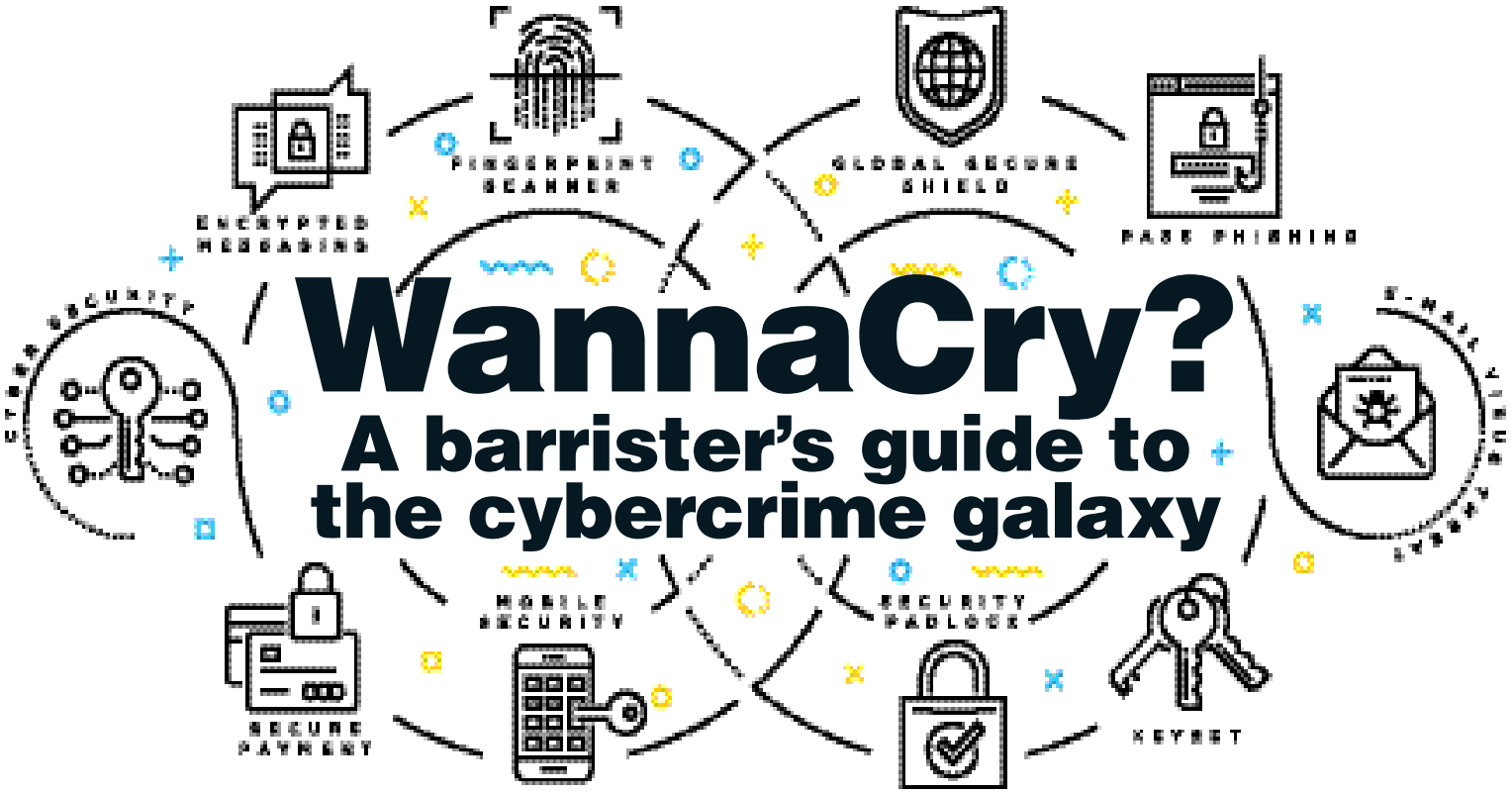


WannaCry?

A barrister's guide to the cybercrime galaxy

Malware is on the rise and there's a whole cybercrime industry – said to be worth $1bn globally – eager to hold your data to ransom. You could be struck at home, in transit or chambers and the legal sector reported a sharp jump in incidents last year. Sandip Patel QC briefs readers on the key dangers

2017 brought unrelenting growth in cybercrime including ransomware, phishing, hacking, social engineering and targeted campaigns, some state-sponsored. The World Economic Forum (WEF) has ranked cybercrime in the top three risks the world will face in 2018. According to its statistics, 357 million malware variants were released in 2016 alone and banking trojans (designed to steal account login details) on sale for just $500. Ransomware, said to be worth $1bn globally, continues to dominate the malware landscape and has grown by 56% according to McAfee Lab's 2018 Threats Prediction Report. An IBM X-Force study has reported that 70% of victims pay the ransom (*Ransomware: How Consumers and Businesses Value Their Data*).

Threats are greater than ever

The high profile WannaCry virus spread to almost 100 countries on its first day, affecting the NHS and other organisations running unsupported software. One firm, which estimated the virus cost them £20m in terms of new equipment and lost business, resorted to paper and pencils to keep operating. The virus left a trail of devastation unprecedented in its reach and impact, having attacked 200,000 computers in 150 countries.

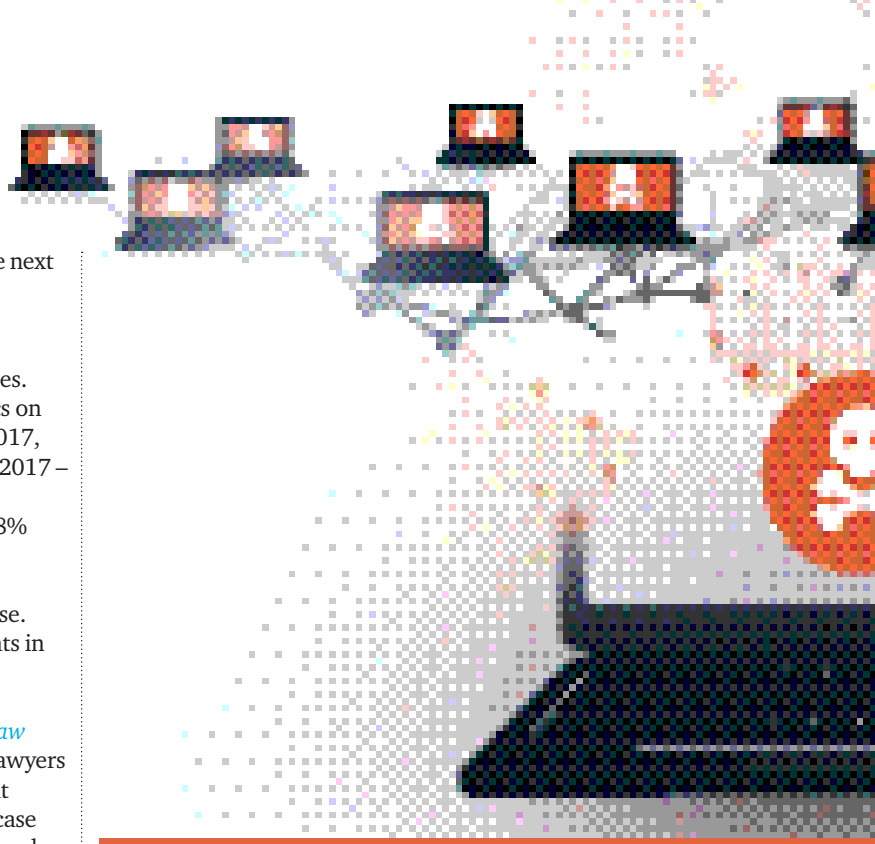
The NotPetya virus targeted Ukrainian businesses using compromised tax software. The malware spread to major global businesses, including FedEx, British advertising agency WPP, Russian oil and gas giant Rosneft, and Danish shipping firm Maersk. In September, FedEx attributed a $300m loss to the attack. The company's subsidiary TNT Express had to suspend business.

The list of prominent data breach victims is long and will surely lengthen in 2018. It includes Target, Yahoo update (revised upwards from 1 to 3 billion users) and Equifax whose massive data breach involved 143 million customers. Uber covered up a data loss of 57 million accounts in 2016. A report [from the UK's National Cyber Security Centre] breaks down the brands which have been most successfully protected from criminals for each month (see below).

The Internet of Things

Proliferation of the Internet of Things (IoT) means attacks will rise owing to the increased use of home devices accessible over the internet. The top three botnets on the Dark Web attack one million devices a month. The Mirai botnet cyber-attack in 2017 was the largest attack of its kind. The malware in question scanned for insecure routers, cameras, DVRs, and other IoT devices still using their default passwords and added them into a botnet network, which was then used to launch Denial of Services (DoS) attacks on websites and internet infrastructure. In December 2017 three young men in the USA pleaded guilty to being behind the attack.

The huge rise in use of cloud services across the world has also led to a major increase in attacks on IoT devices, of which 8.4 billion are in use today. At present, the annual cost of responding to cyberattacks



is £11.7m per company and is expected to rise to US$8trn in the next five years, says the WEF's *Global Risks Report* 2018.

Which countries and sectors are affected?

The UK currently ranks second behind the US for data breaches. The Information Commissioner's Office's (ICO) latest statistics on data security incidents show a 19% increase from Q2 to Q3 2017, with 815 incidents reported between October and December 2017 – a 41% rise on the same period in 2016. No sector is immune.

In the central government sector, there was a shocking 178% increase in reported incidents on Q2, up from 9 to 25. In the education sector, there was a 68% increase, from 57 reported incidents in Q2 to 96 in Q3. In the health sector, a 22% increase. In the legal sector, there was a sharp jump in reported incidents in 2017, some 311, from 216 in 2016.

Don Randall MBE, OSP Cyber Academy and the Bank of England's former chief information security officer, told the *Law Gazette* that law firms were unaware of their susceptibility: 'Lawyers hold an immense amount of sensitive and valuable data. What used to be held in secure filing cabinets is now held in online case management systems. When you consider that organisations such as government agencies and even the Pentagon are hacked, it is only a question of time before a major breach occurs in the legal profession.'

UK's cyber security strategy

The National Cyber Security Centre (NCSC), part of GCHQ, is at the heart of the government's strategy for combatting cybercrime. In February 2018, the NCSC published positive results of its Active Cyber Defence (ACD) programme launched in 2017 (*www.ncsc.gov.uk/information/active-cyber-defence-one-year*). Its key findings are as follows:

- The UK share of visible global phishing attacks dropped from 5.3% (June 2016) to 3.1% (Nov 2017).
- The ACD programme removed 121,479 phishing sites hosted in the UK – and 18,067 worldwide – spoofing the UK government.
- The takedown availability times for sites spoofing government brands down from 42 hours to 10 hours.
- A dramatic drop of scam emails from bogus '@gov.uk' accounts (total of 515,658 rejected in year)
- An average 4.5 million malicious emails per month were blocked from reaching users (peak 30.3m in June)
- More than 1 million security scans and 7 million security tests were carried out on public sector websites.

Scam domains promoted by phishing emails that had been removed included *onlinehmrc-gov.uk*, *refunds-dvla.co.uk* and *nationalcrime-agency.com*. The ten most spoofed government brands in the year were the HMRC (most targeted with 16,064 fake websites taken down), the DVLA, the Student Loans Company and the Crown Prosecution Service. Amongst the organisations best defending themselves from spoof attempts thanks to implementing ACD are local authorities such as Northumberland County Council (59,405 attempts in August), Cardiff Council (31,728 in December) and Denbighshire County Council (25,627 in May).

How does GDPR fit in with all this?

GDPR (short for the General Data Protection Regulation) is the EU's new data protection and privacy law. It takes effect on 25 May, and will be one of the most important pieces of legislation brought into force in 2018. It runs to 87 pages, contains 99 articles and is the most complex regulation the EU has ever produced. Any organisation – barristers and chambers represent just as strong a potential risk to the security and privacy of data and systems as any other organisation – that process EU citizens' data should assess how GDPR applies to their organisation and implement a plan to prepare for the new law.

GDPR marks a paradigm shift in data management and poses unique challenges. GDPR is not affected by Brexit. To this end, there is a Data Protection Bill ('the Bill'), which was introduced in Parliament on 13 September 2017 and is currently making its way through both houses. DPB will replace the Data Protection Act 1998 with a new law that provides a comprehensive and modern framework for data protection, stronger sanctions for malpractice, and new standards for protecting general giving people more control

RISK MITIGATION FOR BARRISTERS AND CHAMBERS

Set up a firewall to secure an internet connection

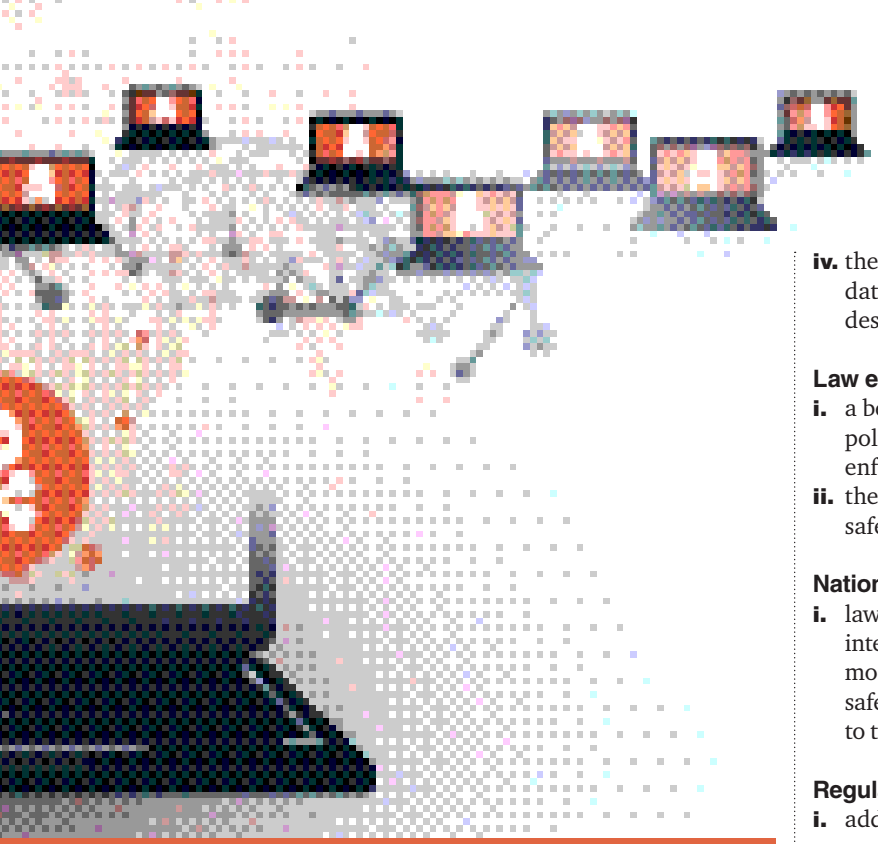
Macs essentially look after themselves. To enable a firewall in Windows 10: (1) Open the 'Control Panel' (type 'Control Panel' into search box on the right of the Windows Start icon); (2) In the Control Panel select 'System and Security' then 'Windows Firewall'; (3) Ensure that both the private and public network firewalls are turned on. Also tick 'Notify me when Windows Firewall blocks a new app.' Once you have selected both, click 'OK.'

Passwords and security settings

Choose the most secure settings for devices and software. Always check the settings of new software and devices. Use strong passwords and change default ones. For important accounts, such as banking and IT administration, use two-factor authentication, also known as 2FA eg when a code sent to your smartphone must be entered in addition to a password. Never save payment information for future online purchases.

Control who has access to data and services

To minimise the potential damage that could be done if an account is misused or stolen, staff accounts should have just enough access to software, settings, online services and device connectivity functions for them to perform their role. Extra permissions should only be given to those who need them. Check what privileges your accounts have - accounts with



administrative privileges should only be used to perform administrative tasks. Standard accounts should be used for general work. Ensure that staff don't browse the web or check emails from an account with admin privileges; an attacker with unauthorised access to an administrative account can cause more damage than one accessing a standard user account. Never enter confidential information on sites that do not have 'https' in the beginning of their URLs. Never use free hotspots for online banking or online shopping.

Protection from viruses and other malware

Use anti-virus and anti-malware software. Only download apps for mobile phones and tablets from manufacturer-approved stores. Turn on the firewall. Keep your computer up to date. Don't be tricked into downloading malware. Read all security warnings, license agreements, and privacy statements. Never click 'Agree' or 'OK' to close a window you suspect might be spyware. Instead, click the red 'x' in the corner of the window or press Alt + F4 on your keyboard to close a window. Be wary of popular 'free' music and movie file-sharing programs, and make sure that you understand all the software packaged with those programs.

Keep devices and software up to date (aka 'patching')

In Windows 10, security updates are downloaded and installed automatically. However, check Start > Settings > Update & security > Windows Update > Check for Updates. iOS: Settings > General > Software Update > Download and Install. Android: Settings > About Phone > System Updates. MacOS: click on the Apple icon at the top of your screen and hit Software Update.

over use of their data, and providing them with new rights to move or delete personal data. The Bill's main elements are as follows:

General data processing:

i. implementation of GDPR;
ii. clarity on the definitions used in GDPR in the UK context;
iii. special provisions for sensitive health, social care and education, appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes;
iv. the age from which parental consent is not needed to process data online at age 13, supported by a new age-appropriate design code enforced by the Information Commissioner.

Law enforcement processing:

i. a bespoke regime for the processing of personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes;
ii. the unhindered flow of data internationally whilst providing safeguards to protect personal data.

National security processing:

i. laws governing the processing of personal data by the intelligence services remain up-to-date and in-line with modernised international standards, including appropriate safeguards with which the intelligence community can continue to tackle existing, new and emerging national security threats.

Regulation and enforcement:

i. additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws;
ii. higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4% of global turnover for the most serious breaches;
iii. powers to bring criminal proceedings against offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request.

In October 2017, the Bar Council issued a GDPR guide for barristers and chambers (*www.barcouncilethics.co.uk/GDPR*). It is important to understand the roles and responsibilities in the data supply chain, particularly in respect of GDPR, as an important first step in assessing and managing the risks to data, systems and ensuring compliance. The main takeaway points are:

- every individual practising barrister is a data controller;
- each chambers is [likely to be?] a data controller;
- each chambers is likely to be a data processor;
- the appointment and role of a Data Protection Officer;
- a barrister's obligation of confidentiality is not limited to personal data; and
- stringent penalties are levied upon any person or legal entity subject to a data breach and found not to be in compliance.

Barristers should:

i. know about GDPR and its governing principles – in particular relating to transparency, accountability and data minimisation;
ii. be aware of the data they hold, the lawful bases to hold it, whether it may be shared and with whom, how data is accurately maintained, stored and responsibly disposed. All recorded in supporting documentation;
iii. comply, and apply GDPR principles to their practice, including a risk assessment of (i) chambers' work environment, (ii) home work environment, (iii) transportation of data, (iv) IT security and practices, (v) digital and hard copy storage procedures.

Failure to observe satisfactory data safeguards may have severe consequences. In *Various Claimants v WM Morrison Supermarket Plc* [2017] EWHC 3113 (QB), an employer was held liable in damages for the wrongful conduct of an employee who disclosed personal information of around 100,000 colleagues on the internet outside working hours and from the employee's personal computer. ●

Contributor Sandip Patel QC is Chairperson of the Cybercrime Practitioners Association