



CORPORATE
FINANCE
FACULTY



HM Government

CYBER-SECURITY IN CORPORATE FINANCE



LEADING TREASURY
PROFESSIONALS

afme/



The Law Society



London
Stock Exchange



ACKNOWLEDGEMENTS

It is becoming more important by the day to ensure that businesses, advisers, investors, regulators and other stakeholders understand the threat to cyber-security. This is vital in corporate finance transactions, which are a major area of economic activity and source of entrepreneurship, innovation, expansion and growth for companies.

This publication will help not only to raise awareness of the cyber-security risks that businesses face, but also show how they can – with expert help – begin to tackle those risks when they are raising finance, undertaking M&A and restructuring.

On behalf of ICAEW, I would like to thank the many organisations and individuals who have contributed to *Cyber-Security in Corporate Finance*, including:

- Association of Corporate Treasurers
- Association for Financial Markets in Europe
- British Private Equity & Venture Capital Association
- Cabinet Office
- Confederation of British Industry
- Deloitte
- EY
- KPMG
- The Law Society
- London Stock Exchange
- PricewaterhouseCoopers
- The Takeover Panel

I would also like to thank my colleagues in ICAEW who have shown the initiative to bring these important organisations together and coordinate this very important contribution to public awareness.



David Petrie
Head of Corporate Finance, ICAEW

ENDORSEMENTS

The Confederation of British Industry (CBI) has reviewed the suggestions and practices within this publication and fully supports the publication's objectives.

CONTENTS

FOREWORD	01
INTRODUCTION	03
PURPOSE OF THIS PUBLICATION	04
MANAGING CYBER-RISK IN CORPORATE FINANCE	09
INCIDENT MANAGEMENT	22
CONCLUSION	23
ANNEX 1 PARTIES INVOLVED IN A TRANSACTION	24
ANNEX 2 RESOURCES FOR CYBER-HYGIENE	26
ANNEX 3 FURTHER INFORMATION AND ADVICE	28

ISBN 978-0-85760-917-5

Copyright © ICAEW 2014

All rights reserved. If you want to reproduce or redistribute any of the material in this publication, you should first get ICAEW's permission in writing. The Taskforce is not liable for any damages arising in contract, tort or otherwise from the use of any material in this publication, or from any action or decision taken as a result of using this publication. This publication comprises the Taskforce's views; they do not constitute legal or other professional advice. You should consult your professional adviser for legal or other advice.

FOREWORD

I welcome this important publication on cyber-security in the context of corporate finance transactions.

Corporate finance transactions are an important and vibrant element of the economy. They bring together expertise from a range of professions and help to create value across many sectors.

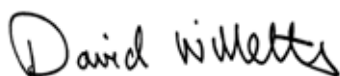
The very features of a corporate finance transaction that help to create this value – the involvement of different professional advisers and financiers, the multiple flows of information and data – also create vulnerabilities that can be exploited. As this publication notes, sharing so much information so widely, above and beyond the daily course of business, presents a real challenge. Cyber attacks are a threat to all businesses today. Indeed the Director of GCHQ, Sir Iain Lobban, reports that Britain is experiencing ‘industrial espionage on an industrial scale.’

Corporate finance transactions are potentially attractive sources of information to a range of parties: commercial data, IP information and sensitive client data may all be involved. All businesses involved in corporate finance need therefore to be aware of these cyber-risks, and of what they can do to help protect their data, their clients and their reputation.

This publication offers practical steps that those involved in corporate finance transactions can take to protect themselves from cyber-risks. It builds on approaches to risk management already undertaken in corporate finance, including a focus on due diligence. It is aimed at the corporate finance community, the wide range of finance houses and professional advisers typically involved in a corporate finance transaction. It also aims to help companies that are seeking to raise capital in some way.

The publication offers some sensible questions that those involved in a transaction should ask, and offers straightforward measures that all parties can adopt to protect their transactions, their data and their company.

I thank ICAEW and all the Taskforce members for developing this publication, and encourage readers to follow the very valuable steps that it suggests.



David Willetts
Minister of State for Universities and Science

January 2014



WHAT WE **DO** KNOW

**CYBER-RISK IS
A BUSINESS RISK
THAT MUST
BE MANAGED
WITHIN AN
OVERALL
INFORMATION
AND RISK-
MANAGEMENT
FRAMEWORK.**

INTRODUCTION

Cyber-security is widely recognised as a challenge for governments and businesses alike. It was once considered the sole preserve of IT departments and security professionals but companies now recognise that a wider response is required. Company boards are putting it on their agenda, seeing cyber-risk not as a technology risk, but as a strategic, enterprise-wide risk.

The reason for this is cyber-risk is a business risk – and like any business risk, it needs to be managed appropriately, in this case within an overall information and risk-management framework.

For anyone involved in corporate finance transactions, **cyber-security needs to be treated as a high priority**. The large volumes of information shared in the process of completing a transaction and the number of people involved in every stage of a transaction are greater than in the course of ‘normal’, business-as-usual operations. These factors heighten the risk of cyber-attack, the compromise of a firm’s networks, systems and data. At the same time, corporate finance transactions can involve types of information that are potentially very attractive to cyber criminals, competitors or counterparties in a transaction. Examples might be:

- the intellectual property (IP) data held by a car designer about to be acquired by a competitor;
- the law firm that holds the financial data of a FTSE100 company seeking to re-finance a loan; or
- the contract details of a consumer goods company, seeking finance to enter a new market.

As custodians of 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 deep seam of information waiting to be mined. It is important to guard against over-confidence within circles of trust and question whether all information should be shared with all parties. In addition, a weak link in the security of any of the parties involved, whether internal or external, can easily be exploited by those with malicious intent.

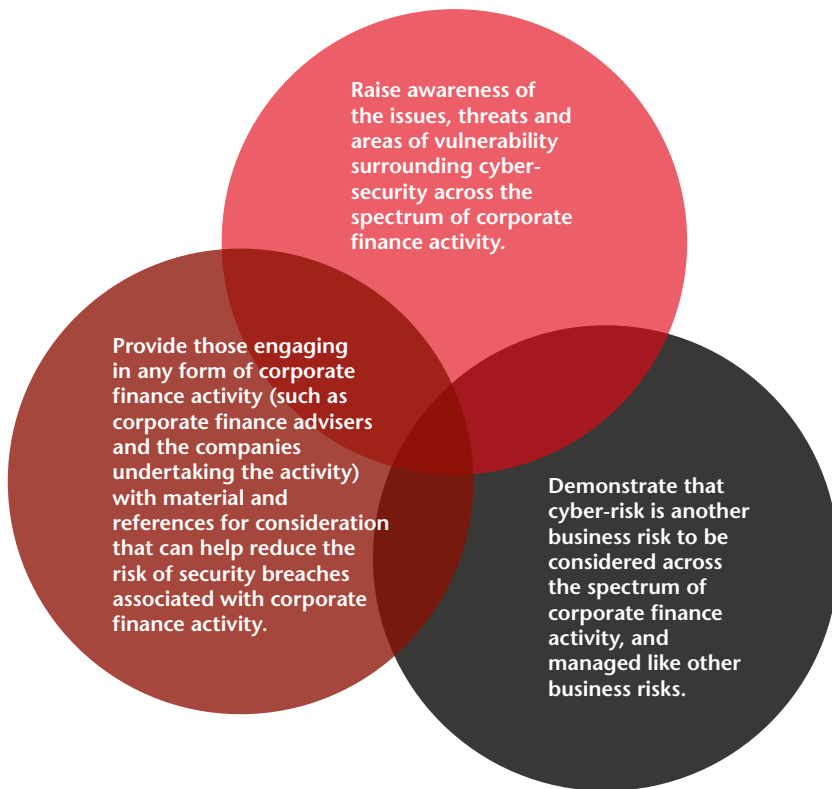
Although cyber-risk may appear as a ‘new’ risk for the corporate finance community, the consequences of this risk materialising are well established: damage to a firm’s reputation; loss of clients; financial loss; disruption to business operations. These are just some of the possible consequences. **The corporate finance community as a whole and individual firms cannot afford to ignore the threat.**

PURPOSE OF THIS PUBLICATION

RAISING AWARENESS AND REDUCING RISK

This publication is designed to help the corporate finance community take proportionate steps to manage cyber-risk. It signposts where you can get help on technical measures, but is focused on how you can manage cyber-risk as a business risk; the questions to ask those involved and the steps that you should think about taking yourself.

This publication is intended to:




This publication brings together examples of good practice within the current framework so that the risk of cyber-compromises can be considered together with other business risks. They may be used as a basis for discussion about the risk of cyber-attack in a corporate finance setting. It is not intended to establish mandatory norms for managing cyber-risk or to provide a statement of practices that are required under existing law and regulation.

Many of the suggestions are already being adopted by organisations as good information management practice. Not all will be relevant in every situation – one size does not fit all companies, business models or transactions. Rather, they form a useful reference tool for the purposes of implementing informed cyber-risk management in the context of corporate finance activity.

WHAT DO WE MEAN BY CORPORATE FINANCE AND THE CORPORATE FINANCE COMMUNITY?

For the purpose of this publication, corporate finance transactions are those where an organisation's capital structure may be changed to develop, acquire or dispose of elements of that business.

This will include refinancing and substitution of existing capital structures. Those involved or participating in corporate finance transactions will include advisers, company management, corporate treasurers, financial institutions and investors (for a list of typical participants see Annex 1). For the purpose of this publication the range of participants is referred to as the corporate finance community.

A photograph of two wolves in a snowy field. One wolf is in the foreground, looking towards the right, and another is behind it, also looking right. The background is a bright, snowy landscape.

**THE THREATS
COME FROM A
CONTINUOUSLY
CHANGING RANGE
OF SOURCES,
INCLUDING, BUT
NOT LIMITED TO:**

INDIVIDUALS

who understand the value of sensitive data that they can sell on to interested parties in a transaction.

**ORGANISED
CRIME NETWORKS**

that see cyber-crime as a low-risk, high-return activity seeking, for example, stock exchange gains after obtaining information before transactions are officially announced.

COMPETITORS

looking to gain advantage in deal negotiations or spotting an opportunity to access confidential information or pricing data, given the information exchange that occurs during a transaction, or providing a potential client with a better proposition.

NATION STATES

by way of state-backed or state-sponsored attacks on international transactions. They pose a threat because national governments may seek to sabotage deals and protect and enhance the interests of local companies or to give their own industries an advantage. This is particularly prevalent in deals involving assets or industries considered to be of national strategic importance, although all sectors are at risk.

HACKTIVISTS

driven by political/moral opposition to a particular company, deal or transaction, who might then make an attempt at sabotage.

EMPLOYEES OR CONTRACTORS

who act with a lack of care or whose errors increase the risk of compromise. In addition, some employees or contractors may be either disgruntled for some reason or specifically planted by an organisation looking to gain access to sensitive information.





WHAT WE **DO** KNOW

**TRANSACTIONS ARE
A PRIME TARGET.
COMPANIES'
SYSTEMS HAVE
BEEN HACKED OR
COMPROMISED AT
THE TIME OF AN
IMPENDING DEAL.**

MANAGING CYBER-RISK IN CORPORATE FINANCE

Corporate finance activity involves heightened cyber-risk: the sheer number of people involved in each phase of the process and the volume of information that is shared between the parties in the context of a transaction bring with them a substantial risk of compromise to companies, their advisers, financiers and/or investors.

TRANSACTIONS ARE A PRIME TARGET

CASE STUDY 1

An international manufacturer with a large and highly-skilled UK workforce was targeted during a period of challenging negotiation with a foreign government. The initial compromise was probably by a common form of attack such as a spear-phishing email, well-crafted to appear legitimate. These emails are often sent to many hundreds of employees, but only need to fool one person to gain an initial foothold on a network. In this example, the adversary quickly used that foothold to gain persistent access to the entire network. Poor network architecture enabled them to access the accounts of the company's entire senior leadership team for months – the months when they were engaged in those sensitive negotiations.

CASE STUDY 2

During a merger and acquisition, a major FTSE350 company which was an exemplar of good cyber-security practice had taken over a small business, and thus inherited the very poor state of that company's network security. It suffered a sustained compromise, and the investigation identified that the adversary had unfettered access to the whole network. For a period of over a year, the adversary was responsible for a significant portion of all network traffic, and stole data related to new technology.

CASE STUDY 3

Following a period during which multiple acquisitions were made by a FTSE350 services company, a sophisticated intrusion was discovered that impacted the confidentiality of email communications and customers' data. Due to the hurried way in which business and ICT systems were integrated during the acquisitions, it was extremely difficult for the company to respond to the intrusion effectively as a result of the lack of information available to the response team. Further to this, the acquired systems provided additional routes for the attacker to gain access to the network without raising the alarm.

CASE STUDY 4

A large energy company attempting to enter a new market in a developing nation bid for a high-value project against multiple international competitors. During the bidding process they discovered malware had infected the system of a key employee who was instrumental to the negotiations. It became apparent that their negotiating position had been compromised and it was therefore necessary for the company to take steps to adjust their position and to defend their networks against repeated attacks.

Case study source: UK Government

PREPARATION

Even before an organisation has decided to push the button on a corporate finance transaction, senior management will be starting to gather valuable information from a number of parties to make an informed decision on how best to proceed. Preparation will often include incumbent advisers to the company and/or strategy advisers appointed for this purpose. The very act of putting this information together may alert others that a transaction is imminent if information regarding this transaction is not secured; ie, if systems and processes are not appropriately managed.

QUESTIONS

How can you avoid alerting insiders at this stage that you are considering a transaction?

Which individuals will have access to the information you are gathering? Do you have well-defined internal roles?

How can you avoid alerting outsiders to the possibility of a transaction?

What kinds of agreements do you have with service providers? Are your non-disclosure agreements with service providers up to date and do they include any reference to the security of information held and disseminated by them?

What is your information-risk appetite?

Where are the key information risks in the transaction for your organisation? Which security measures are both proportionate to managing these risks and unlikely to hamper the transaction process unnecessarily? Can you prioritise the most sensitive information to focus security measures on this? Are there information risks that might for some reason be difficult to manage? Are you comfortable with the risk this entails?

Is there someone in the organisation that might understand the risks involved better than you?

Could you ask them for any advice on security? Might there be someone with better intelligence than you on potential threats?

How can you start setting up the right systems that will work securely throughout a potential transaction?

What measures or procedures can you start putting in place so that if a transaction proceeds, cyber-security is appropriately managed across all the phases?

SUGGESTIONS

Limit the number of individuals you bring inside during Phase 1 as far as is practicable.

For companies considering their strategy, perhaps only senior management, incumbent advisers and, if applicable, strategy advisers should be aware of the process.

Map out information and process flows where practicable. Consider whether you might need different/separate data stores from the usual IT system.

Consider appointing an independent IT team to monitor activity around the information you are gathering.

Review current working practices.

Foster a culture of secure information management and incident reporting.

Think about how diaries and meetings are planned and communicated.

Think about your social media profile throughout the transaction and beyond.

Consider if your current profile increases the risk of spear phishing (see Annex 2).

PHASE 1
Preparation

PHASE 2
Engaging, selecting and
appointing external advisers

PHASE 3
Initial approaches

PHASE 4
Preparing information
about the business

PHASE 5
Financing terms
of transaction

PHASE 6
Completion

WHAT WE **DO** KNOW

THE VERY ACT
OF PUTTING THIS
INFORMATION
TOGETHER MAY
ALERT OTHERS THAT
A TRANSACTION
IS IMMINENT IF
INFORMATION
REGARDING THIS
TRANSACTION IS
NOT SECURED.

ENGAGING, SELECTING AND APPOINTING EXTERNAL ADVISERS

Once a decision has been reached to proceed with a transaction, external advisers may be appointed. This stage will start to involve the sharing of information that is additional to that shared during the normal course of business.

One of the key issues to bear in mind here is that many of these parties may not at this stage have a formal contract with the company. Information sharing needs to be carefully and thoughtfully managed to ensure that potential advisers are clear about what is confidential. All parties should be considering who within their organisations should have access to shared information.

QUESTIONS

Who are you sharing your information with and on what basis?

Should there be a small circle of named individuals responsible for managing the information in each of the organisations you are sharing with?

What information is being shared?

How much detail do you need to provide at this stage? How is information security being monitored?

Do there need to be formal agreements about how the information is shared and used?

Do all parties need to demonstrate that they understand their respective responsibilities in managing, using and sharing the data? For example, what is the policy regarding use of personal email addresses?

Do you have adequate monitoring systems in place?

How would you know if you or other parties in a transaction were being attacked or infiltrated?

What would you do if any of the parties involved were the subject of a cyber-attack?

How would you respond? How might you expect others in the information chain to respond?

SUGGESTIONS

Update information and process maps.

Companies and any advisers involved in this phase could keep records of who within their organisations has the information. Where practicable, a need-to-know 'list' could be kept by the information owner.

If practicable, one individual within each organisation could be responsible for the security of information being shared.

Ask which information security standards (if any) the other parties comply with. It is important to establish shared principles for governance of information security. Provided that there is no legal or regulatory requirement to do otherwise, it is generally appropriate to rely on the representations of companies, advisers and agents involved in a transaction that adequate and suitable systems are in place.

Think about due diligence procedures.

Consider resolving any concerns with the company involved about cyber-security arising from the due diligence.

Ask for clarity from the potential issuer/bidder about which information is confidential and/or sensitive.

Find out whether the company believes there is a potential heightened cyber-security risk in any given transaction – senior management may be aware of specific attacks within their industry, for example.

Where appropriate, put in place an incident response plan (see Incident management section).

PHASE 1
Preparation

PHASE 2
Engaging, selecting and
appointing external advisers

PHASE 3
Initial approaches

PHASE 4
Preparing information
about the business

PHASE 5
Financing terms
of transaction

PHASE 6
Completion

LEGAL FRAMEWORK

Organisations should consider applicable legal and regulatory frameworks, especially those regarding risk identification and management obligations. Some of these arise from generic duties to act in the best interests of that organisation. Other obligations apply to particular types of information. Data protection legislation requires organisations to use appropriate technical and organisational measures to protect personal information and those that fail to do so may be subject to regulatory enforcement.

In the UK, the FSA (now FCA) publication *Market Watch 27* on handling inside information contains suggested good practices on what organisations holding sensitive information (regardless of whether it is insider information) might consider as part of their information management processes. (See www.fsa.gov.uk/pubs/newsletters/mw_newsletter27.pdf for more detailed suggestions.) If inside information is involved, even more care will be required although in most corporate finance transactions it is normally (but not always) the transaction itself that is inside information, along with other inside information that may be exchanged as part of it.

Additional security obligations apply to some sectors, such as the telecoms sector, which is now subject to an obligation to report breaches to the relevant regulatory authority and, in some cases, the affected individuals. Equally, organisations in the financial sector are subject to an obligation to organise and control their affairs responsibly and effectively, with adequate risk-management systems, which includes taking appropriate steps to protect themselves against cyber-attack. (See www.fsa.gov.uk/pubs/other/data_security.pdf for further details.)

INITIAL APPROACHES

Once advisers have been appointed, the next phase will generally involve making initial approaches to, for example, target companies, investors, acquirers, private equity houses, venture capital funds, angel investors, funding institutions, etc. More parties will become involved including, in some cases, competitors.

Sound, appropriate and proportionate information management, with proper regard for security of your own information and that of clients becomes ever more important at this and the following stages. Not only is information starting to be shared with still more parties, but the nature of that information is becoming more commercially sensitive.

QUESTIONS

How will you provide information to the various parties in the transaction?

What can you do to for reassurance that they will handle the information securely? Is certain information so sensitive that it should be provided in a secure environment and in a secure format – for example, in paper in an adviser's office?

What information will you provide?

How will you balance the need to provide adequate information with the need to protect sensitive data? Is certain information so sensitive that it should be held back as late as possible?

What is the risk profile of the sector or country you are dealing with?

Has the sector or industry been subject to cyber-attack in the past? Could the sector's activities be viewed as controversial for any reason and therefore at higher risk of attack? Are you considering a transaction involving, for example, assets of strategic importance to a particular country? How are you selecting your intelligence sources?

Have you considered the local regulatory norms?

Are some of the usual security measures, such as encryption, allowed in the jurisdictions included in the transaction?

WHAT WE DO KNOW

ONGOING MONITORING OF ACCESS TO INFORMATION CAN HELP TO HIGHLIGHT SUSPICIOUS ACTIVITY AT THE EARLIEST STAGE POSSIBLE.

SUGGESTIONS

Limit the number of people receiving information as far as is practicable.

Consider the 'need-to-know' principle in a cyber-security context.

If practicable, consider sharing information via a secure data store that is separate from the organisation's usual IT systems or mobile devices.

For example, one large company executing a joint venture overseas set up an entirely separate system for the purposes of agreeing the deal and sharing only the required information. This protected valuable IP on both sides. However, depending on the nature of the system, this can be a costly solution, particularly as it requires separate monitoring. Consider whether the risk merits this approach. When travelling, consider using mobile devices that are password-protected and have appropriate security software. Ensure these are checked on return.

Obtain relevant approval before disclosing confidential information to another party.

While this is simply good practice, it is worth reiterating in a cyber-context. There may be specific reasons that you don't know about that present a cyber-risk to others, such as knowledge of a previous attack.

Obtain confidentiality agreements with all parties.

These will include agreements about what information will be shared, with whom and how it will be used, and should cover cyber-security practice. Consider also which information is necessary for the transaction and avoid sharing more than this.

Understand which security measures are/are not possible.

For example, some states do not allow information to be encrypted without the encryption keys being provided to certain authorities.

Continue to monitor access to information.

Ongoing monitoring of access to information can help to highlight suspicious activity at the earliest stage possible. It may be appropriate to consider an internal review or third-party cyber-security health check on your infrastructure.

PREPARING INFORMATION ABOUT THE BUSINESS

By this stage there will already have been a large number of parties contacted in relation to a transaction and many of these may already have access to some sensitive information. However, it is at this point that increasingly large volumes of information start to be shared with the various participants, such as disclosure documents, information memoranda, prospectuses, vendor due diligence packs and information for relevant regulators. The flurry of activity associated with this may well alert others inside and outside the organisations that a transaction is underway. There is also the heightened risk inherent in large quantities of valuable information being stored or circulated, some of it potentially highly sensitive if accessed by the wrong people.

Consider also the fact that security breaches at this stage might not affect just your organisation and that of your clients, but also suppliers, customers and markets, given the type of information that would need to be gathered for the preparation of these documents.

QUESTIONS

What information really needs to be included in the various types of documentation?

Are you including more than is really necessary and beyond what is required by relevant regulatory and legal frameworks?
Can you cut down the information you widely circulate?

Who will be receiving the documents and how will they be receiving them?

Can you tailor the information or the means by which it is provided, according to the risk profile of each recipient or type of recipient?

Are you protecting the data you have on customers/suppliers, etc?

Do you need authority from the data owner to disclose the information you are providing and in the form you are disclosing it?

SUGGESTIONS

Consider providing information in a different format, depending on the risk profile of the recipient, as long as you provide the information required by relevant regulatory and legal frameworks.

Electronic communication may not be appropriate for some parties if you consider them to have a high risk of cyber-security breaches (or any leak, for that matter). Where practicable, think about alternative means of providing the information, such as inviting them to access information on a separate, monitored data store or even in paper format that should be returned on completion of the transaction.

Manage the risk of over-disclosure.

This is good information management practice in any case, but particularly pertinent in a cyber-context.

PHASE 1
Preparation

PHASE 2
Engaging, selecting and
appointing external advisers

PHASE 3
Initial approaches

PHASE 4
Preparing information
about the business

PHASE 5
Financing terms
of transaction

PHASE 6
Completion

DUE DILIGENCE ON CYBER-SECURITY

Those engaging in corporate finance activities can ask some simple questions about the cyber-security of a target as part of a due diligence exercise. These are not limited to, but may include:

- When did the board last consider cyber-security?
- Who is ultimately responsible for managing cyber-security in the company?
- Has the company audited itself against the *10 Steps to Cyber-security* (see Annex 3)?
- 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 steps did they take to mitigate the impact of this breach?

FINANCING TERMS OF TRANSACTION

By now, the transaction has proceeded to an advanced stage. Many of the risks already outlined will apply here. However, the level of detail will increase and the nature of the information being shared is likely to be of a highly sensitive nature. For example, there are risks faced by participants such as bidders in a transaction. There are known incidents of bidders' highly sensitive information, such as bid prices and financing terms, being intercepted by rival bidders in a transaction even before any bid has been submitted. This is clearly damaging to the bidder and could put the transaction in jeopardy.

QUESTIONS

How high is the risk of compromise or theft at this phase?

If the transaction has so far been relatively low risk, do you need to step up some of the security measures? Do you need to consider some of the suggestions already outlined in earlier phases of the transaction?

What would be the consequences of a breach at this stage?

What would be the worst-case scenario? How would you manage this effectively? How could you mitigate the effects of such a breach?

CAVEAT EMPTOR – DUE DILIGENCE ON CYBER-SECURITY

A multinational company was the subject of a cyber-security attack. Passwords had been stolen from a number of senior executives, including the CEO. This enabled intruders to access the company's computer networks and download sensitive files including R&D information, business plans and email communications.

The attacks used deeply-embedded malware that was difficult to detect. The business subsequently ceased operations and was sold piecemeal. The buyers, many of them sophisticated businesses in the IT and communications sector, claim they had no knowledge of the breaches at the time of sale. It is unknown – publicly, at least – whether the breaches have affected the acquirers' systems. However, the likelihood of them proceeding with the deal and the purchase price they paid may well have been materially different if they had known about the attacks.

SUGGESTIONS

Think about where non-disclosure and confidentiality agreements are appropriate.

If the information you are sharing/requesting from others is open source or otherwise publicly available, these may not be necessary and may in fact hamper the progress of the transaction. Instead, it may be better practice and more feasible to concentrate on getting the necessary agreements in place with those handling information that is confidential or sensitive.

Consider whether 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, but added in by hand by a senior member of the deal team en route to the meeting.

Consider whether the information you are requesting or disclosing is beyond standard market practice.

If acquiring a business, carry out due diligence on its cyber-security measures and past record of dealing with breaches.

As the case studies on p09 highlight, many businesses and other organisations have already 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. Consider some of the issues outlined in the case studies. Many companies may not yet be following practices that meet a buyer's expectations or requirements and if so, consider what the risks might be of a past or future attack and what measures might be necessary to bring the company to a level that meets your risk appetite.

Consider putting an incident management plan in place.

If there is not a plan devised for the transaction specifically at this point, now may be the time to put one in place, particularly if the deal is high profile or considered to be sensitive (see Incident management section).

DUE DILIGENCE AND VIRTUAL DATA ROOMS

The due diligence process, possibly more than any other part of the transaction, poses high information theft and interception risk. Vast quantities of information will be gathered, collated and circulated to inform the relevant participants, such as buyers and investors, and to verify information. This could include strategic information on pricing, valuable IP, customer and supplier data and personal and financial data. While most of those involved will be well versed in handling sensitive commercial information, it is worth stressing that any weaknesses in the system or procedures followed could be exploited by those with malicious intent.

The development of virtual data rooms to provide much of the necessary information has made this part of the process more streamlined, efficient and cost-effective, but it has brought additional risk as much of the information is stored online and could therefore be vulnerable to attack. Those involved in a corporate finance transaction and considering using a virtual data room (VDR) may consider undertaking due diligence on the VDR provider to satisfy themselves that the vendor is continuously providing a secure service and has not been breached. Moreover, organisations adding information to data rooms should not only consider whether that information is secure, but also if it should be included in the data room in the first place. Here are some examples.

- Personal information should only be included in the data room if it is strictly necessary for the evaluation of the relevant corporate finance transaction.
- Third-party information. Some information might relate to a third party and the organisation might be under a duty to keep it confidential. In some cases it may be necessary to obtain the relevant third-party's consent to its inclusion in the data room.
- Staged release. In some cases, it may be appropriate to have a staged release of information, for example by providing some information only to short-listed bidders.

COMPLETION

By now there will already have been large numbers of individuals involved in the transaction. However, it may be that only during or following completion, that the transaction becomes public knowledge. If this is the case, and the transaction is sensitive or of public interest for some reason, information risk might intensify at this stage. Once a transaction is widely known, there may be a greater threat of compromise via a cyber-attack.

There will be heightened risk as funds are transferred to complete the transaction. The act of moving funds presents a risk of interception. 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 strategic papers about how they might benefit from the deal and their next steps on, for example, potential synergies, integrating a new business unit, separating a company from its parent, plans about how it will enter new markets, 100-day plans, etc. Much of this information would be highly valuable to competitors and to states looking to protect and enhance the interests of national companies.

QUESTIONS

Who will be involved in the transfer of funds and document signing?

Are there parties or individuals that have not so far been involved? How satisfied are you that information risks have been appropriately managed through the course of the transaction?

Is the transaction in the public domain?

Is there now a greater risk to the information you are sharing and storing? What measures might you practicably put in place to protect it?

What is your policy for storing sensitive information post-completion?

How will any IT systems acquired as part of the transaction be updated and checked?

Might the systems of acquired parties have been compromised?

SUGGESTIONS

Continue monitoring access to documents relating to the transaction.

It may be that, even post-transaction, the risk of intrusion remains.

Think about how any funds relating to the transaction will be moved.

Consider whether there might be any weaknesses in the systems being used for transfer and storage of funds.

Consider the need to review information management and security policies across the organisation.

Post-transaction, your organisation may be at increased threat of cyber-attack. Consider strengthening any policies or procedures if appropriate.

PHASE 1
Preparation

PHASE 2
Engaging, selecting and
appointing external advisers

PHASE 3
Initial approaches

PHASE 4
Preparing information
about the business

PHASE 5
Financing terms
of transaction

PHASE 6
Completion

WHAT WE **DO** KNOW

THE ACT OF MOVING FUNDS PRESENTS A RISK OF INTERCEPTION



INCIDENT MANAGEMENT

While the kinds of good cyber-security measures outlined in this publication will go a long way to protecting sensitive and valuable information, they cannot completely eradicate cyber-threats. If an individual or organisation is determined and motivated enough, the chances are that they will still be able to compromise security in some way. Good defences will deter many attacks, but effective cyber-resilience strategies will also include plans to reduce the impact of an attack and the time it takes to recover from it.

While many organisations may already have a cyber-attack incident management plan devised for the intrusions that occur during the normal course of business, it may be worth considering what might happen if your systems or those of other parties involved in the transaction are compromised while the transaction is underway. It may even be worthwhile putting in place an incident management plan (including lists) specifically for the transaction.

QUESTIONS

Would any existing incident management plan/crisis management plan work under this scenario?

If you already have detailed plans in place, it may be that you could adapt these to include responses to the specific threats to transactions. An incident management plan would typically include escalation procedures.

How might you contain an attack?

What steps could be taken to isolate and remove the threat? How sophisticated could your technical response be? Might you need systems and networks to be taken offline? And if so, how would that affect your organisation?

If an attack is detected, who might you need to inform?

Does a comprehensive list of interested parties exist? Depending on the nature and severity of an attack, it may be that other parties need to be informed so that they can take the appropriate precautionary measures and monitor their own systems for similar attacks.

Do you need to notify enforcement authorities?

If the incident constitutes a criminal offence, you may need to contact the police and/or other agencies to report it. The relevant authority may then need to investigate, so you may need to factor in time and resources for this. Are there cross-border implications to consider when communicating with law enforcers?

Who else might be affected by an attack on your systems?

In addition to anyone involved on the deal, you might need to consider the impact in your customers/clients, suppliers as well as your position with regulators.

How might an attack affect the transaction?

How high is the risk that an intrusion/leak might prevent the transaction from going ahead or hamper its progress? How could you ensure the transaction could still go ahead?

How should you respond publicly?

What if the attack reaches the public domain? Who would be responsible for briefing stakeholders, the media and other outside parties? What messages should they put out? Do you need public relations advisers? How should they be briefed?

What is the worst-case scenario?

What could happen if there was a serious breach? What would constitute a serious breach for you? How would that impact the business's operations and reputation? Which resources might you need to redeploy to manage the impact of such an attack? And what effect might that have on the day-to-day running of the business?

How would you resume business as usual?

What kinds of analysis and reviews would you need to take to ensure your systems are secure enough to get back to normal business operations?

CONCLUSION

CONSTANT DEVELOPMENT

No organisation is immune to the challenges posed by cyber-security. As with any risk, the key to effective management is identifying and understanding the threats, understanding the level of the risks involved and putting in place security measures that are appropriate and proportionate to those threats and risks. We hope that some of the questions and suggestions contained in this publication help you to focus your thinking and consider the different circumstances in each individual transaction.

However, it is also worth stressing that the threats are constantly evolving, according to the business model and the technical environment, and the nature, extent and means of cyber-attacks are under constant improvement. As organisations become better at protecting their valuable information, so those with malicious intent will find new ways of compromising the flow of information and data across corporate and personal networks. Those most effective at safeguarding their own and their clients' assets will be the ones that continually gather intelligence on the new threats emerging in their industries and sectors, proactively investigate breaches and review their overall risk management plans regularly to take account of these developments. Just as the threat does not remain static over time, so systems, procedures and the way business and communications are conducted will need to be constantly developing to keep pace.

In recognition of the constant development of new threats and new ways of managing these threats, the Taskforce will keep these suggestions under review and may update these in the future.

WHAT WE DO KNOW
FOR ANYONE
INVOLVED IN
CORPORATE
FINANCE
TRANSACTIONS,
CYBER-SECURITY
NEEDS TO BE
TREATED AS A
HIGH PRIORITY.

ANNEX 1

PARTIES INVOLVED IN A TRANSACTION

Who might be involved in your transaction?

There will be many different parties receiving and sending information throughout the transaction process. Listed here are some of the main parties involved in transactions in the UK and the phase in which they tend to be involved. The number and type of parties and the relevant phase will depend on the nature of the transaction and different parties may be involved in transactions in other jurisdictions.

	PHASE 1	PHASE 2	PHASE 3	PHASE 4	PHASE 5	PHASE 6
Senior management of the company executing the transaction and its incumbent advisers	●	●	●	●	●	●
Strategy advisers and consultants	●				●	●
Subsidiaries	●	●	●	●	●	●
Corporate finance advisers	●	●	●	●	●	●
Funding institutions	●	●	●	●	●	●
Senior management of any potential target or acquiring company (potentially a competitor)			●	●	●	●
Financial advisers to the company executing the transaction			●	●	●	●
Legal advisers to the company executing the transaction				●	●	●
Legal advisers to the potential target or acquiring company or companies				●	●	●
Financial advisers to the potential target or acquiring company or companies			●	●	●	
Specialist advisers eg, pensions, property, intellectual property	●	●	●	●	●	●
Tax advisers					●	●
Economic and political risk consultants					●	●
Individuals connected with personal references					●	●
Recruitment consultants					●	●
Current investors/owners of the business, if private	●	●	●	●	●	●
Analysts					●	●
Potential investors			●	●	●	●

	PHASE 1	PHASE 2	PHASE 3	PHASE 4	PHASE 5	PHASE 6
Potential funding sources eg, banks and/or debt investors			●	●	●	●
Investment banks				●	●	●
Private equity houses and their advisers			●	●	●	●
Venture capital houses and their advisers			●	●	●	●
Government departments (for example, in the case of public-private partnership transactions)			●	●	●	●
Industry regulators				●	●	●
Market regulators				●	●	●
Independent advisers to the target company in a public takeover		●	●	●	●	●
Debt advisers		●	●	●	●	●
Brokers		●	●	●	●	●
Sponsors and Key Advisers (Main Market)			●	●	●	●
Nominated Advisers (AIM)	●	●	●	●	●	●
Corporate Advisers (ISDX Growth Market)					●	●
Reporting accountants			●	●	●	●
Public relations advisers		●	●	●	●	●
Investor relations advisers		●	●	●	●	●
Accountants	●	●	●	●	●	●
Lawyers	●	●	●	●	●	●
Other lawyers to associated parties					●	●
Vendor due diligence providers				●	●	
Specialist due diligence providers (financial, technical, environmental, market, etc)					●	
Employees involved in the transfer of funds						●

ANNEX 2

RESOURCES FOR CYBER-HYGIENE

For ease of reference, we have included below some sources of good-practice guidance put together by other organisations that may help frame discussions about how an organisation manages information and follows basic cyber-hygiene practices. For information purposes, we have also included an outline of the most common means attackers use to compromise systems.

10 Steps to Cyber Security

There are some cyber-hygiene factors that all organisations need to consider at board level. The UK Government has assembled a list in *10 Steps to Cyber Security*.

Initiatives aimed at raising awareness

Many programmes across the world are now being initiated to raise awareness of the risks of cyber-attack. The UK Government has a cyber-security strategy that includes measures to improve cyber-awareness among UK citizens and businesses. In the US and the EU, similar government initiatives are also underway. In addition, many financial services and professional organisations are working towards the same aim with their members. One such initiative is currently under consultation among National Futures Association members as it believes that cyber-attacks on the financial services sector will increase over the next 18 months. The organisation has, as an interim step, issued a set of suggestions to help safeguard valuable information. These are good practice and are likely already to be followed by many organisations in any case to protect client confidentiality, but are worth reiterating.

Source: www.nfa.futures.org/news/newsletter2.HTML

Existing frameworks

There may be specific regulatory frameworks, principles and guidelines that companies and their advisers may need to adhere to or have adopted as a matter of good practice. As an example, one of these is the principles outlined in the FSA (now FCA) publication *Market Watch 27* on handling inside information. The principles provide some useful suggestions of how organisations party to sensitive information (regardless of whether it is inside information) might consider their information management processes. In particular, the principles point to some good practices about IT.

WHAT WE **DO** KNOW
THE CORPORATE
FINANCE
COMMUNITY AS
A WHOLE AND
INDIVIDUAL FIRMS
CANNOT AFFORD
TO IGNORE THE
THREAT.

Understanding how attackers get in

While IT systems are usually designed to be robust to attacks, the actions of individuals can compromise security. For example, if a store of information is password-protected, it may be considered at least reasonably secure. Yet if the access details are circulated via email, the security of that store is highly compromised as this form of communication is very easily intercepted.

Consider some of the ways in which intruders are able to access information.

Phishing and spear phishing – one of the most common means of gaining unauthorised access to an organisation's systems. A phishing attack, in simple terms, is an email designed to deceive the recipient in some way, perhaps by convincing them to reveal their password to access a particular system. Spear phishing attacks are targeted at specific individuals such as senior executives. The two main defences that an organisation can adopt to mitigate the threat posed by spear phishing are technical controls and security awareness training. Some simple questions that employees can ask when receiving an email with a suspicious link to an attachment include the following.

- Who is the sender? Can the recipient verify it has definitely come from them and is it someone from whom they would expect to receive emails on this subject?
- Is the style of writing consistent with the sender? Does anything appear unusual about the tone, spelling, or urgency of the email?
- Is the request out of the ordinary? (eg, to open a file that the recipient wasn't expecting)
- Have other colleagues received a similar email?

Spear phishing attacks are often based on information that the intended victim has posted on a social media site, such as a business networking site or personal sites. To help reduce the risk posed by spear phishing, employees (at all levels) should consider the information that they have published about themselves on a social media site, including names and addresses, date of birth, place of work, position in the organisation and area of responsibility.

Theft of physical devices (including accidental loss) – This could include laptops, mobile phones or tablets, etc. Sometimes these devices are stolen to order if there is a particular target in mind or this may be done opportunistically. The objective is to access systems or steal sensitive information. There have been incidents in which business travellers' devices have been stolen or lost and then returned, either once the information has been scanned and/or copied or with malware or similar malicious software introduced with the intention of accessing or disrupting an organisation's IT systems.

USB sticks/CD ROMs and other removable devices – These could be used to download information or to infect a system with malware.

Unauthorised access to virtual data rooms – See section on due diligence and data rooms, in Managing cyber-security on corporate finance – phase 5.

See www.cpni.gov.uk/advice/cyber for further information.

ANNEX 3

FURTHER INFORMATION AND ADVICE

Search under 'keeping the UK safe in cyberspace' in www.gov.uk to find all of the current UK Government advice and guidance on cyber-security in one place.

10 Steps to Cyber security – Executive Companion. Produced by the CESG, Cabinet Office, CPNI and BIS. Available online: www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

BIS – *Information Security Breaches Survey 2013* – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191671/bis-13-p184es-2013-information-security-breaches-survey-executive-summary.pdf

BIS – recent initiative to name a preferred organisational standard for cyber-security – <https://www.gov.uk/government/consultations/cyber-security-organisational-standards-call-for-evidence>

CESG – provides a list of accredited cyber-incident response management companies. www.cesg.gov.uk/servicecatalogue/cir/Pages/Cyber-Incident-Response-providers.aspx

CPNI – www.cpni.gov.uk. This website contains a series of guides for managers and IT professionals on good cyber-security practice, including on spear phishing: www.cpni.gov.uk/advice/cyber

EC Proposed Directive on network and information security and EU's Cyber-security plan – <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>

FSA Principles of good practice for handling inside information (now under FCA guidance) – could be relevant for other sensitive information handling. www.fsa.gov.uk/pubs/newsletters/mw_newsletter27.pdf

Get Safe Online – includes advice for business. www.getsafeonline.org/businesses/

ICAEW – icaew.com/cyber

Information Commissioner's Office – website contains guidance on the use and sharing of data, including advice on 'Bring Your Own Device' (BYOD) policies and cloud computing. www.ico.org.uk

Owasp (Open Web Application Security Project) – https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure

SEC – guidance on disclosure of cyber incidents www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

THANKS

We would like to thank the following individuals for their contributions to the Cyber-Security in Corporate Finance project:

Umerah Akram

Senior Manager, Primary Markets,
London Stock Exchange

Richard Anning

Head of IT Faculty, ICAEW

Patrick Aylmer

Finance Director, Fox Investments
& Elton John AIDS Foundation

Shaun Beaney

Manager, Corporate Finance
Faculty, ICAEW

William Buckley

Partner, Linklaters

Simon Clark

Chairman, British Private Equity
& Venture Capital Association

Hayley Conboy

Principal Policy Adviser,
Enterprise, CBI

Massimo Cotrozzi

Assistant Director, EY

Martin Donovan

Deputy Policy and Technical
Director, Association of Corporate
Treasurers

Neil Favager

Associate Director of IT
Consulting, Baker Tilly

William Ferrari

Managing Director, Equity Capital
Markets & Corporate Finance,
Association for Financial Markets
in Europe

Nick Fluck

President, Law Society

Tim Hames

Director General, British Private
Equity & Venture Capital
Association

Tim Hill

Technology Policy Adviser,
Law Society

Robert Hodgkinson

Executive Director,
Technical Strategy, ICAEW

Simon Horner

Director – Policy & Public Affairs,
British Private Equity & Venture
Capital Association

Michael Izza

Chief Executive, ICAEW

Katerina Joannou

Manager, Capital Markets Policy,
ICAEW

Jack Knight

Office Manager,
Panel on Takeovers & Mergers

Simon Lewis

Chief Executive, Association for
Financial Markets in Europe

James Lockyer

Development Director, Association
of Corporate Treasurers

Mike Maddison

Partner, Deloitte

Peter Matza

Engagement Director, Association
of Corporate Treasurers

Vicky Meek

Freelance business journalist
and editor

David Petrie

Head of Corporate Finance,
ICAEW

Alex Petsopoulos

Partner, Deloitte

Philip Robert-Tissot

Director General, Panel on
Takeovers & Mergers

Angela Teke

Managing Director, Compliance,
Association for Financial Markets
in Europe

Nick Toyas

Toyas O'Mara

Colin Tyler

Chief Executive, Association
of Corporate Treasurers

Martin Tyley

Partner, KPMG

Paul Walker

Partner, EY

Grant Waterfall

Partner, PwC

We are also grateful for the comments and advice received from representatives from the Department of Business, Innovation and Skills (BIS), Centre for the Protection of National Infrastructure (CPNI), Government Communications Headquarters (GCHQ) and the Cabinet Office and from the various committees within each of the Taskforce organisations.

THE TASKFORCE

ICAEW Corporate Finance Faculty (Coordinator) – www.icaew.com/cff

Association of Corporate Treasurers – www.treasurers.org

Association for Financial Markets in Europe – www.afme.eu

British Private Equity and Venture Capital Association – www.bvca.co.uk

Cabinet Office – www.gov.uk/government/organisations/cabinet-office

Deloitte – www.deloitte.com

EY – www.ey.com

KPMG – www.kpmg.com

The Law Society – www.lawsociety.org.uk

PricewaterhouseCoopers – www.pwc.co.uk

London Stock Exchange – www.londonstockexchange.com

The Takeover Panel – www.thetakeoverpanel.org.uk

ICAEW CORPORATE FINANCE FACULTY

The Corporate Finance Faculty's professional network includes 6,000 members and more than 70 member organisations.

Its membership is drawn from major professional services groups, specialist advisory firms, companies, banks, private equity, venture capital, law firms, brokers, consultants, policy-makers and academic experts. More than 40 per cent of the faculty's membership is from beyond ICAEW.

The faculty is ICAEW's centre of professional excellence in corporate finance. It contributes to policy development and many consultations by international organisations, governments, regulators and other professional bodies.

The faculty provides a wide range of services, events and media to its members, including its magazine *Corporate Financier*.

The faculty initiated the development of the first international Corporate Finance qualification (including the 'CF' designation) for practitioners and launched a Diploma in Corporate Finance with the CISI in 2012.

ICAEW

Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK

T +44 (0)20 7920 8685

E cff@icaew.com

icaew.com/cff

 [linkedin.com](https://www.linkedin.com/company/icaew-corporate-finance-faculty) – ICAEW Corporate Finance Faculty

 [twitter@ICAEW_CORP_FIN](https://twitter.com/ICAEW_CORP_FIN)