NAVIGATING RANSOMWARE DURING M&A

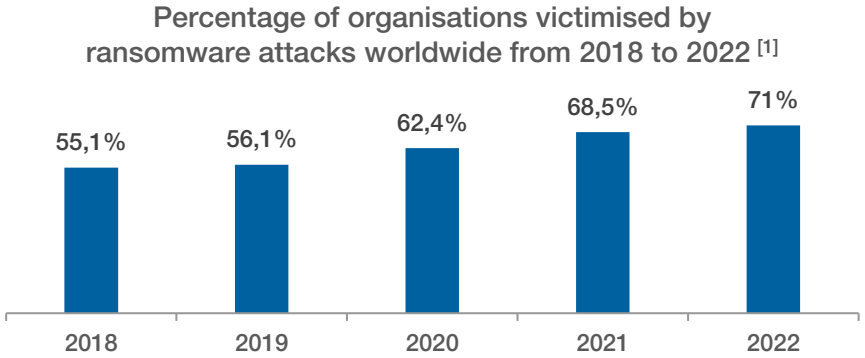
KEY CONSIDERATIONS FOR INVESTMENT TEAMS, OPERATING PARTNERS AND CORPORATE M&A PRACTITIONERS

NOVEMBER 2022

NAVIGATING RANSOMWARE DURING M&A

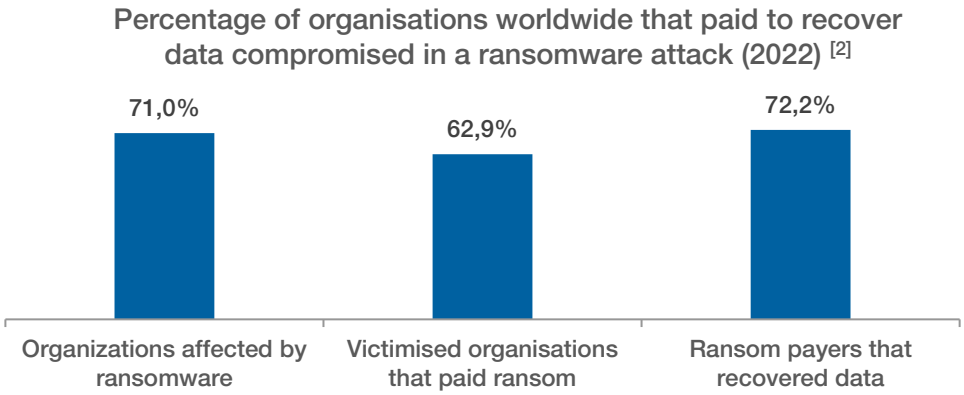
FOREWORD

Any cyber-attack can do significant operational, financial and reputational damage to an organisation. Of the various types of cyber-attacks, ransomware is increasingly favoured by cyber criminals who seek financial gain through digital extortion. Cases of ransomware attacks are on the rise. The annual number of ransomware attacks worldwide increased nearly twofold from c.300 million attacks in 2020 to c.600 million attacks in 2021. In 2022, 71% of businesses worldwide have been affected by a ransomware attack and there is consensus amongst experts that this trend will continue for the foreseeable future as cyber criminals become more innovative in developing new forms of ransomware.



During a ransomware attack, cyber criminals infiltrate the organisation's network and deploy malicious code designed to encrypt systems and data, often crippling operations. A ransom is then demanded to restore access to the systems and data. Perpetrators of ransomware attacks are increasingly using data exfiltration (also known as leakware) to motivate victims to make ransom payments. Data exfiltration is when attackers steal sensitive data, often releasing a few documents as a teaser to prove that they have the data. This is a technique that perpetrators use against victims who may be able to fend-off the initial attack by restoring systems and data through an effective IT disaster recovery plan.

Data breaches, including those that result from ransomware, are a costly affair for an organisation to deal with. The average cost of a data breach in the United Kingdom was 2.5 million GBP in 2022, with sectors like Energy, Financial Services and Retail topping the list with the highest costs. Furthermore, the public nature of a data breach can have serious reputational implications that a business may never recover from. This is likely the reason that a high number of organisations (63% in 2022) that suffer ransomware attacks decide to pay the ransom.



It is evident that ransomware is becoming increasingly damaging - a trend which is expected to continue, driven by the surge in threat actors' use of data exfiltration as a method of exerting additional pressure on victims to pay. Along with other cybersecurity threats, it is increasingly becoming a topic of discussion during the M&A process where risk and value implications must be considered. In this article we examine what investment teams, operating partners and corporate M&A teams need to know concerning ransomware on both buy and sell sides of a transaction. We cover some essentials regarding cyber incident reporting requirements in the UK and Europe and we offer recommendations on how to navigate ransomware related risk that is increasingly likely to be encountered during the M&A process.

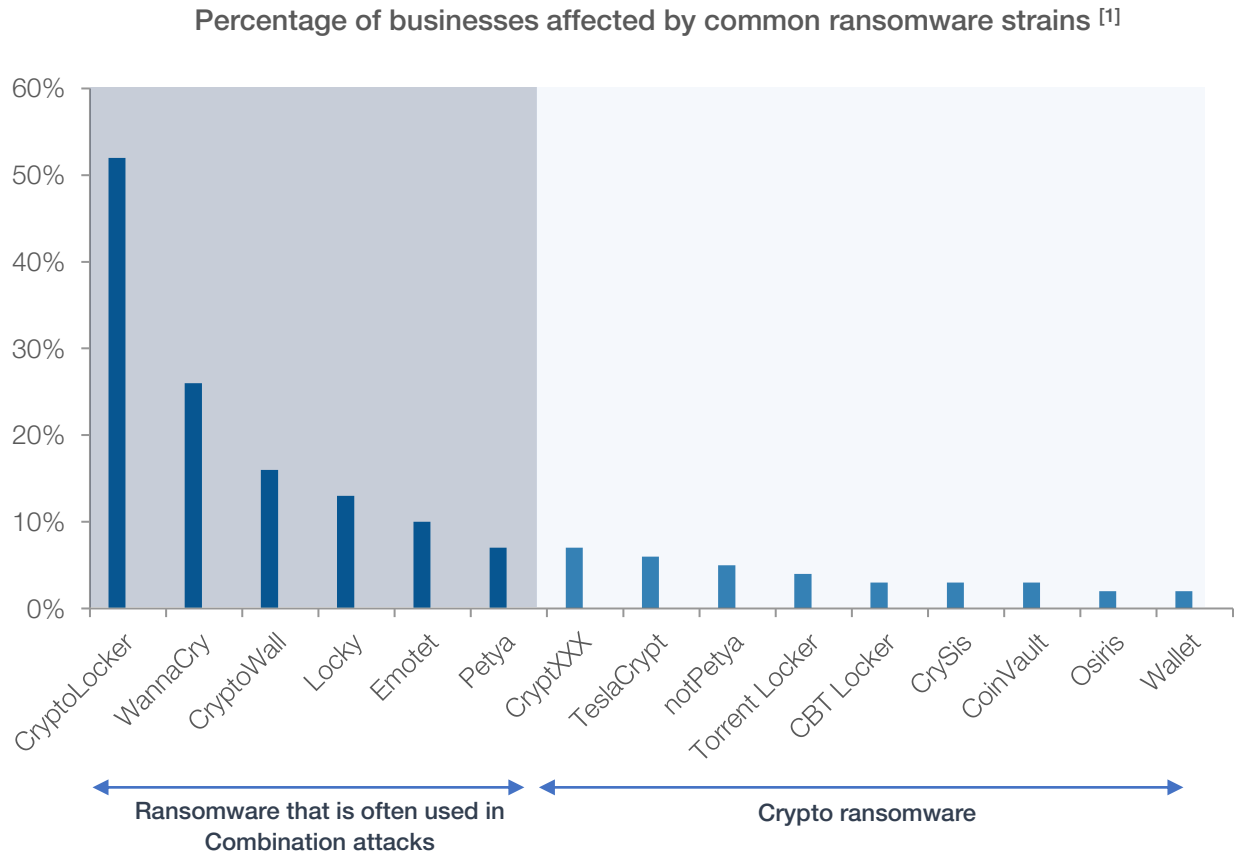
[1], [2] : https://www.statista.com/study/43873/ransomware/

RANSOMWARE TYPES AND THEIR ASSOCIATED RISK LEVELS

There are many strains of ransomware in circulation today. When dealing with an ongoing or recent ransomware attack in the context of a transaction, it is important for M&A practitioners to understand the type of ransomware being dealt with as the risk and value implications vary.

Ransomware Type	Description	Risk level / Impact to Business
Locker	Also known as screen lockers, these are the most basic form of ransomware that are designed to lock users out of their systems. Usually, users are only allowed to view the lock screen or interact with a screen containing the ransom demand. Locker ransomware doesn't destroy the data – it only prevents access to it.	**Low -** It is generally easier to recover from screen-locking attacks. For example, it may be possible to remove the ransomware from a machine by rebooting it in safe mode and running antivirus software
Crypto	This is one of the most common forms of ransomware. In a crypto ransomware attack, the perpetrator encrypts the victim's data so its unreadable and then demands a ransom in exchange for decryption keys. Attackers will often encrypt live data as well as back-up data – to prevent restoration.	**Moderate -** It is generally more challenging to recover from a crypto ransomware attack without the decryption key. However, if the victim is in the habit of taking regular offline or remote backup, a restore may be possible if the perpetrator was not able to reach the back-up to encrypt it.
Leakware	Also known as exfiltration or doxware, leakware typically has the most severe consequences for both the organisations and the individuals affected. When used in combination with Crypto, this type of ransomware encrypts files and exports data that is used to blackmail victims into paying a ransom.	**High** - In the case of leakware, even if a ransom is paid and the attack appears to have been resolved, the victim can never be sure that the perpetrator who has stolen data will not resurface or attempt to sell the confidential data on the dark web.
Double-Extortion (Combination)	A combination of locker-ware, crypto-ware and leak-ware, these forms of attacks can be the most devastating. In these attacks, perpetrators infiltrate systems and then may steal, encrypt and lock data. This means that even if the victim is able to somehow restore data from an offline or remote backup system, the attacker still maintains leverage because of the confidential data that has been stolen.	**High -** In the case of combination attacks, there are usually two demands for ransom payment. The first payment of ransom is to restore systems using a decryption key. The perpetrators then demand a second payment to prevent a data leak. Again, the victim can never be sure that the stolen data will not resurface.

COMMON RANSOMWARE STRAINS AND THE RISE OF 'RAAS'



Ransomware-as-a-Service (RaaS)

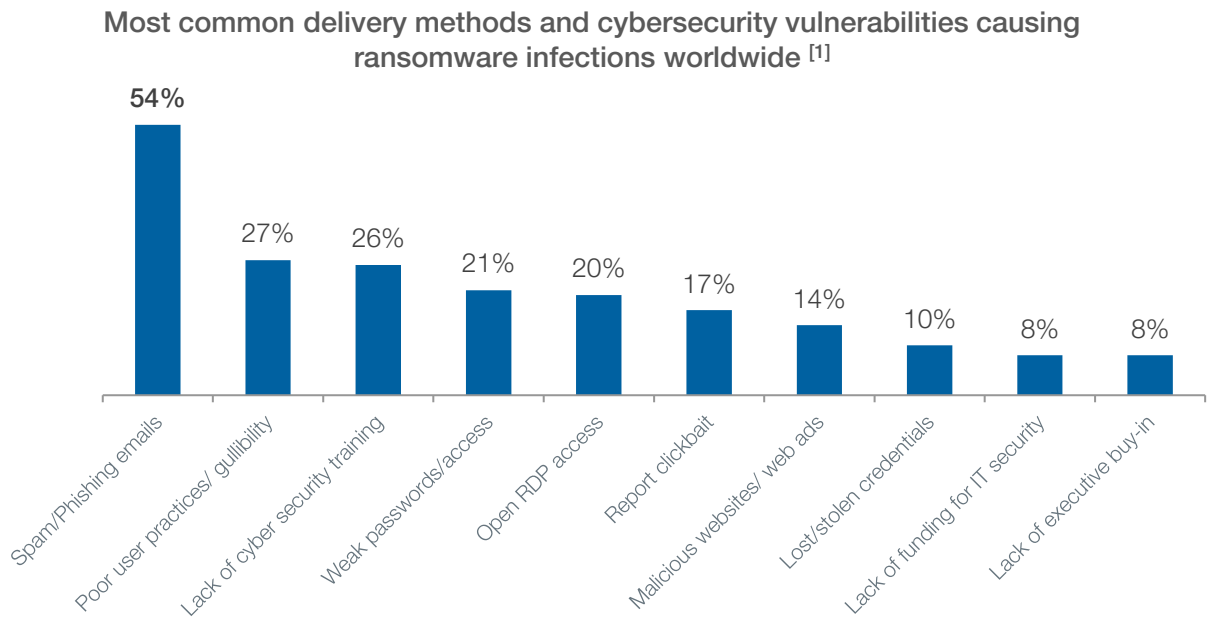
The increase in combination attacks can be attributed to Ransomware as a Service (RaaS) models. RaaS represents a dangerous evolution in how ransomware is propagated amongst criminals. Through RaaS, the access to sophisticated extortion software is no longer restricted to advanced cyber criminals. Instead 'common criminals' can pay for ransomware services that are commoditized by advanced operators. Criminals with low technical knowledge subscribe to RaaS that is made available to them on the dark-web (much like a SaaS business model).

The RaaS operators typically support the criminal affiliates with the packaging and deployment of the ransomware. Several RaaS providers are known to offer subscribers the ability to build their own ransomware packages which can contain combinations of malicious code. RaaS operations are known to provide subscribers with a ransom payment portal and a dedicated leak site for publishing stolen data. In return, RaaS operators may receive a monthly subscription payment or may have a profit-sharing arrangement with affiliates who use their software. The RaaS model is one of the primary reasons for the recent dramatic increase in ransomware attacks. RaaS is dangerous because operators are known to be sophisticated, they regularly disappear, reorganise, and re-emerge with newer and better ransomware variants.

[1] : https://www.statista.com/study/31368/cyber-security-of-companies-in-the-united-kingdom-statista-dossier/

RANSOMWARE ATTACK PROGRESSION AND PREVENTIVE MEASURES

While details of how an attack takes place may vary from one ransomware variant to the next, attacks tend to follow a common pattern that begins with the infiltration of malicious code into a victim's IT estate. As shown below, the most common delivery method for ransomware is through Spam or Phishing emails (54%).



Almost all ransomware delivery methods can be traced back to gaps in operational security practices. The top two vulnerabilities relate to poor user practices. For management teams, this highlights the importance of building threat awareness across the workforce through security training. During the M&A process, the rigour in IT and operational security practices must be validated through due-diligence to provide comfort that the risk and exposure to ransomware is adequately managed.

[1] : https://www.statista.com/study/31368/cyber-security-of-companies-in-the-united-kingdom-statista-dossier/

RANSOMWARE ATTACK PROGRESSION AND PREVENTIVE MEASURES

The following diagram illustrates the progression of a typical combination-ransomware attack. At each stage, there are preventive measures that apply. But as the attack progresses there are fewer options available to management.

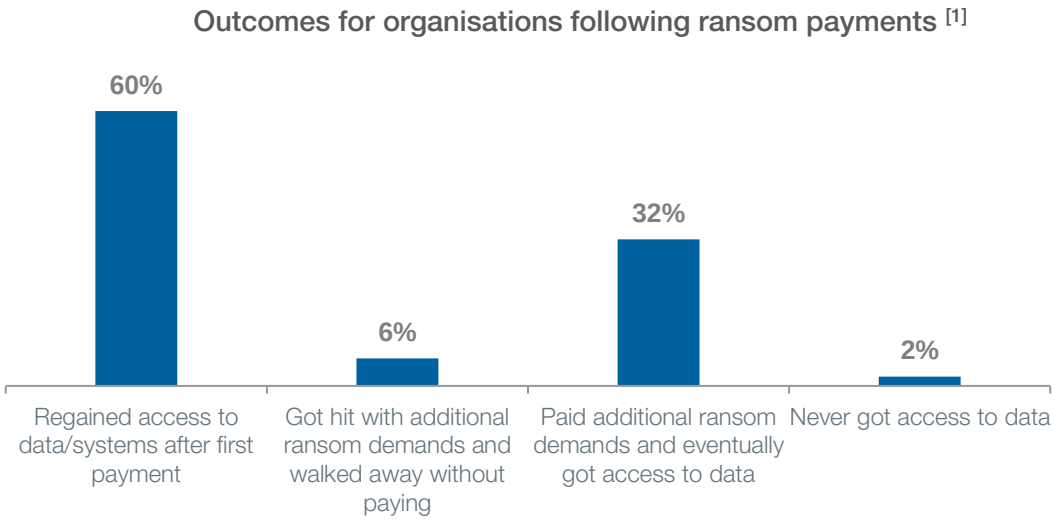
	Phase 1: Infection	Phase 2: Distribution	Phase 3: Encryption	Phase 4: Pay Day
Attackers objective	**Infiltration & Installation**	**Lateral Movement & Exfiltration**	**Encryption of Files**	**Secure Payment**
Ransomware behaviour	Ransomware infiltrates the victim's system   Ransomware is installed and begins the attack process	Malicious code begins communicating externally and uploading data   Scan for sensitive content both locally and across network	Malware begins to encrypt files across systems 	 Ransom Note is deployed with payment instructions
Preventive measures	• Email and web filtering • End point detection and response • Regular Patch management • Principle of Least Privilege (POLP access control) • Security Training	• Network, File and Process activity monitoring • End point monitoring • AI driven Security Automation	• Network, File and Process activity monitoring • AI driven Security Automation	(Countermeasures) • Cyber incident response • Disaster Recovery

The existence and effectiveness of security practices and preventive measures shown above should be validated during due-diligence. However, ransomware threats and strains are evolving and therefore no system can be 100% secure. Therefore, it is important that cyber incident response plans and disaster recovery plans include consideration for the latest ransomware patterns and that recovery plans are rehearsed to the extent possible. M&A practitioners should therefore also examine the effectiveness of the countermeasures that are in place during diligence.

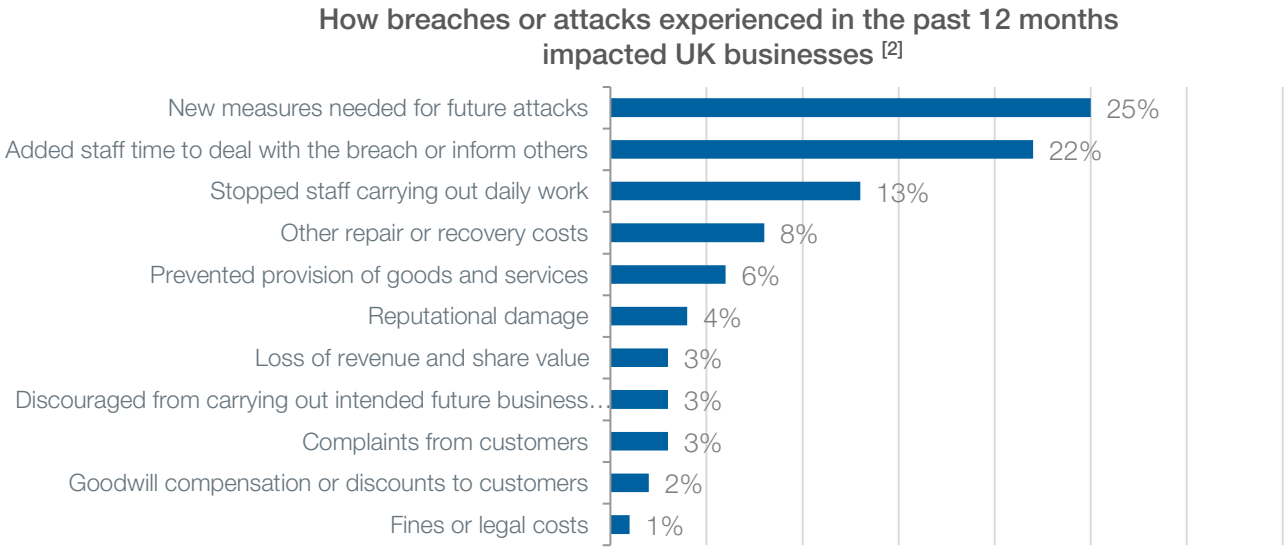
Finally, as part of the cyber incident response plan, management and investment teams may want to consider the implications of a successful ransomware attack. A policy can be established in consultation with legal advisors and regulatory bodies, regarding negotiations with cyber criminals. Some of the key considerations are the criticality and value of the data at stake, and the damages that the public release of the data will cause.

AFTERMATH OF AN ATTACK

As we have shown, the majority of organisation's that are breached after a ransomware attack end up paying the ransom. However, as depicted below, there is little honour among cybercriminals as a ransom payment does not always completely resolve the attack.



Furthermore, the residual effects of a ransomware attack can mean additional costs to the business. Data suggests that among private sector organisations, 86% reported that ransomware attacks caused a loss in business and revenue. Apart from the reputational damage, other challenges include non-value-added staff time dealing with recuperation from the breach, delays in provisioning critical goods and services, legal charges and other operations that are hindered. For M&A practitioners, rigorous operational due-diligence can aid in determining a target's operational resilience, as well as the recurring and one-off cost implications of a recent attack.



[1], [2] : https://www.statista.com/study/43873/ransomware/

REGULATORY CONSIDERATIONS

It is important for operating partners and management teams to possess an understanding of what needs to be done when a ransomware attack is encountered. It is also helpful to make a distinction between government approved regulatory bodies that mandate incident reporting, and government endorsed technical authorities that can be consulted without obligation.

Furthermore, cyber incident reporting requirements vary according to geography and sector. Management teams should always consult with legal advisors to ensure that appropriate incident reporting requirements are adhered to. For example, in the UK, certain health care providers affiliated to local councils are required to report attacks and potential data breaches to the respective council.

United Kingdom

In the UK there are two primary bodies that play a role in responding to ransomware attacks and other cyber-crime: the National Cyber Security Centre (NCSC) and the Information Commissioner's Office (ICO). The NCSC is the technical authority for cyber incidents in the UK. It was formed to provide a unified national response to cyber threats. The NCSC engages directly with victims to understand the nature of an incident and provides free and confidential advice to help mitigate the impact in the immediate aftermath. As the UK government's cybersecurity agency, the NCSC is also responsible for managing cybersecurity incidents of national importance.

The Information Commissioner's Office (ICO) is the UK's independent regulator for data protection and information rights law. The ICO can take action to change the behaviour of organisations and individuals that collect, use and keep personal information. This includes criminal prosecution, non-criminal enforcement and audit.

The NCSC is not a regulator and will not notify regulatory bodies (including the ICO) of a cyber incident unless there is "an extremely serious public interest reason such as protection of national security" [1] .There is no obligation for a victim to notify the NCSC of a cybersecurity incident. There are, however, requirements to notify the ICO of cyber incidents and there are also requirements, defined by the ICO, to take certain remedial action.

Germany

In Germany, two of the relevant authorities for cyber security incidents and data breaches are the Federal Office for Information Security (BSI, Bundesamt für Sicherheit in der Informationstechnik) and the Federal Criminal Police Office (BKA). The BKA conducts investigations in the field of cybercrime where federal authorities, facilities or sensitive parts of critical infrastructures are affected or where the BKA has been requested to conduct investigations.

The BSI is the German federal agency in charge of managing computer and communication security for the German government. The BSI, together with the NCCA (National Cybersecurity Certification Authority), can perform evaluations of an organisation's IT systems. As the national certification body for assurance levels, they are known to carry out audits, award and withdraw certificates and impose penalties in accordance with German regulation. The BSI must be notified within 72 hours of certain cyber security related events and can impose fines on organisations that fail to signal cyber disruptions or compromised systems.

As per the German Annual Cybercrime report in 2021 [7], ransomware was the primary cybersecurity threat Germany faced in 2021. The same report also estimated that ransomware resulted in 24 billion Euros in damages to German companies in 2020-2021, a nearly five-fold increase compared to 2019 figures and that large and critical businesses were preferred targets for ransomware criminals.

[1] https://www.ncsc.gov.uk/files/NCSC_Incident_brochure.pdf
[2] https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/

REGULATORY CONSIDERATIONS

France

In France, the national authority for cyber defense, network and information security is ANSSI (Agence nationale de la sécurité des systèmes d'information). It operates as a representative body within the ENISA (European Network and Information Security Agency) to support the development of national cybersecurity capabilities and cooperation among the EU member states. The ANSSI studies and certifies the security architecture standards of organisations. The CSPN (Certification de Sécurité de Premier Niveau) can be awarded by ANSSI as recognition of adequate preventive measures against breaches.

In the event of a data breach, organisations are required to notify the national data protection authority, CNIL (Commission nationale de l'informatique et des libertés) within 72 hours of event identification. In 2021, CNIL received 5,037 notifications of personal data breaches – about 14 notifications per day – a 79% increase compared to 2020 [1]. Among the notified data breaches, 58% were the result of cyber attacks, particularly ransomware – which saw a 128% increase compared to 2020 [2]. The CNIL also issues formal notices and regulatory fines to organisations when it identifies poor data security practices that have resulted in a breach.

Benelux

In Belgium, the CCB (Centre for Cybersecurity Belgium) is the national authority for cybersecurity. It supervises, coordinates and monitors the application of the national cybersecurity strategy. The Belgian Data Protection Authority (BE DPA) is responsible for enforcing compliance with data protection regulations. Data breaches must be reported to the BE DPA.

In the Netherlands, the NCSC (National Cyber Security Centre) is responsible for overseeing digital security at the national level. Its role is to keep vigil, monitor potential threats and advise organisations on improving their cybersecurity measures. Any breach must be reported to the Dutch Data Protection Authority (AP) within 72 hours in addition to filing a complaint with the Dutch police. In Luxembourg, the CNPD (Commission Nationale Pour La Protection Des Donnes) must be contacted within 72 hours of a data breach.

[1], [2] : https://www.cnil.fr/sites/default/files/atoms/files/cybersecurity-2021_gdpr-the-best-prevention-against-cyber-risks.pdf

SUMMARY RECOMMENDATIONS FOR M&A PRACTITIONERS

1 Adopt a proactive approach to prepare for the worst; conduct thorough Operational and Technology due-diligence to test resilience and agility in the event of an attack

Targets should be able to demonstrate disaster recovery arrangements and a cyber-incident response plan that is robust, comprehensive, and tested and updated regularly. Remember, cyber incident response and disaster recovery are more than just IT topics, they should contribute to the overall business continuity plan. Key questions to consider:

- If technology platforms and systems are unavailable for an indefinite period, are operational teams equipped and trained to adapt and continue to function?
- How will service levels be affected and when and how will systems and technology will be restored in case of an incident?

When an M&A target is experiencing an ongoing cyber incident or ransomware attack and has systems locked up, operational due-diligence should be employed to review the likelihood and implications (including liabilities, costs and fines) of a data breach arising from this attack. Diligence should also cover the operational impact from the outage and the efforts and costs associated with a prolonged period of manual workarounds, as well as the "catch-up" or data update efforts that may be required once IT systems are restored.

2 Assess cybersecurity vulnerabilities across the supply-chain and technology ecosystem

Targets should demonstrate an awareness of the size and scale of the cyber impact surface and an understanding of the confidentiality of data being processed. The acceleration in technology transformation has meant that most businesses have an ever-expanding digital footprint. Furthermore, greater communication and collaboration between suppliers and customers results in technology ecosystems that expand the cyber-impact surface. A target's supplier onboarding and evaluation processes should include cybersecurity criteria that is appropriate for the industry and type of data being exchanged. Where sensitive data or Personally Identifiable Information (PII) is shared with the supplier, greater scrutiny of cybersecurity arrangements is required. The related supplier management practices should be reviewed during due-diligence.

3 Review gaps in public facing technology elements which can reveal deep-rooted security issues

Public facing technology elements of the target should be reviewed for gaps and for insights into security practices. For example, out-of-support web components on a target's website can be easily identified and can signal deep-rooted issues of poor security culture or underinvestment in cybersecurity that may warrant rigorous technology due-diligence. Dark web scanning and monitoring can help uncover past breaches (known or unknown to management), as well as employee credentials or other sensitive data being traded on the dark web. Much of this can be tested outside-in, without access to the target or the management team.

SUMMARY RECOMMENDATIONS FOR M&A PRACTITIONERS

4 Include cybersecurity investment in the business plan

Management teams should demonstrate a security strategy and roadmap that is evidenced by investment. There are several benchmarks available that provide guidance on what percentage of revenue or what percentage of the IT budget should be spent on cyber-security but these vary across industries and should always be considered in the context of the business. More important than how much is being spent is what it is being spent on. Outsourcing of workforce security training and certain automated security platforms can introduce cost efficiencies. During diligence we recommend a review of security solutions, practices and planned investments that is catered to the business and deal strategy.

5 Consider the costs and benefits of cybersecurity insurance

Typically, cybersecurity insurance covers financial losses following a cyber event or data breach. However, the increase in ransomware attacks and other cyber-attacks over the last two years has contributed to higher premiums and selectivity from insurance providers about who and what gets covered. Furthermore, insurance providers tend to demand higher premiums and higher standards where there has been a history of cyber incidents. Most cyber security insurance policies usually include significant assistance with and management of the incident itself, which can be essential when faced with reputational damage or regulatory enforcement. Given the rise in ransomware, it is important that buyers also ensure that coverage explicitly includes cyber extortion. We recommend that active cyber insurance policies are reviewed during diligence to ensure that meaningful and lasting coverage is in place. We also recommend that cost forecasts include consideration for spiraling cyber insurance premiums.

6 Review cybersecurity risks and findings with legal advisors

We recommend that any significant cybersecurity risks or findings uncovered during diligence are reviewed with legal teams and/or legal advisors so that consideration is given for appropriate protections in transaction documents. Buyers typically seek special indemnification covering the cost of remediation and cost of any future external claim/fee arising from ongoing or recent attacks. Sellers tend to ask for a financial cap on the indemnification amount and a limitation on the period during which indemnity claims can be made.

CONTACTS

Nick Neil-Boss
Partner at Eight Advisory
nick.neilboss@8advisory.com

Jean-Christophe Fuzzati
Partner at Eight Advisory
jeanchristophe.fuzzati@8advisory.com

Tom de Troyer
Partner at Eight Advisory
tom.detroyer@8advisory.com

Samuel Chandrasekaran
Director at Eight Advisory
samuel.chandrasekaran@8advisory.com

Nick Breadner
Director at Eight Advisory
nicholas.breadner@8advisory.com

Hans Wamsteker
Director at Eight Advisory
hans.wamstekar@8advisory.com

Romit Dutta
Senior at Eight Advisory
romit.dutta@8advisory.com

EIGHT ADVISORY

40, Rue de Courcelles
75008 Paris / France

17 rue de la République
69002 Lyon / France

34 rue du Pré Gauchet
44000 Nantes / France

28 boulevard du Colombier
35000 Rennes / France

Les Docks, Atrium 10.4
10, place de la Joliette
13002 Marseille / France

48 Pall Mall Saint James's
SW1Y 5JG London / UK

53 Avenue des Arts
1000 Brussels / Belgium

Amstelveenseweg 500
1081 KL Amsterdam / Netherlands

Mainbuilding, Taunusanlage 15
60325 Frankfurt am Main / Germany

Rudolfplatz 3
50674 Cologne / Germany

Pacellistr. 8
80333 Munich / Germany

Neuer Wall 80
20354 Hamburg / Germany

Brandschenkestrasse 90
CH-8002 Zurich / Switzerland

Urmi axis, Seventh floor, Famous
Studiolane, Mahalaxmi
Mumbai 400 011 / India

EIGHT INTERNATIONAL

12 Rue Jean Engling
L-1466 Luxembourg

FRP
110 Cannon Street
London, EC4N 6EU/ UK

JP Weber
Ul. Wspólna 70,
00-687 Warsaw / Poland

JP Weber
Rynek 39/40,
50-102 Wroclaw / Poland

New Deal Advisors
Via Santa Maria Fulcorina,
2-20123 Milan / Italy

contact@8advisory.com

contact@8-international.com

8 EIGHT INTERNATIONAL

EIGHT ADVISORY 8