Global Investigations Review

# The Guide to Cyber Investigations

**Editors**
Benjamin A Powell, Leah Schloss, Maury Riggan and Jason C Chipman

# The Guide to Cyber Investigations

Editors:

Benjamin A Powell

Leah Schloss

Maury Riggan

Jason C Chipman

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2019
For further information please contact Natalie.Clarke@lbresearch.com

GIR
Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.globalinvestigationsreview.com





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 978-1-83862-223-7

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

# Acknowledgements

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

RICHARD DENATALE

HUNTON ANDREWS KURTH 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 third 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

# 10

# Cyber Trends and Investigations in the European Union: A Practitioner's Perspective

**Rosemarie Paul and Edward Machin**[1]

## Cyber requirements under EU law

Many organisations in the European Union, and those in the rest of the world that offer products or services to individuals in the EU, associate cybersecurity with four letters: GDPR. However, the General Data Protection Regulation[2] is only one thread in a patchwork of cybersecurity laws and best practices in the EU 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 will be subject to the GDPR.[3] Accordingly, the extent to which digital business is now borderless means that the influence and scope of EU cybersecurity laws is no longer a strictly regional concern.

The development of the EU'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 is compromised. These concerns are not unwarranted: in February 2019, it was reported that nearly 60,000 personal data breaches had been notified since the introduction of the GDPR on 25 May 2018.[4] Even

1 Rosemarie Paul is a partner and Edward Machin is an associate at Ropes & Gray LLP.

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].

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.

4 'DLA Piper GDPR data breach survey: February 2019' (www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/). Last accessed on 11 March 2019.

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 cyber threats. 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 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 these approaches 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. Recent public pronouncements from DPAs in the EU indicate that there is an appetite to investigate and penalise infringements of the GDPR's security principles, utilising the higher fines available under the GDPR (i.e., €20 million or 4 per cent of global annual turnover, whichever is higher).[9] 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.

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 11 March 2019.

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 Article 83(5) of the GDPR.

## 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.[10] That being said, certain baseline standards are likely to apply to most organisations, including network perimeter defences, malware protection, password policies and secure configuration.[11]

## 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.[12] The regulator must be notified without undue delay and within 72 hours of becoming aware of the breach,[13] otherwise the organisation may face liability of up to €10 million or 2 per cent of global annual turnover, whichever is higher.[14] The threshold for mandatory notification to a DPA is where there is 'a risk to the rights and freedoms' of individuals;[15] the requirements for notification to affected individuals are higher still.[16] While certain breaches will be obviously reportable, some organisations appear to be struggling to assess breaches at the lower end of the spectrum 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.

10 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 (https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf). Last accessed on 11 March 2019.

11 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'.

12 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.

13 Article 33(1) of the GDPR.

14 Article 83(4) of the GDPR.

15 Article 33(1) of the GDPR.

16 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.'

A recent report by the Dutch DPA is instructive: of the 20,881 breach notifications the DPA received in 2018, it took action in fewer than 300 cases.[17] 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[18] (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[19] and to report all incidents that have a substantial impact on the provision of their services.[20] Both laws require covered organisations to consider 'the state of the art'[21] 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 incident under the GDPR, and 'without undue delay' under the NISD),[22] 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,

17 Autoriteit Persoonsgegevens, 'Medlplicht datalekken: facts & figures', 1 February 2019 (https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarrapportage_meldplicht_datalekken_2018.pdf). Last accessed on 11 March 2019.

18 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].

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

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

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

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

regulatory guidance [23] 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.[24] The answer to this and other questions should become clearer as a line of reportable decisions and regulatory enforcement actions appear in the (hopefully) near future.

## Cybersecurity Act

In December 2018, the European Parliament, the Council and the European Commission reached political agreement on the Cybersecurity Act, which establishes an EU framework for cybersecurity certification and creates a permanent mandate for the European Union Agency for Network and Information Security (ENISA) to better support Member States in responding to cyber threats and attacks. The EU-wide cybersecurity certification framework enables parties in the information and communications technology 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 for enterprises. It is hoped companies will have the incentive to invest in cybersecurity and make this a competitive advantage.[25]

## Trends

As technology moves faster than law, so technology crime continues to outpace innovations in security. Cyber criminals 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, 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.[26] As highlighted in a Report on the Risks and Vulnerabilities in the EU Financial System by the Joint Committee

23 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 11 March 2019.

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

25 European Commission, 'Cybersecurity Act: EU negotiators agree on strengthening Europe's cybersecurity', 11 December 2018 (https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en). Last accessed 18 March 2019.

26 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.

of the European Supervisory Authorities, a particular concern relates to the measures required to address legacy IT systems.[27] 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.[28]

## Consumer-facing businesses

It should come as no surprise that consumer organisations are a prime target for cyber criminals, 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 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. The regularity with which consumer-facing companies are suffering large data breaches (British Airways,[29] Ticketmaster [30] and Marriott International [31] have all been hacked within the past year) 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.[32] That much of this information reveals detailed, and often deeply personal, insights into individuals' private lives makes it especially attractive to bad actors. Approximately 277 million Internet of Things units are predicted to be in use in the EU by 2020,[33] including for use in 'smart' homes, cars, hospitals, airports and cities. Data about the time we leave and return

27 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 11 March 2019.

28 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 18 March 2019.

29 J Spero, 'British Airways says customer hack much bigger than it thought', *Financial Times*, 25 October 2018 (https://www.ft.com/content/f8505c34-d863-11e8-ab8e-6be0dcf18713) [ J Spero, *Financial Times*]. Last accessed 12 March 2019.

30 R Jones and P Collinson, 'Identity theft warning after major data breach at Ticketmaster', *The Guardian*, 27 June 2018 (https://www.theguardian.com/money/2018/jun/27/identity-theft-warning-after-major-data-breach-at-ticketmaster). Last accessed 18 March 2019.

31 J Cook, 'Private data of 500 million Marriott guests exposed in massive breach', *The Telegraph*, 30 November 2018 (https://www.telegraph.co.uk/technology/2018/11/30/private-data-500-million-marriott-guests-exposed-massive-breach/). Last accessed 18 March 2019.

32 In a 2017 speech, the executive director of the European Union Agency for Network and Information Security [ENISA] stated that the internet of things world 'will result in everything being connected everywhere. And it needs to be secure'. Professor Dr Udo Helmbrecht, 'Security Challenges and best practices in the IoT Environment', 7 November 2017 (https://www.enisa.europa.eu/publications/ed-speeches/security-challenges-and-best-practices-in-the-iot-environment/). Last accessed on 11 March 2019.

33 Statista, 'Internet of Things (IoT) in Europe – Statistics & Facts' (https://www.statista.com/topics/4123/internet-of -things-iot-in-europe/). Last accessed on 11 March 2019.

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 – to cyber criminals. 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 [34] and health of societies,[35] 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. 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.[36] They do so in spite of the requirements of the revised Payment Services Directive,[37] 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,[38] and sell financial data to third parties in online marketplaces.[39] In 2016, total card frauds in the EU reached a value of €1.8 billion from 17.3 million separate incidents, of which 73 per cent were carried out online (a 66 per cent increase over five years).[40]

34 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.

35 ENISA, 'The cost of incidents affecting CIIs' (footnote 32).

36 See, e.g., the 2018 British Airways hack: J Spero, *Financial Times* (footnote 24).

37 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.

38 See European Central Bank [ECB], 'Executive summary (fifth report on card fraud)', 26 September 2018 (https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html#toc3). Last accessed 12 March 2019.

39 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 11 March 2019.

40 See ECB, 'Executive summary (fifth report on card fraud)', (footnote 36).

### Traditional personal data

Personal data is any information that relates to an identified or identifiable living individual.[41] 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.[42] Of all the different types of data targeted by hackers, personal data is the most frequently obtained.[43]

### 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.[44] 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.[45] 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 2015, a Canadian private company was targeted because it was seen to be promoting infidelity.[46] The Panama Papers exposed a multinational industry that facilitated fraud, tax evasion and the avoidance of international sanctions.[47] The most high-profile example is Edward Snowden, who disclosed information about the US National Security Agency and a global citizen surveillance programme. 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.

41 Article 4(1) of the GDPR.

42 Europol, 'Internet Organised Crime Threat Assessment 2018' (https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018). Last accessed on 12 March 2019.

43 Verizon, 'Data Breach Investigations Report: Tales of dirty deeds and unscrupulous activities', 2018 (https://enterprise.verizon.com/en-gb/resources/reports/dbir/). [Verizon Data Breach Investigations Report]. Last accessed on 11 March 2019.

44 European Commission, 'Big data and digital platforms' (https://ec.europa.eu/growth/industry/policy/digital-transformation/big-data-digital-platforms_en). Last accessed 12 March 2019.

45 ENISA, 'The Value of Personal Online Data', 2018 (https://www.enisa.europa.eu/publications/info-notes/the-value-of -personal-online-data). Last accessed 12 March 2019.

46 A Hern and S Gibbs, 'Ashley Madison hackers release vast database of 33m accounts', *The Guardian*, 19 August 2015 (https://www.theguardian.com/technology/2015/aug/19/ashley-madison-hackers-release-10gb-database-of -33m-infidelity-site-accounts). Last accessed 12 March 2019.

47 International Consortium of Investigative Journalists, 'Giant Leak of Offshore Financial Records Exposes Global Array Of Crime And Corruption', 3 April 2016 (https://www.icij.org/investigations/panama-papers/20160403-panama-papers-global-overview/). Last accessed 12 March 2019.

## 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.[48] The techniques for brute force attacks are largely unsophisticated and easy to notice, which results in the vast majority being negated.[49] However, the simplicity of such methods means they are easily deployed and are increasingly popular (an estimated 5 per cent of global data breaches in 2017 were the result of brute force attacks).[50]

### 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.[51] The most notorious example is the 2017 NotPetya attack, in which computer files of Ukrainian banks, energy firms and senior officials were wiped by hackers suspected of being associated with the Russian military. High-profile cases such as the NotPetya attack and allegations of interference in foreign elections have significantly raised public awareness of government-targeted hacking.[52] The unique structure of the EU creates additional challenges, which is being seen in the increasing number of attacks aimed at its IT systems. For example, in 2016, the European Commission reported 110 separate attacks on its servers, a 20 per cent increase on the previous year.[53]

### Criminal attackers

It is estimated that the cybercrime economy now generates more than US$1.5 trillion in revenues every year.[54] 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

48 Kaspersky Lab, 'What's a Brute Force Attack?' (https://www.kaspersky.com/resource-center/definitions/brute-force-attack). Last accessed on 11 March 2019.

49 eSentire Threat Intelligence, 'Annual Threat Report: 2017 Summary & 2018 Predictions' (https://www.esentire.com/resource-library/2017-annual-threat-report). Last accessed on 11 March 2019.

50 Verizon Data Breach Investigations Report (footnote 41).

51 ENISA, 'Securing the Cyber Space in the Light of State Sponsored Activities', May 2017 (https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/securing-the-cyber-space-in-the-light-of -state-sponsored-activities). Last accessed on 11 March 2019.

52 A Rettman, 'EU raises alarm on fake news and hacking', 11 January 2017, (https://euobserver.com/foreign/136503?utm_content=44319878&utm_medium=social&utm_source=twitter). Last accessed on 11 March 2019.

53 A Beesley, 'EU suffers jump in aggressive cyber attacks', *Financial Times*, 8 January 2017 (https://www.ft.com/content/3a0f0640-d585-11e6-944b-e7eb37a6aa8e). Last accessed on 9 March 2019.

54 M McGuire, 'Into the Web of Profit' (footnote 34).

money.[55] The ill-gotten gains can then be laundered through legitimate online technologies, such as payment systems and cryptocurrencies such as bitcoin.[56]

### 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.[57] However, these assumptions were challenged in 2018 when the American company IBM showcased a hacking program developed with AI at a security conference.[58] As a result, security experts in the EU are increasingly concerned about AI and its potential for use in hacking and cybercrime.[59]

## Nuances in investigative practices and regulatory enforcement

### Regulatory enforcement

There has been limited enforcement of the EU's cybersecurity laws to date: at the time of writing, the only substantial fine levied under the GDPR relates to transparency and consent.[60] Enforcement of security failings have, thus far, resulted in significantly lower penalties. For example, the DPA of Baden-Wurttemberg recently issued two fines, one relating to a controller's failure to encrypt passwords (resulting in a €20,000 penalty), and the other relating to a failure to adopt appropriate internal controls for processing sensitive personal data (resulting in an €80,000 penalty).

The largest security-related fine under the GDPR (€400,000) was issued in October 2018 by the Portuguese DPA. It concerned the failure of the Centro Hospitalar Barreiro Montijo (a hospital near Lisbon) to process personal data with appropriate security measures in place.

While the size of these penalties is unremarkable (and is lower than those issued under the DPD), this is unlikely to be the case for long. 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 it is only a matter of time before seven- and eight-figure fines for cybersecurity failures will become, if not commonplace, then unsurprising in their regularity.

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

56 M McGuire, 'Into the Web of Profit' (footnote 34).

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

58 J Menn, 'New genre of artificial intelligence programs take computer hacking to another level', *Reuters*, 8 August 2018 (https://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.

59 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.

60 On 21 January 2019, the CNIL issued a €50 million fine for infringements of the GDPR's rules on transparency and consent. The fine is currently being appealed.

### Guidance

In contrast to the lack 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 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.[61] In addition, the EDPB's published guidance will continue to influence both how organisations discharge their obligations under the GDPR and how DPAs will enforce these obligations. 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.

## EU litigation considerations

Cybersecurity litigation in the EU is in its infancy. This is to be expected, given that its two main omnibus laws have been in force for little more than 12 months. Nevertheless, practitioners should prepare for a steady increase in contentious activity in the coming year 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'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 also soon become a feature of EU 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.[62] 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.[63] Indeed, the scope for emotional damage caused as a result of cybersecurity incidents

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

62 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.'

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

(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 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 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.[64] At the time of writing, these provisions are not being applied evenly (if at all) across the EU, 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).

## EU law

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.[65] Such fragmentation also exists in respect of Member States' approach to collective redress. 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 reveals the extent to which the current landscape is uneven.[66] 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. We consider it likely that some, if not all, of these considerations will be addressed in due course, albeit perhaps not specifically in the cybersecurity context. Nevertheless, the wider emphasis on consumer protection by the EU'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.

64 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 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.

65 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.

66 Policy Department for Citizens' Rights and Constitutional Affairs, Study, 'Collective redress in the Member States of the European Union', October 2018 (http://www.europarl.europa.eu/RegData/etudes/STUD/2018/608829/IPOL_STU(2018)608829_EN.pdf). Last accessed on 11 March 2019.

# Appendix 1

## About the Authors

**Rosemarie Paul**
Ropes & Gray LLP

Rosemarie Paul specialises in UK financial regulatory matters, with a particular focus on regulatory investigations and enforcement proceedings involving the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA). She has a particular interest in cybersecurity and operational resilience issues for firms.

Rosemarie joined Ropes & Gray's litigation and enforcement practice in 2018 from the London office of another international firm. Prior to joining private practice in 2012, she was a member of the Enforcement and Financial Crime Department at the Financial Services Authority, where she provided legal advice to the investigatory teams in the Enforcement Division, led cases through Decision Committee and Upper Tribunal hearings and advised on contested applications for authorisation and approved persons.

Rosemarie has a detailed understanding of the regulators' supervisory process. She assists clients in anticipating and addressing issues that arise under the UK regulatory framework and is able to identify how the FCA's and PRA's regulatory requirements will affect her clients. She is also experienced in cross-border investigations.

**Edward Machin**
Ropes & Gray LLP

Edward Machin joined the privacy and cybersecurity group of Ropes & Gray's London office as an associate in 2018. Before joining the firm, Edward worked in the Tier 1 data protection practice of a UK law firm, advising clients on a variety of privacy, data security, e-commerce and information law issues.

Edward's practice encompasses regulatory compliance, advisory, public policy and transactional work for start-up and established companies across the technology, life sciences, food and beverage, professional services, entertainment and media sectors. He also represents clients before EU regulators and in litigation relating to privacy and data protection.

During his training contract, Edward was seconded to a global pharmaceutical firm where he advised on a range of data protection matters, including subject access requests, direct marketing campaigns and medical consent requirements. Before commencing his training, Edward worked for six years as an award-winning legal journalist.

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

ISBN 978-1-83862-223-7