can be a force for positive change. By sharing our insight, expertise and understanding we can help to create sustainable economies and a better future for all.

charteredaccountantsworldwide.com
globalaccountingalliance.com

ICAEW
Chartered Accountants' Hall
Moorgate Place
London
EC2R 6EA UK

T +44 (0)20 7920 8100
E generalenquiries@icaew.com
icaew.com

* includes parent companies. Source: ICAEW member data March 2023, Interbrand, Best Global Brands 2022

ABOUT THE CORPORATE FINANCE FACULTY

The Corporate Finance Faculty is ICAEW's centre of professional expertise in corporate finance. It contributes to policy development and responds to consultations by international organisations, governments, regulators and other professional bodies. It provides a wide range of services, information, guidance, events and media to its members, including its highly regarded magazine Corporate Financier and its popular series of best-practice guidelines.

The three major themes for the faculty's initiatives are: Global Investment and M&A; Innovation and Sustainable Recovery; and Future Advisory Professionals.

The faculty's international network includes member organisations and individuals from major professional services groups, specialist advisory firms, companies, banks and alternative lenders, private equity, venture capital, law firms, brokers, consultants, policy-makers and academic experts. More than 40% of the faculty's members are from beyond ICAEW.

T +44 (0)20 7920 8902
E cff@icaew.com

Chartered Accountants Worldwide
Member

Global Accounting Alliance

ICAEW is carbon neutral