TRAVELERS

Power of Attorney

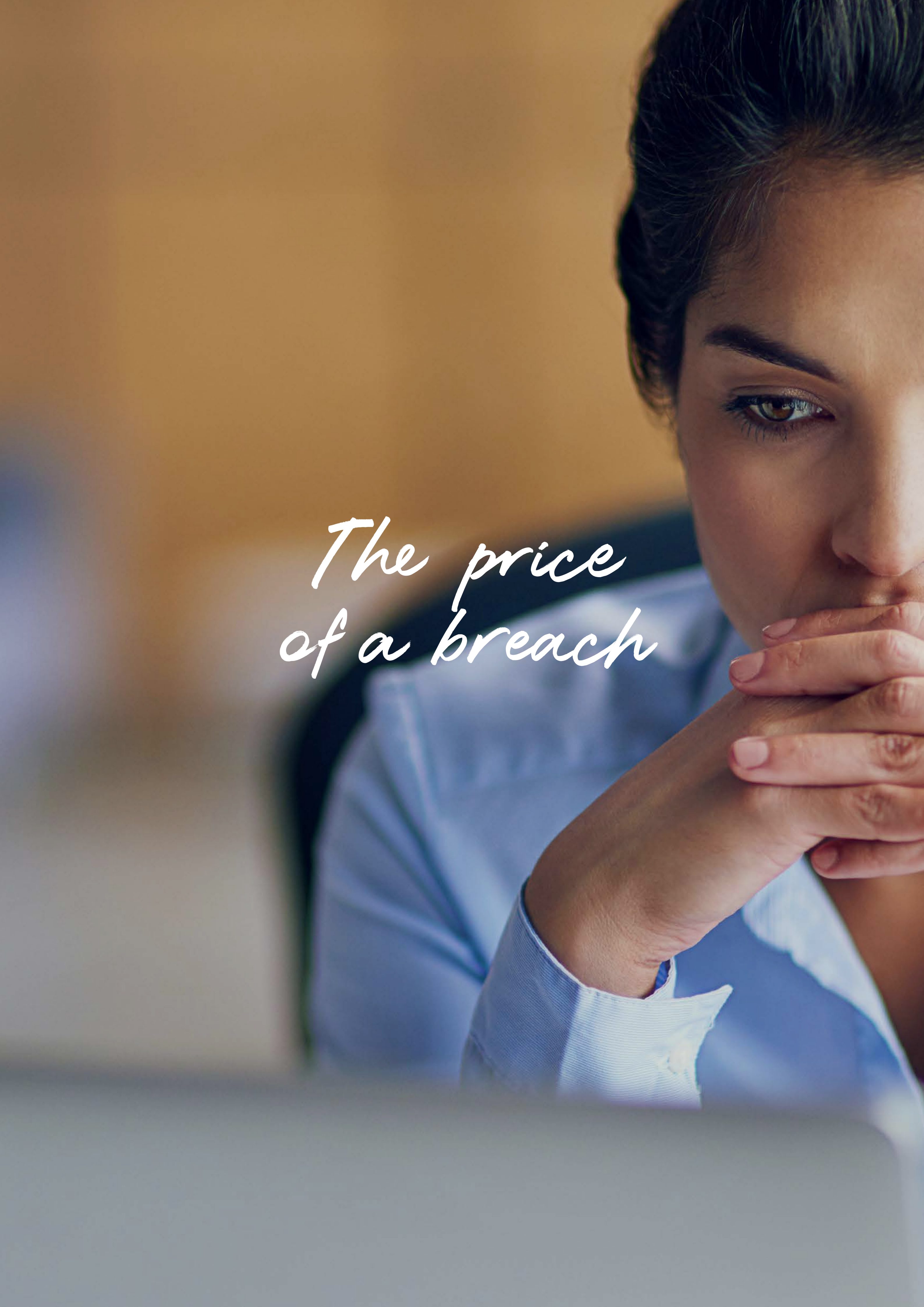
How Law Firms Can Strengthen Their Cyber Security

Imagine for a moment how you would conduct business if you were unable to communicate with your clients. What if you could not access your internal case management systems or client data? What if thousands — or millions — of pieces of that data were suddenly stolen and held for ransom?

Cybercrime is making hypothetical situations like these into increasingly common, costly realities for law firms. Sixty-two percent of all law firms in the UK experienced a cyber security incident in 2017, according to the PwC Law Firms Survey. That figure is up from 45 percent just a couple of years before. Unfortunately, as cyberattacks have transitioned from being front-page news to simply another risk of conducting business, law firms have been slow to prepare adequately. The Logicforce Q4 2017 Law Firm Cyber Security Scorecard found that 62 percent of law firms do not have a dedicated information security professional, only 31 percent have formal cyber security training programs, and just 41 percent have formally documented cyber security policies.

Even firms in the business of offering cyber security expertise have not been immune to attacks. In the wake of the cyberattack against DLA Piper in June 2017, Peter Wright, chair of the Law Society's Technology and Law Reference Group and Managing Director of DigitalLawUK, said if one of the largest law firms in the world lacks adequate safeguards to protect against a ransomware attack, it begs the question, "Who does[1]?"

[1] Max Walters, "DLA Piper Among Victims of Cyber Global Attack," The Law Society Gazette, 27 June 2017.



The price of a breach

A report from cyber security firm McAfee and the Center for Strategic and International Studies estimates that cybercrime costs the global economy $600 billion a year. Cybersecurity Ventures predicts cybercrime will cost the world $6 trillion annually by 2021, representing the greatest transfer of economic wealth in history. Those estimates don't seem all that farfetched in light of the "Panama Papers" leak of 11.5 million documents in 2016, which exposed a complex global network of offshore holdings that heads of state, celebrities and criminals allegedly used to hide billions of dollars.

Yet even in far less extreme cases, where a breach is suspected and quickly managed before it causes extreme financial damage, significant disruption can still result. When criminals hacked into several email accounts of Anthony Gold Solicitors last year, they were able to send emails to 16,000 clients and partners. The messages contained malicious attachments but had the appearance of being legitimate and urgent (they used the subject line "Action Required – Matter for Attention" and carried a "secured" attachment). The firm received a large number of inquiries from recipients asking about the validity of the emails and promptly alerted everyone who received them[2]. While the attack was a time-consuming disruption and caused the firm to generate news headlines for the wrong reasons, the consequences could have been far more severe if the recipients of the messages and the firm itself had not been vigilant.

Cyber threats come in many forms, ranging from ransomware and malware to stolen login credentials, credit card information, medical information and other personally identifiable information that can be used to obtain credit. "There's a massive black market driving a lot of the activity we see," said Davis Kessler, Head of CyberRisk at Travelers Europe. "Cybercrime is overtaking all other forms of crime for the first time, so the need for protection is definitely there. If a firm holding information for individual or corporate clients is breached — via malware, phishing schemes, or numerous other ways — the firm will be liable."

> "There's a massive black market driving a lot of the activity we see."
>
> **Davis Kessler**, Head of CyberRisk - Travelers Europe

[2] "Hackers Breach Anthony Gold Solicitors' Email Accounts, Launch Phishing Attacks," Teiss, 17 Dec. 2017.

The appeal of law firms

Cyber criminals target law firms because of the wealth of client information they manage, along with the trade secrets and intellectual property they possess. A merger or acquisition negotiation could present an opportunity for a cybercriminal to intercept and redirect funds when payments are issued, or to buy stocks and profit from the deal. In 2016, for example, three traders were able to make $4 million in illegal profits after hacking into the computer systems of some of the most prominent law firms in the United States, including Cravath Swaine & Moore LLP, and stealing sensitive information about mergers and acquisitions, presumably for the purposes of insider trading[3].

It only takes one weak link in an organisation for significant losses to occur. At a Toronto-area law firm in 2012, hackers accessed a bookkeeper's computer through a virus believed to have been launched by an email attachment or free screensaver. The hackers were able to access the firm's trust account, which was used to wire funds to foreign countries once deposits were made. The attack generated six figures' worth of financial damage for the firm[4].

Even seemingly benign details such as the images and professional backgrounds of lawyers in a firm can be manipulated for profit. Last year at Bates Wells Braithwaite, photographs and details pertaining to several of the firm's lawyers were taken and reposted (with first names or full names changed) on a scam website to "lend legitimacy to a money-laundering scam[5]."

"It's important to look at what you have as an organisation that might be of interest to an attacker — a lot of information handled by firms is monetary or monetisable but it might not always be obvious," said Andrew Beckett, Managing Director in the Cyber Security and Investigations practice in Europe, the Middle East, and Africa for Kroll. "Criminals can use the information they collect from a law firm to take out a mortgage or a loan. Having multiple pieces of data will help them access a lot more. Law firms need to understand how their electronic records can be targeted for those purposes."

Though both small and large firms face significant cyber risks, their challenges often differ. "In larger firms, the prize is bigger," said Kessler. "They hold more private information due to their customer base, they have more computers and employees. But on the flip side, larger firms have more resources to devote to information security so they have better systems in place. Many already have a breach response plan with vendors set up, and they may have gone through exercises where they devote a day to an example breach, so the people involved have some experience when the real event occurs. That's much less likely for a small firm, regardless of the industry. They are less likely to have an established incident response plan and their employees haven't received as much training."

[3] Sarah Randazzo and Dave Michaels, "U.S. Charges Three Chinese Traders with Hacking Law Firms," The Wall Street Journal, 27 Dec. 2016.
[4] Jnana Settle, "Top 10 Law Firm Cyber Attacks," Disruptor Daily, 12 Dec. 2017.
[5] Max Walters, "City Firm Tells of Copycat Cyber-Fraud," The Law Society Gazette, 1 Nov. 2017.

Small firm? Try these security safeguards.

For many small firms, hiring onsite expertise to help anticipate and respond to cyber threats is out of reach. Still, there are tech tools that can enhance a small firm's protection. Law Firm Suites, a US company that provides professional services to lawyers setting up their own practices, suggests taking steps like these:

- **Enable two-factor authentication on frequently visited websites:** The website twofactorauth.org provides a list of companies and organisations that offer this extra layer of security, or try an app called Duo, which you can install on your mobile device to secure other apps with two-factor authentication.

- **Use a password manager to strengthen passwords:** 1Password and LastPass are two options you can use to set more complex codes for your accounts.

- **Encrypt your email and files:** If you don't already use encrypted law practice management software to communicate with clients and store files, consider using Enlocked, Delivery Trust or Virtru to encrypt your email. To protect files, try the BitLocker full-disk encryption feature included in Windows (or FileVault on the Mac).

- **Protect your devices:** Mobile device management software including Accellis, MobileIron and Sophos can all encrypt your smartphone data and, if you were to leave your phone behind on the train, allows you to wipe your device clean remotely.

- **Browse online more securely:** Adblock removes ads from the sites you visit, and HTTPS Everywhere can help secure your browsing by automatically rewriting any HTTP URLs you visit to HTTPS.

For many small firms, hiring onsite expertise to help anticipate and respond to cyber threats is out of reach.

GDPR makes a response plan critical

Of course, as cybercrime evolves and becomes more commonplace, the steps you take following an attack are just as critical as those you take to impede one. The importance of having a strong cyber incident response plan became even more significant on 25th May 2018, when the General Data Protection Regulation (GDPR) came into force. The regulation raised the stakes for firms, which now face far larger fines in the wake of a personal data breach, along with a 72-hour time frame in which to report a breach to regulatory authorities. "Figuring out what happened, what personal data was breached, who was affected and providing notification to The Information Commissioner's Office (ICO) within that time frame can be remarkably difficult," Kessler said. "That's why the real value in buying a cyber policy from a reputable insurance carrier is the access provided to top-of-the-line post-breach services."

Pinsent Masons is one such firm on the front lines of post-breach response services. It partners with insurers to help their policyholders manage the damaging consequences of a breach. "There is often a lot of work to do quickly to understand the incident and be in a position to report to regulators, so our first step is to fact find — to determine what happened and when, as well as what steps the insured has taken so far," said Ian Birdsey, Partner and Head of Cyber at Pinsent Masons. "It's critical that any third parties such as IT forensics are engaged right away to gather evidence in anticipation of litigation and ensure maximum protection in terms of legal privilege." Depending on the insured's needs and the nature of the cyber event, public relations support, credit monitoring for customers or other services may also be provided.

> "Figuring out what happened, what personal data was breached, who was affected and providing notification to the ICO within that time frame can be remarkably difficult."
>
> **Davis Kessler**, Head of CyberRisk - Travelers Europe

Mind the (coverage) gap

Unfortunately, many firms are unprepared for a breach from the start. Seven years ago, cyber security did not even rank among the top 10 risks prioritised by company boards, according to the 2011 Lloyd's Risk Index. Many boards did not understand how cyber security meshed with risk management and therefore did not allocate resources to conducting security program assessments, assigning responsibilities to privacy and security roles, and receiving regular reports on cyber security risks[6].

That understanding has improved significantly in the past few years as boards have acknowledged their role in protecting cyber security, but even now, companies don't adequately appreciate the specific protection they need. Beckett says that while 50 percent of CEOs believe they have cyber insurance in place, only 10 percent do — generally because their understanding of what "cyber" means differs from what their policy actually covers. For instance, they may believe their Professional Indemnity (PI) cover insures more cyber-related risks than it does.

When reviewing insurance options, consider how your cyber policy would protect your firm, in conjunction with your PI cover, if it were to experience an attack:

- Would it cover the financial costs of a breach, whether from business interruption or the reputational damage your firm suffers as a result of the attack?
- What kind of cyber incident response does it provide? Will your policy support not only the notification of regulatory authorities but any improvements your systems would need to prevent a subsequent attack?
- Are the policy's payout limits sufficient to cover likely costs? Consider the expenses your firm would likely incur in the event of a breach, from customer notifications to credit monitoring to public relations.
- What does your policy exclude? Understand where your PI cover ends and your cyber cover begins. For example, while PI insurance could reinstate missing funds in client accounts and cover other third-party losses, the firm's losses and investigation costs would be covered by a cyber policy.

Unfortunately, many firms are unprepared for a breach from the start.

[6] McAfee, "Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity", February 2017.

Secure your firm for the future

Many firms, as they adapt to a new generation of worker, are adopting technology and work arrangements that not only help them compete for talent but also compete for business in the global marketplace.

"We live in a world where work no longer happens within the confines of an office," said Max Ingwersen, Consultant with McKinsey & Company. "Information is moving around the world like never before and you can't compete without being able to work from anywhere. Succeeding in this agile environment is about building awareness around what your risks are."

Shielding a firm from cyber security incidents is not just about having technology-based protections in place but also adopting behaviours that can limit the damage of an event. Preventing attacks is no longer a realistic goal for firms — it's a case of preparing and responding as quickly and effectively as possible.

"Sometimes I think we take the definition of data protection too far and we try to protect information that can't be protected," said Will Hogg, Managing Director and Founder of Kinetic Consulting. "I'm not so worried about people stealing an IP. I'm more concerned with a business that can't learn, unlearn and relearn in this environment."

Indeed, while firms must take general precautions to protect their information through the use of strong passwords, two-factor authentication, back-up systems that can help restore data quickly, and regular system updates and security patches, a firm's people are a critical defence when it comes to safeguarding computer systems. "Investing in staff training is the most cost-effective protection for both small and large multinational firms," said Beckett. To help enhance your firm's cyber security, you should:

- **Empower your passwords:** Reinforce the need for employees to use complex passwords that they do not use to access other accounts. Require two-factor authentication, particularly when employees are accessing your network remotely.

- **Train employees in how to spot a likely suspect:** Your staff should know how to identify phishing emails or fake requests for credentials — if an employee spots and reports a suspicious email, there is a chance for a company to block the IP address it comes from before a breach occurs. Run a cyber simulation exercise in which employees must make the kinds of decisions they will have to make in the event of live incident.

- **Review your rules for access:** Identify your firm's sensitive and non-sensitive data, and then assign different security measures and levels of employee access accordingly. Security Innovation Europe suggests classifying data according to whether it is restricted, private or public. *Restricted data* could cause severe damage if compromised and should carry the highest level of security, with access allowed on a need-to-know basis. *Private data* is moderately sensitive, poses a relatively low risk, and requires fewer security protections and employee access rights. ***Public data*** poses no risk to your organisation and therefore requires minimal security and restriction of access.

- **Conduct a cyber security audit:** Research from LogicForce found that of the US law firms that faced hacking attempts between 2016 and 2017, 40 percent did not even know the attack had occurred. An expert should assess your firm's technology infrastructure and high-risk practices so you can identify your vulnerabilities before a breach — and know how to detect one after the fact.

- **Obtain a Cyber Essentials badge to improve and demonstrate your cyber resilience:** The UK government, in partnership with Information Assurance for Small and Medium Enterprises (IASME) and the Information Security Forum (ISF) developed this set of basic technical controls to help organisations protect themselves from common cyber security threats.

- **Don't assume your tech will protect:** As an article in *The Economist* noted: "Software developers and computer-makers do not necessarily suffer when their products go wrong or are subverted. That weakens the incentives to get security right[7]."

All employees should understand they are responsible for protecting information security at the firm. "Very few companies are really ready for a breach," Birdsey said. "We always say managing cyber risk is a team sport — not just a legal issue, not PR, not IT — and so it needs a joined-up response. It's important to understand each other's roles and share in advance of an incident what you're doing to prepare. The fact that an organisation has an incident isn't news anymore. It's about having the right response."

When organisations provide such a response, they have the power to turn a negative story into a positive one.

"Organisations (and their management teams) will be judged not on the fact that they have been subject to a cyber incident, but on how they respond to it, including the decisions they make," Birdsey said. "A recent client was able to generate positive PR from the successful management of its own event and use that experience to provide breach-related services to its members.

> "We live in a world where work no longer happens within the confines of an office."
>
> **Max Ingwersen**, Consultant with McKinsey & Company

[7] The Economist, "Incentives need to change for firms to take cyber-security more seriously," 20 December 2016.

Key Contacts

Davis Kessler
Head of CyberRisk Underwriting

T	+44 (0) 203 207 6571
M	+44 (0) 7425 623831
E	dkessler@travelers.com

Lisa Farr
CyberRisk Underwriter

T	+44 (0) 203 207 6567
M	+44 (0) 7918 086698
E	lfarr@travelers.com

TRAVELERS

travelers.co.uk /cyber
Travelers Insurance Company Limited (Co. Reg. No. 1034343) is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.
Registered Offices: 23–27 Alie Street, London, E1 8DS
TRV2778 Sept18