Linklaters

Cyber Security Handbook

Version 2: The Essential Handbook for In-house Counsel

linklaters.com

CYBER SECURITY: THE ESSENTIAL HANDBOOK FOR IN-HOUSE COUNSEL

Cyber security was historically the preserve of information security teams. Few laws covered information security and there was little reason for lawyers to take a deep dive into such a complex and technical arena. But as cyber-attacks have grown in sophistication, the legal framework has expanded, claimants have unleashed a wave of class actions, and regulators have prioritised this issue – in-house counsel are being thrust squarely into the cyber arena.

We have had lots of questions from our clients about cyber over the years. Some are about the legal framework, but many are about a much broader issue; what is the role of in-house counsel in ensuring an organisation is prepared for cyber threats?

We have consolidated our answers in this handbook. It reflects our experience that an effective and informed in-house counsel is critical – not just to advise on regulatory requirements and potential liability – but also to help guide and co-ordinate the wider cyber response.

This doesn't mean that you need a complete understanding of what is happening at the binary level, but you need to know about what governance models work best, the types of technology involved and regulatory expectations about how that technology is deployed. This handbook is intended to provide that baseline understanding and address new AI risks.

Please note that this handbook is designed to be a general resource, and you will also need to take into account any particular rules that your organisation is subject to, depending on the nature of the business and where it operates.

Georgina Kon
Partner, London
Tel: +44 20 7456 5532
georgina.kon@linklaters.com

Tom Cassels
Partner, London
Tel: +44 20 7456 3755
tom.cassels@linklaters.com

1

MAKE SURE YOUR SENIOR MANAGEMENT ARE ON BOARD

1 MAKE SURE YOUR SENIOR MANAGEMENT ARE ON BOARD

1.1 Why is this important?

Effective cyber security is the culmination of many moving parts within any organisation.

As with any complex and dynamic scenario, it is difficult to identify a single feature as the most important or most relevant. But if you are thinking about creating and maintaining a programme that is effective in the long-term (and as in-house counsel long-term thinking is a must) then it is crucial to engage senior management, and where applicable, the board.

1.2 What are the wider benefits of senior buy-in?

Part of this benefit is obvious; getting the board on-side will help set the right tone from the top. Instilling a culture that cyber security is serious and is everyone's responsibility, will help drive a consistent and co-ordinated approach across your organisation. In addition, there is an increasing number of rules and regulations that specifically require senior management oversight or approval.

However, senior buy-in can also benefit your organisation in more subtle ways by helping to drive a more disciplined and systematic approach to cyber security.

One good example is the way board reporting drives the need for verified information and metrics, which generate the types of workstreams associated with good cyber security (see Board scrutiny drives reporting). If a board requires annual reporting of the organisation's cyber security posture, and such reporting is addressed by purely narrative and conclusory statements, as opposed to the identification and reporting of relevant metrics, that should be a potential source of concern. We look at what your board reporting might include in section 2.6.

Anyone who has worked in a large corporate enterprise will understand just how many (mostly beneficial) workstreams are typically generated by reporting requirements to senior management or the board.

Board scrutiny drives reporting

When a board requires periodic reporting on cyber security, the very first question from anyone with that reporting responsibility is, what are the metrics that would be useful for reporting purposes? Do we as an organisation actually track them at all? Do we have the technology to track them systematically?

Imagine a CISO that has just taken the helm of a fairly immature cyber security programme. Tasked with a board reporting requirement regarding the state of the organisation's cyber security, that CISO now needs to determine what information is available to support a meaningful report.

One of those topics might be the organisation's efforts in identifying and patching known vulnerabilities. Prior to a reporting requirement, the CISO might rely on her team to provide some level of confirmation that vulnerabilities are being managed. However, with a reporting requirement, the CISO now needs to present meaningful reporting to her board regarding the organisation's vulnerability management efforts.

That means metrics. How many new vulnerabilities are being identified every day? What is the average time to patch such vulnerabilities, and how much of that is due to testing? Does the organisation need greater investment in this area to reduce the time between identification of a vulnerability and patching it successfully? The idea is that these are things that every organisation should track, and having a reporting requirement incentivises such tracking.

1.3 How do you get buy-in?

If you find yourself covering your organisation's cyber security, you may be blessed with senior management that is active and engaged on issues of cyber security. If not, you may be wondering whether it is the role of the in-house lawyer to put this on the board's agenda. The answer is that it absolutely is.

Cyber security concerns are no longer purely operational and instead must reflect the numerous regulatory regimes driving the creation of relevant internal governance and policies, and requiring organisations to assess themselves against such standards. These are likely to fall squarely within the job description and require senior buy-in.

> "for business leaders. . .there are the sorts of things that you have to go through as part of your rite of passage. A hostile takeover, an activist attack, probably a boardroom scandal. . .these are warp and weft of business stress, and a cyber-attack is part of that.
>
> **Sir Archie Norman[1]**

While this should be an easy sell, if you feel additional attention to your cyber security programmes is needed there are some fairly standard practices that can be used, at the appropriate volume, to get this on the board's radar. These include:

- **Peer experiences and near misses:** Highlighting the impact of cyber-attacks on your peer group is an easy way to demonstrate the significance of the cyber security threat. Similarly, "near misses" for your organisation can provide the impetus for new investment or a change of approach to cyber security.
- **Tabletop exercises:** These are discussed in section 4.3, but this provides an ideal opportunity to bring the cyber threat to life and make it real for your senior management. As the head of cybersecurity at the NY Department of Financial Services stated: "decision makers such as the CEO should not be testing the incident response plan for the first time during a ransomware incident".
- **Risk assessments:** Externally led risk assessments can be costly and timely. But these are terrific ways to map the controls to the frameworks and regulations, and to benchmark against other companies. Senior management and the board can then get an executive summary, and future updates can track remediation against open issues. In-house counsel should be centrally involved in these exercises.
- **Direct regulatory obligations:** Some regulations now place direct obligations on the board to undergo cyber training and to supervise and approve the organisation's cyber stance. Breach can also result in personal liability for your directors.

1 Discussing the cyber-attack on Marks & Spencer. See, *The Rest is Money podcast* (Episode 235)

2

GET YOUR GOVERNANCE RIGHT

2 GET YOUR GOVERNANCE RIGHT

- Obtain senior management buy-in
- Identify which board committee is responsible for cyber security
- Create appropriate reporting metrics
- Conduct regulatory mapping of your cyber obligations
- Set out your information security programme
- Create appropriate information security policies
- Ensure compliance with the information security programme is audited and enforced

2.1 Overall structure

By governance we mean the policies, procedures, protocols, and other corporate mechanisms, used to control and operate your organisation.

How an organisation approaches governance is a product of size, structure, culture, industry, regulation, and a host of other factors. For example, an effective information security programme may be written down in a single policy document, or more likely across many different policies.

In practice, substantial parts of any information security programme may not be written down at all. However, the larger your organisation is, the more difficult it is to ensure that the correct processes are being followed and interpreted uniformly across the entirety of the organisation without setting them out in writing. As a result, some sort of documentation is needed.

This is reflected in the increasing number of cyber security regulations that require a written information security programme. Additionally, whether or not required by law or regulation, any regulator or potential claimant will see the lack of a written information security programme as a clear sign that the organisation is not serious about protecting its digital assets.

2.2 What should an "Information Security Policy" look like in practice?

The information security policy should record and reflect the various measures (whether governance, processes, or controls), used by your organisation to protect the confidentiality, integrity, and availability of your networks, data, and services.

For some this means dense, highly technical written documents with very specific requirements. Others maintain tiers of documents relating to the overall information security programme, with a more general top-tier policy document outlining general mandates and obligations that are fleshed out in lower-tier documents (eg standard operating procedures, technical standards, playbooks, and incident response plans).

There isn't necessarily a right answer as to what these documents should look like, but we find that a tiered approach helps ensure that senior management and supporting functions like legal and compliance are fully engaged with the organisation's cyber security efforts on a substantive level (whilst also retaining the more granular technical detail).

The documentation also needs to be suitable for the end audience. Highly technical documents are unlikely to be suitable for your general workforce, who are likely to need a more practical policy written in plain English.

2.3 What does a reasonable "Information Security Programme" need to cover?

At the highest level of generality, your information security programme needs to be reasonably designed to protect against threats to the confidentiality, integrity, and availability of its data, systems, or services.

What that means for a specific organisation depends on the size and complexity of its network, the data it houses, and the services supported by that network. With that said, there are some fundamental principles that a good information security programme is generally expected to incorporate.

Example of key non-technical controls and policies

The universe of policy documents making up your information security policy will vary but the non-technical policies typically might include the following. This is not a complete list of all governance documents, but rather identifies substantive areas of governance often considered integral to a reasonable cyber security programme. Your list of policies should also reflect any

regulatory "benchmarks" (e.g. the NIS II Implementing Regulation – see section 9).

Incident Response Plan: This sets out how you would respond to an incident. We consider what this should contain in section 4.2.

Minimum Supply Chain Controls: This sets out how you will address security risks from third parties, particularly from your supply chain and your minimum standards for contracting with these entities. We look at this in section 7.3.

Acceptable Use: This should set out the key dos and don'ts for your employees. While this is likely to focus on wider behavioural controls (such as not viewing inappropriate material), it should also contain key cyber security guardrails, such as not downloading unauthorised software from the internet.

Privacy Policy: The obligations in your privacy policy (such as not collecting excessive data) will often help with wider data hygiene. The privacy policy should also alert employees to the fact that their system usage may be monitored as, in many jurisdictions, this is a key prerequisite for such monitoring.

Document Retention and Destruction: Your retention policy helps ensure that data is not retained longer than necessary. A frequent problem with data breaches is that the compromised data is old and should have been deleted long ago. Under data protection law, this can be an aggravating factor in assessing fines or damages.

Data Loss Prevention (DLP): DLP solutions tend to involve extensive and intrusive monitoring of your own network to prevent data loss (see section 8.2.3). As such, it may well need its own policy and governance.

Data Governance and Classification: This policy should set out the sensitivity of different types of information and the specific handling measures, eg whether that information can be sent by email? What level of encryption must be applied? Should highly sensitive data be kept within a more secure enclave within your network?

On top of these non-technical policies, you would also expect a range of technical controls addressing issues like patching, penetration testing, access controls, etc.

2.4 Why is regulatory mapping essential?

Your approach to governance should also be shaped by the regulatory obligations placed upon you, as they form the minimum baseline for your compliance.

There has been a significant growth in cyber security over the past few years (eg see Annex Snapshot of Cyber Laws on page 11) so this mapping exercise is not always straightforward, particularly if you operate in multiple jurisdictions. Added to this complexity is the rapid evolution of laws, as both new laws are enacted and as guidance is released in relation to the interpretation of existing laws.

A regulatory mapping exercise should address the following five areas:

Security requirements: Most obviously, these laws are likely to impose obligations on you to ensure the security of your systems. That might either be expressed in general terms,[2] or by reference to specific steps or types of system. You need to understand what these obligations are so you can verify your compliance as part of the governance process.

Notice of breach: Many of these laws also impose obligations on you to notify breaches to regulators and affected individuals. It is important to identify these obligations prior to any breach, as many require notification within a very short period (see section 4.6.1).

Organisational measures: These laws increasingly require organisation measures, such as staff training or vetting, reflecting the need for good cyber aware culture, see section 3. For example, the EU NIS II Implementing Regulation contains provisions that require (amongst other things) security awareness and training, background checks on staff and a disciplinary process for transgressive employees (section 9).

Supply chain: Similarly, these laws are increasingly addressing supply chain risks; see section 7. For example, EU DORA extends the competence of financial regulators to critical third-party suppliers (such as AWS and Google Cloud) whilst also imposing prescriptive rules on contracts with third-party IT suppliers; (see section 7).

Resilience: Another growth area is specific obligations to ensure the resilience of your information technology systems, i.e. the ability to absorb and recover from a cyber incident (see section 6).

The Cyber Risk Institute has carried out an extensive mapping of information security controls to key information security regulations,[3] albeit this is mostly US based and mostly for financial services. However, the profile they developed is completely free on their website and is an amazing tool to understand how this mapping can work.

2 For example, some EU legislation imposes a general obligation to use "appropriate technical and organisational measures" (TOMs) to secure systems. If this sounds "fluffy", it isn't. Regulators flesh this out by reference to their own guidance and extensive guidance from third parties such as the NCSC or NIST.

3 https://cyberriskinstitute.org/the-profile/

2.5 How do you ensure your information security programme is more than a paper tiger?

Getting the right governance in place is only half the fight; you also need to ensure you are complying with your own internal control mandates.

Failure to comply with your own internal controls is a major own goal in any regulatory investigation that may well be used as evidence of non-compliance.

EXAMPLE

Talking the talk, but not walking the walk

The Interserve Group was subject to a ransomware attack. This followed a depressingly familiar fact pattern. A phishing email was sent to an employee containing a ZIP file that needed "urgent review". When opened the ZIP file installed malware that gave the attacker control over the employee's device.

The device was subject to Endpoint Detection and Response (EDR) which removed some files and reported that malware to the company's security operations centre (SOC), but nothing was done. The attacker retained access to the device and used it to move laterally across the network to compromise 283 systems and 16 accounts (including 12 privileged accounts) across four domains. Using that privileged access the attacker uninstalled the anti-virus software and then encrypted four HR databases containing details of 113,000 individuals.

Part of the problem was that Interserve was running unsupported software, including Microsoft Server 2003 R2 which reached end-of-life five years beforehand. In other words, they were no longer the subject of security updates to fix known vulnerabilities in the system which could be exploited by malicious actors.

There is little doubt this was a serious security failing. When deciding to issue a £4.4m fine the Information Commissioner relied upon the best practices standard NIST 800-53 which requires organisations to plan for and implement a technology refresh schedule through the system development life cycle.

However, more damning was Interserve's own Systems Management Policy which expressly stated that all of its systems should be supported and patched. Failure to comply with your own internal policies is a major own goal in any regulatory investigation. From a practical perspective, it should also be a major red flag.

Regulators have some understanding it is impossible to ensure that 100% of your employees will comply with 100% of your policies 100% of the time, but a serious or systematic failure to implement those controls will be seen as a very different matter.

The exact method of compliance testing will vary from organisation to organisation, but in many cases you can use your existing compliance testing model. For example, if you operate a three-lines-of-defence model, it will normally work well with cyber compliance testing.

Three lines of defence in cyberspace

The "three lines of defence" is a cornerstone to operationalising risk management programmes, particularly in the financial services sector. It provides a structured approach to risk management and internal controls by defining roles and responsibilities, and the relationship between those different areas. It maps relatively easily onto cyber security compliance.

1st Line **IT function and the business**	> Define risk appetite > Make risk-based decisions in day-to-day operations > Implement technical controls > Mitigate or escalate risks
2nd Line **Risk management**	> Establish governance structure > Create Information Security Programme > Monitoring and oversight
3rd Line **Internal audit**	> Independently verify compliance with controls > Report to board on effectiveness > Satisfy regulatory disclosure requirements

Many clients ask us about the right role for Compliance in information security. With so many subject matter experts in the information security organisation, does Compliance really need to hire its own subject matter experts? In a large organisation, the answer is yes. In smaller organisations, it should be treated like other areas.

2.6 What involvement should your senior management and board have?

Sitting at the top of your governance model is your senior management and the board. The starting point is to work out who is responsible for cyber security. In many cases, that will be the audit committee, who will play a strategic role in relation to cyber security in its capacity of overseeing risk and policies and procedures. A recent survey suggested that 96% of Fortune 100 companies have at least one board-level committee that is charged with oversight of cyber security and that in 78% of cases that is the audit committee.[4]

Another question is what sort of board reporting is needed. This might include some quantitative metrics (see box below) which will not only provide great visibility but also (as noted in section 1.2) drive a number of beneficial workstreams.

New EU legislation increasingly requires the management bodies of critical entities to approve and supervise the organisation's cyber security risk management measures, as well as undergoing specific cyber training.[5]

Key metrics – if you can't measure it, you can't improve it

Quantitative reporting metrics provide a useful overview of your organisation's cyber stance, including the ability to track trends over time. Those metrics will vary from case to case but might include:

- **Number of intrusion attempts:** This might be broken down to include details of phishing emails alongside direct hacking attempts.
- **Number of security incidents:** As well as the total number of incidents, this might be broken down to provide details of the mean time to detect (MTTD) and mean time to recovery (MTTR).
- **Patching cadence:** This might include details of the mean time to patch, and the time to patch high-risk vulnerabilities.
- **Access controls:** This might include details of the number of users with high-level privileges and the mean time to deactivate former employees' credentials.
- **Third-party suppliers:** This might include details of the total number of third-party suppliers, number of new third-party suppliers and number of third-party suppliers that have been audited or risk assessed.
- **Training:** This might include the number or percentage of employees to have completed cyber security training, including specific details for new employees.

However, like all metrics, these need to be used carefully to ensure they drive the right behaviours. A report that states no security incidents have been identified may be more of a concern than one with a list of potential incidents.

4 Cyber and AI oversight disclosures: what companies shared in 2025, EY, October 2025 (https://www.ey.com/en_us/board-matters/cyber-disclosure-trends).

5 For example, EU NIS II and DORA. See Snapshot of cyber laws.

It should also include qualitative reporting, such as details of:

- **Events/incidents:** Update on any new or continuing or significant recent cyber events or security incidents. This should include an update on any regulatory investigations or civil litigation.
- **Threat landscape:** Details of the current cyber threats, with a particular focus on new threats and identification of suitable mitigating measures.
- **Audit/verification:** Details of current internal or external audits or other verification and testing of security measures. This should include measures to confirm any previously identified vulnerabilities have been addressed.
- **Regulatory/reporting obligations:** Update on any proposed or new regulatory or breach reporting issues and details of the measures taken to comply with them.

The final point is what sort of questions the board should ask their information security function. How can someone without deep technical expertise get the information they need to assess the effectiveness of the company's defences? We have suggested some questions and topics to explore (see box).

Hard questions – things for the board to ask

Flipping this round, here are some suggestions for questions the board can ask to better understand their company's information security stance.

- Did we make any decisions in favour of convenience and efficiency (including customer convenience) that meant weaker security? Assuming the answer is yes, what were those decisions?
- JP Morgan is spending over half a billion a year on cyber security.[6] Is that consistent with our spend on a percentage basis? What are they spending money on that we are not?
- What would you have done with more budget last year? How about with more people?
- If you had more budget and people for next year, what would you do with it?
- Notwithstanding all of our advancement in cyber, if you had to predict a way in for hackers, what would it be?
- Can you quantify the cyber risk? For example, does the company face US$500m in cyber risk this year? Could we reduce that risk by increasing our cyber budget by 10% or 25%?
- Have we had any significant departures from our cyber talent pools? Did any of them complain about resources and priorities?

6 JP Morgan have published the fact it invested US$600m to defend against phishing activities and other threats https://www.jpmorgan.com/commercial-banking/solutions/treasury-payments/business-resiliency

3

A CYBER-AWARE CULTURE – TRAINING AND ENFORCEMENT

3 A CYBER-AWARE CULTURE – TRAINING AND ENFORCEMENT

> Culture eats strategy for breakfast.
>
> **Peter Drucker**

3.1 Tone from the top

Cyber security is not a "*technical issue*" that can be relegated to the back office. A strong response requires everyone within the organisation to understand their role in defending the organisation from attacks.

That means ensuring everyone has good personal cyber hygiene, for example not reusing passwords, opening unexpected email attachments or trying to download software from the internet. It also means understanding the importance cyber has in projects so time is set aside to ensure new systems are properly assessed and tested and not rushed to meet arbitrary business deadlines.

It also means being alert to potential data breaches and attacks and reporting them promptly. The failure to recognise the seriousness of an attack, and to escalate the matter, was part of the reason why a UK bank was sanctioned for a botched response to a cyber-attack (see Case Study: Who you gonna call? When incident response plans go wrong).

This is only possible if there is the right tone from the top and there is a clear commitment from the company's senior management and board that cyber security is important.

3.2 Training

Even if you have the right culture in place, you still need to make sure your employees know what to do to minimise the cyber threat and who to contact if they suspect there is a breach.

That training is going to vary greatly from organisation to organisation – how homogenous is the employee population? How much sensitive data do they handle? What are the specific risks they face?

There may well be a need for bespoke training to particular departments or cohorts, but most organisations will want some form of introductory entity-wide training. If your employees know the basics, they are likely to avoid obvious mistakes and if the regulator comes knocking they will want to know that your policies are not academic exercises and are integrated into your working practices.

How to create a great cyber eLearning module

One way to deliver training to a large group of disparate employees is to use an eLearning tool. This has the added benefit of allowing you to train people remotely and track completion of that course.

However, your cyber training is going to have to compete with a multitude of other training modules, so how do you make sure you get your key messages across and deliver meaningful change in the way your employees approach cyber security?

- **Show your leadership is on board:** The training provides an ideal opportunity for your leadership to set the tone and explain why this is important.
- **Make it relevant:** Cyber security is relevant to everyone, but you want to show why it is specifically relevant to your organisation. Use examples and relevant events to make it real.
- **Use story telling:** One of the most effective ways to influence people is to use story telling. Consider how to create an engaging narrative to make your points.
- **Avoid the jargon swamp:** Think about your audience. If they are not technical then neither can your training be. Use plain English not technical jargon.
- **Pick out five key points:** Think about the five points you want your audience to take away and hammer them home.
- **Check people are listening:** The excitement of a test at the end of the module will keep your audience engaged and reinforce the key points.

3.3 Enforcement

Regardless of how much effort you put into training your employees, things are still likely to go wrong from time to time. How should you react?

The most important factor is to keep your employees' trust so they tell you when they make a mistake or something doesn't feel right. This is a valuable early warning system and a vital part of any monitoring system. Someone who is afraid of being disciplined will keep quiet.

Clearly if the employee has deliberately created the breach, or is behaving in a reckless and irresponsible manner, the position is different, but in most cases punishing employees delivers poor outcomes in the long run.

Are simulated phishing exercises counter-productive?

An example of maintaining employee trust is simulated phishing exercises. We all know that phishing is a major attack vector. So why not send some simulated phishing emails to your employees to check they are being careful? (And have paid attention to your cyber training.)

In practice, it turns out there are a range of reasons why this can be a bad idea. No training programme will allow your employees to spot every phishing email and asking employees to review every email they receive in detail is not realistic. More importantly, blaming employees who click on links is likely to cause some anxiety and create distrust between them and your information security function.

For this reason, security bodies such as the UK National Cyber Security Centre do not recommend using simulated phishing exercises and instead recommend a multi-layered defence.[7] For example, blocking phishing emails at an organisational level, stopping spoofed email and preventing malware from executing if it's downloaded.

7 This position is not shared universally. Some cyber security agencies and commentators suggest that simulated phishing exercises can be useful provided that employees who fail the test are not "punished".

4

HOW TO RESPOND TO AN INCIDENT

4 HOW TO RESPOND TO AN INCIDENT

- Create an incident response plan
- Test that response plan through a tabletop exercise
- Identify and onboard the right advisers
- Implement a suitable logging system
- Identify any regulatory, contractual or other notifications
- Create a communications plan and templates
- Set out a framework for responding to ransomware demands

> When everything gets really complicated and you feel overwhelmed, think about it this way. You gotta do three things. First, get the cow out of the ditch. Second, find out how the cow got into the ditch. Third, make sure you do whatever it takes so the cow doesn't go into the ditch again.
>
> **Anne Mulcahy, Xerox**

4.1 Fail to prepare? Prepare to fail

Cyber incidents come in many forms. Some are minor or irrelevant. However, a serious cyber incident can be a traumatic experience requiring significant decisions to be made immediately against a background of potentially incomplete and inaccurate information.

The more you can do to prepare for – and practice – your response, the less painful this experience will be. The facts will never be the same but the journey is likely to be similar.

4.2 Develop a plan

The starting point is to check your incident response plan is in good shape, up to date and the right people know where to find it.

The table below sets out the key things you should include in your incident response plan. That plan should be a "living document" that is reviewed and updated regularly.

What should the incident response plan cover?

A broad outline of the issues you should consider covering in your incident response plan are set out below, with some of the analysis underpinning them set out elsewhere in this note.

(a) Triage and escalation
The plan should set out appropriate thresholds to categorise the seriousness of the breach with corresponding appropriate escalation paths. Cyber breaches come in many shapes and sizes, so it is important to calibrate the response.

(b) Internal team and responsibilities
The plan should contain a list of internal stakeholders that need to be informed, consulted or directly responsible for the response to the cyber breach (including emergency contact details and alternates). This will vary according to the seriousness of the breach. It is helpful to include actual names, and update the plan yearly to update names.

The "gold" team should include suitable stakeholders from across the business, which for serious breaches should include representatives from the business, IT, InfoSec, Privacy, Legal, Comms and HR. Each part of the team should have clearly defined roles and responsibilities. Of course, companies without all these functions will need to adapt to a smaller set of core participants.

(c) Internal communications and updates
The plan should also set out the format, means and cadence of any team updates and meetings; which in the early stages of serious breach is likely to require daily update calls as a minimum. Failure to have these daily (or twice daily) update calls typically leads to a lack of co-ordination and does not, in practice, save the perceived time wasted on the calls.

(d) External advisers
The plan should identify the preferred external advisers to help with any breach. Given the time lag bringing some advisers on-board (particularly technical advisers), suitable engagement terms should be agreed in advance (see section 4.4).

(e) Fact-finding and analysis
The plan should set out the various tools and processes that will be used to determine the scale of any incident and to analyse the effect on the business, including its impact on critical systems and data. This aspect of the response is likely to rely heavily on any SIEM and network logging in place, and might also require the involvement of external advisers to analyse that data.

(f) Containment, recovery and resilience
The plan should set out the potential options to contain any infiltration – including in serious cases, shutting down or disconnecting networks – as well as an assessment of the business impact of those measures. Similarly, it should identify the means to recovery, including options to restore those systems to their pre-incident state (see section 6).

(g) Notification obligations
The plan should identify the key notification obligations that arise following a cyber breach. These typically arise because of regulatory notification obligations and any contractual commitments made to third parties (see section 4.6).

(h) Ransomware
The extortion of money via a cyber-attack raises its own particular issues both as to the legality and morality of paying-off cyber criminals. The plan should set out the framework to your response to these demands (see section 4.8).

(i) Communications
Clear and timely communications are an important part of any response. The plan should have a strategy for communications within your organisation, with external stakeholders and with the press. In some cases, this can be a significant undertaking. For example, a large consumer facing business might have to contact hundreds of thousands, if not millions of customers, which can be a demanding logistical exercise (see section 4.7).

> Everyone has a plan until they get punched in the mouth.
>
> **Mike Tyson**

4.3 See if the plan works – tabletop exercises

Military wisdom indicates that no plan survives first contact with the enemy. The botched execution of an incident response plan was also a major reason behind a recent fine by the UK FCA (see Case Study: Who you gonna call? When incident response plans go wrong).

This means you need to test out your response to an incident through a tabletop exercise that works through the life cycle of a cyber-incident. That exercise should involve the decision makers who will have to take the key calls in practice, which is likely to mean representatives from across the C-Suite. It allows the key decision makers to role-play their way through an incident.

This type of exercise typically takes around three hours and should be tailored to your particular business, systems and corporate structure. The prospect of taking a large chunk of your C-Suite's diary seems daunting, and you may well get some initial push-back. However, in our experience a well-designed tabletop exercise that provides a realistic simulation of how a cyber incident would play out in practice is almost universally welcomed by your senior decision makers.

As the head of cyber security at the NY Department of Financial Services recently stated: "*decision makers such as the CEO should not be testing the incident response plan for the first time during a ransomware incident*".

CASE STUDY

Who you gonna call? When incident response plans go wrong

The attack on Tesco Bank illustrates the need to have a well-tested incident response plan and what happens when that plan fails. It became subject to a cyber-attack involving the submission of fraudulent debit card transactions exploiting a payment method known as "PoS 91".

What went wrong?

The attack started at 2:00 am on Saturday. The operations team identified they were under attack but instead of telephoning the on-call fraud analyst (as the bank's procedures required), they emailed the fraud strategy inbox. That email account was not monitored at the weekend.

In the meantime, the fraudulent transactions multiplied, and the bank's social media account started receiving posts about the incident. However, this did not result in any further escalation and the bank ceased monitoring the account during Saturday evening, during which time a further 28 posts were sent about the fraud.

Only at 11:00 pm on Sunday (21 hours after the initial email) did someone call the strategy team. Once alerted, that team created a rule at 1:00 am on Sunday to block PoS 91 transactions.

However, the strategy team did not monitor the operation of the rule and discovered hours later that not only was it ineffective, but the fraudulent transactions had escalated. The rule was modified but some fraudulent transactions were still getting through so external experts were engaged. Only at 1:00 am on Monday was the torrent of fraudulent transactions blocked. By that time the attackers had netted £2.26m.

Sanctions

The UK FCA fined the bank £16.4m. Much of the fine was for configuring its systems to allow fraudulent PoS 91 transactions in the first place, but part of the fine was for the botched response. The UK FCA also criticised the late invocation of the crisis protocol meaning the bank's senior management were not alerted until 3:00 pm on Sunday.

The UK FCA was, however, broadly happy with the overall governance approach noting that the Executive Risk Committee had identified "Cyber Crime/Financial Crime" as among the bank's top risks and established the Cyber Crime Steering Group to address the issue. The bank had also deployed a three lines of defence model to address cyber risk.

The UK FCA made it clear that firms "*cannot eliminate the risk of cyber crime*" but can "*ensure that their cyber-crime controls are well designed, that the individuals who design and manage those controls understand how they work, and that their crisis management plans are clear and well-rehearsed*".

4.4 Get the right advisers on board

Getting the right advisers on board in a timely manner is vital to any breach response. This may well include a technical incident response team, crisis communications firm, identity theft monitoring firm and ransomware negotiator.

Our experience is that many companies do not select specialist incident response advisers. We strongly recommend finding teams that have this focus. For example, many information security teams turn to their standard information security advisers but the advisers that help set up systems are not experts at incident response. The same goes for communications teams. Business marketing and PR advisers are not the same as crisis communications firms.

You should aim to have engagement terms in place with this roster well in advance of any breach occurring, for the following reasons:

- **Identifying the right adviser is important.** Advisers have a range of different skill sets and the market is becoming highly specialised. The process of working out who is right for you takes time and that is a luxury you don't have during a live incident.

- **Engaging advisers takes time.** Similarly, once you have identified the right adviser, bringing them on board will likely take time. Trying to agree engagement terms while an incident is unfolding will waste precious time and mean you have little or no leverage over those terms.

- **Advisers have limited capacity.** Finally, the best advisers are busy and have limited capacity. If you don't have an existing

relationship, you can't assume they will drop everything to come to your aid. We have seen advisers turn down very large engagements simply because they lack the capacity. In contrast, if you engage them beforehand you can reserve the capacity you need in advance.

4.5 Getting the facts

Key to a good response is a solid understanding of the facts. While every breach will be different, a list of the key facts you need to chase down is set out in the box below.

Top 10 questions that need immediate answers

1. What data and which systems have been compromised?
2. Are those systems operational and, if not, how long might it take to restore them?
3. How and when did the breach take place?
4. Has the breach been contained, or might the attackers still be in those systems?
5. Has the vulnerability that led to the breach been addressed?
6. Is the attack just on my organisation or are others affected?
7. Is there any evidence of exfiltration or misuse of the data?
8. How many customers/clients/employees are affected? Are they clearly identified if you need to contact them?
9. Who is likely to be behind the breach?
10. Have the attackers demanded a ransom or otherwise tried to make contact?

Getting this information will likely depend on having the right logging system (eg SIEM) in place to allow you to extract and analyse the relevant network data, though it may help to get specialist technical advisers on board to help analyse that information.

4.6 Identify who you have to tell

4.6.1 Regulatory notifications

The security breach may well trigger a range of obligations to notify regulators, affected individuals and counterparties about the breach.

For example, over the last few years there has been significant expansion in the number and variety of notice of breach laws (see Annex Snapshot of Cyber Laws). While the overall approach of these laws is similar, the detailed notification obligations are very different in terms of:

- **Who must be notified?** The regulator that must be notified varies from law to law and some breaches might require you to notify multiple regulators. Some laws also require affected individuals to be notified.
- **What is the trigger for notification?** Each law will set its own trigger for notification, which might be based on the overall risk of the breach, the impact on a service or simply require all breaches to be notified.
- **What is the timeline for notification?** The time within which each breach must be notified varies, though many must be notified on a relatively short timescale. For example, the GDPR requires risky data breaches to be notified to the regulator within 72 hours.[8] New cyber laws have even shorter notification periods – for example, the EU's NIS II Directive requires an early warning notification to be sent to regulations within 24 hours with detailed follow up reporting obligations.[9]
- **What information must be included in the notification?** Finally, the information that must be provided in the notification varies from case to case.

The complexity of the breach notification process increases if you are operating across multiple jurisdictions as the breach might trigger multiple notification in multiple jurisdictions.

Added to this is the fact that, as noted above, breach notifications often need to be made within a short space of time. The period of 72 hours for notification in the case of a risky personal data breach under the GDPR may sound like a long time, but given the need to investigate the reason why the breach occurred, it can go quickly (though the GDPR does allow an initial notification to be made with a follow up notification once further details become clear). Mapping out your breach notification obligations so you know who needs to be notified and by when can be enormously helpful.

The notification also needs to be carefully drafted. Not only will regulators examine it to determine if further investigations are needed but it is increasingly common to see requests for these notifications as part of civil litigation claims. This means it is important to draft them clearly and precisely. In many cases, regulatory breach notifications can be submitted on a preliminary basis, with follow-up in due course once further details of the breach become clear.

8 The EU has issued its proposed Digital Omnibus which makes a number of helpful changes including limiting the reporting of personal data breaches to "high risk" breaches, increasing the deadline to report personal data breaches to a weekend-saving 96 hours and creating a single-entry point for breach notifications under GDPR, NIS II, eIDAS2, DORA and the Critical Entities Resilience Directive.

4.6.2 Contractual notifications

Companies rarely have a list of contractual notification obligations at the ready. Remedying that today will save many headaches in the event of a breach.

For example, if you act as a "data processor" under the GDPR you must notify your controller of a "personal data breach" affecting the controller's personal data. Obligations to notify counterparts of data breaches also occur in a range of other contexts.

These notification obligations might well come in many different shapes and sizes, with different trigger points and timelines. Ideally, you would try and standardise your approach but, at the least, you need a clear record of all your data breach notification obligations. Scrabbling through your contracts once a breach has occurred is not recommended.

4.6.3 Other notifications

On top of these are a range of other notifications you might wish to consider, including:

- **Insurers:** If you have cyber insurance, it is likely that will be subject to the provision of prompt notification about the breach. It's also worth noting that some insurance policies exclude acts of war, meaning cyber-attacks committed or supported by state actors in context of ongoing conflicts may not be covered by your cyber insurance policy.
- **Law enforcement:** In some jurisdictions, notifying the appropriate law enforcement agency – such as the Federal Bureau of Investigation in the US – can provide significant benefits. While it won't always be possible to track down and prosecute the perpetrators, the law enforcement agency may be able to provide advice and share valuable information about them (particularly if it is a well-known hacking group). However, this is not always the case and notifying some other law enforcement authorities may be less helpful as their priorities might not match up with your objectives.
- **Cyber security agencies:** It may also be helpful to seek assistance from specialist cyber security agencies. In the UK, the National Cyber Security Centre has specifically not been given any regulatory enforcement duties to ensure it can work constructively with businesses that have suffered a cyber-attack (ie it does not see that interaction as a precursor to regulatory action). It also does not tell regulators about any companies seeking assistance.

9 NIS 2 also requires a detailed report within 72 hours, a final report within 1 month (or a progress report if the incident is ongoing at the 1-month mark) and, if requested, an interim report in the meantime.

4.7 Plan your communications

4.7.1 What do you need to cover?

All of these potential notifications should form part of your wider communications strategy. Your incident response plan should address:

- **Press and social media strategy:** When and how will you make any public announcement about the incident? What channels will you use? While it is impossible to draft any statement in advance, you can prepare a template with optional drafting that highlights the issues that will need to be addressed.
- **Telling your customers:** When and what will you tell your customers about the incident? It is important to note the significant logistical challenges this can create. For example, if you have a number of customers who you deal with only by post then printing or posting very large volumes of communications can take time (typically weeks not days). In addition, those customers might well want further information. Some of this can be dealt with through Q&As on your website but you should also address how you will deal with a surge in calls to your customer service centres and make sure your contact staff are properly briefed to deal with questions.
- **Telling your staff:** Finally, of equal importance to the steps set out above, is the question of what you will tell your staff. Informing and empowering your staff to deal with the incident can make a real difference.

4.7.2 Listen as well as speak

The communications strategy should also involve not just speaking but also listening. Understanding how the outside world is reacting to the incident which is evolving will help refine future communications. Interestingly, the failure to use intelligence from social media to respond to an attack was part of the reason for a recent fine by the UK FCA (see Case Study: Who you gonna call? When incident response plans go wrong).

Listening is a particular issue for social media where a story can gain momentum in an instant and die away just as quickly. Whether and how you engage with users on social media – particularly where you think the facts are misrepresented or distorted – is worth consideration.

4.7.3 Why does it matter?

Taking control of the narrative helps protect your reputation. It is unlikely that a serious incident will ever be "a good thing" but being able to show you have responded honestly, competently and compassionately can minimise any harm.

Unfortunately, the press narrative can also have a significant effect on your potential liability. An incident that is high-profile and appears to be poorly dealt with is likely to go to the top of any regulator's inbox. Regulators will want to show the public they are responding to their concerns so there is a strong correlation between negative press headlines – and enforcement.

Similarly, there is a correlation between negative press and civil class actions. This is particularly the case for opt-in class actions (such as Group Litigation Orders in the UK) where heavy press coverage will help claimant firms with their book building exercise.

How to write a great press release

The tone and content of your first (and any subsequent) press release will be crucial to shape the public's response to the incident, which is why it is worth preparing a template in advance. Key factors in a great press release are set out below.

- **Get the facts right:** This is one reason why a fast-fact-finding exercise is so crucial to the incident response. The more confident your understanding of the incident, the more confident you can be in public. However, it is difficult to ever be 100% sure about any cyber incident so you should caveat any statements to reflect the fact the investigation is ongoing. Getting the facts wrong risks you looking incompetent – or worse – dishonest.
- **Say it once, say it fast:** In a similar vein, you want this to be a one-day-story which is best achieved if you provide all the relevant facts in one go before the press have already created their own narrative. Drip feeding new developments out over a period of days or weeks will only prolong the agony.
- **Balance contrition and protection:** The tone of the statement is really important and often leads to tension between different stakeholders. On the one hand you want to demonstrate empathy with those affected by the breach and acknowledge the need to do better in the future. On the other hand, an admission of liability is going to be very unhelpful in any future regulatory or civil proceedings. The line between the two is fine, but can be navigated.

4.8 Ransomware

4.8.1 Morality v reality

Extortion attempts raise their own particular issues and commonly lay bare the difference between morality and reality.

On the one hand, paying a ransom is wrong. You are enriching criminals who have damaged your company. Worse, you support a business model that will lead to other companies being damaged in the same way. Put simply, if everyone stopped paying ransoms, the ransomware market would dry up overnight.

On the other hand, the impact of the ransomware attack can be catastrophic. If your computers are locked up, your business might cease to function. If third parties have exfiltrated your data and are threatening to publish it, that could have a devastating effect on your company.

The decision whether to pay up is incredibly difficult. We suggest that you not make the decision up front and instead your incident response plan can set out the factors you will consider when making a decision.

4.8.2 Legality

There is also a separate question about whether paying a ransom is legal.

We conducted a survey of over 140 countries and regions to evaluate the legality of ransomware payments, which revealed that only three outlaw ransomware payments altogether, whereas the majority outlaw ransomware payments in certain situations.

In many cases, the answer depends on whom you are paying. In particular, in 113 of the jurisdictions we surveyed, payment to a sanctioned person might well constitute an offence, whereas payment to a "basic" ransomware gang is not. Most jurisdictions also have legislation in place to prevent money laundering and terrorist financing which may be triggered by a payment to an entity with money laundering or terrorism connections.

This means that you may need to conduct some form of due diligence into the gang you are paying, which is likely to require the help of specialist advisers or law enforcement. In particular, in the US, one advantage of bringing the FBI into the loop is that they may be able to assist determining whether any payment is likely to be an offence.

The position here is not always clear and the tide is moving against paying up, with a number of governments considering outlawing ransomware payments.

The legality of ransomware payments

In the US, paying a ransom in response to a ransomware attack is not illegal under federal criminal law, though federal agencies including the White House, FBI, DOJ, Department of Homeland Security, and Critical Infrastructure Security Agency (CISA) strongly advise against it. However, any payment must comply with US sanctions and counterterrorist financing regulations. If a ransomware payment has any connection to a sanctioned individual or entity on OFAC's Specially Designated Nationals and Blocked Persons List, that payment is sanctionable on a strict liability basis. OFAC guidance emphasizes the importance of having sanctions compliance programmes, implementing cybersecurity controls, and cooperating with law enforcement as mitigating factors in any enforcement action. Additionally, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) when implemented (expected May 2026) will require covered critical infrastructure entities to report substantial ransomware payments to CISA within 24 hours.

In the UK,[10] the National Cyber Security Centre and the UK ICO have jointly stated companies should not pay ransomware demands. Their view is that this does not reduce the risk to individuals and is not considered as a reasonable step to safeguard data.[11] The UK ICO will not take payment of ransoms into account as a mitigating factor when considering the type or scale of enforcement action taken in relation to a cyber breach. More seriously, payment to a sanctioned entity is an offence under UK law, and this may be a strict liability offence, meaning that you can be liable for paying a sanctioned person even if you were not aware of this. In addition, payment that breaches terrorist finance or anti-money laundering legislation is an offence, and organisations in the regulated sector will also need to consider their obligations to report suspected money laundering.

In certain jurisdictions in Asia, such as Singapore and Hong Kong, there are specific legislative provisions relating to preventing property being used for an indictable offence or criminal conduct. In Hong Kong, there is a reporting obligation to the Hong Kong Police upon suspicion of property being used in connection with an indictable offence. A breach of this obligation to report would attract criminal liability of imprisonment and fines. In Singapore, it is an offence for an organisation to assist another person to retain or use the benefits of criminal conduct.

In Mainland China, PRC laws remain silent regarding the legality of paying a ransom, but certain reporting obligations which apply under anti-money laundering regulations for financial institutions' client transactions which reach prescribed statutory thresholds or appear suspicious might be relevant (albeit the likelihood of this is relatively remote since ransom payments to the threat actor are unlikely to constitute a client transaction). For prudence, if financial institutions are involved, they should enquire with the People's Bank of China to confirm whether any AML reporting is needed.

Businesses should approach any payment carefully in light of these complex and overlapping requirements. The legal analysis will often be guided by your ransomware negotiator, who will typically provide a report on the likely background of the threat actor.

4.8.3 Practicality

Finally, the threat of ransomware raises its own practical issues:

- **Recovery point:** An important part of the decision whether to pay the ransomware attackers is the implications of not paying. If they have encrypted your data, what measures did you have in place to securely back it up, and if you restore your data from those back-ups, how much data will be lost? You need this information to make a decision.

- **Trust and proof of life:** Will the ransomware gang actually unlock your computers and/or destroy the data they exfiltrated if you pay up? Curiously, many ransomware gangs have quite a good reputation and excellent "customer service" as it supports their business model. However, this is not always the case (eg none of the computers compromised by the NotPetya virus were ever unlocked by the attackers) so getting specialist advice on exactly who you are dealing with is important. So is proof of life. It's obvious if your computers have been locked up, but if someone says they have extracted your data, you want evidence.

- **Specialist advisers:** All this means is you need the right advisers on board. Cyber security is an increasingly specialised industry, so your top forensic investigation firm may not be the top ransomware negotiator.

- **Persons unknown orders:** Finally, the courts are increasingly willing to grant "Persons unknown"/John Doe orders against the attackers, requiring those attackers to not disclose the data, deliver it up and identity themselves.[12] The threat of committing contempt of court is not a game changer, given that the attackers will have already committed serious criminal offences, However, such orders can help when dealing with third parties who have become mixed up in the breach (eg those hosting exfiltrated data).

10 The UK has announced proposals to ban ransomware payments by operators of regulated-critical national infrastructure and the public sector. It is also considering a ransomware payment prevention regime that would require prior notice of ransomware payments to be made to the Government.

11 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/07/ico-and-ncsc-stand-together-against-ransomware-payments-being-made/

12 For example, see PML v Person(s) Unknown [2018] EWHC 838.

4.9 The role of privilege

Privilege is the right to withhold evidence from being produced to a third-party, the court or regulators. In most jurisdictions, the rationale for allowing parties to claim privilege is the idea that parties should be free to seek legal advice and prepare for litigation without worrying that they will have to reveal the content of those communications in the future.

Typically, after a cyber incident, many clients anticipate that they may be on the receiving end of an investigation or one or more legal claims. Therefore, maximising your ability to assert privilege over communications is often at the forefront of clients' minds.

However, it is vital to think first about where you may later be compelled to disclose documents. Some jurisdictions simply don't recognise privilege as a concept or only permit documents to be withheld in very limited circumstances.[13] If that's the case, then fretting over privilege and setting up detailed communication protocols may be pointless.

Where privilege can be asserted, it's important to recognise its limitations. For example, in England and Wales, privilege will in broad terms only apply to: (i) communications that are genuinely made for the purposes of providing legal advice; and (ii) communications that are genuinely made for the purposes of preparing for or advising on anticipated litigation.

This means, a technical investigative report on the causes of a cyber incident may not be privileged unless it is genuinely prepared for anticipated litigation. Other jurisdictions, like the US, take a broader approach, but even so, the scope of privilege has narrowed in the US in response to recent case law, and whether privilege can ultimately be upheld is a very fact-specific issue. For example, in the US a technical investigative report of the causes of a cyber incident prepared by forensic consultants may be privileged if it was prepared at the direction of counsel for the purposes of providing legal advice to the company or in anticipation of litigation. Where disclosure in the US is in prospect, there may be ways to structure engagements to maximise privilege.

Either way, it is often important not to let the privilege tail wag the incident response dog. Usually, there is a need to accept that attempting to curtail communication patterns to maximise the chances of asserting privilege may be detrimental to your ability to respond in a swift and effective manner.

13 See https://www.linklaters.com/insights/publications/legal-professional-privilege/2023/global-guide-legal-professional-privilege

5

INVESTIGATING AFTER THE EVENT

5 INVESTIGATING AFTER THE EVENT

5.1 Finding out how the cow got into the ditch

After any cyber incident, there will be a need to find out how the "cow got into the ditch". Finding out how a cyber incident was able to occur is an integral part of ensuring that it never happens again. But there may be other reasons to investigate too. Sometimes, this can be to satisfy the expectation of a regulator or to get ahead and establish the facts ahead of any anticipated external investigation or litigation. Other times, it may be required to explain to your shareholders, customers or other stakeholders exactly what occurred. Whatever the reason for investigating, it is important to get things right from the outset.

5.2 Principles for a good investigation

When planning an internal investigation, there are several key principles to bear in mind.

- **Independence:** The first principle is independence. For the company to have faith in findings of the investigation, the investigation needs to be conducted with an appropriate degree of independence from those involved in the cyber incident itself. Exactly how far you need to go with this will depend on the situation. For instance, for a highly public cyber incident where you have committed to publishing the findings of the investigation, you may want an entirely independent investigation team reporting to, for instance, a group of independent non-executive directors. For a smaller and less high-profile incident, it may just be ensuring that the investigating team are not the same people who were involved in the incident and who would therefore be "marking their own homework". Either way, it's crucial to give this topic thought at the outset to avoid knotty issues later on.

- **Scope:** The second key topic to consider is the scope of the investigation. You may think it's obvious – it's investigating what led to the cyber incident – but it's very common for different individuals within a company to have different impressions of exactly what is being investigated, and for there to be scope-creep as the investigation progresses. For instance, is the investigation purely focused on the incident that occurred or similar "near-misses"? Is the investigation examining all the factors that led to the incident or purely focused on the most proximate technical causes?

  Our experience is that the best way to be clear on the scope of an investigation is to write terms of reference for the investigation that specify the questions that the investigation is seeking to answer. Often, these terms of reference have to be revisited as the investigation progresses and new issues are identified - but that in itself is a useful mechanism to ensure that your stakeholders are sighted and in agreement with the scope of the investigation.

- **Output:** The final topic to consider is how the output of the investigation will be used. For instance, if you anticipate that you may face legal action as a result of the cyber incident, the purpose of the investigation may be to ensure that you are prepared for future litigation. This may mean that you adopt a different approach for interviews and document creation than you would if, say, the investigation report is going to be published.

There is no "one size fits all" approach to investigations. The context of each situation will determine how the factors above are balanced to create a proportionate and appropriate investigation plan and to determine the governance to oversee the investigation.

5.3 But what about privilege?

Privilege is a key issue to bear in mind for any investigation. Put simply, privilege is the right of a party not to reveal the content of particular communications to another party. However, the rules of privilege vary significantly across different jurisdictions, and indeed don't exist at all in some countries.

Therefore, before investigating, it's vital to think about whether you are likely to want to assert privilege in any investigations or proceedings in future. Often, courts will apply the rules of their own jurisdiction to determine if a document is privileged. So if, for instance, a US headquartered company is subject to a cyber-attack that leads to litigation in the English courts, the English courts are likely to apply English rules of privilege to determine if documents that fall to be disclosed can be withheld on the grounds of privilege. Therefore, even if the investigation is carried out in the US by US people, it may be English rules that will ultimately determine what has to be handed over to your opponents.

This means that mapping out the jurisdictions where you may face claims or investigations and understanding their rules on privilege or confidentiality is an important step to take at the outset of a cyber investigation.

5.4 Hold fire a second…

That said, there may be times when kicking off an internal investigation is not the right thing to do. In the past, authorities across the world have cautioned companies about "*trampling the crime scene*", for instance where serious criminality is suspected and regulators would expect a company to give them the first opportunity to conduct interviews. Whether pausing is the right approach to take will again depend on the circumstances at hand but, again, it is worth considering this before diving into an investigation.

5.5 Setting the investigation up for success

Once you've concluded that investigating is the right thing to do – and the shape and scope of the investigation has been decided upon – thought then needs to be given as to how to execute the investigation. This will involve:

- **Getting the right team in place:** Again, depending on the situation, this may mean some combination of technical specialists, forensic technologists, lawyers and others. The degree of independence required, and whether there is a need to try to assert privilege over communications connected to the investigation will also be relevant factors to choosing the "right team".
- **Fail to plan, plan to fail:** A good investigation should have a clear scope (ideally, in terms of reference) and a clear plan. This should deploy all the usual hallmarks of good project management – defined phases, timescales, deliverables and a budget – but with the flexibility to adapt as the investigation progresses.
- **There is no "one size fits all" approach to sequencing an internal investigation:** For instance, sometimes, early-stage interviews are the best way to quickly develop an understanding of the key individuals and events. Other times, the review of documents and databases first followed by interviews can be more efficient. Sometimes, it is vital to reach "quick and dirty" early findings; other times, that would be entirely unhelpful.
- **The dog ate my homework:** Once you have scoped the investigation, it is vital to think about document retention. No-one wants to get midway through an investigation to find that key data has been destroyed as part of a routine process. Furthermore, there may be a positive requirement on you to preserve relevant documents and to prevent their destruction - for example, if litigation is threatened. Therefore, identifying the key sources of relevant data and ensuring they are retained is an integral part of the investigation plan.
- **People problems:** Any investigation will involve examining what people within your organisation did (or didn't do…). Therefore, handling individuals well and being mindful of their employee rights is crucial. Typically, companies will want to encourage individuals to be frank and honest when investigating. This can lead to awkward questions from interviewees – for instance, asking for assurances that they won't be subject to disciplinary action as a result of what they say. These kinds of requests need to be treated with extreme caution and, indeed, in some regulated sectors may be impossible to even consider offering. Typically, you don't want to tie your hands: what if that employee discloses to you that they were the insider that caused the cyber incident?

  In our experience, anticipating these questions and explaining that investigations are purely about establishing the facts – without any assurances being given about what may occur once those facts are established – is the most effective approach. Trickier issues often require specialist employment advice for the relevant jurisdiction.

5.6 The art of investigating

Finally, it may be obvious, but conducting investigations is a skill. Devising the parameters for the extraction and review of data, deploying the latest tools to get to the most relevant material quickest, conducting interviews in a way that is most likely to elicit the interviewees' true recollections, and balancing competing and contradictory accounts when forming conclusions: these are all topics that could form their own booklets. Botching the investigation can be worse than not investigating at all.

But done well, a robust, efficient and appropriately independent internal investigation can leave an organisation with a thorough understanding of what went wrong, a good chance of preventing similar incidents in future, and on a firm footing to interact with any future external investigations or litigation.

6

TIE THIS INTO YOUR OPERATIONAL RESILIENCE

6 TIE THIS INTO YOUR OPERATIONAL RESILIENCE

6.1 Impact and response

It is not enough to only ensure that an appropriate, and regularly tested, Incident Response Plan is in place (something that organisations have traditionally focused on), but also that those plans factor in the impact of any cyber-attack and that resilience activities have been undertaken to prevent issues before they occur.

Resilience involves identifying the risks and vulnerabilities associated with critical business services/processes and performing detailed risk assessments of the impact of an outage. These risks must then be treated.

6.2 WAR: Withstand, absorb, recover

Regulators sometimes talk about companies needing to be on a WAR footing: to be able to withstand, adapt, recover.[14] Put differently, what would happen to your organisation if it (or a critical counterparty) was unable to operate its information technology systems for an extended period of time.

The steps necessary to minimise the impact of any cyber-attack for your company will vary, but if you lose one or more critical systems what measures would you take to restore those systems and continue the business running in the interim?

In the cyber security space, that is likely to mean backing up data securely in a manner that would protect it against a ransomware attack and testing the quality of these back-up procedures to confirm that they can actually be used to restore those systems.

Another common factor is internal communications. If your email systems are locked up then communicating with staff, customers, regulators, etc. may rapidly become a problem. Clearly defined alternative communication systems, or even fall-back cloud-based email accounts might be necessary to keep lines of communication open.

CASE STUDY

NotPetya – the ultimate operational resilience challenge

The NotPetya was one of the most serious cyber-attacks to date. Originally planned as a targeted attack on companies in Ukraine, the malware spread to infect the networks of a large number of international organisations; in some cases, almost entirely disabling their computer systems.

In the aftermath of the attack, many of those companies had to improvise significantly. In almost all cases, employees lost access to corporate email and had to fall back on consumer tools like WhatsApp and personal Gmail accounts. Others had to fall back on manual systems and printed documents to try and keep the business running.

Similarly, many businesses found that NotPetya compromised their back-up applications, impairing their ability to restore their systems.

One of the impacted organisations, Maersk, was reportedly saved by a power cut in Nigeria. A copy of its Active Directory in Lagos went offline shortly before the attack, preserving it from the virus and allowing Maersk to rebuild its network using clean software.

The NotPetya virus is a salutary lesson on the potentially catastrophic impact of a cyber-attack. The attack is thought to have originated from Russia so also provides a vivid illustration of the growing threat of cyber-warfare. Nation-state actors have very significant technical and economic resources so have the capability to launch truly devastating attacks.

14 Resilience and continuity in an interconnected and changing world, June 2018, Bank of England (https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/resilience-and-continuity-in-an-interconnected-and-changing-world-speech-by-lyndon-nelson).

7

THIRD PARTIES AND YOUR SUPPLY CHAIN

7 THIRD PARTIES AND YOUR SUPPLY CHAIN

- Create a risk assessment framework for suppliers
- Conduct risk-based diligence into your suppliers
- Consider the role of third-party security certification
- Create a playbook with minimum contractual obligations
- Impose incident notification and response obligations on your suppliers

7.1 The threat

Attackers will try to penetrate your systems using lots of different routes. You should expect both direct attacks on your systems and attacks via the third parties you deal with, particularly your suppliers. Your supplier may have been given access to your systems (for example so the systems can talk to each other) and that may be something that the attacker can exploit.

This all means that a proper information security programme needs to go beyond the boundaries of your firewalls and look both up and down your supply chain.

CASE STUDY

A cyber-attack on a supplier portal

British Airways hosted a Citrix Access Gateway to allow remote access to certain of its applications. That included access by third-party suppliers, including Swissport who provide cargo services to British Airways.

A Swissport employee based in Trinidad and Tobago had their username and password compromised. The exact method by which this happened is not clear, but the gateway was not subject to multi-factor authentication, so the username and password were all the attackers needed to get access.

The Citrix Access Gateway should have provided a secure environment to contain the attackers, but they were subsequently able to “break out” and access the personal data for around 430,000 customers.

7.2 Risk assessments and diligence

While third-party diligence is an essential activity, it is also practically and logistically challenging. Most large organisations deal with hundreds, if not thousands, of third parties. A full assessment also requires you to look beyond your immediate suppliers to also consider their sub-contractors and sub-processors.

Just as the seven wives with seven sacks each containing seven cats meant a large number of travellers from St Ives, so the number of entities that present a risk to your systems expands exponentially as you move past your immediate counterparty down to their supply chain. This is not just a theoretical risk – we helped a client with a data breach caused by the negligence of a sub-sub-sub-sub-processor, six steps down the supply chain.

All of this means that a blanket approach to suppliers is likely to be both inefficient and ineffective. A proper risk assessment needs to be undertaken to identify and focus resources on the suppliers of greatest risk.

7.2.1 Inherent risk

The starting point is to assess the risk of each supplier. This can be assessed in two dimensions – the degree of access the supplier has to your systems and the sensitivity of the data being processed.

There are varying degrees of sophistication to this assessment. Some businesses set out specific criteria for this assessment using grids that refer to the number of records processed by the supplier and the specific types of data (eg so that sensitive information, such as health information, will always be treated as high risk).

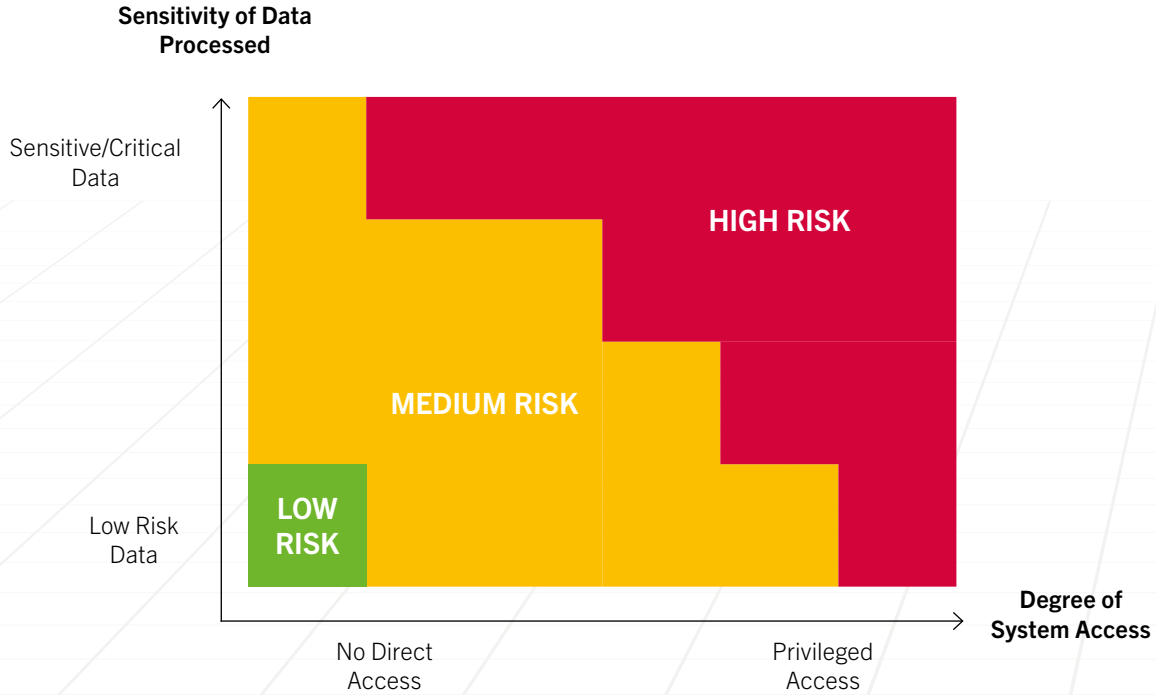
CASE STUDY

The need to focus not only on the sensitivity of the data which your supplier has access to, but also the degree of access to your systems, is best illustrated by the attack on Target Corporation.

Target used a small Pennsylvanian company to maintain some of Target's heating, ventilation and air-conditioning (HVAC) systems. The HVAC company was given access to a vendor portal to help manage those services.

The attackers used a phishing email to compromise the HVAC company's systems and then leveraged its access to the vendor portal to infiltrate Target's network, eventually accessing its point-of-sale systems and the details of more than 41 million customers.

The HVAC company is highly unlikely to ever be flagged in a security assessment based solely on the sensitivity of the data it handles. However, it is still a security threat because of the direct systems access.



7.2.2 Security due diligence into suppliers

The next question is the level of due diligence needed for each supplier. You should adopt a systematic and defensible approach based on your initial risk assessment.

That due diligence might consist of:

- **Doing nothing:** If the supplier does not handle sensitive data and has no access to your systems or premises, it might be sufficient to do nothing and focus your resources elsewhere. If your paperclip supplier does not have direct access to your networks, then a detailed security review may not be a good use of your limited resources.

- **Fact gathering and questionnaires:** The next step up is to obtain information about various aspects of the supplier's approach to information security. While suppliers might have their own description of their information security measures, this would ideally be done by way of a standardised questionnaire to ensure that precise information is obtained and to allow easier benchmarking against the minimum standards (which might vary to be more accommodating for low-risk suppliers).

- **Audit:** A more intrusive and resource intensive measure is to audit the security measures used by the supplier to directly verify the security measures they are employing. This level of diligence is expensive and time consuming (for you and your supplier) so will typically be limited to the highest risk suppliers.

- **Penetration testing:** The most intrusive form of diligence will be to conduct pen testing on the supplier's systems. This will only rarely be appropriate. Not only is this an intrusive and very expensive exercise, but it should also only be carried out with prior written approval from the supplier (particularly because in many jurisdictions pen testing without consent is likely to be a criminal offence).

Finally, it is important to keep proper records of the diligence conducted. For example, under Article 28 of the GDPR, controllers must only use processors that they can demonstrate provide "*sufficient guarantees to implement appropriate technical and organisational measures*" in relation to security. If your processor is subject to a data breach, data protection regulators will want to understand what steps were taken to verify that the processor has adequate security measures in place.

7.2.3 Third-party certification

In a multi-tenanted environment, it is increasingly common for suppliers to push back on bespoke diligence exercises and instead point customers to third-party audit and certification as a means to demonstrate that they have appropriate security measures in place.

This is inherently more efficient as it involves a single supplier-initiated in-depth security assessment; rather than multiple, potentially superficial customer-initiated audits (which might themselves become a security risk). Other benefits include the fact that those third-party audits are typically free (or at least already baked into the charges) and immediately available (subject to any confidentiality arrangements), minimising the cost and delay in this aspect of the contracting process.

However, third-party certification is not a universal panacea. At the least you should consider:

- **Date:** Is the third-party certification current and will the customer receive ongoing access to future certifications?

- **Scope:** Does the certification apply to the whole of the service actually being provided to the customer as opposed to a sub-set of the services? (Or a completely different service?)

- **Depth and quality:** Which certifications has the supplier achieved (and which do they not hold)? How deep is the assessment needed for that certification? Has the certification been issued by a reputable auditor?

- **Regulation:** Some regulatory regimes, particularly the GDPR and some financial services regulation, mandate direct audit rights so preclude you solely relying on third-party certification.

7.3 Standard clauses and playbooks

Alongside the practical diligence described above, you should make sure you get appropriate contractual protections from your suppliers. This can be helpful to verify and evidence the security measures the supplier purports to provide, and may provide a valuable contractual claim if you suffer liability due to the supplier's breach.

7.3.1 Minimum requirements

The starting point is to clearly identify the minimum contractual requirements you wish to place on your suppliers. These will originate from:

- **Regulation:** You may well be subject to regulatory obligations that require you to include specific obligations in your contracts with suppliers. The best-known example is Article 28 of the GDPR. However, there are a growing number of new supply chain requirements, such as under EU NIS II and DORA (see section 10.2). Similar requirements are set out, for example, in regulations issued by the Monetary Authority of Singapore and the Hong Kong Monetary Authority, each regulating financial institutions and outsourcing requirements in their respective jurisdictions.

- **Commercial stance:** You may have your own commercial requirements for the security standards you expect your suppliers to conform to, which might include flowing down obligations from your own customers.

We have set out a short checklist of the sorts of clauses typically used in relation to a third-party processing data on your behalf (see box High-level controls – third-party processors).

High-level controls – third-party processors

Set out below are the contractual commitments you need to ensure that minimum cyber security standards are met by your suppliers, and to provide a remedy if they don't live up to them.

Security

- The supplier should provide a general commitment to use appropriate technical and organisational measures to protect your information*
- The supplier should comply with specific security obligations in relation to matters such as encryption of data*
- The supplier should ensure that its systems are patched and up to date
- The supplier should use appropriate anti-malware software and have appropriate EDR systems to detect any intrusions into its network

Personnel

- The supplier should ensure that its personnel keep your information confidential* and access rights to your information are limited
- The supplier should ensure that all its personnel complete appropriate cyber security training
- The supplier should ensure that access to its systems is subject to multi-factor authentication

Supply chain

- The supplier should only use sub-processors with your permission or after notifying you of their use*
- The supplier should flow down security obligations to sub-processors and ensure that the sub-processor complies with those obligations*

Verification

- The supplier should have appropriate measures in place to test and verify its security measures*
- The supplier should produce evidence that it is complying with these obligations*
- The supplier should allow you to audit that compliance*

Notice of breach

- The supplier should tell you promptly, possibly within a specific time limit, if they suffer a data breach*
- The supplier should provide you with details in relation to the breach to enable you to respond*
- The supplier should take appropriate remedial measures following any breach

Data

- The supplier should return or delete your information at the end of the relationship*
- The supplier should put appropriate measures in place to safely and securely back-up your data*
- The supplier should ensure that all data is deleted securely

Remedy

- Ensure that you have rights to recover any losses that result from the supplier's breach
- Ensure that you have the right to terminate if there is a serious data breach

* These are mandatory under the GDPR if you are a controller and employing a supplier who acts as a processor.

7.3.2 Standard clauses and playbooks

These minimum standards should be reflected in a set of standard clauses to ensure that they are applied consistently across the whole of your supplier base.

However, it may be sensible for these clauses to flex according to the risk associated with a particular supplier. Recognising that not every supplier will automatically sign up to every clause they are presented with, these should normally be supplemented by a playbook or other identified fallback positions that can be accepted in relation to information security.

One common point of contention in relation to these clauses is whose security standards should apply. A customer will often want its particular standards to apply, whilst the supplier might well have existing information security processes that it does not want to amend to meet the peculiarities of one customer.

The resolution of this issue will partly depend on each party's leverage, though customers can help by ensuring that the requirements they mandate are genuinely necessary and not excessively specific. In other words, those standards should set out a broad and genuine baseline of security principles which all suppliers should be able to agree to.

7.3.3 Unlimited liability and indemnities

Another point of significant contention is whether liability for breach of these security obligations should be uncapped and if recovery of liability should be on an indemnity basis.

The answer to this issue will vary greatly depending on each party's leverage, the governing law of the agreement and market practice. However, under English law at least, it is increasingly common for customers to ask for unlimited liability, or at least a super-cap, for data breaches. It is also common for customers at least to ask for recovery liability on an indemnity basis (albeit suppliers will push back hard on this request and under English law it is not clear that this materially enhances a straight claim for breach of contract).

7.4 Incident response for suppliers

Finally, you should ensure that your incident response process addresses breaches originating from your suppliers.

The starting point is to ensure that your suppliers provide you with prompt notification of any such security breach. This obligation should be directly imposed on your supplier in the relevant contract (see section 7.3.3) and should address the following issues:

- **Trigger:** What is the trigger for the supplier to notify you? While you very much expect to be notified if your data is affected by an actual breach, should you also be notified if the supplier just suspects that a breach might have taken place? This lower trigger might result in some false alarms but also provides valuable early warning, given the potential lag between a suspected breach and confirmation that the breach has actually taken place.

- **Timing:** How long should the supplier have to notify you once it suspects/becomes aware of the breach? These timeframes are now typically relatively short, driven by the short notification window under the GDPR, meaning that suppliers will typically be obliged to notify their customers promptly and likely within 24/48 hours.

- **Details:** The mere fact that a breach has taken place is not enough. You will also need to know exactly what data has been compromised, when it was compromised, how it was compromised and what is being done to remediate the situation. This information is needed to calibrate any response, and might also be needed for regulatory notifications and notifications to affected clients and individuals.

- **Remediation:** You would expect the supplier to also commit to remediate the current breach and to remediate any security vulnerability that allowed the breach to take place. This might also include providing a report detailing the reasons for the original breach.

- **Liability:** Your supplier's breach may cost you time and money, both in terms of your own investigation and any potential liability you may have to your clients. An obligation on the supplier to reimburse you for these costs can be a valuable remedy.

8

THE INSIDER RISK

8 THE INSIDER RISK

8.1 The threat

While much of the cyber focus is on external attacks, it is important to always remember the threat from insiders.

Those risks range from simple negligence (such as an employee who accidentally opens an email with a virus), to criminal behaviour (such as espionage), through to deliberate attempts to damage the business.

8.2 Solutions

The insider risk is inherently difficult to address as the threat comes from within your network. It can be very difficult to determine if a user is simply doing their job, rather than doing something malicious or negligent.

8.2.1 Staff vetting

This makes staff vetting important. You need to ensure, at the least, that new users are who they say they are and do not arrive at your organisation with a track record of past misbehaviour or criminal offences.

However, the extent to which background vetting is permitted varies from jurisdiction to jurisdiction. In particular, there are a number of jurisdictions in which the ability to verify individuals' criminal history is either limited or non-existent. The UK Govenment maintains an international survey of who can apply, how to apply and contact details for criminal record checks overseas.[15]

CASE STUDY

Insider risks – from Cillit Bang to Edward Snowden

Insiders create a wider range of risks to contend with. Disgruntled employees have chosen to take out their frustrations on their employers in a wide range of ways.

For example, Mr Sobolewski was employed by a market research company. He was upset that he didn't get a pay rise. In revenge, he spent nearly three years pouring Cillit Bang into the company's servers. The servers failed repeatedly, costing his employer thousands of pounds in out-of-hours fixes and business disruption. Mr Sobolewski was jailed for eight months for criminal damage.

An insider was also the cause of a major data breach at the supermarket Morrisons. Mr Skeleton was part of Morrisons' IT audit team and sold slimming drugs on e-Bay as a side-hustle. He was disciplined after posting packages of the slimming drugs using Morrisons' post room. In revenge, Mr Skeleton extracted a file containing personnel details for all 100,000 Morrisons employees and then leaked it online. This led to a significant class action which was ultimately dismissed on the basis that Morrisons were not vicariously liable for Mr Skeleton's action. Mr Skeleton was jailed for eight years for fraud, computer misuse and unlawful disclosure.

Insiders' access to sensitive systems can mean they represent a potentially significant information security risk. The most well-known insider is Edward Snowden. He was a computer intelligence consultant working for the US National Security Agency. After the concerns he raised were dismissed, he used his administrator privileges to extract millions of highly confidential documents which were then provided to the press. Mr Snowden now lives in exile in Russia.

15 https://www.gov.uk/government/publications/criminal-records-checks-for-overseas-applicants

8.2.2 Zero trust and access controls

It is also important to put the right technical controls in place to prevent misuse by staff on your network.

The zero trust principle (discussed below) means assuming that even those inside your network are potentially malicious actors and so need to be continuously validated. This should be backed up by a process to properly define the access rights given to those staff.

The general principle is that those staff should have the minimum access rights necessary to do their job and those access rights should be reviewed on a regular basis. One particularly effective way to do this is for those access rights to automatically expire after a certain time, obliging the users to reapply for those access rights if they are still needed. This not only helps protect against a malicious insider but also protects against third-parties who, once they have a foothold in your systems, will look to traverse your network to attack other systems.

8.2.3 Data loss prevention (DLP)

DLP technology allows you to detect and prevent the unauthorised exfiltration of sensitive data from your network. It does this by inspecting the content of messages and conducting a contextual analysis of data sent via the network or stored on a device. It can then use an internal ruleset to flag suspicious activity.

For example, the technology might scan all emails and flag any containing more than a certain number of credit card numbers or social security numbers. Those emails can then be blocked and/or manually inspected.

8.2.4 SIEM and UEBA

Security information and event management (SIEM) software and user and entity behaviour analytics (UEBA) can be used to combine data from multiple sources and to analyse aberrant conduct that may point towards the risk of data loss. Some view this technology as profiling. It has seen increasing usage across businesses, but requires significant legal oversight and review.

8.3 Privacy issues can constrain solutions

While tracking and monitoring the activity of users on your network is an important security measure, it is not always straightforward and in some jurisdictions it can conflict with other laws, particularly data protection laws.

For example, organisations operating in the EU will have to contend with both general data protection rules under the GDPR and specific wiretap laws, which can prevent organisations from looking at the content of messages, even those travelling over their own networks.

It is important to identify these constraints before rolling out this type of technology and to take the correct remedial steps, such as notifying staff of the technology and consulting with the relevant Works Council.

EXAMPLE

Conflicting national approaches to DLP

The UK: The use of DLP and similar technology to track and monitor employees in the UK will need to comply with two key pieces of law. The first is the UK GDPR, which applies broad data protection obligations. The second is the Investigatory Powers Act 2016, which prohibits the interception of electronic communications save in limited cases, such as where it is done for business purposes under the Investigatory Powers (Interception by Businesses etc.) Regulations 2018.

DLP and similar technology are not inherently incompatible with these laws, but you should:

- ensure that the technology is only used in a legitimate and proportionate manner and that a data protection impact assessment has been carried out to assess the potential privacy risk;
- notify employees about the use of technology (though there is no need to get their consent); and
- make sure that other relevant measures are taken, such as ensuring the security of any information collected and not keeping it for an excessive period.

France: In contrast, the position in France is more restrictive. Monitoring will have to comply with not just the EU GDPR, but also the Labour Code and rights to privacy under the French Constitution.

In practice, this means that in addition to the controls necessary in the UK, any monitoring should not be continuous and should not include personal communications. There are also additional administrative steps such as consulting the relevant Works Council, and the Labour Inspectorate may need to be notified as well.

Reconciling these controls with the need for a robust DLP solution can be challenging.

9

ESSENTIAL TECHNICAL SECURITY MEASURES

9 ESSENTIAL TECHNICAL SECURITY MEASURES

- Conduct a regulatory mapping exercise to identify baseline obligations
- Ensure that data is encrypted where appropriate
- Ensure that strong passwords and MFA are used
- Control/restrict the use of privileged accounts
- Ensure that a robust patching policy is in place
- Confirm that appropriate malware detection and end point detection tools are used
- Confirm that appropriate SIEM and data logging tools are used
- Conduct a threat modelling exercise
- Ensure that periodic penetration testing and frequent vulnerability scanning is carried out
- Address new AI risks

9.1 Prevention is better than cure

The best way to deal with a cyber-attack is to stop the attackers getting into your system in the first place. Poor security means attacks are more likely to be successful and to cause more damage. It also means much greater exposure to regulatory enforcement and civil claims.

Putting in robust information security measures is complex and wide-ranging and requires significant technical expertise. Like many other specialist areas, it also has its own language and jargon.

This handbook can only scratch the surface of this topic. However, we identify the key building blocks you would expect any large business to have in place and identify some of the key technical terms used in this field.

The presence or absence of these building blocks are seen as "proxies" for good or bad security. For example, if attackers gain access to your system through long-unpatched servers and you haven't got multifactor authentication in place, regulators and claimants will rightly see that as *prima facie* evidence of bad security.

9.2 Defence in depth

> to assume what they call the perimeter can't be penetrated is probably delusional.
>
> **Sir Archie Norman**[16]

Importantly, there is no silver bullet you can use to ensure your systems are fully protected. Your cyber security strategy should apply multiple layers of protection to prevent attackers from penetrating your systems. However, it should also assume those measures will not always be effective and so then seek to detect and minimise the harm if those initial protections fail.

The most serious information technology incidents are typically those in which either there has been a failure by creating a single point of vulnerability or there have been multiple failings across different systems.

For example, the Interserve ransomware attack was initially caused by an employee falling for a phishing attack and installing malware on their device. The EDR solution identified the malware but failed to properly remove it, and there was no further investigation. Having obtained a foothold, the attackers then used vulnerabilities in unpatched internal servers to encrypt various internal databases. Had any one layer of defence been stronger, the attack might have been averted; or at least been much less harmful.

16 Discussing the cyber attack on Marks & Spencer. See *The Rest is Money* podcast (Episode 235).

9.3 Regulatory mapping and standards as benchmarks

Your security measures also need to match up to your regulatory obligations.

Historically these have been expressed in broad and flexible terms. For example, the key obligation under the GDPR is to implement "appropriate technical and organisational standards to ensure a level of security appropriate to the risk". While this is fleshed out with broad references to encryption, resilience and testing, the obligation is still expressed in very high-level terms.

There are benefits to regulating in broad terms. It is technologically neutral, loophole free and won't ever become outdated. It also looks superficially attractive to companies, suggesting broad discretion about what measures are applied. Nevertheless, regulators will often flesh out these obligations by interpretating them as requiring compliance with all relevant guidance. This means that these generalised standards are often much tougher than expected.

However, it is increasingly common for new cyber legislation to set out detailed and prescriptive security obligations (see The NIS II checklist) and these requirements may well become a de facto "benchmark" for companies, even if not directly subject to that legislation.

CASE STUDY

Pay attention to guidance – the Marriott breach

This breach arose out of an intrusion into the IT systems of Starwood Hotel which had recently been acquired by Marriot.

This was a breach of the general requirement in the GDPR to use "appropriate technical and organisational measures" to ensure an appropriate level of security. While this feels likely a vague and woolly standard, it was fleshed out through heavy reliance on guidance. This led to four detailed technical security failings:

- Insufficient monitoring of privileged accounts. Some controls were in place, but greater logging might have helped Marriott to detect unusual behaviour by the attackers.
- Insufficient monitoring of the customer databases. Marriott had three logging and intrusion detection systems (one of which alerted Marriott to the intrusion), but the regulator considered that the alert triggers should have been broader and so detected the attackers earlier.
- Failure to properly control the software running on its servers through the use of "binary software whitelisting". While the regulator appears to accept that this was rarely implemented at the time and might not have been effective, it considered that the failure to use binary software whitelisting was a breach.
- Encrypting card data on its database but not other personal data, such as passport details. This was for performance reasons, but Marriott could not provide a risk assessment to support this decision.

The penalty notice refers to no fewer than nine different pieces of IT security guidance, including guidance from NIST and Microsoft.

For UK companies, compliance with NCSC guidance should now be seen as mandatory.

9.4 Key technical defences

Encryption

Encryption is a basic and fundamental security measure. If your staff are storing sensitive information on unencrypted laptops, or sending it by email in an unencrypted attachment, you will face difficult questions from regulators and civil claimants if they go astray.

However, you also need to look at encrypting sensitive information stored within your network. A classic example of this is password files which should not only be hashed (a form of one-way encryption) but also salted (which effectively hashes each password slightly differently). Similarly, other sensitive information should be encrypted. In the Marriott breach (see Case Study: Pay attention to guidance – the Marriott breach) the regulator was highly critical of the decision not to encrypt servers containing information such as passport numbers.

Strong, properly managed passwords

Everyone knows about the need for strong passwords. If your employees are still able to use weak passwords to access your systems (eg "*passw0rd*", "*letmein*" and "*123456*") that is a major risk.

Complex passwords containing mixed cases and special characters are better. Even better are more memorable phases such as three random words (eg "*cirrus_socrates_particle*").

Your systems should also have measures to prevent brute force password attacks (eg making multiple attempts to guess the password). That might include locking the account after a certain number of incorrect guesses or limiting the rate at which log-in attempts are allowed. Regulators will have little sympathy if you don't at least get these basic points right.

Malware and software whitelisting

You should have a range of measures to detect and prevent malicious software operating within your environment. That is likely to mean using anti-malware software.

It also means controlling which software can run within the environment so that only vetted applications can be executed – for example, maintaining a "binary whitelist" of approved applications and preventing users from installing any application that is unsigned or has an invalid signature.

Multi-factor authentication (MFA)

Even a strong password may not be enough. It might be compromised, for example if a password file is compromised or the password is used across multiple sites.[17] Multi-factor authentication (MFA) identifies an individual by a combination of two (or three) of the following – something the individual knows, something the individual has or something an individual is.

For example, to log in, a user might have to provide a password and would then provide a one-time code sent to their mobile phone. An attacker would need to know the password and have access to the phone, to succeed.

We have seen multiple cases in which the lack of MFA has led to security incidents. As a result, it is no longer truly optional. With every regulator calling for it, MFA is required as "reasonable security."

Privileged accounts (PAMS)

Accounts with elevated permissions or administrative rights are generally more capable of doing harm to a system than a 'standard' user account. They may be able to install malicious software or disable protective controls, for example, which is why they are a valuable target for cyber attackers.

For this reason, 'day-to-day' activity should always be performed in the context of a 'standard' user account, without administrative rights.

Administrative rights should be tightly managed and only granted to designated staff for specific tasks, when required. Best practice is for IT admins to have separate, individually identifiable accounts for such purposes and for their use to be monitored and logged.

Consider the use of a privileged account management tool to assist with this.

17 Obviously, password files should be hashed and salted, but sharing passwords across multiple sites is still very bad practice.

Patch management

Another common - but very serious - failing is the lack of a proper vulnerability and patch management programme. Modern software is complex and often has security weaknesses. Once those weaknesses are discovered, they can be exploited by attackers but also patched by the software provider. Failure to apply those patches leaves the software wide open to attack (see Case Study: Patch! Patch! Patch! The Equifax breach).

In simple terms, it's like everyone becoming aware that they can get into your house via the back door because the lock doesn't work – and then just not fixing the lock.

All businesses should have a process in place to identify these vulnerabilities and apply patches in a timely manner. This is a particular issue for open-source software as there is generally no third-party proactively sending you the patch – you need to get it yourself.

Endpoint Detection and Response (EDR)

Even if you have done all the right things, you should still assume that the bad guys will get in. The right security mindset is to approach each measure on the basis that all the others have failed. In other words, to protect yourself, you need more than a hard perimeter to your environment but also multiple layers of security and intrusion detection underneath it.

You should check that you have deployed EDR – a form of intrusion detection. It looks for anomalous activity and tries to stop it. Years ago, it was a sophisticated tool used by only by the most sophisticated companies. Now everyone needs it.

SIEM and logging

SIEM allows you to move beyond simple end point detection and look for suspicious activity right across your systems.

It operates by collecting a wide range of signals from across the network and then will typically use machine learning or other advanced models to identify potential anomalies in that data that are indicative of potential infiltration. For example, a SIEM might look for a number of different trigger correlations, such as:

- **Brute force:** Very fast and repeated attempts to access resources (eg guessing URLs or file locations) are a trigger, given that this may be done faster than humanly possible and is an inherently suspicious activity.
- **Suspicious locations:** A user who ends the working day using an IP address in London but logs in a couple of hours later from Bangkok would trigger an alert, given the physical impossibility of physically transferring between those locations within that time.
- **Large scale copying:** Attempts to copy or move large amounts of data around might trigger an alert if this is unusual, as this is indicative of the potential exfiltration of data.

The use of SIEM technologies depends on initially collecting suitable logging data. This data should also be securely stored (likely for a number of months) to allow you to retrospectively look at potential incidents.

These logs are a vital record to unpick if you have been infiltrated, how you were infiltrated and what you need to do to remedy the situation. Without them, you are flying blind.

Secure vendor portals

There have been numerous examples of customers whose suppliers have been compromised and whose access to a vendor portal has then been used to compromise the customers' systems (such as the compromise of British Airways Citrix Access Gateway or the infiltration of Target Corporation).

Accordingly, any vendor portal or other systems to which those suppliers have access are properly hardened, so that even if hackers do get access to them, they cannot break out into the wider network. You should also make sure that your suppliers have minimum security standards in place to prevent their systems being compromised.

Zero trust

Similarly, you can protect the inside of your network through a zero trust security framework – this essentially means assuming that even those inside your network are potentially malicious actors and so need to be continuously validated.

As an analogy, it means not just checking your staff's passes when they enter your building in the morning, but also continuously checking them through the day as they move between rooms, use facilities etc.

Network segmentation and data enclaves

Finally, your approach should reflect the underlying risk of the data or systems, with the most sensitive being segmented into their own sub-network. This enclave can be subject to additional security and access controls and all data entering or leaving that enclave will be subject to careful inspection. Your crown jewels need special protection.

The sensitive data or systems might even be kept on an air-gapped system with no connection to any outside network. However, this is usually reserved for critical systems such as air traffic control systems, financial markets infrastructure or control systems for nuclear power plants.

> The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts.
>
> **Gene Spafford**

CASE STUDY

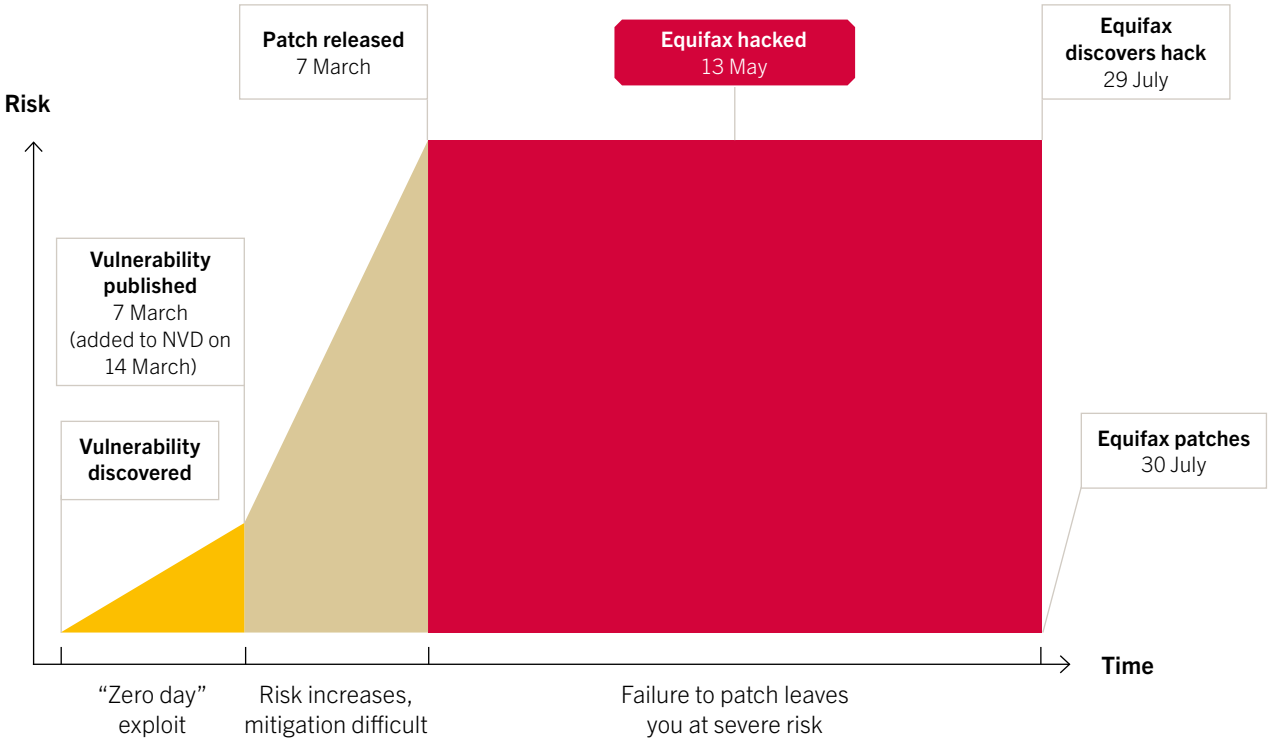
Patch! Patch! Patch! The Equifax breach

A lack of patching resulted in Equifax suffering a data breach affecting hundreds of millions of people. The breach was extremely serious and triggered investigations and litigation from around the globe. Equifax says it has spent US$1.4bn on clean-up costs and measures to improve its security. It also reached a US$700m settlement with the FTC to resolve consumer claims.

The breach had multiple causes but at its heart was a failure to patch its software. Modern software packages are extremely complex and almost all have weaknesses – known as vulnerabilities – that can be exploited by hackers. The key questions are who knows about the vulnerability first, when it is fixed and how quickly that fix is applied.

This is a particular issue for open-source software. Given that such software is normally used without any formal support or maintenance package, users are responsible for tracking vulnerabilities and patches themselves. Failure to do this can be devastating.

In this case, Equifax used Apache Struts, a popular open-source software tool used for websites. On 7 March, a vulnerability was discovered and a patch was promptly released the same day. However, Equifax did not apply that patch and over two months later it was hacked, on 13 May. Equifax did not detect the attack for a further two months. While it patched the vulnerability the day after discovering it, the damage had already been done.



9.5 Testing those defences – red v blue teams

Your "blue" team has the job of pulling these security measures together, but the real test comes from your "red" team, who will try and take them apart.

There is no point putting these security measures in place unless they are effective to secure your systems. In other words, you need a red team to check that they actually work. Being able to demonstrate that there has been an effective and independent validation of the security of your systems is a powerful factor to help defend against regulatory and civil liability should an incident occur.

9.5.1 Threat modelling

The starting point is threat modelling: carrying out a systematic and structured process to assess the environment, identify potential vulnerabilities and consider potential attackers.

This is an open-textured exercise but there are numerous different frameworks that can be used to help (eg NIST has its own threat modelling methodology), but the broad outline for these exercises is set out below.

The four stages of threat modelling

	Eg
Who might attack?	> Cyber criminals (eg ransomware) > Nation states > Hacktivists > Insiders > Espionage
What are the key risks?	> Business disruption > Damage to critical infrastructure > Reputational damage > Loss of IP > Fraud/extortion > Regulatory and civil liability
What types of attacks might I face?	> Phishing/spear phishing > Denial of service > Supply chain attack > Vulnerability exploitation
How do I mitigate those attacks?	> Withstand > Absorb > Recover

This process of identifying and ranking threats to your systems is a valuable way to double check the security measures you have in place and to help prioritise your resources.

9.5.2 Penetration testing

The core of any validation exercise is penetration or pen testing. This is the acid test for any information security programme – it effectively involves attempting to gain access to your systems using the sorts of tools and techniques an attacker might use.

A 'successful' pen test will reveal vulnerabilities that can be rapidly addressed to help harden the system against future attacks. An 'unsuccessful' pen test will provide some degree of comfort that those systems are secure.

Key pen test considerations:

> **Who carries out the penetration testing?** Organisations can test their own systems, but they are most often conducted by specialist third-party penetration testing providers. That will not only ensure that this is done by experienced testers, but also that they will be independent. There are various lists of "approved" pen testers, such as the accredited CBEST service providers who have been through an accreditation process that is undertaken by the Bank of England.

> **What to test?** The testing will clearly need to cover the critical systems used by the business but you shouldn't forget other systems, particularly legacy systems. There are numerous examples of old legacy systems being compromised and the hackers then using that system to pivot their attack to mission critical systems.

> **How often to test?** Information security is dynamic, with new attack vectors emerging over times. Similarly, systems change potentially creating new vulnerabilities. This means that the penetration testing should occur on a regular basis. A typical approach would be to test at least annually, along with additional testing whenever there is a significant system change (usually included within the scope of the project delivering that change).

Penetration testing is an essential means to ensure the security of your systems in practice, but it is important to recognise the dangers and limitations of penetration tests.

Two key pitfalls are incomplete penetration testing, and not fixing problems identified in the penetration testing. The former is problematic because if a non-tested system is compromised, regulators may see this incomplete testing as a culpable failing. The latter is positively dangerous and a huge own goal when dealing with regulators or civil claims.

9.5.3 Vulnerability scanning

Vulnerability scanning makes use of automated tools to sweep across an organisation's systems looking for known vulnerabilities such as missing software patches, out of date software, or misconfigurations.

Vulnerability scanning is not an alternative to penetration testing. It is a good housekeeping practice that should be performed on a continual basis, with IT admins responding to any issues raised in the scanning reports. It also helps to validate whether patching processes are being implemented effectively.

9.5.4 Bug bounties

An extension to penetration testing is to set up a bug bounty programme. This involves making an open offer to pay third parties who alert you to vulnerabilities in your systems.

This can be a valuable exercise, particularly for large scale consumer services, as it ensures that you are alerted to any vulnerabilities in a timely manner and should progressively 'harden' your systems as vulnerabilities are identified and fixed.

A number of large technology companies have bug bounty programmes, such as Apple, which has doubled the pay-out for finding vulnerabilities to a maximum of US$2m for a network attack with no user interaction – one of the highest payouts in the industry.

However, these programmes need to be carefully structured to not only clearly identify which vulnerabilities qualify and how the bounty will be calculated, but also to make sure that this does not provide carte blanche to hack your systems. For example, the programme might carefully delineate exactly what types of attacks are permitted and to strictly control what happens with any data collected as part of that process.

Regulatory "benchmarks" – The NIS II checklist

There are various detailed cyber requirements which are increasingly seen as *a de facto* cyber benchmark. For example, in the US the NIST Cybersecurity Framework 2.0 is voluntary, but is increasingly seen as best practice in the US by regulators and the courts.

Similarly in the EU, the NIS II Directive is supplemented by an implementing regulation (Implementing Regulation (EU) 2024/2690). While that regulation only applies to certain types of entities (such as cloud computing providers, managed service providers, online marketplaces and social networks) others would be well advised to consider its requirements given it may form *a de facto* regulatory baseline for cyber security.

This implementing regulation sets out a long list of headline obligations (below), each of which is then supplemented by specific and detailed requirements, which are then in turn subject to further guidance from ENISA (including examples of evidence and mapping to standards (e.g. ISO/IEC and NIST).[18] Some of those more detailed requirements are mandatory but others operate on a "comply or explain" basis. In other words, if an entity considers it is not appropriate or feasible to comply with that obligation, it must document its reasons why.

- **Overall security policy:** This should include defined roles and responsibilities.
- **Risk management policy:** This should set out a risk management framework and compliance monitoring measures, and allow for an independent review of cyber security.
- **Incident handling:** This requires an incident handling policy, measures to monitor and log network and information systems, mechanisms for event reporting, and assessment, classification and response processes (including carrying out post-incident reviews).
- **Business continuity and crisis management:** A business continuity and disaster recovery plan should be in place, supported by backup and redundancy measures and a crisis management framework.
- **Supply chain security:** A supply chain security policy is required alongside the use of minimum cyber security obligations in contracts and a directory of suppliers.
- **Security in acquisition, development and maintenance:** This requires appropriate measures to be used in the acquisition of services and products alongside ensuring appropriate configuration management and the use of secure development lifecycle and change management.

Added to that are measures for security testing, patch management, network security, segmentation, virus detection, vulnerability handling and disclosure.

- **Process to assess the effectiveness of cybersecurity risk-management measures:** This includes ensuring appropriate policies are in place.
- **Basic cyber practices and security training:** Measures should be in place to raise awareness of cyber and train staff.
- **Cryptography:** Measures should be in place to encrypt and use cryptographic authentication where appropriate. These should be supplemented by appropriate policies on key handling and algorithm selection.
- **Human resources:** Staff should be subject to background checks and commit to comply with cyber measures. Appropriate disciplinary processes should be put in place for violations of the entity's security policies.
- **Access controls:** Appropriate policies and processes should be in place to manage access rights, particularly privileged and administrator accounts. Appropriate measures should be in place in relation to identification and authentication, including the use of multi-factor authentication.
- **Asset management:** Assets should be classified and inventoried, and be subject to appropriate handling policies, including in relation to removeable media. Assets should be returned on termination of employment.
- **Environmental and physical security:** A broad range of measures should be in place including assessing the risk to power and communications, protecting assets from physical and environmental risks and putting appropriate physical access contr

9.6 New AI risks

Artificial intelligence is an important new technology. It will have significant and far-reaching effects for most businesses. That applies to cyber security just as much as any other issue.

9.6.1 Turbo charging threat actors

One key change is threat actors' use of AI tools to turbo charge their operations. These tools can be used to suggest potential attacks, automatically generate code and even execute those attacks. The net effect is to bring down the "barriers to entry" and increase the threat actors' efficiency.

The AI tools are also being used for social engineering and AI phishing. They can automate the work needed to gather information on persons of interest and craft more effective personalised phishing emails. All this means that the volume of attacks is likely to rise and a broader range of targets will be attacked.

These tools might not match the capabilities of an expert human threat actor, but that doesn't really matter. If a broader spread of less sophisticated attacks allows a threat actor to penetrate your systems, that is all that matters. In addition, while most AI tools are configured to prevent them being used for cyber-attacks, there are a large number of tools out there and some can be jailbroken.

Finally, this is not a one-sided affair. AI tools also have an important role defending businesses against cyber-attacks, e.g. by helping to automate penetration tests and enabling more sophisticated SIEM to detect intruders. However, the rules of the game are changing and businesses need to adapt.

9.6.2 Risks to LLMs and other AI systems

The second issue is that most businesses are rolling out LLMs and similar AI systems for use by their employees in their normal day-to-day activities.

The information contained in those systems can be extremely sensitive. In a recent case, a consultancy's in-house AI system was compromised using a SQL injection. This identified the system had over 40 million prompt messages that, one assumes, contain highly sensitive information about the consultancy and its clients. Added to that, were around 200,000 documents uploaded to the system and the system prompts and AI model configurations.

- **Rapid deployment:** Part of the concern is the speed at which these models were rolled out and upgraded. Pressure from the business or leadership to roll-out these tools should not short cut the normal processes to test and assess any new application. A proper (AI)DLC is still needed.

- **Prompt injections and other novel attacks:** There are also a new range of ways to attack these systems, such as prompt injections which use specially crafted instructions to trigger an LLM to execute unexpected or malicious actions. Existing firewalls and other mechanisms may not be able to conduct the semantic text analysis needed to detect these attacks. Your penetration testing strategy should now explicitly address these new risks.

- **Supply chain:** Your tools will often rely on third party models or AIaaS. These may be novel and rapidly evolving so might not have the security maturity of other software applications.

- > **DoLLM:** Many companies are turning to AI-powered chatbots as the first point of call for their customers. There is concern these could be subject to denial-of-service attacks due the higher computational load of chatbot responses and the fact these attacks might not be detected by existing traffic-based DDoS tools.

9.5.3 Policy framework

Finally, it is worth considering how these new risks are addressed by your Information Security Programme. These risks are new, but not that new. Regulators will expect them to be explicitly dealt with in your policy framework.

10

SPOTLIGHT ON FINANCIAL SERVICES

10 SPOTLIGHT ON FINANCIAL SERVICES

10.1 Under the regulators' spotlight

Financial services regulators have often led the way in setting and policing cyber security standards, as failings in this area pose a real threat both to customers and to the stable operation of markets and the financial system generally. These risks have only increased as the provision of financial services has become increasingly digital.

Improving cyber security is therefore a clear priority for regulators across the globe. For many firms, we see that translating into increasing supervisory engagement on cyber security and an increasing source of enforcement risk.

10.2 EU DORA

Within the EU, the regulatory landscape for financial services entities has been transformed as a result of the EU's Digital Operational Resilience Act, commonly referred to as DORA. This imposes burdensome new obligations, reflecting the critical role played by the financial sector and the potential for serious and systemic wider societal harm from cyber-attacks.

The obligations under DORA are significant, complex, and not restricted to cyber, and so are not described exhaustively in this handbook. Instead, we just highlight some key aspects of this new law:

- **Broad and pre-emptive scope:** The framework for financial services in the EU is generally fragmented depending on the type of activity a firm conducts. However, DORA has very broad scope applying to almost all EU financial services firms. It also pre-empts or replaces existing legislation and guidance in this area, such as NIS II and the EBA outsourcing guidelines.
- **The devil is in the detail:** Despite the detailed nature of DORA, it is not comprehensive and is supplemented by a number of secondary instruments, typically Regulatory Technical Standards ("RTS"). These RTS address a wide range of issues such as managing ICT risks, reporting of major incidents to financial regulators and subcontracting of ICT services.
- **Strong cyber obligations:** Financial services firms are obliged to implement a broad range of measures. This includes implementing a comprehensive risk management framework but also taking specific measures such as identifying and documenting their ICT environment, implementing intrusion detection systems, putting continuity and back up measures in place and conducting pen testing.
- **Breach notification:** Major incidents require initial notification of 4 hours after classification or 24 hours after detection of the incident. An intermediate report is required within 72 hours and a final report 1 month from the incident.
- **Supply chain:** There are detailed supply chain controls in DORA, including extensive minimum contractual provisions for contractors. In the case of ICT services supporting critical or important functions, this includes obligations such as co-operation with pen testing, full service descriptions and clear exit obligations.
- **Direct regulation of critical third parties:** ICT suppliers that have a particularly critical role can be designated as such and become subject to direct oversight by EU financial supervisory authorities. The supervisory authorities have used this power to designate suppliers such as Accenture, AWS and Microsoft.
- **Senior leadership:** The management body is responsible for the ICT risk management framework, including setting the budget for cyber activities and bearing the ultimate responsibility for managing the financial entity's ICT risk. The management body also needs to keep their cyber knowledge and awareness updated.

10.3 UK regulatory scrutiny and expectations

EU DORA does not apply in the UK, but UK financial regulators apply rules that seek similar outcomes. They are also focusing on firms' cyber and information security arrangements, particularly in the context of significant change programmes, even where no cyber incident has taken place.

As well as this bilateral engagement, firms may also be included in regulators' thematic work, including the Cyber Coordination Groups co-ordinated by the UK FCA[19] and the UK PRA's cyber stress testing and triennial CBEST penetration testing programmes.[20]

While firms are required to be transparent with the regulator, particular care is required in responding to such supervisory scrutiny, drafting written responses and preparing senior managers ahead of discussions, as where concerns are identified this can lead to independent reviews or testing being required (eg a skilled persons review or firm-specific CBEST testing) or even enforcement. The UK FCA and UK PRA have consulted on operational incident reporting rules which would clarify how firms and senior management can fulfil their existing notification responsibilities.

19 The most recent report can be found here FCA Cyber Coordination Group Insights 2024 | FCA

20 See Thematic findings from the 2024 Cyber Stress Test | Bank of England

The UK FCA and UK PRA have jointly issued rules and guidance aimed at improving operational resilience generally and cyber security as an element of that. These rules acknowledge that disruption – through cyber-attack or otherwise – is inevitable and so focus on improving firms' readiness to respond to disruption.

In summary, these rules require firms to identify important business services (where disruption risks customer harm, market integrity or systemic instability), set impact tolerances for the maximum tolerable disruption, assess whether it is able to respond and recover within those tolerances, and develop plans to come and remain within those tolerances. Extensive documentation of the relevant processes will be required, including internal and external communications plans.

Baked into the rules is an expectation of senior oversight and responsibility. A senior management function holder (the chief operations function, SMF24) is responsible for operational resilience, and boards are required to regularly review and sign off the firm's operational resilience strategy and self-assessment.

The UK FCA's cyber resilience capability questionnaire (CQUEST) makes clear their expectation that even a firm that is not subject to the operational resilience rules should have a board-approved cyber security strategy that identifies how it identifies and protects critical cyber assets and how it detects and responds to an incident, recovers from it and learns lessons from doing so.

If a cyber incident occurs, the FCA has issued guidance confirming that material cyber incidents must be reported. The UK FCA has said that an incident may be material if it:

- results in a significant loss of data, or the availability or control of a firm's IT systems;
- affects a large number of customers; or
- results in unauthorised access to, or malicious software present on, a firm's information and communication systems.

The Bank of England and UK PRA plan to consult on their policy relating to ICT and cyber risk management in 2026.

GLOSSARY

CISO
Chief Information Security Officer

DLP (Data Loss Prevention)
Technology that will attempt to detect, and stop, sensitive data from being exfiltrated from your systems (eg by scanning emails to see if they contain sensitive data)

EDR (End point Detection and Response)
Technology used to detect and prevent intrusions into your systems

EU DORA
The Digital Operational and Resilience Act (Regulation (EU) 2022/2554)

EU GDPR
The General Data Protection Regulation (Regulation (EU) 2016/679)

EU NIS II
The Network and Information Systems Directive II (Directive (EU) 2022/2555)

Incident Response Plan
The plan setting out how you will respond to a cyber incident

Information Security Policy
The policy, or policies, that set out your organisation's approach to protecting your data and systems

Information Security Programme
The measures your organisation takes to protect your data and systems

Malware or viruses
Malicious software intentionally designed to take unauthorised action such as disrupting a system or leaking confidential information

MFA (Multi Factor Authentication)
Accessing a system based on more than one of the following factors – something you know, something you have or something you are

NCSC
The UK National Cyber Security Centre. A government body that provides advice and support for the public and private sector in how to avoid computer security threats

NIST (National Institute of Standards and Technology)
A US non-regulatory agency that, amongst other things, issues voluntary cyber security guidance

Patching
Updating your software and systems in order to, amongst other things, remove vulnerabilities

Penetration testing (or pen testing)
An exercise to attempt to penetrate an organisation's systems to see if they have any vulnerabilities

Phishing
The sending of one or more fraudulent message to encourage the recipient to take an action such as providing information or opening an attachment

PRC or Mainland China or China
The People's Republic of China, which, for the purposes of this handbook, excludes the Hong Kong and the Macau SARs and Taiwan

Privileged accounts
Accounts which have a higher level of permissions/access than a standard user account (ie those accounts which can make changes to systems, update other accounts or take similar action)

Ransomware
Malware used by criminals to extort payments

SIEM (Security information and event management)
Use of data from multiple sources to try and identify aberrant conduct

Tabletop exercise
A simulation of a cyber security attack

TOMS
Refers to the use of appropriate technical and organisational measures which is a common benchmark in EU cyber legislation

UK FCA
The UK's Financial Conduct Authority

UK GDPR
The version of the EU General Data Protection Regulation assimilated into UK law after the UK left the EU

UK ICO
The UK Information Commissioner

UK PRA
The UK's Prudential Regulatory Authority

Vulnerability scanning
Automated assessments of systems, identifying common exploitable vulnerabilities

WAR
An assessment of your organisation's resilience. Can you withstand, absorb and recover?

Zero trust
A security model that is based on verification, not trust, such that devices are not trusted by default even if used within a network

Annex: Snapshot of cyber laws

Asia – Key cyber security/critical infrastructure laws[21]

	PRC	Singapore
Legislation/ legislative proposal	Cyber Security Law Measures for the Reporting of Cybersecurity Incidents	Cyber Security Act 2018
Who does it apply to?	Network operators, including "critical information infrastructure operators" (as designated by competent authorities). Network operators refers to owners and administrators of networks or network service providers.	"Critical Information Infrastructure Owners". "Provider of an essential service responsible for the cybersecurity of third-party-owned critical information infrastructure". "Owners of Systems of Temporary Cybersecurity Concern".
Security obligation	Various obligations to ensure that the network is free from interference, disruption or unauthorised access, and to protect network data. This includes the implementation of internal governance frameworks, anti-network attack measures, incident handling and logging, data classification, back-up and encryption.	Compliance with codes of practice and standards of performance, including restriction of access to authorised personnel, having processes in place to detect cyber security events, establishing disaster recovery plans, and conducting regular audits. Other obligations include requirements to conduct cyber security audits, risk assessments, cyber security exercises, and complying with written directions from the Commissioner.
Notice of breach obligation	Cybersecurity incidents are classified into four tiers: "general", "relatively severe", "severe", and "particularly severe". For incidents classified as "relatively severe" and above, there is a one-hour deadline in the case of critical information infrastructure operators.	A Critical Information Infrastructure Owner must notify the Commissioner of Cyber Security within two hours after becoming aware of a cyber security incident and must then provide supplementary details within 14 days of the initial notification.
In force	June 2017 (Cyber Security Law) November 2025 (Measures for the Reporting of Cybersecurity Incidents)	March 2018 (Cyber Security Act 2018 with significant amendments in October 2025)

21 Other countries with no substantive cyber legislation may have sector specific regulation, such as Indonesia which has regulation appliable in the financial services sector.

Hong Kong	Thailand	Japan
Protection of Critical Infrastructures (Computer Systems) Ordinance	Cyber Security Act B.E. 2562 (2019)	Economic Security Promotion Act Active Cyber Defense Law
Designated Critical Infrastructure Operators ("CIOs"), being entities which operate critical infrastructure.	"Critical information infrastructure". Draft amendments propose expanding scope to include cloud service providers and data centre operators hosting data for critical information infrastructure entities.	"Specified Essential Infrastructure Service Providers" across 15 business sectors including energy, telecommunications, finance, transportation, and postal services.
Various obligations including setting up and maintaining a computer-system security management unit, submitting and implementing a security management plan, conducting security risk assessments, carrying out security audits, submitting and implementing an emergency response plan, and notifying computer security incidents.	Various obligations including requiring that every critical information infrastructure entity must have a code of practice, organisational measures and a cyber security framework with prescribed minimum standards depending on the security category of the critical information infrastructure entity. This includes monitoring cyber threats and incidents, participating in cyber security exercises and governance requirements.	Various obligations including cyber security risks assessments, with appropriate incident response plan and internal accountability/control systems. The Economic Security Promotion Act also sets out a review process from the regulator on when and how a Specified Essential Infrastructure Service Provider can (i) introduce or (ii) entrust to a third-party the implementation of critical infrastructure facilities.
For a computer-system security incident which has disrupted, is disrupting or is likely to disrupt the core function of the critical infrastructure, the CIO must notify the Commissioner of Critical Infrastructure within 12 hours. For other incidents, the required timeframe is 48 hours.	The competent regulatory authority has to be notified swiftly in the event of a cyber security incident. Draft amendments propose changing this to 24 hours.	The Active Cyber Defense Law introduces mandatory reporting obligations to all Specified Essential Infrastructure Service Providers. The exact details and timelines will be set out in more detail as the implementation of the law progresses and comes into full effect in 2027.
1 January 2026	May 2019 (Cyber Security Act B.E. 2562 (2019)	May 2024 (The Economic Security Promotion Act) 2026 to 2027 (The Active Cyber Defense Law)

EU – Key cyber security laws

The key EU instruments imposing cyber security obligations on private companies are set out below. There are a variety of other cyber security instruments which are not set out below, such as the Cybersecurity Act which strengthens the EU cyber security agency, ENISA, and establishes a cyber security certification framework for products and services. Member States will also have a range of national cyber security laws which are not described below.

	Cyber Resilience Act (Regulation (EU) 2024/2847)	**DORA** (Regulation (EU) 2022/2554)	**NIS II Directive** (Directive (EU) 2022/2555)[22]
Who does it apply to?	**Providers of products containing digital technology**	**Financial services**	**Critical infrastructure**
Security obligation	Providers of products containing digital technology must ensure they are protected against cyber-attacks.	Applies a wide range of detailed obligations including conducting pen testing, putting incident response plans in place and prescriptive rules for their ICT service suppliers. Directors are responsible for the risk framework and must keep up to date with cyber risks.	General TOMs obligation including specific measures such as incident handling and supply chain control. The NIS II Implementing Reg contains further detailed obligations. Directors must be trained on cyber and can be liable for breaches.[23]
Notice obligations[24]	Incidents and exploited vulnerabilities must be notified to ENISA and national cybersecurity authorities of within 24 hours.	Major incidents require initial notification of 4 hours after classification and 24 hours after detection of the incident. An intermediate report is required within 72 hours and a final report 1 month from the incident.	Incidents having a "significant impact" on the relevant service must be notified "without delay" to the relevant regulator, with an initial notification within 24 hours, detailed report within 72 hours and a final report within one month.
Applies	December 2027	January 2025	October 2024

22 The EU Commission issued proposals to further amend NIS II in January 2026.

23 NIS II is a Directive so must be implemented by each EU Member State. This has led to a number of different approaches, including in relation to director liability which can result in directors facing direct fines in some jurisdictions or, in the case of Cyprus, even imprisonment.

24 The EU Digital Omnibus suggests creating a single entry point for breach notifications across a range of these instruments.

EECC Directive (Directive (EU) 2018/1972)	**GDPR** (Regulation (EU) 2016/679)	**ePrivacy Directive** (Directive 2002/58/EC)[25]
Telecoms	**All businesses**	**Telecoms**
General obligation to use TOMs.	General obligation to implement TOMS with specific reference to encryption, testing and resilience.	General obligation to use TOMS.
Security incidents having a significant impact on the operation of networks or services must be notified without undue delay.	Breaches that create risks for individuals must be notified to the regulator within 72 hours. Breaches that create high risks must be notified to the individuals.	In case of a particular risk of a breach of security of the network, the provider must inform the subscribers. All "personal data breaches" must be notified to the regulator within 24 hours.[26]
December 2020	May 2018	May 2011

25 As amended by Directive 2009/136/EC.

26 The 24-hour period arises under EU Regulation 611/2013, see Art 2(2).

US – The complex framework of federal cyber security laws and advisories

Please note this section addresses general federal cybersecurity laws and guidance. It does **not** cover sector-specific rules or state law. For example, all 50 US states have adopted data breach notification laws that vary significantly. This includes variations in the definitions of a "breach" and personal information, and the corresponding reporting obligations. In particular, New York and Massachusetts have stringent cyber incident reporting requirements and require companies to have robust written information security programmes.

	Law/Advisory Guidance	Date	Issued by	Summary
1	Cybersecurity Maturity Model Certification ("**CMMC**") 2.0	September 2025	Department of War	This CMCC is a unified standard for implementing cybersecurity across the defense industrial base. Phased implementation started in November 2025, with full rollout over three years to integrate the CMMC into Department of War contracts.
2	Executive Order on Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Orders 13694 and 14144 ("**E.O. 14306**")	June 2025	The White House	This E.O. 14306 mainly applies to federal agencies and revises prior executive orders to mandate measures such as zero-trust architectures and advanced persistent threat (APT) detection systems with enhanced AI integration. It updates incident response protocols and creates a framework for secure software development.
3	Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons and CISA Security Requirements for Restricted Transactions	April 2025 January 2025 (Security Requirements)	Department of Justice; CISA	This Rule prohibits U.S. persons from engaging in transactions that provide "countries of concern" (e.g. China, Russia, Iran and North Korea) or "covered persons" access to bulk sensitive US personal data and certain government-related data. Any restricted transactions must comply with CISA's data security requirements modelled on NIST and CISA's Cross-Sector Cybersecurity Performance Goals.
4	Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Record-Keepers, Plan Participants	September 2024	Department of Labor	Guidance for all ERISA-covered benefit plans on best practices for maintaining cybersecurity. The guidelines cover hiring service providers, best practices for recordkeepers, and online security tips for participants.
5	Protecting Americans' Data from Foreign Adversaries Act ("**PADFA**")	April 2024	Congress	This prohibits data brokers from selling, licensing, or transferring personally identifiable sensitive data of US individuals to foreign adversary countries (e.g. China, Russia, Iran, North Korea). "Sensitive data," includes information such as government IDs, health information, financial data, biometric data, geolocation, and online activity information.

	Law/Advisory Guidance	Date	Issued by	Summary
6	NIST Cybersecurity Framework 2.0	February 2024, updated December 2025	National Institute of Standards and Technology	The NIST Cybersecurity Framework 2.0 provides comprehensive guidance for organisations to manage and reduce cybersecurity risks. While this is voluntary it is increasingly seen as a national "benchmark" for best practice in the US by regulators and the courts.
7	Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies	September 2023	Securities and Exchange Commission	This final rule requires public companies to disclose material cybersecurity incidents, outline processes for assessment, identification, and management of material cybersecurity risks specific to the company, and report on the board of directors' oversight of cybersecurity risks.
8	Cyber Incident Reporting for Critical Infrastructure Act ("**CIRCIA**")	March 2022 (Final rules expected May 2026)	Congress	This imposes mandatory disclosure requirements for critical infrastructure, with a 72-hour reporting deadline after a significant breach and a 24-hour reporting deadline for a ransomware payment. However, final implementing rules are awaited.
9	Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments	September 2021	Department of Treasury	This advisory continues prior advisory comments affirming the US Government's position discouraging companies from making ransomware payments, suggesting proactive steps for mitigating ransomware risks. This memo warns about sanction risks from ransomware payments.
10	Protecting Personal Information – A Guide for Business & Start with Security	October 2016	Federal Trade Commission	These documents offer guidance on what the FTC sees as simple steps to protect personal information. It advises that a sound data security plan cover five key principles: take stock; scale down; lock it; patch it; and plan ahead.
11	Federal Trade Commission Act	1914	Federal Trade Commission	The FTC has broad authority under section 5 of this Act to prohibit unfair methods of competition and to proscribe unfair or deceptive acts or practices affecting commerce. This includes marketing and public statements about cybersecurity.

KEY CONTACTS:
CYBER AND DATA, INVESTIGATIONS AND FINANCIAL SPECIALISTS

KEY CONTACTS

Cyber and Data

UK

Richard Cumbley
Partner, London
Tel: +44 20 7456 4681
richard.cumbley@linklaters.com

Greg Palmer
Partner, London
Tel: +44 20 7456 2925
greg.palmer@linklaters.com

Georgina Kon
Partner, London
Tel: +44 20 7456 5532
georgina.kon@linklaters.com

Europe

Sonia Cissé
Partner, Paris
Tel: +33 1 56 43 57 29
sonia.cisse@linklaters.com

Daniel Pauly
Partner, Frankfurt
Tel: +49 69 710 03 570
daniel.pauly@linklaters.com

Guillaume Couneson
Partner, Brussels
Tel: +32 2 501 93 05
guillaume.couneson@linklaters.com

Asia

Adrian Fisher
Partner, Singapore
Tel: +65 6692 5856
adrian.fisher@linklaters.com

Alex Roberts
Partner, Shanghai
Tel: +86 21 2891 1842
alex.roberts@linklaters.com

USA

Ieuan Jolly
Partner, New York
Tel: +1 212 903 9574
ieuan.jolly@linklaters.com

Kris Ekdahl
Counsel, New York
Tel: +1 212 903 9415
kris.ekdahl@linklaters.com

Investigations

UK

Tom Cassels
Partner, London
Tel: +44 20 7456 3755
tom.cassels@linklaters.com

Andrew Poulton
Partner, London
Tel: +44 20 7456 3301
andrew.poulton@linklaters.com

Ben Packer
Partner, London
Tel: +44 20 7456 2774
ben.packer@linklaters.com

Europe

Jean-Charles Jaïs
Partner, Paris
Tel: +33 1 56 43 58 00
jean-charles.jais@linklaters.com

Kerstin Wilhelm
Partner, Munich
Tel: +49 89 418 08 506
kerstin.wilhelm@linklaters.com

Daniella Strik
Partner, Amsterdam
Tel: +31 20 799 6338
daniella.strik@linklaters.com

Asia

Andrew Chung
Partner, Hong Kong SAR
Tel: +852 2901 5238
andrew.chung@linklaters.com

Jelita Pandjaitan
Partner, Singapore
Tel: +65 6692 5881
jelita.pandjaitan@linklaters.com

USA

Adam Lurie
Partner, Washington
Tel: +1 202 654 9227
adam.lurie@linklaters.com

Financial Regulation

UK

Nikunj Kiri
Partner, London
Tel: +44 20 7456 3256
nikunj.kiri@linklaters.com

Clare McMullen
Partner, London
Tel: +44 20 7456 2129
clare.mcmullen@linklaters.com

Europe

Andreas Dehio
Partner, Frankfurt
Tel: +49 69 710 03 583
andreas.dehio@linklaters.com

Asia

Peiying Chua
Partner, Singapore
Tel: +65 6692 5869
peiying.chua@linklaters.com

USA

Brad Caswell
Partner, New York
Tel: +1 212 903 9362
brad.caswell@linklaters.com

Abu Dhabi | Amsterdam | Antwerp | Bangkok | Beijing | Berlin | Brisbane* | Brussels | Cape Town*** | Dubai | Dublin
Düsseldorf | Frankfurt | Hamburg | Hanoi* | Ho Chi Minh City* | Hong Kong SAR | Jakarta** | Johannesburg***
Lisbon | London | Luxembourg | Madrid | Melbourne* | Milan | Munich | New York | Paris | Perth* | Port Moresby*
Riyadh | Rome | São Paulo | Seoul | Shanghai[Δ] | Singapore | Stockholm | Sydney* | Tokyo | Warsaw | Washington, D.C.

** Office of integrated alliance partner Allens*
*** Office of formally associated firm Widyawan & Partners*
**** Office of collaborative alliance partner Webber Wentzel*
[Δ] Linklaters Shanghai and Linklaters Zhao Sheng (joint operation office with Zhao Sheng Law Firm)

linklaters.com

This content is intended merely to highlight issues and not to be comprehensive, nor to provide legal advice. Should you have any questions on issues reported here, please get in touch. © 2026 Linklaters.

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of the LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, 20 Ropemaker Street, London, EC2Y 9AR, England or on www.linklaters.com and such persons are either solicitors or registered foreign lawyers. Please refer to www.linklaters.com/regulatory for important information on our regulatory position. LIN.GBR.612