STEPHENSON HARWOOD

Cybersecurity: Fail to prepare; prepare to fail

Introduction to the increasing cyber threat

The level of cybercrime continues to grow at an unprecedented rate in the UK and across the globe, with UK Government figures from a DCMS 2022 survey showing that nearly 40% of businesses surveyed had suffered cyber security breaches or attacks in the last year. Over recent years the threat of attacks has been exacerbated by the increase in staff working from home, and from increased political tensions and activity from hostile states.

Ransomware continues to be a focus of cybercriminals and is now the most prominent and immediate cyber threat to businesses, and one which should be at the top of the corporate agenda. However, many organisations seem to be inadequately prepared.

Examples of recent incidents include ransomware attacks on KP Snacks in January 2022 (that impacted its ability to process orders and dispatch goods) and on the payroll provider Kronos in December 2021 (affecting the payroll of major business in the UK and US), and multiple attacks against several oil logistics companies across Europe in February.

Key takeaways

- The current threat level is high.
- Organisations holding valuable IP and/or data are a key target.
- Supply chains often create the most material vulnerabilities.

Key actions

- Audit and test technical security measures in place.
- Review, refresh and test response plans.
- Map, audit and test supply chains.
- Produce a "grab sheet" with key information on a couple of pages.
- Engage third party professionals – forensic IT and legal – so they are available in an emergency.
- Refresh training to key stakeholders.

In this latest insight we look at which industry sectors are particularly exposed, the regulatory landscape, and cover the technical and practical ways that organisations can prepare for, and plan their response to, a cyber-attack.

Key target organisations

There seems to be no obvious trend in the target of ransomware attacks, other than being levied against organisations which have the means to pay the demands and would face immediate (financial, reputational, and regulatory) pressures to resume business as usual. However, some of the key characteristics that cyber criminals target include:

- organisations that hold a significant amount of valuable and sensitive data, in particular personal or financial data – this can be sold by attackers on the black market or encrypted as part of a ransomware attack;
- intellectual property rich industries – attacks on IP assets puts pressure on organisations to comply with ransom requests in order to protect their IP;

- luxury brands – the risk of reputational damage caused by attacks can drive up ransom demands and make them more lucrative; and
- regulated businesses, such as financial institutions and key infrastructure providers – the added pressure of regulatory requirements to ensure critical services remain open gives cybercriminals extra leverage.

Organisations that hold valuable IP and trade secrets are at an increased risk of industrial espionage and attacks from foreign states looking to disrupt markets or steal technology and other IP assets to help their own domestic firms compete. Organisations that have complex structures and supply chains, with significant specialist services being outsourced, are also more vulnerable as the integration of services and information exchange points open up weak points that cybercriminals can exploit.

It is important to understand that cybercriminals are now "professionals", undertaking their own detailed research on which organisations and sectors are most vulnerable and who to attack.

What is at risk?

Cyber security breaches or attacks carry a number of risks, including:

- data/information loss – sensitive and personal data and confidential information could be exposed to third parties;
- business interruption – systems could be corrupted, or encrypted beyond use;
- extortion – ransomware attackers request payments for de-encrypting data and systems;
- additional expense – breach remediation can be costly and a drain on internal resources;
- exposure to regulatory fines – organisations could be fined for breach of their legal obligations;
- reputational damage – adverse publicity can be damaging to the organisation and any associated products/services, projects or partnerships;
- company valuations – at a time of enhanced M&A activity across many sectors, a cyber-attack could adversely affect a company's valuation or share price; and
- legal claims - individual and group actions could be taken against the organisations.

Regulatory requirements

A number of different sectors are subject to specific regulatory obligations and breach reporting requirements, such as financial service providers regulated by the Financial Conduct Authority or Prudential Regulation Authority. Generally, business operating in regulated sectors must understand their regulatory obligations to protect against cyber security risks (such as under FCA Principle 3, and SYSC 3.1.1 and 3.2.6), and have processes in place to comply with specific reporting requirements.

On a more general level (but still sector specific), the Network and Information Systems Regulations 2018 (NIS Regulations) impose certain obligations on organisations to take appropriate and proportionate measures to ensure the security of network and information systems and to notify competent authorities of security breaches. The NIS Regulations apply to certain operators of essential services and relevant digital service providers (and implements the EU Network and Information Systems Directive into UK law). The NIS Regulations set out a detailed matrix of who they apply to, and the relevant competent authorities responsible for enforcement (such as the Ofcom, Ofgem and the ICO). Sanctions for non-compliance apply on a sliding scale, with maximum penalties ranging from £1m to £17m depending on the nature of the contravention.

From a corporate governance perspective, publicly listed companies are required to maintain appropriate risk management and internal control systems and, in some instances, may need to confirm in their annual report that they have carried out a robust assessment of the main risks facing the company, which may now likely include cyber security risks.

Organisations must also comply with their obligations under relevant data protection laws, including the obligations under the UK/EU General Data Protection Regulation to have clearly documented policies and implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This is a broad obligation and imposes duties to ensure both internal and external systems are robustly protected.

In the event of a cyber-attack, organisations (and potentially other connected data controllers affected by the breach) must report any personal data breach to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned. In some instances organisations must also communicate the personal data breach to the data subjects themselves, and an incident may be reportable even if data is not extracted or publicly released – unauthorised access to personal data constitutes a personal data breach under the UK/EU GDPR and can trigger reporting obligations.

Penalties for non-compliance with data protection laws can be up to the greater of £17m/€20m or 4% of total annual worldwide turnover of the group.

The main cyber security threats

Ransomware, a form of malware, is now the biggest cyber threat to most businesses. This malicious software is used to encrypt target data/information and disable access to systems, so that cybercriminals can extort a ransom in exchange for the decryption key.

Typically, ransomware attacks are delivered through phishing emails, that then enable attackers to gain access to the underlying network to deploy encryption software on the data assets. In combination with this, cybercriminals also often extract files and data that they can share with the target as proof of their control and access over the network. They also often threaten to release these files if the ransom is not paid.

This type of attack would paralyse most businesses, by disabling access to systems and data, preventing business as usual transactions, and threatening the security of underlying sensitive intellectual property. As a result, organisations often face the difficult discission of having to consider paying the ransom demands, often in cryptocurrencies that are almost impossible to recover at a later date.

When faced with the prospect of paying a ransom demand, careful consideration needs to be given to compliance with anti-money laundering regulations and international sanctions and counter-terrorism legislation. Regulators and law enforcement agencies in most jurisdictions are yet to confirm their stance on paying ransoms, but in many instances such payments are not illegal.

Other key threats include:

- Phishing: seeking to obtain information whilst appearing to be from a legitimate source or contact. These attacks can be used to target individuals (spearfishing) e.g., to appear to be a genuine email from a CFO requesting a revenue controller to make an urgent payment or to request sensitive payment details.
- Hacking: gaining access to systems via IT vulnerabilities to steal information, such as bank account details, or to obtain valuable intellectual property. There are also threats from hacking by individuals who hack systems as a "hobby", or to test and train their cyber skills.
- Data leakage: obtaining access to data and confidential information through vulnerabilities and unauthorised transmissions – these can occur through the sharing of unencrypted files, or backdoors on websites. Data leaks by internal personnel, both by error and maliciously, also pose a threat.

Supply chain risks

When considering cyber vulnerabilities, it is imperative that the analysis covers all potential supply chain vulnerabilities. Whether that is trade partners, suppliers of internal systems, or other third-party service providers. These can often be easy and rewarding targets for cybercriminals, as gaining access to their environment may more easily allow access to multiple underlying end users. For example, in

2021 over 1,000 companies were affected by a ransomware attack perpetrated through vulnerabilities in a virtual system administrator software package developed by Kaseya (a US software company), which was used by a large number of managed IT service providers. The REvil group (a now dismantled Russian "Ransomware-as-a-Service operator) claimed credit for the attack, and it is reported they initially sought $70m in ransom payments to unlock the affected systems, and that one affected supermarket chain was forced to rebuild its systems from scratch.

In order to assess these potential risks, it is important to gather relevant information, undertaking a detailed mapping exercise to understand what third parties are engaged by the business, the nature of the services they provide, what access they have to underlying data/information and financials, and what access and integrations there are into the organisation's systems (or systems of other suppliers). To start this mapping exercise, it can be helpful to work with finance and IT teams to run through each supplier engaged by the business.

This information can then be used to create a supply chain risk map, to categorise "high risk" suppliers and particular vulnerabilities.

The next step is to conduct a detailed review of the obligations and protections set out in each contract. For example, checking that the contracts impose adequate minimum-security requirements, rights to conduct penetration testing (where appropriate), and contain audit rights and security breach notification requirements. It is also important to consider the contractual allocation of risk and governance responsibilities, liability and exclusions, and gather information on reporting lines and key contacts.

In relation to new contracts (or renewals of existing contracts) now is a good time to ensure that procurement policies and standard templates - contracts, security requirements, governance schedules etc. - are appropriate and up to date.

In assessing and managing the supply chain risks, it is important to:

- document key contractual information, reporting obligations and contact details in an easily accessible format – in the event of a breach, it is vital to have this basic information readily to hand;
- ensure documented minimum-security requirements are kept under review to ensure they reflect industry best practice;
- maintain a dialogue with key suppliers to understand how they are taking action to mitigate evolving cyber risks;
- carry out security audits to ensure suppliers are complying with their security and data handling obligations,
- where relevant, carry out routine penetration testing on supplier systems and interfaces (or ensure suppliers carry out, and report back on, such testing); and
- include your key suppliers in your business continuity plans and get them to participate in continuity testing activities.

What should organisations be doing to implement appropriate security measures?

Organisations should ensure that they have access to expert internal IT resources, and where relevant external specialists should be engaged to assist with implementing, monitoring, and updating technical security measures.

As a minimum, organisations should ensure that the following security fundamentals are implemented:

- carry out regular (or ideally real-time) back-ups of systems and data and implement continuity arrangements for failover support;

- monitor the network to check for suspicious activity or unauthorised access - typically using endpoint threat detection and response (ETDR) software;
- disable the use of removeable media such as USB memory sticks or ensure that systems force scans on them for malware;
- limit access controls to highly sensitive data, information, and systems to only those that need access to fulfil their specific role;
- regularly test networks and systems for vulnerabilities and test the interfaces and data exchanges with third parties;
- ensure staff are trained on cyber security, have read, and understood policies on the acceptable use of IT, and are aware of their own obligations to maintain the security and confidentiality of information and data assets and to report any potential breaches; and
- monitor key threats and updates, such as from the National Cyber Security Centre who publish threat reports and provide other excellent resources and services.

Those responsible for implementing security controls should ensure that any off-site networks and servers, such as at warehouses, regional offices and manufacturing sites (that may use standalone IT systems) are included within the scope of any cyber security measures.

Cyber incident response planning

It is almost impossible to quickly respond to, and mitigate the effect of, a cyber security breach or attack if you do not have adequate response processes and tools in place. However, the temptation is often to produce lengthy, detailed, policy documents and response plans. These can be useful reference points when checking security requirements or supplier assurance steps during a procurement process, but they aren't necessarily helpful on a Friday afternoon when an incident comes to light (and in practice, can be so cumbersome they are totally disregarded).

From our experience, to supplement any detailed policy document, organisations should ensure that they have a short "grab sheet" of no more than a couple of pages that documents the key information. This should set out contact details of who forms the initial response team - including details of external third-party specialists, such as forensic IT consultants and legal advisors – and a prioritised checklist of actions to initiate. This will ensure that the "first responders" can be mobilised quickly, and critical containment activities can be implemented without delay.

Bringing all of this together, set below are our top tips for incident response planning:

- produce a grab sheet, keep it updated, and keep it to hand;
- set up notification email addresses – one for reporting potential incidents, and one to cascade internal notifications;
- build a good relationship with an IT consultancy business that can deploy forensic IT specialists at short notice to assist with initial investigations and containment activities;
- engage external legal counsel on a retainer – you need to know a trusted legal advisor who can step in and support on critical incidents (and you don't want client/matter onboarding admin to delay their ability to respond and advise);
- ensure you understand any legal reporting obligations, such as to the Information Commissioner's Office (and other relevant regulators), including applicable timescales;
- raise awareness of cyber risks across the organisation by ensuring everyone has participated in relevant on-going training;
- ensure key stakeholders, and in particular those listed on the grab sheet, are trained on handling a cyber incident; and
- understand the terms of any insurance cover, including any breach notification requirements (which should be noted on your grab sheet).

We are here to help

Cyber risks will continue to evolve at a rapid pace, and the risk levels in the UK are likely to remain high for the immediate future. Organisations must therefore maintain their resilience to cyber-attacks, and ensure that their internal controls, governance, and planning are up-to-date and fit for purpose.

Should you wish to discuss any of the matters raised in this insight, or require assistance with reviewing and updating your organisational cyber security measures and response plans, please contact one of our experts and we will be happy to discuss further.

Our cyber security services

- Policy reviews and updates
- Supply chain audits and risk mapping workshops
- Regulatory guidance
- Bespoke training sessions
- Response planning – grab sheets and containment plans
- Incident management
- Advice on regulatory notifications
- Post-breach litigation

Simon Bollans
Partner
Commercial, Outsourcing & Technology
T: +44 20 7809 2668
E: simon.bollans@shlegal.com

STEPHENSON HARWOOD