TRAVELERS

Ready and Responsive

Strengthen your Cyber Security Shield

Your ability to communicate with customers and manage their needs is central to running your business. So what would happen if you suddenly could not access customer data you use to conduct day-to-day business functions? How would you operate if millions of pieces of that data were stolen and held for ransom?

Cybercrime is making hypothetical situations like these into increasingly common, costly realities for companies. Just under half of all businesses in the UK experienced at least one cyber security breach or attack, according to the UK government's 2017 Cyber Security Breaches Survey. The figure is even higher for medium-size companies (66 percent) and large companies (68 percent). In the past five years, cyberattacks have transitioned from being front-page news to simply another risk of conducting business. That risk carries an expensive price tag: 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.

Cyber threats come in many forms, ranging from 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 company holding information for individual or corporate clients is breached — via malware, phishing schemes, or numerous other ways — the company will be liable."

Though both small and large companies face significant cyber risks, their challenges often differ. "In larger companies, 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 companies 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 company, regardless of the industry. They are less likely to have an established incident response plan and their employees haven't received as much training."

It's important for companies to assess their organisation for any pieces of information that might interest an attacker because it either has monetary value or is easily monetisable. That information may not always be obvious — consider not just customer data but also trade secrets and intellectual property. How can your company's electronic records be targeted by a cybercriminal for profit?


GDPR makes
a response
plan critical

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 companies, which 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 companies 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[1].

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 kind of protection they need. Andrew Beckett, Managing Director in the Cyber Security and Investigations practice in Europe, the Middle East, and Africa for Kroll, 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.

When reviewing insurance options, consider how your cyber policy would protect your organisation, 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 organisation 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 organisation 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 cyber insurance ends and other cover begins.

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


People, passwords,
policies and
practice

Many companies, as they adapt to a new generation of workers, 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."

In an environment where cyber threats are common and continue to evolve, shielding an organisation from cyber security incidents is not just about having complex passwords, two-factor authentication, encryption and other 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 companies — 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."

Employees are a critical defence for a company looking to safeguard computer systems. "Investing in staff training is the most cost-effective protection for both small and large multinational organisations," said Beckett. To help enhance your organisation'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.

- **Train employees in how to spot a likely suspect:** Teach employees 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 organisation'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:** An expert should assess your organisation'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."[2]

All employees should understand they are responsible for protecting information security at the company. "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, PR or IT issue— 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 can 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."

2 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

TRV2779 Sept18