MARSH & McLENNAN COMPANIES

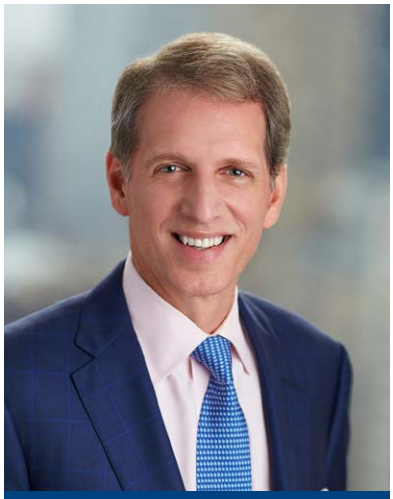
CYBERSECURITY AND THE EU GENERAL DATA PROTECTION REGULATION: THE TIME FOR ACTION IS NOW

The countdown has begun. In less than a year, tough new rules on data protection will come into effect in the European Union. For the first time, companies will be required to notify regulatory authorities, and potentially consumers, in the event of a significant cyber breach. In elevating the rights of consumers, the EU General Data Protection Regulation (GDPR) represents a sea change in how companies will have to operate — and many are not ready.

Oliver Wyman, one of the Marsh & McLennan Companies, predicts that fines and penalties in the first year alone may total GBP5 billion, for FTSE 100 companies. Adherence to GDPR requirements will require senior management — and not solely IT departments — to assume greater responsibility for cybersecurity. This shift means more than drafting a new organisational chart. It represents a profound transformation in how industries retain, use, and manage data and how leaders understand, mitigate, and respond to cyber intrusions.

To compound matters, the WannaCry worm showed just how vulnerable companies are. In the span of 48 hours, the WannaCry malware infected more than 300,000 computers across multiple continents. The attack provides a glimpse into a dark future, where cybercriminals operate with growing ease and impunity. Given the array of hacking tools reportedly stolen from the US National Security Agency in April, experts believe that more variants of WannaCry will be deployed shortly.

As the cyber threat landscape grows more complex, European regulators are not alone in mandating greater accountability at the executive level. For example, in May, New York state adopted a sweeping new regulation requiring financial services institutions to perform risk assessments, meet minimum protection standards, report breaches, and certify compliance. The Chinese Government has also imposed broad new cyber requirements.



Peter Beshar
Executive Vice President and General Counsel
Marsh & McLennan Companies, Inc.

These myriad changes will impact virtually every aspect of a company's operations. In Europe, for example, newspapers will likely be filled next spring and summer with stories of significant breaches as companies begin reporting under the GDPR. And as consumers are alerted to breaches, regulators and data protection authorities will likely jump into the fray.

MARSH & McLENNAN COMPANIES

Moreover, the GDPR grants EU consumers broad rights to access, correct, and delete their personal data. As a consequence, Oliver Wyman estimates that at least 90 million gigabytes of data may be implicated. Supervisory boards will demand assurances from management teams that are likely not yet accustomed to this level of scrutiny.

Even those companies that do not fall under the new regulation should take proactive measures to protect their businesses against a cyber breach. Steps that businesses may wish to consider include:

- **Set a tone at the top of awareness and urgency.** In heightening anxiety worldwide, the WannaCry attack provides an opportunity for executives to demonstrate leadership by prioritising cyber preparedness. Companies should use this moment — with memory of the attack still fresh — to remind their teams of the importance of good cyber hygiene.
- **Identify translators.** Too often, the technical team that defends systems and detects and combats cyber incidents speaks a language the C-suite does not understand. Executives need to have the right people in place who can provide them with timely and strategic advice. These translators need to be able to understand both the reputational risk to the company's brand and the technical requirements of the company's systems.
- **Implement best practices.** Senior management cannot afford to be detached from their company's cybersecurity plans any longer. A vital lesson from WannaCry is the importance of developing consistent protocols for patching known software flaws. Executives should engage directly with their IT teams around emerging best practices like multifactor authentication, encryption tools, and penetration testing.
- **Start communicating with customers and shareholders now.** Companies should prepare their stakeholders for an era of greater transparency and disclosure and the almost inevitable day when cyber intrusions occur. Help your customers understand how you collect and use their personal data. Nothing will be worse for your company — or your customers — than over-promising and under-delivering on cybersecurity.
- **Make up for lost time.** The penalties for non-compliance with the GDPR are severe — up to 4% of a company's total turnover. For companies with annual revenues of GBP12 billion for example, potential fines will run up to GBP500 million. Companies should test their cyber incident response plans through drills or simulations, and develop cross-department muscle and relationships of trust that will be needed in the event of a serious breach. Executives should also reach out to regulators, law enforcement authorities, and policymakers — not so much to lobby but rather to share insight, information, and help shape the rules as they evolve. No one has all the answers.

Sound practices and sheer chance ultimately stopped the WannaCry malware and saved countless institutions from even worse breaches. It is unlikely the unprepared will be so lucky next time. Corporate leaders must act today to ensure their companies can adapt and excel in a world of growing risk, opportunity, and significant new regulations.

GRAPHICS NO. 17-0622a