Global Investigations Review

The Guide to Cyber Investigations

Editors
Benjamin A Powell and Jason C Chipman

Second Edition

The Guide to Cyber Investigations

Editors:

Benjamin A Powell

Jason C Chipman

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2021
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as at May 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: natalie.clarke@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-595-5

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON MORI & TOMOTSUNE

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

CRAVATH, SWAINE & MOORE LLP

RICHARD DENATALE

HUGHES HUBBARD & REED

K&L GATES LLP

KROLL, A DIVISION OF DUFF & PHELPS

BRIAN MCDONALD

QUINN EMANUEL URQUHART & SULLIVAN, LLP

ROPES & GRAY LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Publisher's Note

The Guide to Cyber Investigations is published by Global Investigations Review – the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature and provide an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its fifth edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation, from discovery to resolution.

The Guide to Cyber Investigations takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Guide to Cyber Investigations* as the close-up.

The Guide to Cyber Investigations is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

Contents

Part II

Jurisdictional, Regional and Sectoral Nuances

12

Cyber Trends and Investigations in Europe: A Practitioner's Perspective

Rohan Massey, Kevin Angle, Edward Machin and Raffi Teperdjian[1]

Cyber requirements under EU law and laws in the UK

Many organisations in the European Union and the United Kingdom, and those in the rest of the world that offer products or services to individuals in the EU or UK, associate cybersecurity with four letters: GDPR. However, the General Data Protection Regulation and its counterpart in the UK, the UK GDPR,[2] are only one thread in a patchwork of cybersecurity laws and best practices in the EU and UK that, when viewed together, comprise some of the most comprehensive security requirements faced by businesses in any region of the world. The challenge of complying with these laws is compounded by their extraterritorial effect. For example, a company with a single office in California offering holiday packages to individuals in the EU or UK may be subject to the GDPR.[3] Accordingly, the extent to which digital business is now borderless means that the influence and scope of cybersecurity laws in the EU and UK is no longer a strictly regional concern.

The development of the EU's and UK's cybersecurity framework has coincided with a wider appreciation of, and anxiety about, the value – monetary and otherwise – of personal information. Of particular alarm to individuals is the regularity with which data

1 Rohan Massey is a partner, Kevin Angle is a counsel, Edward Machin is an associate and Raffi Teperdjian is an associate at Ropes & Gray LLP. The authors would like to recognise the work of Rosemarie Paul who was a key contributor to the previous edition of this chapter.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC – the General Data Protection Regulation [GDPR]. With respect to the UK, 'UK GDPR' refers to the definition in the Data Protection Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019). For ease of reading, the GDPR and the UK GDPR will be referred to in this Chapter as the 'GDPR'.

3 The GDPR significantly extends the scope of the previous regime – Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data – which applied only to controllers and processors with an EU presence.

is compromised. These concerns are not unwarranted: in January 2021, it was reported that nearly 281,000 personal data breaches had been notified since the introduction of the GDPR on 25 May 2018.[4] Even though cybersecurity is now firmly a board-level issue,[5] many businesses still have insufficient procedures in place to address the loss or disruption caused by cyberthreats. This chapter discusses how important it is that businesses address these gaps, as a matter of priority.

General Data Protection Regulation

The concept of personal data security in the EU and UK does not begin with the GDPR. Indeed, in requiring that data controllers and processors implement 'appropriate technical and organisational measures' to ensure a level of security appropriate to the risks of their data processing, the GDPR[6] closely tracks the language of the previous legislation (Directive 95/46/EC, the Data Protection Directive (DPD)), which states:

> *Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.*[7]

> *Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.*[8]

The difference in approaches between 1995 and today is largely one of context, particularly given the change and the degree to which we interact with technology now. Cybersecurity did not rank highly on legislative, corporate and public agendas in 1995. By contrast, high-profile hacks and the misuse of personal data are now so commonplace that enforcement actions arising from organisations' cybersecurity failings have become a key priority for data protection authorities (DPAs), and one that all levels within a business need to engage with. Enforcement by DPAs in the EU and UK indicate that there continues to be a growing appetite to investigate and penalise infringements of the GDPR's security principles,[9] with

4 'DLA Piper GDPR data breach survey: January 2021' (www.dlapiper.com/en/uk/insights/publications/2021/01/gdpr-data-breach-survey-2021/) [DLA Piper, 'GDPR data breach']. Last accessed on 23 March 2021.

5 Department for Digital, Culture, Media and Sport, 'Cyber Security Breaches Survey 2018' (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf). Last accessed on 23 March 2021.

6 Article 32(1) of the GDPR.

7 Article 17(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

8 Article 17 of the GDPR.

9 For example, Resolución De Procedimiento Sancionador, Air Europa Lineas Aereas, SA., PS/00179/2020 (15 March 2021) (Spain); Penalty Notice, Marriott International Inc., COM0804337 (30 Oct. 2020) (United Kingdom), available at https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-internationa l-inc-mpn-20201030.pdf.

fines available under the GDPR of up to €20 million or 4 per cent of global annual turnover, whichever is higher [10] (though fines of such magnitude have not been imposed and all fines must be proportionate to the offence).[11] Practitioners should take a two-pronged approach to these requirements: first, by focusing on the technical and organisational measures that comprise an appropriate (i.e., compliant) security programme; and second (and relatedly), by remaining alive to the nuances that will often be required when advising on the GDPR's mandatory data breach notification requirements.

Technical and organisational measures

Practitioners are advised to focus their assessment on an organisation's policies and procedures relating to security, whereas a review of technical requirements or measures will usually be undertaken in conjunction with a third-party security provider. Ultimately, there is no one-size-fits-all approach to GDPR compliance and whether a programme is defensible will be assessed in each case.[12] That being said, certain baseline standards are likely to apply to most organisations, including network perimeter defences, malware protection, password policies and secure configuration.[13]

Mandatory breach notification

One of the changes brought in by the GDPR is the requirement to notify data breaches to the regulator and, in certain circumstances, to the individual.[14] The regulator must be notified without undue delay and within 72 hours of becoming aware of the breach,[15] otherwise the organisation may face liability of up to €10 million or 2 per cent of global annual turnover, whichever is higher.[16] The threshold for mandatory notification to a DPA is where there is 'a risk to the rights and freedoms' of individuals;[17] the requirements for notification to affected individuals are higher still.[18] While certain breaches will be obviously reportable, some organisations appear to be struggling to assess breaches at the lower end of the spectrum

10 Article 83(1) of the GDPR.

11 Article 83(1) of the GDPR.

12 This approach has been recognised by data protection authorities in France and the United Kingdom, among others. See, e.g., Commission Nationale de l'Informatique et des Libertés (CNIL), 'Security of Personal Data', 2018 Edition (www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf). Last accessed on 23 March 2021.

13 Article 4(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ePrivacy Directive) similarly requires that providers of publicly available electronic communications services 'must take appropriate technical and organisational measures' to safeguard the security of their services, having regard to 'the state of the art and the cost of implementation'.

14 In addition, Article 4(2) of the ePrivacy Directive requires providers of publicly available electronic communication services, where there is a risk of a breach to the security of the network, to inform the subscribers of such a risk.

15 Article 33(1) of the GDPR.

16 Article 83(4) of the GDPR.

17 Article 33(1) of the GDPR.

18 Article 34(1) of the GDPR: 'When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without delay.'

that may not be reportable. In such cases, practitioners should consider any guidance issued by the European Data Protection Board (EDPB) (previously the Article 29 Working Party) or public statements made, and the enforcement actions taken, by the DPA to which a report would be required. Indeed, notwithstanding that the GDPR was designed to harmonise Member States' disparate approaches to implementing the DPD, certain subtle differences in approach among DPAs are already becoming clear in the context of breach reporting.

With that said, most reportable breaches do not result in enforcement. A recent report by the UK Information Commissioner's Office (ICO) is instructive: of the 38,514 data protection complaints the ICO received in 2019/20, only 0.1 per cent resulted in an administrative fine, compliance audit or enforcement notice being served.[19] These figures should not be interpreted as meaning that the vast majority of breaches are not reportable. However, it does illustrate the point that organisations should not be overly cautious in their assessments of personal data breaches. Practitioners should be aware of the potential liability for failing to notify the regulator. However, if an organisation has undertaken a detailed and reasoned approach to investigating and analysing the breach, has carefully considered its impact (if any) and has documented why notification is not required, its assessment will often be shared by the DPA.

Network and Information Security Directive

Unlike the GDPR, which applies only to the processing of personal data, the Directive on Security of Network and Information Systems[20] (NISD) is concerned with network security and the continuity of services and applies both to personal and non-personal data. The NISD is the first EU-wide law on cybersecurity and regulates two types of entities: (1) operators of essential services, being critical organisations in the energy, transport, financial services, health, water supply and digital infrastructure sectors; and (2) providers of digital services, being online marketplaces, online search engines and cloud services providers. The NISD allows Member States to choose the maximum fines that their regulators can impose; in the United Kingdom, breaches of the NISD can result in penalties of up to £17 million.

Like the GDPR, the NISD requires covered entities to implement technical and organisational security measures that are appropriate and proportionate to the risks posed[21] and to report all incidents that have a substantial impact on the provision of their services.[22] Both laws require covered organisations to consider 'the state of the art'[23] measures and the risks posed to individuals in designing their security programmes. While both regimes require notification to the appropriate authority (within 72 hours of becoming aware of a reportable

19 For example, Guidelines 01/2021 on Examples regarding Data Breach (Draft 19 Jan. 2021) (comment period closed). https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf. Last accessed on 23 March 2021.

20 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security and information systems across the Union [NISD]. The NISD was implemented in the UK prior to Brexit through the Network Information System Regulation (the 'NIS Regulation'), which remains in effect. For convenience, this chapter will refer to both the NISD and the NIS Regulation as the NISD.

21 Articles 14(1) and 16(1) of the NISD.

22 Articles 14(3) and 16(3) of the NISD.

23 Article 32 (1) of the GDPR; Articles 14(1) and 16(1) of the NISD.

incident under the GDPR, and 'without undue delay' under the NISD),[24] there are a number of key differences in the scope of these obligations. Incident reporting is stricter under the NISD, as any significant disruption of services must be notified. In contrast, although breaches under the GDPR must only be notified if the breach leads to destruction, loss, alteration, unauthorised disclosure of or access to personal data, the notification may require disclosure to a wider audience, namely DPAs and affected individuals.

A breach of one law can result in a breach of the other: for example, an avoidable hack of personal data under the GDPR could be separately enforced under the NISD. In such cases, regulatory guidance [25] suggests that dual notifications will be required. However, it is unclear whether separate but related actions will be brought by the regulators in such cases.[26] The answer to this and other questions may be addressed in proposed changes to NISD announced by the EU Commission in December 2020, which include removing the distinction between operators of essential services and digital service providers and expanding the scope of NISD to cover all medium and large companies in selected sectors that are defined by their criticality for the economy and society, as well as smaller businesses with high security-risk profiles. Additionally, there will be an enhanced Cooperation Group to shape strategic policy decisions on emerging technologies and new trends; and increases in information sharing and cooperation between Member State authorities, especially in cyber crisis management.[27]

Cybersecurity Act

On 27 June 2019, the EU Cybersecurity Act[28] came into force promoting an EU framework for cybersecurity certification and creating a permanent mandate for the European Union Agency for Network and Information Security (ENISA) to better support Member States in responding to cyberthreats and attacks. The Act strengthened the coordination and cooperation in cybersecurity across EU Member States and EU institutions. The tailored certification schemes established under the Cybersecurity Act allow companies to certify specific categories of information and communication technologies (ICT) products, processes and services only once and obtain certificates that are valid across the EU. The EU-wide cybersecurity certification framework enables companies in the ICT sector to demonstrate that their products and services meet one of three security standards (basic, substantial or high). The intention of the new rules is to improve trust for consumers, as they can choose between products (such as internet of things devices) that are cyber-secure. The one-stop-shop cybersecurity certification is expected to achieve cost savings and remove potential market barriers

24 Article 33(1) of the GDPR; Articles 14(3) and 16(3) of the NISD.

25 Information Commissioner's Office, 'The Guide to NIS: GDPR and NIS' (https://ico.org.uk/for-organisations/the-guide-to-nis/gdpr-and-nis/). Last accessed on 23 March 2021.

26 Article 8(6) of the NISD states that competent authorities must 'consult and co-operate . . . with national data protection authorities'.

27 Proposal for directive on measures for high common level of cybersecurity across the Union, 16 December 2020 (https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union). Last accessed 23 March 2021.

28 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act).

for enterprises. It is hoped companies will have the incentive to invest in cybersecurity and make this a competitive advantage.

Trends

As technology moves faster than law, so technology crime continues to outpace innovations in security. Cybercriminals tend not to be sentimental – as one patch is rolled out, another vulnerability opens. That being said, we now consider some of the recurring themes in cybersecurity in the EU and UK, as well as highlighting the key trends of which practitioners should be aware.

Targets

Financial services

Given the volume and sensitivity of personal and confidential information that financial institutions process, and the increasing number and sophistication of cyberattacks, information security remains a high priority for the financial services sector.[29] As highlighted in a Report on the Risks and Vulnerabilities in the EU Financial System by the Joint Committee of the European Supervisory Authorities, a particular concern relates to the measures required to address legacy IT systems.[30] Indeed, even the process of upgrading these systems can be perilous: in April 2018, UK bank TSB's migration to a new IT platform resulted in millions of customers being unable to access their accounts for up to one week, as well as increased reports of fraud, and rectification being needed.[31] More recently, the outbreak of covid-19 has required most companies across the EU and UK financial sector and beyond to switch to remote working, resulting in an uptick of digital activity. This greater use of a virtual environment has put even more confidential data and ICT systems at increased risk of becoming targets of hackers and other cybercriminals.[32]

Consumer-facing businesses

It should come as no surprise that consumer organisations are a prime target for cybercriminals, given the volume and range of data they hold and the variety of ways in which security weaknesses can be exploited – from credit card fraud, to identity and intellectual property

29 In the banking sector, 42 per cent of respondents to a 2017 European Banking Authority Risk Assessment Questionnaire reported that these were the main drivers for increasing operational risk; European Banking Authority, 'Risk Assessment Questionnaire – Summary of Results, December 2017' (https://eba.europa.eu/documents/10180/2085616/Risk+Assessment+Questionnaire+-+December+2017). Last accessed 18 March 2019.

30 Joint Committee of the European Supervisory Authorities, 'Joint Committee Report on Risks and Vulnerabilities in the EU Financial System', 20 April 2017 (https://esas-joint-committee.europa.eu/Publications/Reports/Spring%20Joint%20Committee%20Risk%20Report%20(JC%202017%2009).pdf). Last accessed on 24 March 2021.

31 See Letter from Andrew Bailey (Chief Executive of the Financial Conduct Authority) to Nicky Morgan MP (Chair of the Treasury Committee), 30 May 2018 (https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/correspondence/fca-to-chair-tsb-300518.pdf). Last accessed 23 March 2021.

32 Joint Committee of the European Supervisory Authorities, 'Joint Committee Report on Risks and Vulnerabilities in the EU Financial System', 4 September 2020 (www.eiopa.europa.eu/content/report-risks-and-vulnerabilities-eu-financial-system_en). Last accessed on 25 March 2021.

theft, among others. At the same time, individuals now expect businesses to have robust security measures in place to protect their data and have a better awareness of their data protection rights. Translated quantitatively, a 2020 report concluded that the average cost of a data breach in the UK is about £2.9 million[33] (even without including the additional reputational cost). The regularity with which consumer-facing companies are suffering large data breaches (Virgin Media,[34] British Airways,[35] Ticketmaster[36] and Marriott International,[37] among many others) demonstrates just how difficult it has become for these organisations to give their customers peace of mind – and why criminals continue to target them.

Internet of Things devices

Internet-connected devices offer criminals a wealth of opportunities to access personal data.[38] That much of this information reveals detailed, and often deeply personal, insights into individuals' private lives makes it especially attractive to bad actors. Approximately 305 million Internet of Things units are predicted to be in use in the EU and UK by 2025,[39] including for use in 'smart' homes, cars, hospitals, airports and cities. Data about the time we leave and return home, how long we shower, and how much electricity we use can all be used to build profiles that are valuable. The result is that this abundance of new data, being stored in systems with multiple points of entry, is increasingly becoming accessible – and valuable

33 L Irwin, 'The cost of a data breach in 2020', *IT Governance*, 3 September 2020 (www.itgovernance.co.uk/blog/the-cost-of-a-data-breach-in-2020). Last accessed on 25 March 2021. See also P Muncaster, 'Cost of UK Data Breaches Rises to £2.7 million', *Infosecurity Magazine*, 11 July 2018 (www.infosecurity-magazine.com/news/cost-of-uk-data-breaches-rises-to/). Last accessed on 25 March 2021.

34 'Virgin Media data breach affects 900,000 people', *BBC*, 5 March 2020 (www.bbc.com/news/business-51760510). Last accessed on 25 March 2021.

35 J Spero, 'British Airways says customer hack much bigger than it thought', *Financial Times*, 25 October 2018 (www.ft.com/content/f8505c34-d863-11e8-ab8e-6be0dcf18713) [J Spero, *Financial Times*]. Last accessed 23 March 2021.

36 R Jones and P Collinson, 'Identity theft warning after major data breach at Ticketmaster', *The Guardian*, 27 June 2018 (www.theguardian.com/money/2018/jun/27/identity-theft-warning-after-major-data-breach-at-ticketmaster). Last accessed 23 March 2021.

37 J Cook, 'Private data of 500 million Marriott guests exposed in massive breach', *The Telegraph*, 30 November 2018 (www.telegraph.co.uk/technology/2018/11/30/private-data-500-million-marriott-guests-exposed-massive-breach/). Last 23 March 2021.

38 In November 2020, the European Union Agency for Network and Information Security [ENISA] released a report entitled 'Guidelines for Securing the Internet of Things' outlining threats to IoT supply chains and best practices for ensuring their security. ENISA, 'Guidelines for Securing the Internet of Things', 9 November 2020 (www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things). Last accessed on 24 March 2021. In a December 2018 speech, the executive director of ENISA stated that there would be an estimated 20 billion operational devices by 2020. Professor Dr Udo Helmbrecht, Cybersecurity best practices', 12 December 2018 (www.enisa.europa.eu/publications/ed-speeches/cybersecurity-best-practices). In actuality, this figure was reached much sooner. By the end of 2018 there were an estimated 22 billion IoT connected devises in use around the world and forecasts suggest that by 2030 there will be 50 billion. Statista, 'Number of Internet of Things (IoT) connected devices worldwide in 2018, 2025 and 2030', (www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/#:~:text=By%20the%20end%20of%202018,in%20use%20around%20the%20world).

39 Statista, 'Number of Internet of Things (IoT) units in the electronics industry in the European Union (EU) in 2017, 2020 and 2025' (www.statista.com/statistics/691885/iot-electronics-in-the-eu/). Last accessed on 23 March 2021.

– to cybercriminals. For this reason, the Cybersecurity Act's certification scheme will have an important role in allowing manufacturers of internet-connected devices to demonstrate to consumers that data security is a fundamental aspect of their products and services.

National infrastructure

Cyber incidents affecting critical information infrastructures can have debilitating effects on the security, economy [40] and health of societies,[41] and the protection against which is a key pillar of the NISD. With the exception of state-sponsored actors, incidents involving national infrastructure are often less focused on access to information than the widespread disruption that results – the multiple recent malware attacks on Ukraine's power grid being a case in point.[42] Mirroring the challenges faced by financial services firms, the use of outdated technology in many core infrastructure systems compounds their exposure to even relatively unsophisticated cyberattacks.

Targeted information

Financial and payment data

Hackers most commonly target credit card and debit card details, including 'skimming' data from online retailers by introducing hidden code onto their websites.[43] They do so in spite of the requirements of the revised Payment Services Directive,[44] under which payment providers must implement measures to ensure the security of payment transactions and customer data. Criminals also use social engineering techniques, such as phishing campaigns and scam emails,[45] and sell financial data to third parties in online marketplaces.[46] In 2018, total card frauds in the EU and UK grew 13 per cent from the previous year, reaching a value of €1.8 billion from 21.05 million separate incidents, of which 79 per cent were carried out online (a 39 per cent increase over five years).[47]

---

40 The economic impact of this type of cybercrime in certain Member States, e.g., Germany and the Netherlands, can be as much as 1.5 per cent of gross domestic product. ENISA, 'The cost of incidents affecting CIIs', August 2016 (https://www.enisa.europa.eu/publications/the-cost-of -incidents-affecting-ciis). Last accessed on 11 March 2019.

41 ENISA, 'The cost of incidents affecting CIIs' (footnote 44).

42 A Greenberg, "Crash Override': The Malware That Took Down a Power Grid', *Wired*, 12 June 2017 (www.wired.com/story/crash-override-malware/). Last accessed on 25 March 2021. See also 'Ukraine power cut 'was cyber-attack", *BBC*, 11 January 2017 (www.bbc.com/news/technology-38573074). Last accessed on 25 March 2021

43 See, e.g., the 2018 British Airways hack: J Spero, *Financial Times* (footnote 38).

44 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC.

45 *See* European Central Bank [ECB], 'Executive summary (sixth report on card fraud)', 13 August 2020 (https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202008~521edb602b.en.html). Last accessed 23 March 2021.

46 M McGuire, 'Into the Web of Profit: Understanding the Growth of the Cybercrime Economy', April 2018 (https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf [M McGuire, 'Into the Web of Profit']. Last accessed on 23 March 2021.

47 See ECB, 'Executive summary (sixth report on card fraud)', (footnote 49).

Traditional personal data

Personal data is any information that relates to an identified or identifiable living individual.[48] Online digital services have helped turn this data into a financially valuable commodity. Typically, it is targeted (1) to extort individuals (i.e., the victim pays to prevent disclosure), (2) to assist other frauds, and (3) to sell via online markets.[49] Of all the different types of data targeted by hackers, personal data is the most frequently obtained.[50]

Non-traditional personal data

Big Data – the use of large data sets produced by a diverse range of sources – is viewed by the European Commission as fundamental to the future knowledge economy.[51] As part of this drive, esoteric information about all aspects of human life is being collected by governments and businesses with the aim of driving innovation and efficiency.[52] This includes data on individuals' voices, spending habits and gait, among other things, which can potentially constitute personal data.

Unethical data

Hacking is not always driven by financial or malicious intent; occasionally, 'ethical hackers' seek to expose unpopular or illegal behaviour. The targets of their activities are not limited to any particular industry or the size of the organisation. For example, in 2021, hackers exposed vulnerabilities in security cameras of hospitals, schools, factories, jails, and corporate offices to call attention to the dangers of mass surveillance.[53] In 2015, a Canadian private company was targeted because it was seen to be promoting infidelity.[54] The Panama Papers exposed a multinational industry that facilitated fraud, tax evasion and the avoidance of international sanctions.[55] The most high-profile example is Edward Snowden, who disclosed information

48 Article 4(1) of the GDPR.

49 Europol, 'Internet Organised Crime Threat Assessment 2020' (www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020). Last accessed on 24 March 2021.

50 Verizon, 'Data Breach Investigations Report', 2020 (https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf). [Verizon Data Breach Investigations Report]. Last accessed on 24 March 2021.

51 European Commission, 'Industrial applications of artificial intelligence and big data' (https://ec.europa.eu/growth/industry/policy/advanced-technologies/industrial-applications-artificial-intelligence-and-big-data_en). Last accessed 24 March 2021.

52 ENISA, 'The Value of Personal Online Data', 2018 (https://www.enisa.europa.eu/publications/info-notes/the-value-of -personal-online-data). Last accessed 24 March 2021.

53 M O'Brien and F Bajak, Security camera hack exposes hospitals, workplaces, schools', *Associated Press*, 10 March 2021 (https://apnews.com/article/hacking-california-e7b942f436f11b9feb7dc704d4eb3a6b). Last accessed 24 March 2021.

54 A Hern and S Gibbs, 'Ashley Madison hackers release vast database of 33m accounts', *The Guardian*, 19 August 2015 (www.theguardian.com/technology/2015/aug/19/ashley-madison-hackers-release-10gb-database-of-33m-infidelity-site-accounts). Last accessed 24 March 2021.

55 International Consortium of Investigative Journalists, 'Giant Leak of Offshore Financial Records Exposes Global Array Of Crime And Corruption', 3 April 2016 (www.icij.org/investigations/panama-papers/20160403-panama-papers-global-overview/). Last accessed 24 March 2021.

about the US National Security Agency and a global citizen surveillance programme.[56] Although less common than traditional hacking, cases of ethical hacking almost always hit newspapers' front pages and can cause massive reputational harm, as well as potentially legal and regulatory consequences.

Type and nature of actors and actions

Brute force attacks

Brute force attacks involve hacker programs applying trial and error to correctly identify passwords and user names and to find hidden web pages.[57] The techniques for brute force attacks are largely unsophisticated and easy to notice, which results in the vast majority being negated.[58] However, the simplicity of such methods means they are easily deployed and are increasingly popular (an estimated 80 per cent of global data breaches related to hacking in 2020 were the result of brute force attacks or use of stolen credentials).[59]

Government or state-sponsored entities

It is now widely accepted that governments engage in hostile cyber activities to undermine the information and network security of other countries.[60] The most notorious example is the 2020 SolarWinds hack, in which a major United States information technology firm was subject to a cyberattack that was spread to its many clients going undetected for months.[61] High-profile cases such as the SolarWinds hack and allegations of increases in cyber incidents involving European infrastructure have significantly raised public awareness of government-targeted hacking.[62] The unique structure of the EU and UK creates additional challenges, which is being seen in the increasing number of attacks aimed at its IT systems. For example, in 2020, ENISA reported that government administration is among the most targeted sectors for cyberattacks, and that the covid-19 pandemic has contributed to an uptick of attacks in the already strained healthcare sector.[63]

---

56 'Edward Snowden: Leak that exposed US spy programme', *BBC*, 17 January 2014 (www.bbc.com/news/world-us-canada-23123964).

57 Kaspersky Lab, 'What's a Brute Force Attack?' (www.kaspersky.com/resource-center/definitions/brute-force-attack). Last accessed on 24 March 2021.

58 eSentire Threat Intelligence, 'Annual Threat Report: 2019 Summary & 2020 Predictions' (www.esentire.com/resources/library/esentire-annual-threat-intelligence-report-2019-perspectives-and-2020-predictions). Last accessed on 24 March 2021.

59 Verizon Data Breach Investigations Report (footnote 54).

60 ENISA, 'Securing the Cyber Space in the Light of State Sponsored Activities', May 2017 (www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/securing-the-cyber-space-in-the-light-of-state-sponsored-activities). Last accessed on 24 March 2021.

61 I Jibilian and Katie Canales, 'Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal', *Business Insider*, 25 February 2021 (www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12). Last accessed on 24 March 2021

62 Associated Press, 'EU unveils revamp of cybersecurity rules days after hack', *ABC News*, 16 December 2021 (https://abcnews.go.com/Technology/wireStory/eu-unveils-revamp-cybersecurity-rules-days-hack-74756142). Last accessed on 24 March 2021.

63 ENISA, 'Main incidents in the EU and worldwide', 2020 (www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents). Last accessed on 24 March 2021.

Criminal attackers

It is estimated that the 2020 cost of cybercrime reached over US$1 trillion – a more than 50 per cent increase from 2018.[64] By some estimates, cybercrime may be the third-largest economy in 2021.[65] The financial rewards, coupled with low risks and low conviction rates, means that cybercrime is an increasingly attractive prospect. Revenues are generated through online illegal markets, where criminals can buy and sell stolen information, from companies' intellectual property to personal information. Criminals also make money through extortion, whereby attackers corrupt computer files with ransomware and then exchange the remedy for money.[66] The ill-gotten gains can then be laundered through legitimate online technologies, such as payment systems and cryptocurrencies such as bitcoin.[67]

AI-assisted hacking

Artificial intelligence (AI), such as machine learning, has the potential to create computer programs that can evade even the most sophisticated cyber defence systems. Traditionally, it was assumed that only state-sponsored entities had the resources to hack using AI.[68] However, these assumptions were challenged in 2018 when the American company IBM showcased a hacking program developed with AI at a security conference.[69] As a result, security experts in the EU and UK are increasingly concerned about AI and its potential for use in hacking and cybercrime.[70]

Nuances in investigative practices and regulatory enforcement

Regulatory enforcement

Enforcement of the EU and UK's cybersecurity laws has been growing of late with the amount of GDPR fines rising 40 per cent in the past year.[71] Whereas past enforcement of security failings produced marginal consequences, more recent GDPR enforcement actions have resulted in significantly higher monetary penalties for businesses.

One of the largest fines under the GDPR (€35 million) was issued in October 2020 by the Data Protection Authority of Hamburg against H&M for the company keeping 'excessive' records regarding employees' families, religions, illnesses and details of their vacation

64 Z Smith and E Lostri, 'The Hidden Costs of Cybercrime', McAfee, December 2020 (www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf). Last accessed on 24 March 2021

65 Marc Wilczek, 'Cybercrime May Be the World's Third-Largest Economy by 2021', *Dark Reading*, 4 April 2020 (www.darkreading.com/vulnerabilities---threats/cybercrime-may-be-the-worlds-third-largest-economy-by-2021/a/d-id/1337475). Last accessed on 24 March 2021.

66 Check Point and Europol, 'Ransomware: What You Need to Know', 15 December 2016 (www.europol.europa.eu/publications-documents/ransomware-what-you-need-to-know). Last accessed on 11 March 2019.

67 M McGuire, 'Into the Web of Profit' (footnote 50).

68 See, e.g., the Stuxnet programme allegedly developed by the United States, which shut down Iran's uranium enrichment facilities between 2005 and 2010.

69 J Menn, 'New genre of artificial intelligence programs take computer hacking to another level', *Reuters*, 8 August 2018 (www.reuters.com/article/us-cyber-conference-ai/new-genre-of-artificial-intelligence-programs-take-computer-hacking-to-another-level-idUSKBN1KT120). Last accessed on 11 March 2019.

70 D Rafter, 'Cyberthreat trends: 2019 cybersecurity threat review' (https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html). Last accessed on 11 March 2019.

71 DLA Piper, 'GDPR data breach' (footnote 5).

activities.[72] In February 2020, another large fine (€27.8 million) was issued by the Italian Data Protection Authority against Telecom Italia for several instances of 'unlawful processing for marketing purposes'.[73] The two largest security-related fines issued to date have been from the Information Commissioner's Office's (UK's Data Protection Authority), against British Airways[74] (€22 million) and Marriot (€20.4 million).[75]

If there was ever any doubt in the years leading up to GDPR's rollout, and shortly thereafter, that the legislation was capable of empowering regulators with significant enforcement abilities, those notions have clearly been dispelled by now. Indeed, the heightened regulatory focus on data security and breach notification, coupled with the substantial monetary penalties that can be issued under the GDPR and the NISD, indicate that seven- and eight-figure fines for cybersecurity failures will continue to become more commonplace.

Guidance

Along with the growing number of reported decisions in this area, practitioners have a growing body of guidance from which to draw when advising clients on how regulators are likely to view the requirements, and potential violations, of EU and UK cybersecurity laws. At the national level, numerous DPAs have been updating their security guidance to reflect the changes introduced by the GDPR, particularly around breach notification.[76] At the supranational level, in January 2021 the EDPB issued additional draft guidance on the type of personal data breaches that require notification under the GDPR. Organisations such as ENISA (in relation to the NISD as well as the wider cyber security context) and sector-specific regulators will also have an important role in helping organisations to equip themselves for the challenges they face in becoming, and staying, compliant with applicable cyber laws.

---

72 European Data Protection Board, 'Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre', 2 October 2020 (https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en). Last accessed 11 April 2021. See also 'H&M fined for breaking GDPR over employee surveillance', *BBC*, 5 October 2020 (www.bbc.com/news/technology-54418936). Last accessed on 11 April 2021.

73 European Data Protection Board, 'Marketing: The Italian SA Fines TIM EUR 27.8 Million', 1 February 2020 (https://edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-278-million_en). Last accessed 11 April 2021. Last accessed 11 April 2021. See also 'Italian DPA issues 27.8M euros for GDPR violation', IAPP, 3 February 2020 (https://iapp.org/news/a/italian-dpa-fines-spa-27-8m-euros-for-gdpr-violations/#:~:text=The%20Italian%20data%20protection%20authority,promotional%20phone%20calls%20without%20consent). Last accessed on 24 March 2021.

74 'ICO fines British Airways £20m for data breach affecting more than 400,000 customers', ICO, 16 October 2020 (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/#:~:text=The%20Information%20Commissioner's%20Office%20(ICO,than%20400%2C000%20of%20its%20customers.&text=The%20law%20now%20gives%20us,%2Dto%2Ddate%20security.%E2%80%9D). Last accessed on 24 March 2021.

75 'ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure', ICO, 30 October 2020 (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/). Last accessed on 24 March 2021.

76 See, in particular, detailed guidance issued by data protection authorities in Ireland and Spain.

EU and UK litigation considerations

Cybersecurity litigation in the EU and UK remains small relative to longer established areas of regulation. This is to be expected, given that its two main omnibus laws have been in force for less than three years. Nevertheless, practitioners should prepare for a continuing increase in contentious activity in the coming years and beyond, particularly relating to the fallout from personal data breaches and other high-profile security incidents. In addition to the type of follow-on claims that are common in the antitrust sphere, disputes brought directly by data subjects or their representatives are likely to reshape the EU and UK's cybersecurity landscape in a way that was not contemplated (or, in some cases, possible) under the DPD. The extent to which individuals are now aware of their rights under data privacy and security laws, and the relative ease with which they can be enforced, make it likely that some of the defining aspects of US litigation – large settlement awards and group actions, among others – may become an increasingly common feature of EU and UK cyber disputes.

General Data Protection Regulation

The GDPR provides for two forms of private action. Article 79(1) entitles individuals to an effective judicial remedy when their rights are infringed by the processing of personal data by a controller or processor in violation of the GDPR. Article 79(1) has a wider application than the DPD regime in two important respects.

First, it does not limit liability for compensation to controllers, the result being that if controllers and processors are involved in data processing that infringes the GDPR, each shall be held liable to the data subject for the entire damage.[77] Second, Article 82(1) makes it clear that both material and non-material damage is actionable under the GDPR (i.e, compensation is not limited to when an individual suffers financial harm). Practitioners may be familiar with the decision in *Vidal-Hall*, in which the English Court of Appeal in 2015 interpreted that country's pre-GDPR regime as permitting compensation for non-pecuniary losses.[78] Indeed, the scope for emotional damage caused as a result of cybersecurity incidents (e.g., the distress associated with the theft of personal information) means compensation claims for non-pecuniary losses are likely to be a defining feature of the EU and UK litigation landscape in the coming years.

Article 80 of the GDPR entitles not-for-profit bodies and other public interest organisations to seek effective judicial remedy on behalf of individuals. The ability to issue group proceedings in respect of cyber incidents is a significant development for the EU and UK, and may come to represent a key tool by which controllers and processors are held to account. However, the extent to which this prospect will be realised depends in part on the Member States, as they are given discretion as to whether, and if so how, the GDPR's collective redress provisions are implemented in each territory.[79] Indeed, in early 2021, the UK government

77 Article 82(5) of the GDPR: 'Where a controller or processor has . . . paid full compensation for the damage suffered, [it] shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage.'

78 *Google Inc v. Vidal-Hall &* Ors [2015] EWCA Civ 311.

79 Article 80(1) of the GDPR provides that Member States (1) must permit an individual to mandate a third-party organisation to lodge a complaint against a data protection authority and/or seek judicial remedies against a controller or processor, but (2) have discretion as to whether that organisation can receive compensation on

announced that it would not allow consumer groups and other not-for-profit bodies to bring actions on individuals' behalf on an opt-out basis. At the time of writing, these provisions are also not being applied evenly across the EU and UK, with early indications suggesting that Member States are unwilling to grant not-for-profit bodies the ability to bring actions on data subjects' behalf (i.e., in a manner similar to the opt-out class actions with which US practitioners will be familiar). In the UK, for example, a court recently ruled that a law firm's costs of building a group action by soliciting potential claimants (e.g., marketing and other advertising costs) were not recoverable costs, thus likely impacting the profitability of organisations seeking to bring about these kinds of actions.[80]

Differences between EU laws and national laws

A key driver behind the introduction of the GDPR was the lack of harmonisation that had developed as a result of the diverging approaches Member States had taken in implementing the DPD.[81] Such fragmentation also exists in respect of Member States' approach to collective redress, and following Brexit this divergence may continue apace in the UK. This is particularly important in the context of cybersecurity, given that (as noted above) some national legislatures may be unwilling to implement the provision in Article 80(2) of the GDPR that permits a form of opt-out class action. A study commissioned by the European Parliament and published in October 2018 revealed the extent to which the landscape remains uneven.[82] Among other things, the Member States surveyed differed – often significantly – in the forms and scope of redress available, the standing to bring actions, and the fees and funding models. For example, contrary to their previously restrictive approach, German courts are increasingly granting significant damages in mass data litigations. To address these considerations, on 25 November 2020, the EU and UK adopted a new directive dealing with representative actions that will allow qualifying organisations to bring about collective actions on behalf of consumers throughout the EU and UK.[83] In addition to these developments, the wider emphasis on consumer protection by the EU and UK's governing bodies makes it probable that, in addition to the GDPR's provisions on collective actions, individuals will in the near future have a range of tools with which to bring mass claims in relation to cybersecurity and related incidents.

behalf of the individual. Article 80(2) of the GDPR provides that Member States have discretion as to whether the organisation can, independently of the data subject's mandate, lodge a complaint against a data protection authority or seek judicial remedies against a controller or processor.

80 *Weaver & Ors v. British Airways Plc* [2021] EWCA 217 (QB).

81 Whereas Member States have a significant degree of discretion in transposing the requirements of an EU Directive into national law, an EU Regulation has general application and is directly applicable and binding in its entirety.

82 Policy Department for Citizens' Rights and Constitutional Affairs, Study, 'Collective redress in the Member States of the European Union', October 2018 (www.europarl.europa.eu/RegData/etudes/STUD/2018/608829/IPOL_STU(2018)608829_EN.pdf). Last accessed on 24 March 2021.

83 Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC.

Appendix 1

About the Authors

Rohan Massey
Ropes & Gray LLP

Rohan Massey is a leader of Ropes & Gray's data, privacy and cybersecurity practice and focuses his practice on data protection, data security, e-commerce, and IT. As well as advising on complex global data protection and security compliance programmes, Rohan also advises on issues of risk and value in relation to data and intellectual property in corporate transactions. Rohan's expertise focuses on the intersection of the extra-territorial scope of national data protection laws and data transfer issues for multinational organisations. Rohan has advised on a number of leading breach data management cases, and has assisted clients in successfully obtaining BCR approval from EU regulators. His industry-focused expertise covers asset management and financial services; life sciences and clinical trials; as well as media, sponsorship, advertising, sales promotions; and intellectual property issues, marketing issues in the sports apparel and food and drink sectors. His client base is international in scope, as he works extensively across Europe, the United States and Asia.

Kevin Angle
Ropes & Gray LLP

Kevin Angle is counsel in the data, privacy & cybersecurity group, based in Ropes & Gray's Boston office. He represents a broad range of companies on privacy and cybersecurity matters, guiding clients through the existing patchwork of US federal and state laws as well as the European Union's comprehensive General Data Protection Regulation (GDPR) and other international privacy and cybersecurity laws. Kevin advises clients on privacy and cybersecurity matters arising in corporate transactions. He also assists clients in responding to data breach incidents, helping clients in assessing their legal obligations following a breach and in responding to regulatory authorities and others.

Edward Machin
Ropes & Gray LLP

Edward Machin is an associate in the data, privacy and cybersecurity group, based in Ropes & Gray's London office. He provides clear and business-focused advice on a wide range of legal and regulatory issues in the rapidly evolving areas of privacy, data protection and security, e-commerce and marketing, and information law. Secondments at data-rich businesses in the life sciences and market research sectors have given Edward a deep understanding of what clients want – and these experiences inform his approach to providing practical legal and commercial solutions to organisations across Europe, the United States and Asia.

Edward's practice encompasses regulatory compliance, advisory and transactional work for founders, start-ups, corporates, venture capitalists and asset managers across the technology, life sciences and healthcare, financial and professional services, food and beverage, consumer goods, entertainment and media sectors. He regularly advises on the development and operationalisation of global compliance programmes, new products and services, complex international data transfer issues, and emerging technologies and regulatory trends (such as the use of alternative data and covid-19-related compliance).

Raffi Teperdjian
Ropes & Gray LLP

Raffi Teperdjian is an associate in the intellectual property litigation group at Ropes & Gray's Washington, DC office. Raffi's legal work includes the intersection of blockchain and emerging technologies with intellectual property, financial technology, data privacy and cybersecurity. He has published articles on the regulation of blockchain by the EU's GDPR, proposing options for United States cybersecurity regulation of smart contracts, and studying the national security implications of cryptocurrency financing. Prior to, and concurrently with, his study of the law, Raffi worked on a variety of systems development and big data analysis projects in both federal and commercial information technology consulting.

Ropes & Gray LLP
60 Ludgate Hill
London EC4M 7AW
United Kingdom
Tel: +44 20 3201 1500
Fax: +44 20 3201 1501
rohan.massey@ropesgray.com
edward.machin@ropesgray.com

Prudential Tower
800 Boylston Street
Boston, MA 02199
United States
Tel: +1 617 951 7000
Tel: +1 617 951 7050
richard.batchelder@ropesgray.com

kevin.angle@ropesgray.com

1211 Avenue of the Americas
New York, NY 10036-8704
United States
Tel: +1 212 596 9000
Fax: +1 212 596 9090
anne.conroy@ropesgray.com
Three Embarcadero Center
San Francisco, CA 94111-4006
Tel: +1 415 315 6300
Fax: +1 415 315 6350
danielle.bogaards@ropesgray.com
sara.ramsey@ropesgray.com

2099 Pennsylvania Avenue, NW
Washington, DC 20006-6807
United States
Tel: +1 202 508 4600
Fax: +1 202 508 4650
nameir.abbas@ropesgray.com
raffi.teperdjian@ropesgray.com

www.ropesgray.com

Data breaches and similar incidents pose a unique challenge – those targeted must both respond and investigate simultaneously. It is an art that is impossible without preparation.

Businesses wishing to prepare will find this volume, *The Guide to Cyber Investigations*, invaluable. It identifies every issue to consider when creating a response template and implementing it, giving both the law and plenty of practical and tactical advice.

Written by leading contributors, all with broad experience of serious data incidents, it is an indispensable desktop guide and a worthy companion to GIR's larger volume on cross-border investigations, *The Practitioner's Guide to Global Investigations*.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-595-5