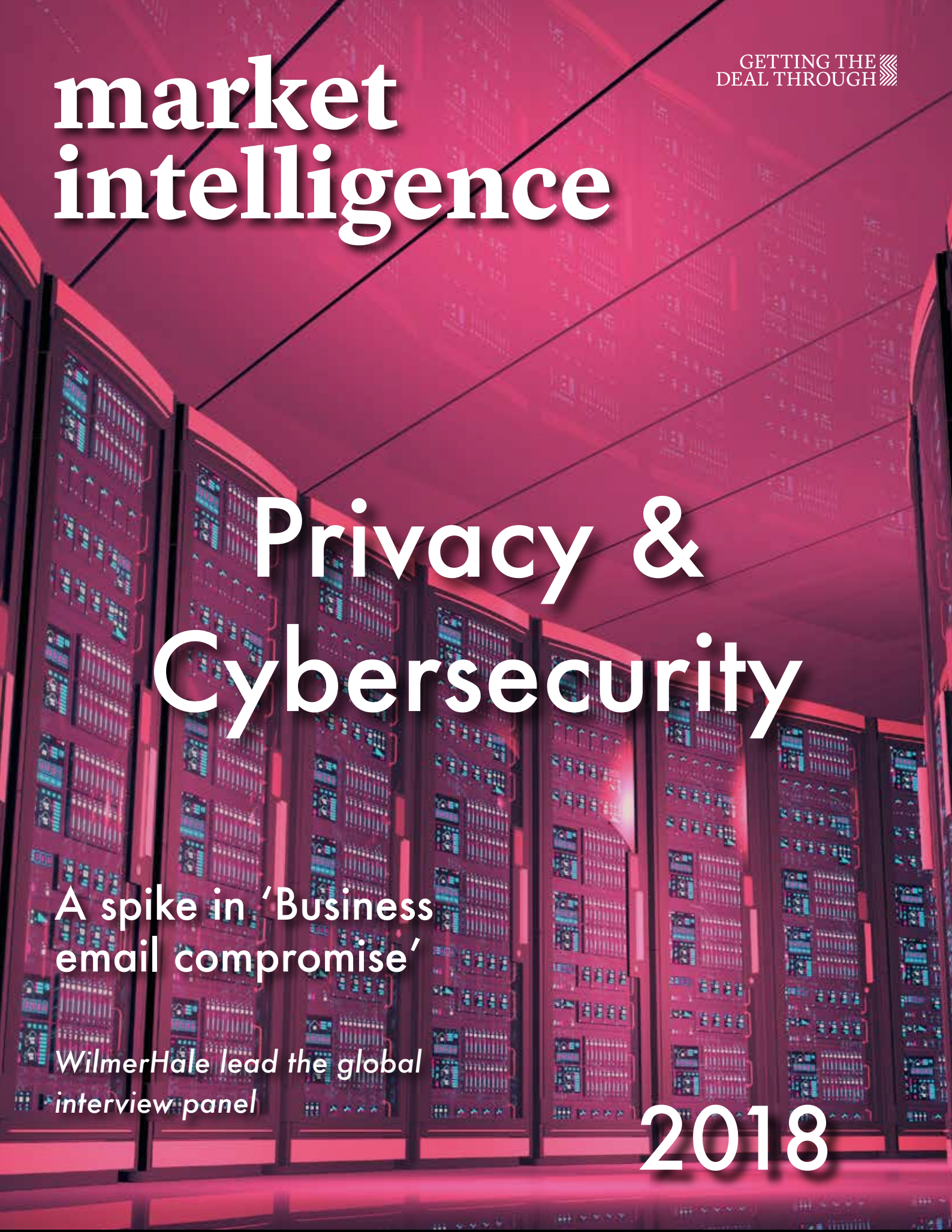

GETTING THE DEAL THROUGH

market intelligence

Privacy & Cybersecurity

A spike in 'Business email compromise'

WilmerHale lead the global interview panel

2018

North America • Asia-Pacific • Europe • Latin America
Regulatory developments • M&A risks • Best practice • Cloud computing

Publisher: Tom Barnes
Senior business development manager: Adam Sargent
adam.sargent@gettingthedealthrough.com
Business development manager: Dan Brennan
dan.brennan@gettingthedealthrough.com
Product marketing manager: Kieran Hansen
subscriptions@gettingthedealthrough.com

Head of production: Adam Myers
Editorial coordinator: Gracie Ford
Subeditor: Janina Godowska
Designer/production editor: Harry Turner

Cover: iStock.com/Maxiphoto

Published by
Law Business Research Ltd
87 Lancaster Road

Law Business Research

London, W11 1QQ, UK
Tel: +44 20 3780 4104
Fax: +44 20 7229 6910

ISBN: 978-1-78915-086-5

GETTING THE DEAL THROUGH

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

market intelligence

Welcome to GTDT: *Market Intelligence*.

This is the 2018 edition of *Privacy and Cybersecurity*.

Getting the Deal Through invites leading practitioners to reflect on evolving legal and regulatory landscapes. Through engaging and analytical interviews, featuring a uniform set of questions to aid in jurisdictional comparison, *Market Intelligence* offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most interesting cases and deals.

Market Intelligence is available in print and online at www.gettingthedealthrough.com/intelligence.

Getting the Deal Through
London
August 2018

Contents

Global Trends 2
Australia 4
Brazil 11
European Union and Belgium 18
Germany 32
Hong Kong 38
Mexico 44
Netherlands 49
Peru 55
Russia 61
Taiwan 67
United Kingdom 72
United States 80

Photo by Javier M. on Unsplash

PRIVACY AND CYBERSECURITY IN THE

NETHERLANDS

Quinten Kroes heads Brinkhof's data protection practice and has been active as a lawyer in the telecommunications, media and technology (TMT) sectors since 1995. He advises a broad range of companies on data protection. He has supported various companies that have been the subject of investigations by the Dutch Data Protection Authority.

Gerrit-Jan Zwenne was a partner at Brinkhof from 1 February 2016 until 1 September 2018. He specialises in privacy, telecommunications and internet law. In addition, Gerrit-Jan is Professor of Law and the Information Society at Leiden University.

Both Quinten's and Gerrit-Jan's individual reputations are recognised as top tier in legal directories, as is the quality of Brinkhof's data protection practice.


Quinten Kroes


Gerrit-Jan Zwenne

GTDT: What are the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

Quinten Kroes and Gerrit-Jan Zwenne: In February 2018, a new proposal for a Cybersecurity Act was sent to the Lower House of Parliament. This Cybersecurity Act is meant to implement the EU Directive on Security of Network and Information Systems (also known as the NIS Directive), which should have been incorporated into Dutch law on 9 May 2018. The aim of the NIS Directive is to create an overall higher level of cybersecurity in the EU. The directive significantly affects digital service providers (DSPs) and operators of essential services (OESs). Both DSPs and OES must report major security incidents to their national competent authorities and computer security incident response teams.

The new proposal is set to replace the existing Data Processing and Notification Duty Cybersecurity Act, parts of which will be incorporated into the new Cybersecurity Act. Although the existing act already imposes a notification duty for security incidents on providers of services of which the availability or reliability are considered essential for Dutch society, it does not yet fully meet the requirements of the NIS Directive. To achieve full compliance, the new Cybersecurity Act will maintain the existing duty to notify the National Cyber Security Centre, and introduce a new duty for DSPs and OESs to also notify their competent supervisory authority (eg, the Dutch central bank for financial institutions). These authorities will see to it that mandatory security requirements and the notification duty have been complied with and may impose sanctions if this is not the case.

Another significant development is the new Intelligence and Security Services Act, which was approved by the Dutch Upper House of Parliament in July 2017. The act grants intelligence and security services more powers to use modern technologies for the prevention of crime. Although the majority of stakeholders were in agreement that the old act was outdated and not suited for the online threats of modern society, the replacement act faced a storm of criticism, not only from civil rights organisations but also from industry, specifically concerning oversight safeguards and the periods for which data can be retained by intelligence services. In an attempt to address concerns, the government agreed to evaluate the effectiveness of the new powers, and their safeguards, two years after the act will have entered into force, instead of the usual five.

However, this concession failed to eliminate civic opposition to the act, which resulted in a consultative referendum on the act which was held on 21 March 2018. In this referendum, a narrow but decisive majority of all voters (49.44 per cent) voted against the law. Although the referendum itself was non-binding, the Dutch government decided to make some minor amendments to the act to respect the outcome of the referendum. The amended act entered into force on 1 May 2018.

Of course there was also the General Data Protection Regulation (GDPR), which became applicable law on 25 May 2018. The new Act to enable the application of the GDPR entered into force on that same day. Since this new act also effectively withdrew the former Data Protection Act, approximately 40 existing laws now include obsolete references to the old act or use outdated terminology that is not in line with the GDPR. The additional Modification Act, which is meant to fix this, passed both Houses of Parliament (the act was approved by the Upper House on 10 July 2018) and is expected to enter into force later this year. The Modification Act includes restrictions that stipulate that certain GDPR articles do not apply to specific Dutch laws, such as the Dutch Population Register Act and the Dutch Electoral Act. Lastly, a third act has been proposed to modify the Judicial Data and Criminal Records Act in order to implement Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data

by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

GTDT: When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

QK & GJ Z: Pursuant to article 33 of the GDPR, the controller must notify a personal data breach to the supervisory authority, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also, without undue delay, inform the data subjects, communicating in clear and plain language the nature of the personal data breach. This communication is not required when the controller has taken measures to ensure the risk of a breach is no longer likely to materialise.

These breach notification requirements are not new for the Netherlands. Since 2016, the Dutch Data Protection Act included a data breach notification duty that was more or less similar to that of the GDPR.

The Dutch Data Protection Authority (DPA) has issued guidelines in English that can help organisations determine whether a security incident qualifies as a data breach, and if so, whether they must report this breach to the DPA and possibly to the data subjects (https://autoriteitpersoonsgegevens.nl/en/news/data-breach-notification-obligation). Although the policy rules provide guidance for the breach notification under the former Data Protection Act, which was withdrawn when the GDPR became applicable, they continue to be useful for controllers who are confronted with a possible breach, and are in some respects more detailed than the guidance issued in 2017 by article 29 Working Party (in their WP 250). Both guidance documents make it clear that a number of criteria will be relevant to assess whether a notification needs to be made. These include the sensitivity of the data, the number of data subjects affected, the volume of data lost and the possible consequences for data subjects. Moreover, the categories of data subjects are also relevant (eg, data relating to children or other vulnerable groups).

Following its guidelines, the DPA has given further guidance specifically on the question whether ransomware can qualify as a breach that needs to be notified. In short, it takes the position that this is indeed the case, as the illegal encryption of data implies illegal access to data and a circumvention of security measures that should have prevented this. Also, the DPA considers that it will often be hard to establish the precise effects of ransomware, and to exclude the risk that this may have transferred or manipulated personal data, in addition to encrypting the data.

In case of doubt, the DPA recommends to submit a preliminary notification of a possible breach to be on the safe side. The notification can always be amended or even withdrawn at a later time, when the controller has more knowledge of the breach and its consequences. Controllers can notify through a web-based notification tool on the DPA's website. Unfortunately, the tool is only available in Dutch. However, the DPA's guidelines also allow for notification by fax if the notification cannot be made via the tool. This fax should then include all relevant available information about the breach, as listed in an annex to the DPA's guidelines.

GTDT: What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

QK & GJ Z Companies will have to continuously assess both the technical as well as the organisational measures they are taking to protect and secure their personal data. However, after a security incident the company should give priority to fixing the particular security issue and doing its utmost to mitigate the negative consequences of the breach. Measures to be taken will vary depending on the type of incident, from trying to locate a lost data carrier, to contacting the recipients of an email that was wrongly sent or addressed, remote wiping of a portable device or working with a processor to establish the extent of a security incident in their domain. If a hacker has got hold of personal data, the company will have to assess whether or not the data had been sufficiently encrypted, as this is relevant to the question if a notification should be made. If passwords have been leaked the company should force users to change these passwords.

A data breach could be an indication that existing organisational and technical measures are not adequate. Maintaining an appropriate and adequate level of security requires continuous effort, and constant scrutiny through risk assessments, planning, executing, checking and doing the same all over again (the 'plan-do-check-act' cycle). This is a logical consequence of the notion that the adequacy of measures must be viewed in light of current technical standards. This does not mean that technical measures need at least annual renewal to match the most advanced security system available. The strength of the measures should be viewed in proportion to the nature of the data they protect. A pizza shop with a spreadsheet of local customer addresses for spreading promotional flyers won't need military-level encryption. But processing of sensitive data will require measures such as encryption, hashing or, if possible, anonymisation or pseudonymisation. According

to the Dutch DPA, not only categories that have been designated as special in the Directive 95/46/EC and the GDPR should be considered as sensitive data. For example, while researching a navigation system manufacturer, the Dutch DPA considered that location data could be considered sensitive and additional measures were considered necessary to protect consumers. The manufacturer then went on to anonymise this location data by, among other things, removing GPS locations close to the starting location and destination of the driver. This was considered an adequate measure in this context. The Dutch DPA has similarly held that data concerning someone's information consumption (search terms used, TV shows watched, websites visited) is also sensitive in nature.

Organisational measures to be applied include confidentiality agreements with employees, disabling access to personal data for employees who have no need to use the data and adequate contracts with data processors. It should be borne in mind that the data controller remains responsible for the data processing of its processors. Access to data should be logged, and these logs reviewed regularly. Adequate measures should also include clear documentation and instructions on what actions to take if an incident occurs.

GTDT: What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

QK & G-J Z As any other modern networked society, the Netherlands is very much dependent on digital infrastructures. Statistics by the NCSC show that the vast majority of cyber attacks concern phishing, ransomware and DDoS attacks, all of which require vastly different remedies. As a direct consequence of this diversity, the NCSC advises a varied approach. However, as a general observation it can be noted that research shows that it is essential to increase individuals' security awareness, which will not only benefit their security practices at home but also the security of the companies they work for. Updated software and regular backups (patch management) and the need for strong passwords are also essential to resilience against cyber attacks. On a positive note, a fairly recent report shows that incidents of 'skimming' (the practice of stealing the data and PIN code of someone's ATM card) have dropped drastically in the recent years, as a result of improved security and awareness. This may go to show that individuals are very much susceptible to new safety measures.

Small and middle-sized companies are calling for a 'Digital Trust Centre'. They feel somewhat overwhelmed by threats and security demands and need assistance with assessing possible solutions and their cybersecurity in general. Using professionally secured cloud services is among the general advice given to companies to increase their security. Large companies are, of course, better equipped to meet the cybersecurity challenges and may also rely on external experts to become more resilient against cyber attacks. However, even this is no absolute guarantee for safety. Another recommendation given by the NCSC is for companies to use ethical hackers to test their security on a regular basis.

GTDT: Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

QK & G-J Z The controller is and will remain responsible, and liable, for any personal data he collects or processes. An important aspect of cloud services is the location where personal data is actually stored and processed. The GDPR has not changed the existing principle that personal data may only be processed outside the European Union (or more precisely: the European Economic Area) if the third country where the data is processed provides an adequate level of protection.

Compliance can be reached in various different ways, all having to do with adequate safeguards within either the company or the country to which the data is transferred. However, the EU Court of Justice's ruling invalidating the Commission's US Safe Harbour approval in the case of *Schrems* has shown that safeguards in the context of international data transfer can be fragile. So data controllers are well advised to keep a close watch on developments, including periodic reviews of the new Privacy Shield programme (where the European Parliament has recently called on the European Commission to suspend the agreement with the US unless compliance is improved), as well as the challenge to the standard contractual clauses currently making its way to the Court of Justice.

With respect to cloud services in general, the Dutch DPA has published a number of guidelines that are in line with the article 29 Working Party's guidance on the issue. In one of the most recent guidelines (of July of 2017), the DPA takes the view that, even for medical data, there is no need to ask consumers for specific permission for the use of cloud-hosted services. Obviously, depending on the sensitivity of the data and amount of data, the controller will need to implement more security measures before using cloud services.

While this indicates a general openness to cloud solutions, using cloud storage will need to become part of the overall risk assessment the controller makes, and one that may need to involve a data protection impact assessment under the GDPR. Risk assessment does not stop once the choice has been made for a particular cloud solution: if the cloud host faces security

issues, the controller will need to rethink using this particular company. An initial indication of the quality of the host may be found in the availability of certificates (ISO, ISAE, NEN) concerning security.

Furthermore, it is advisable to address any specific concerns a controller may have in the processor agreement. In any case, the controller should ensure access to the data at all times, even in a situation of conflict with the processor. The processor agreement should also address the issue of location explicitly, as this is a specific requirement under the GDPR, and one that may be particularly challenging to address in a cloud-based setting. Other topics that warrant careful deliberation are the security measures to be implemented by the cloud provider, and the provider's obligation to support the data controller's notification duty if a breach should occur in the cloud provider's domain.

GTDT: How are governments in your jurisdiction addressing serious cybersecurity threats and criminal activity?

QK & G-J Z The National Cyber Security Centre (NCSC) was established in 2012. This public–private body advises companies and the government on the usage of software and measures to increase cybersecurity. Its aim is to make the Netherlands more resilient against cybercrime.

In its Cyber Security Assessment Netherlands 2018, the NCSC concluded that the digital resilience of individuals and organisations is lagging behind the increasing threat. Cyberattacks are attractive to cyber criminals because of their big impact on society using relatively limited resources. It also found that the threat of state actors remains prominent. Over 100 countries worldwide use digital means for espionage and perform digital attacks to influence democratic processes. The NCSC identified a willingness among digital criminals to accept collateral damage in third countries that are not the prime target of a cyber attack (eg, the Petya ransomware attack on Ukrainian companies in 2017 resulted in major damage to Dutch companies and the Dutch economy). Moreover, cyber criminals no longer need to have dedicated computers at their disposal, as they can easily hire computing capacity to launch a massive DDoS attack. Recent experience also shows that more than a few cyber security incidents could have been prevented – or at least the damage could have been contained more effectively – if organisations had invested in maintaining basic levels of cybersecurity by regularly installing security updates and software patches.

The new acts mentioned in the response to the first question are the Dutch legislator's latest answer to these cybercrimes and other digital threats. This is especially true of the new Intelligence and Security Services Act, which is intended to strengthen our intelligence services' cyber capabilities. The act not only grants more powers to the intelligence services, but also envisages closer cooperation between these services, and also with foreign intelligence services. Specifically on cybersecurity, the explanatory document acknowledges that the Netherlands relies heavily on a number of large companies, and therefore their technical stability. The intelligence services' mission is also to protect these companies against hacking and spying. The government notes that hacks are often found out only afterwards, which leads it to the general conclusion that more knowledge and information is required to effectively fight (cyber) crime in the modern age. This will be the main focus of the government in the coming years.

GTDT: When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

QK & G-J Z We have seen several examples on the Dutch market of companies having suffered serious damage, reputational and otherwise, as a result of high-profile security incidents. DigiNotar, the Dutch online identity certificate company that fell victim to a large hack in the autumn of 2011, went bankrupt shortly after. Companies are well advised to conduct thorough due diligence on a target's IT environment and previous experience with security incidents, which should be logged internally as a requirement of law under the GDPR. The occurrence of a security incident need in itself not be worrisome. The response of the company to the incident can be much more telling about the company's readiness and level of compliance.

When it comes to privacy and personal data, we note an increased emphasis on compliance in the context of due diligence for M&A deals. This no doubt has everything to do with the new risk presented by the enormous fines that can be

Risk assessment does not stop once the choice has been made for a particular cloud solution.

THE INSIDE TRACK

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

A thorough understanding of cyber threats and the capability to work with relatively new and untested legal regimes, for which there is not yet any case law, nor any textbook answers. This requires an open mind, curiosity and creativity, and sometimes a healthy dose of paranoia about the threats and scepticism about potential remedies. It is also important for the lawyer to have a technical interest, or even a technical background, which will help in bridging the cultural divide between the IT and security specialists on the one hand, and the legal and compliance teams on the other. It may also come in handy if the lawyer has to explain the facts to a public authority or a court.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

Our DPA has been quite active in taking enforcement action. It has always taken a keen interest in new technical developments, such as mobile apps, fitness wearables and WiFi-tracking in retail space, and never shied away from going after large multinational companies such as Google and Facebook. It has also played an active role in the international task forces in which several EU data protection authorities joined forces to go after these US companies.

How is the privacy landscape changing in your jurisdiction?

The landscape is changing, but not only, or arguably even primarily, because of new rules: while the GDPR is more detailed than current data protection law, its most important rules are more or less similar to those we already had before. While the rules themselves may not have changed all that much, the impact on the Dutch supervisory authority is likely to be significant. Its funding is set to increase substantially over the next few years and it has begun to recruit new resources to meet its goals for ambitious growth. Perhaps more significant still is the increased public awareness of privacy threats, as a result of the high-profile security and privacy incidents, such as the recent Cambridge Analytica revelations, and as also evidenced by the outcome of our referendum on the new Intelligence and Security Services Act. Citizens, whether they act as consumers, patients, parents, students, employees, taxpayers or in some other capacity, are more likely to demand privacy compliance. We expect this to be a key driver for further change, which could even result in class action such as litigation, which is supported by the Dutch civil law system, and already makes the Netherlands a venue of choice for cartel damage cases.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

According to the Dutch DPA, the most frequently notified data breaches relate to personal data that have been erroneously sent to the wrong recipients, followed, at some distance, by lost data carriers, hacking, malware or phishing incidents, letters or packages that were lost in the mail or had been opened before return, the inclusion of the wrong customer data in an online portal and the inadvertent publication of personal data. Reported data breaches tend to be relatively small in scale: in the majority of cases, the incident related to 10 or fewer data subjects, and only just short of 9 per cent of all notified breaches involved more than 500 data subjects.

Quinten Kroes and Gerrit-Jan Zwenne
Brinkhof
Amsterdam
www. brinkhof.com

imposed under the GDPR for non-compliance. It remains to be seen how this new enforcement instrument will be wielded in practice. The DPA was already given broader powers to impose fines from the start of 2016. So far, no decisions to impose fines have been published. There is also an increased awareness among competition authorities of the importance of vast collections of data, even if this is not necessarily reflected by equally large market shares. The Commission's merger review of Facebook's acquisition of WhatsApp is an example. The Commission's fining in 2017 of Facebook for having allegedly provided incorrect or misleading information, specifically on its inability for reliable automated matching between Facebook users' accounts and WhatsApp users' accounts, illustrates this new awareness about the importance of big data in mergers. The Dutch Competition and Consumer Rights Authority has also highlighted the collection of data by online platforms as a potential source of market power.

Also available online

www.gettingthedealthrough.com

ISBN: 978-1-78915-086-5