CYBER DECODER

FINANCIAL LINES GROUP NEWSLETTER ISSUE 37

California passes landmark data privacy law

On 28 June, the US state of California passed a major data privacy law under the California Consumer Privacy Act of 2018 (CCPA), the first legislation in the US to mirror key aspects of the EU's General Data Protection Regulation (GDPR).

The legislation does not go into effect until January 2020 and may yet be amended. However, the move is likely to be followed by other states, adding to a growing patchwork of data protection and privacy laws for US and international companies.

MILESTONE

The CCPA was drafted amid growing concern about the misuse of personal data in the political sphere, including the unauthorised use of data belonging to 87 million Facebook users by data analysts. The legislation also followed the introduction of similar laws in Europe under the GDPR, which entered into force on 25 May 2018.

California is the first US state to pass a major data privacy law since the Facebook scandal broke in March. The CCPA would introduce some of the strictest data privacy laws in the US, increasing the data protection rights for California's 40 million residents — the state is key in the digital world, as the world's fifth largest economy and home to the world's largest technology companies.

BROAD SCOPE

The Act gives Californian residents far more control over how organisations use their personal data. Under the legislation, consumers would have the right to know what data a company holds on them, the commercial purpose of collecting

Continued on page 2 ▶▶

the information and whether it has been shared with third parties. It also provides for the rights to access, delete, and transfer personal data, as well as limiting the use of data owned by a child.

The law will apply to companies that hold data on more than 50,000 Californians who live and carry out business in California. It is also said to apply to organisations that have revenues in excess of USD 25 million or derive more than 50% of their revenues from selling personal data belonging to California residents.

Under the Act, organisations would have to disclose to consumers the data they hold on them and how it will be used. They would also need to respond to consumer information requests, as well as honouring their right to be forgotten and opt out of data sharing. The legislation would also prohibit businesses from discriminating against consumers that exercise their rights – so a business would not be able to deny consumers goods or services or charge different rates.

The definitions of personal data and a data owner are broad under the CCPA. The Act covers information that relates to, or is linked directly or indirectly to, a particular consumer or household. Arguably the CCPA covers information like IP addresses, device IDs, email addresses, geo-location data and employment information.

LITIGATION

According to legal experts, the Act aims to limit data privacy litigation. However, several experts believe that the law could increase the prospect of litigation.

The Act provides for a private right of action (but only for security breaches, not privacy requirements) by consumers whose personal information is stolen or disclosed without authorisation.
The CCPA limits private actions by giving the state Attorney General exclusive power to enforce the law, while companies must be afforded the opportunity to put right any violation within a 30 day period. Damages for data breaches under the CCPA are set at between USD 100 to 750 per consumer.

PATCHWORK APPROACH

California is regarded as a pioneer of data and privacy protection in the US, enacting the first data breach notification laws in 2002. However, critics have suggested that the drafting of California's new data privacy laws were rushed and contain overlaps and inconsistencies with existing California privacy laws.

Considering the growing concerns for data privacy, commentators expect that the CCPA will set the standard for data privacy in the US and could trigger similar consumer protection legislation in other states. At present, there is no comprehensive overarching federal data protection law in the US, resulting in a patchwork of rules that differ by state and sector.

The introduction of CCPA could strengthen calls for federal data protection laws, which gained some momentum following the Facebook revelations earlier this year. Some argue that a federal privacy law is needed to avoid fragmented and divergent data protection requirements across the 50 US states, as is currently the case with data breach notifications. However, the current US administration appears to have little appetite for legislating in this area.

GDPR COMPARISON

The CCPA has been compared to the EU's GDPR, which recently introduced more stringent data protection requirements for companies that hold data on EU citizens, as well as new rights for consumers and hefty penalties for organisations that break the law.
The CCPA is similar to aspects of the GDPR in its intent, but significant differences remain, and compliance with the GDPR will not suffice for the CCPA.

For example, the CCPA has a broader definition of personal data and requires certain disclosures and communications that are not prescribed by the GDPR.
The CCPA also has broad rights for consumers and is not consistent with the GDPR when it comes to exemptions. ■

Bank regulators to scrutinise cyber resilience

UK banks and other financial services firms are to face tougher regulatory requirements around cyber resilience, including the need to set tolerances and demonstrate plans for dealing with major IT outages.

The move reflects increasing calls by regulators for better preparedness and reporting of cyber incidents with the growing dependence on technology. Earlier this year the UK's Financial Conduct Authority (FCA) called for prompt reporting of cyber-attacks, as well as making statistics on major operational and security cyber incidents public.

INCREASED SCRUTINY

In July, UK regulators set out their thinking on cyber related operational resilience in Discussion Paper (DP01/18). The paper, published jointly by the Bank of England (BoE), the Prudential Regulation Authority (PRA) and FCA, proposes new regulatory requirements aimed at making the country's banks, insurers and asset managers more resilient to technology-related service disruption; such as a major IT outage, an outsourcing failure or a major cyber-attack.

The focus on operational resilience comes after a string of outages in the financial services sector this year. In May, customers at TSB suffered almost a month of disruption, following a problematic IT upgrade, while Visa's payment system suffered a partial service outage. In July, Lloyd's Bank experienced problems with its fast payment system.

Speaking at a recent conference, PRA Deputy CEO Lyndon Nelson said operational resilience is now one of the most important issues for financial services. Nelson said there has been an increase in the number of operational incidents, caused by either internal failures or from external attack. As a result, regulators must set out clear expectations of firms in respect of their operational resilience, he said.

> The focus on operational resilience comes after a string of outages in the financial services sector this year

NEW APPROACH

UK regulators are already focused on the threat posed by cyber, but the discussion paper marks a gear change with regards to business continuity and the sector's increasing reliance on technology. It sets out regulatory thinking around ensuring continuity of services following a cyber incident and invites firms and international regulators to join the debate.

The paper places emphasis on prioritising the provision of business services, rather than on systems and processes. According to the paper, banks and other financial services providers should plan for the continuity of services regardless of the cause of disruption. Boards should "assume that some (or all) supporting systems and processes will fail" and "increase the focus on back-up plans, responses and recovery options".

Regulators suggest that firms focus on business services that, if disrupted, could lead to significant loss of customers, major financial loss or reputational damage. Examples might include: disruptions to the services that allow customers to transfer funds between accounts; the bank being unable to extend commercial finance; or an insurance company not able to fund and hedge its balance sheet.

The focus on business continuity has important implications for financial services companies that face competitive pressures to upgrade their ageing IT systems and adopt new technologies. The discussion paper says that firms will in future need to prioritise continuity of business services when planning upgrades to their IT systems.

PLANNING, TESTING AND REPORTING

According to the paper, regulators will expect firms to increase their operational resilience, particularly in response to evolving threats like cyber-attacks. It emphasises the need for financial services firms to identify vulnerabilities, plan for disruption and test their business continuity plans. They will then be required to demonstrate to the regulator that appropriate plans are in place.

The discussion paper also places emphasis on the role of the board and senior management in ensuring operational resilience for cyber. In his speech Nelson says that BoE will expect firms' boards to play a key role in setting cyber resilience strategies, including; promoting the development of management information, overseeing resilience programmes and investments in technology, systems and people.

The paper states that regulators will seek assurance that firms have the capabilities to deliver operational resilience. While demonstrating that their practices, processes and culture allow them to adapt and respond to operational disruption. There are a number of ways in which regulators are likely to seek assurances, including increased use of questionnaires to assess operational resilience – for example, a capabilities assessment questionnaire could be derived from the existing National Cyber Security Centre (NCSC) Cyber Assessment Framework.

There are a number of ways in which regulators are likely to seek assurances, including increased use of questionnaires to assess operational resilience

SETTING TOLERANCES

Under the proposals, the BoE's Financial Policy Committee (FPC) is to set tolerances for periods of disruption to the delivery of vital services - the PRA also intends to run a sector-wide exercise to assess the industry's ability to respond to major cyber disruption. The boards of financial services companies will also be required to set their own tolerances for key business services, and justify them in an impact tolerance statement.

The supervisory authorities consider that setting impact tolerances could play an important role in increasing the operational resilience of firms. It suggests that tolerances should be used to take decisions on investments, risk management, business continuity planning and corporate structure.

GLOBAL ISSUE

With growing reliance on technology and outsourcing, international regulators are increasingly turning their attention to the ability of banks and other financial services firms to withstand disruption and maintain their critical services.

The UK regulator sees cyber and operational resilience as an issue requiring cross-border coordination. The discussion paper notes that there is not currently an international framework supporting the regulation of financial services' operational resilience, but given the global and interconnected nature of financial activity, international engagement is "critically important". The PRA says that it is working through the Basel Committee, the Group of Seven (G7), the Organization of Securities Commissions (IOSCO), the Financial Stability Board (FSB) and other international bodies to push for increased international coordination in this area. The Basel Committee, for example, said in June that it is working on plans related to cyber risk and operational resilience that could result in new measures to enhance banks' operational resilience. ■

ICO sends clear signal with Facebook fine

Recent months have seen some big fines dished out to technology companies by regulators in Europe. In July, the EU fined Google a record USD 5 billion for anti-trust practices, while Facebook faces a large fine for the misuse of some 87 million of its users' data by consultants.

Facebook looks to have avoided a more material fine because the misuse of users' data revealed in March occurred before the EU's General Data Protection Regulation (GDPR) was enforced on 25 May. However, comments by the Information Commissioner's Office (ICO) suggest it will be taking enforcement of the GDPR seriously.

MAXIMUM PENALTY

Publishing its provisional findings into the misuse of personal data in political campaigns, the UK's ICO sent the clearest message yet that it is not afraid to seek maximum penalties for serious breaches of data protection laws. Commissioner Elizabeth Denham said the misuse of Facebook user data was a "game changer" and that the fine "sends a clear signal" that the incident and Facebook's failings were regarded as a significant issue.

The ICO said in its July report that it intends to fine Facebook GBP 500,000 for two breaches of the Data Protection Act 1998, the maximum penalty under the UK's pre-GDPR legislation. The ICO

concluded that Facebook contravened the law by failing to safeguard users' information and that it failed to be transparent about how personal data was harvested by third parties.

As part of its wider investigation, the ICO is taking enforcement action against a number of data analytics firms and issued a Notice of Intent to take regulatory action against parenting website Emma's Diary. The company faces a GBP 140,000 fine from the ICO after it was found to have shared data with a political party without users' consent.

EXPECT LARGER FINES

The ICO noted that the timings of these incidents meant that fines were calculated under the Data Protection Act 1998, not the GDPR (although it was able to use some new powers afforded by the GDPR during its investigation). The maximum financial penalty in civil cases under the 1998 law is GBP 500,000, but under the GDPR the ICO can impose a fine of up to EUR 20 million or 4% of global turnover, whichever is highest.

The ICO has since indicated that it may well have issued a larger fine against Facebook, had the breaches occurred after May 25, when the GDPR was implemented. A spokesperson told the media, had the incident been in breach of the GDPR, then the fine issued to Facebook would have been at the "upper end" of the scale. Based on Facebook's 2017 global revenue, a 4% fine would amount to GBP 1.2 billion under the GDPR.

Some experts said the ICO's intention to levy a maximum fine against Facebook demonstrates the regulator's resolve to be tough on GDPR enforcement. They say that the ICO's comments should be taken as a firm indication of its intent to exercise enforcement powers to the fullest extent of the law.

> Based on Facebook's 2017 global revenue, a 4% fine would amount to GBP 1.2 billion under the GDPR

GLOBAL REPERCUSSIONS

Facebook is facing a number of regulatory investigations around the world – the ICO says that it is helping overseas regulators and agencies in their investigations into Facebook. The US Federal Trade Commission and the EU are looking into the conduct of the US technology firm, as are data protection authorities in Australia and Canada.

Facebook also faces legal action in the US and Australia. Class actions have been touted in both countries, as affected consumers and investors seek damages following the privacy breach.

EVOLVING REGIME

It is still early days for the GDPR and regulators have yet to issue significant investigations or fines under the new EU law. However, comments in the media suggest that regulators have already experienced an uptick in notifications under the GDPR. The French data protection regulator reported a 50% increase in the number of complaints since May, while regulators in the UK, Ireland and the Czech Republic have also seen a rise in complaints and/or data breach reports.

Some jurisdictions are expected to be more active on consumer protection than others, in particular Germany, France, the UK and Spain. Germany's privacy regulator has, for example, started an infringement procedure against Facebook in Ireland, its European headquarters, which could result in a maximum fine of EUR 300,000.

A court in Germany recently decided that attempts by US non-profit firm ICANN to obtain data from a third party were not permissible under the GDPR.

The Dutch data protection regulator is reportedly investigating GDPR compliance among the country's largest companies. A sample of 30 companies, across a range of sectors, is intended to check compliance with the GDPR, which requires companies to have certain procedures in place to protect personal data. ■

Employees engage in revenge cyber attacks

A number of recent cyber-incidents are a reminder of the risks associated with disgruntled or departing employees, who may be tempted to steal valuable data.

In June, US technology company Tesla revealed that a disgruntled employee hacked its computer systems and stole company secrets, passing them to third parties. Tesla is suing the former employee, although the person in question denies the allegations and says he was a whistleblower. Separately, a former programmer at security firm NSCO was caught selling code he had allegedly stolen from his former employer, while a former Apple employee is accused of downloading and taking sensitive content on driverless car technology.

THE THREAT WITHIN

Such cases illustrate the threat of insiders hacking and stealing data, as well as potentially altering code with malicious intent.

Verizon's 2018 Data Breach Investigations Report found that 40% of the data breaches it analysed were perpetrated by internal operatives, while a report from PwC shows that current employees are the top source of security incidents – around 30% of incidents are linked to current employees.

Research from cyber security company Clearswift also found that the insider threat is the chief source of cyber security incidents. Direct threats from an employee now represent 38% of all incidents, while threats from former employees make up 13% of incidents, although most incidents are not malicious or intentional.

MALICIOUS INTENT

There are many reasons why an employee may resort to cyber crime. They might want to gain a competitive advantage when moving to a new employer or setting up their own business; they might be looking for data to assist in a criminal or fraudulent act; or they may just want to damage their employer following a dispute, or if threatened with redundancy.

Whatever the motive, a technically savvy employee can cause significant financial and reputational damage; using their access rights or knowledge of systems to steal intellectual property, personal data or to conduct financial crime.

INSURABLE RISK

Many aspects of a malicious employee attack are insurable such as; the first party cost of dealing with the breach, third party liabilities and regulatory costs.

Incidents where an employee has stolen personal data, on customers or employees, from their employer are not uncommon. Last year, healthcare provider Bupa warned customers that a rogue employee had stolen personal data with the intent to sell it to criminals. In the US, three employees at the Department of Homeland Security were accused of stealing a computer system that contained data on over 230,000 employees.

This fact has not escaped regulators, who have instigated criminal proceedings against employees that steal personal data, such as taking client contact details with them when moving to a new firm. However, employers would, under the EU's General Data Protection Regulations (GDPR), be required to notify the regulator of any breach involving personal data.

Last year, victims of a data breach successfully sued UK supermarket group Morrison's after a disgruntled employee stole and then published personal data belonging to 5,500 fellow employees. The case, the first data breach class action in the UK, saw Morrison's held vicariously liable for the actions of the former employee, despite having adequate controls in place to protect personal data.

Theft of intellectual property by an employee, however, is very difficult to insure under a cyber insurance policy because the financial impact can be hard to quantify. However, cyber insurance can cover defence costs and settlements where a data breach results in litigation from the loss of third party data, such as client data or intellectual property belonging to a customer or business partner. ■

The cost and size of data breaches continues to rise

Data breaches are getting larger and costlier, according to an annual study of data breaches from IBM and the Ponemon Institute.

The average global cost of a data breach increased to USD 3.86 million over the past 12 months, a rise of 6% since the 2016 study; while the average cost per lost or stolen record rose almost 5% to USD 148. In the past 12 months, the average size of a data breach also increased by 2.2% to 24,615.

The study also revealed that the more records lost, the higher the cost of the breach. For a mega data breach (over one million records) costs were an average of USD 40 million, while a breach of over 50 million records resulted in an average total cost of USD 350 million. Breaches in the health sector were the most costly at USD 408 per capita, followed by financial services at USD 206, both figures substantially higher than the overall average.

US COMES TOP

US data breaches continue to be the most expensive, at more than double the global total average. The average total cost of a data breach in the US was USD 7.91 million and the average per record costs were USD 233. Notification costs are also highest in the US at USD 740,000.

The next highest average total breach cost was recorded in the Middle East (USD 5.31 million), followed by Canada (USD 4.74 million), Germany (USD 4.67 million), France (USD 4.27 million) and the UK (USD 3.68 million). The consolidated average per capita cost was also highest in the US (USD 233), followed by Canada (USD 202) and Germany (USD 188).

COUNTER MEASURES

The study also showed that the faster a data breach can be identified and contained, the lower the costs. The global average time taken to identify a data breach was 197 days, while the average time taken to contain a breach was 69 days. Companies that identified a breach within 100 days saved USD 1 million, while those that contained a breach in less than 30 days saved over USD 1 million.

> Companies that identified a breach within 100 days saved USD 1 million, while those that contained a breach in less than 30 days saved over USD 1 million

The deployment of a breach response team and the use of encryption were the two most effective methods of reducing breach costs. The average cost savings of using an incident response team was USD 14 per record, while the use of encryption reduced costs by USD 13 per capita. The involvement of business continuity management and training each lowered the cost of a breach by USD 9.

Third party involvement in a data breach, cloud migration at the time of the breach, and compliance failures were the most significant causes of increased cost. Third party involvement added USD 13 to the cost of a breach, while cloud migration and compliance failures added almost USD 12 apiece.

RECURRING PROBLEM

Malicious cyber attacks were the most expensive attacks to resolve, and also the main cause of data breaches in the study (48% of breaches followed a cyber attack, compared with 27% for human error and 25% for glitches). The average cost per record to resolve a malicious or criminal attack was USD 157 (USD 258 in the US), compared with USD 131 following a system glitch and USD 128 for a breach caused by human error or negligence.

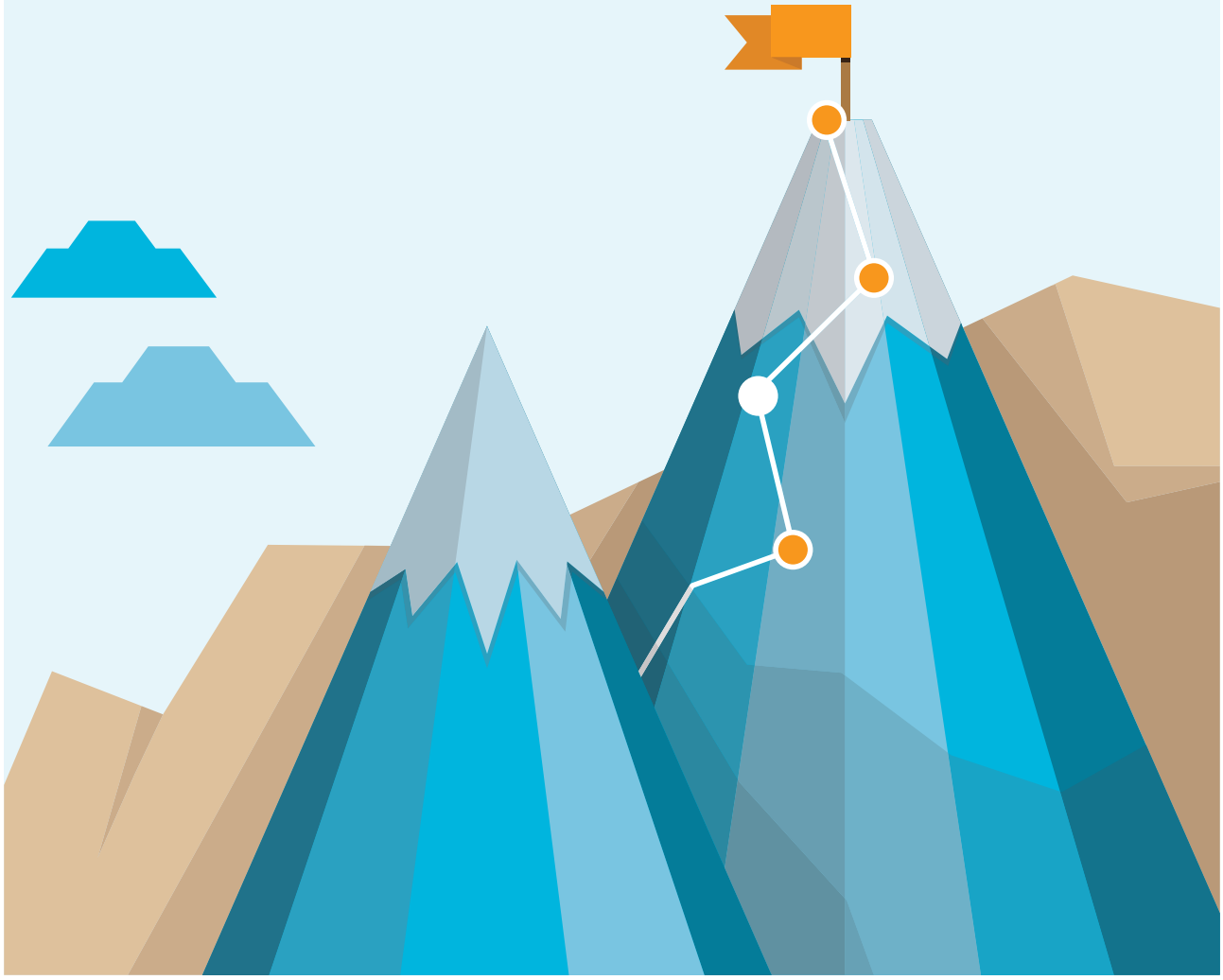
The likelihood of a recurring material breach over the next two years is 27.9%, more or less the same likelihood as the 2017 study. Organisations in South Africa have the highest probability of experiencing a data breach (at 43%), while Germany has the lowest probability of having a future data breach (at 14.3%). ■

JLT Consortium Partner recognised

Congratulations to Berea Associates, a JLT Cyber Consortium partner, on its nomination as a finalist in the Business in the Community's Responsible Business Awards on Tuesday 3 July at the Royal Albert Hall.

Berea, who provide cost effective cyber security advice to small and medium-sized firms, was one of the finalists in the Barclays Developing Resilience category.

Berea's web-based business app, Cyber AMI, delivers the UK Government's Cyber Essentials scheme without the expense of a consultant. Compliance with the scheme can reduce the risk of common threats from the internet by 70% to 80%, helping small businesses avoid incidents like ransomware attacks. ■



Buzzword of the month

HASHING

What does it mean?

Hashing is basically a form of encryption used to keep data safe.

Typically used to protect user passwords, a hashing algorithm turns pieces of data into a random alphanumeric value. So if a hacker manages to access data, such as a password cache, they just find random-looking strings of characters.

Hashing differs from typical encryption, as it cannot be reversed with a key. Hashed data is not designed to be decrypted – a password entered by a user is passed through the hashing algorithm and the result is compared against the hashed password stored on the database. This means organisations can avoid storing passwords on their systems, and just focus on storing the encrypted data.

Hackers deliberately target passwords alongside personal data, like contact details, which they then sell on the dark net or use to access accounts. In June, German sportswear company Adidas warned that hackers may have accessed usernames and encrypted passwords belonging to millions of customers using its US website. A 2017 report estimates that some 3 billion user credentials and passwords were stolen in 2016 alone, a figure that could reach 300 billion passwords by 2020.

Why does it matter?

Hashing is a fairly basic cyber security measure for protecting user passwords and can significantly mitigate the impact of a data breach. Without it, stolen passwords could be used immediately by hackers and cyber criminals. However, depending on the type of hashing used to scramble passwords, it can make a big difference.

Hashed data can be deciphered by a brute force attack, where a computer systematically generates possible combinations until the encrypted data is cracked. Hackers also produce tables of hashed data in advance to compare against stolen encrypted data.

Hashing is easy to perform, but is deliberately difficult to reverse. Done well, hashed passwords become unfeasible to decipher, but some algorithms produce hashed passwords that can be more easily cracked by decrypting techniques. For example, some hashing algorithms are designed to be very fast and efficient, but can be compromised quickly by 'brute force', while algorithms that typically require more computational expense are more secure.

Hashing is also made more effective when users choose strong passwords. Hackers may reveal an encrypted password by comparing it to a list of commonly used (but hashed) passwords. Longer more complex passwords also take longer to crack using brute force. ■

JLT provides insurance broking, risk management and claims consulting services to large and international companies. Our success comes from focusing on sectors where we know we can make the greatest difference – using insight, intelligence and imagination to provide expert advice and robust – often unique – solutions. We build partner teams to work side-by-side with you, our network and the market to deliver responses that are carefully considered from all angles.

Our cyber, content and new technology risks team delivers bespoke risk management and insurance solutions to meet the needs of clients from a variety of industries. The team combines experience and talent with a track record of delivering successful results and tangible value for our clients.

CONTACTS

Sarah Stephens
Head of Cyber, Content and New Technology Risks, JLT Specialty
cyber@jltgroup.com

Top Tweets