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.

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

Oliver Wyman, one of the Marsh & McLennan Companies, predicts that fines and penalties in the first year alone may total £5 billion, or more than $6 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 organizational 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.

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

MARSH & McLENNAN COMPANIES

are alerted to breaches, regulators and data protection authorities will likely jump into the fray.

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 regulations 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 prioritizing 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 $12 billion for example, potential fines will run up to $500 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.

MARSH

#WannaCry: Lessons Learned and Implications

Business disruptions from cyber-attacks are real. The damage is tangible. And the financial impacts can be severe.

The recent large-scale WannaCry attack underscored the potential harm to businesses. This pandemic cyber-attack, which highlighted the increased use of criminal ransomware and the proliferation of military-grade cyber weapons, serves as an opportunity to recognize the following:

- The risk of cyber-caused business interruption (cyber BI) is growing, and demands more attention from business leaders and risk professionals.
- Large-scale, global cyber-attacks will continue to occur and emerge without notice.
- Even relatively unsophisticated attacks can cause significant financial damage under the right conditions.
- More extensive attacks using more powerful cyber weaponry should be expected.
- Routine cybersecurity "blocking and tackling" activities — including software patching, employee cybersecurity training and awareness, cyber incident response planning, and other basic cyber hygiene activities — are essential to reducing risk, yet often get insufficient attention.
- No organization or industry is immune to the threat of a cyber-attack.

To minimize potential disruptions in advance of the next pandemic cyber-attack, companies should review their cyber risk management strategies and make any necessary adjustments. This includes reassessing cyber BI exposures, reviewing and updating cyber insurance programs, and taking active steps to build cyber resilience.

QUANTIFYING CYBER BUSINESS INTERRUPTION RISK

As we prepare for the next global pandemic cyber-attack, one clear lesson is that the technological infrastructure on which we rely is more fragile than is often appreciated. The WannaCry attack reinforced the need for businesses to address the growing risk and financial consequences of cyber BI.

Although historical data can be relied on to estimate the impacts of data breaches, cyber BI costs can be more difficult to determine because every company's IT systems, infrastructure, and exposures differ. How much an event costs will depend on several factors, including the organization's business operations model, incident response capabilities, actual time to respond, and the associated insurance coverages. By undertaking a cyber BI risk quantification analysis, you not only gain a better understanding of the status quo and associated costs, but a foundation for making more informed risk mitigation and transfer investment decisions and improving cyber-attack resiliency.

To more accurately quantify cyber BI risk, businesses can use scenario-based analyses. In the wake of the WannaCry incident, potential disruption scenarios should be reconsidered to include complex ransomware events and their second- and third-order consequences, such as supply chain disruptions or physical damage.

A scenario-based analysis should focus on three factors:

- **Estimating the severity and likelihood of a cyber BI event.** Using realistic scenarios can allow organizations to more accurately quantify the potential financial loss from a cyber BI event. Equally important is to scope these scenarios such that their likelihood of occurrence falls within a preselected range based on enterprise risk appetite and tolerance considerations.

- **Identifying mitigation options.** Depending on the significance of an organization's cyber BI exposures, risk mitigation options could include changing business processes, re-architecting IT infrastructure to improve resilience, enhancing IT restoration capabilities, or strengthening technical cybersecurity controls. To properly evaluate these choices and identify the strategies that will have the greatest impact, it's important to have a credible estimate of potential cyber BI exposure.

- **Evaluating risk transfer options.** Cyber BI is often underinsured or uninsured because many businesses do not fully quantify their risk prior to suffering a loss. But insurers are increasingly offering broader coverage for these exposures in both cyber policies and traditional property all-risk policies. A scenario-based cyber BI risk quantification analysis can support the proper structuring of these insurance options, including selecting appropriate limits.

Although historical data can be relied on to estimate the impacts of data breaches, cyber BI costs can be more difficult to determine because every company's IT systems, infrastructure, and exposures differ.

Organizations need to understand their cybersecurity posture — including business continuity, crisis management, and IT disaster recovery.

RISK MITIGATION

The results of a cyber BI risk quantification analysis can inform how a business develops or updates its enterprise-wide cybersecurity and cyber resilience program to account for ransomware attacks and other cyber threats.

Organizations need to understand their cybersecurity posture — including business continuity, crisis management, and IT disaster recovery. This can be achieved with a thorough enterprise cybersecurity program assessment based on recognized global and/or national standards and frameworks. Such an assessment should include a review of existing program documentation, cybersecurity training and facility surveys, technical assessments and audits, leadership and staff interviews, and comparison of the organization's security posture against industry peers.

Organizations also should consider taking several precautionary steps as part of good cybersecurity hygiene, including:

- **Backing up all files regularly.** Many businesses do not regularly back up files on a separate and/or off-premises system, often due to the potential costs involved. However, being able to recover data from a remote location or separate system can make the loss of access to one source substantially less harmful to the business and worth the investment. You could also benefit from implementing a data strategy that classifies data and has data storage and security protections that reflect each category of classification's criticality.
- **Keeping all software up to date.** The WannaCry malware exploited an old vulnerability in an outdated version of Windows, for which a patch had been released two months prior. Many who faced business interruption impacts from the attack had not deployed the patch, which highlights the importance of regular software and patch updates. Many factors may play into why organizations do not always update software with ideal regularity, including system complexity, perceived short-term financial burden, and lack of understanding of the potential financial and operational consequences of a cyber-attack. As part of an overall cyber risk and business interruption avoidance strategy, your IT administrators should ensure that operating systems, antivirus software, web browsers, and other applications are updated regularly in line with business, risk management, and enterprise cybersecurity objectives and budgets. Web browser security settings should also be in force — for example, to block pop-up ads and potentially vulnerable plug-ins.
- **Testing response plans.** For most businesses, it is not a question of "if" a cyber loss will occur, but "when." WannaCry was a novel piece of malware whose speed and impact were difficult to anticipate. Your organization should create incident response plans and maximize their effectiveness through tabletop exercises before an attack occurs. These exercises should use hypothetical but realistic cyber incidents — allowing risk professionals, IT staff, senior executives, and others across the organization who would be involved in the response to

identify areas for improvement or revision so you can quickly adapt to fast-moving events.

- **Developing cybersecurity operations.** Establishing and maintaining a strong operational framework for your organization's cybersecurity program is essential for all cybersecurity measures to work effectively and deliver a high return on investment. First, your IT teams should properly configure and consistently manage network and system security devices. You should also strengthen your organization's cybersecurity operations center capabilities by implementing procedures for event detection, escalation, and response. Finally, establish a workforce development program specifically for cybersecurity operations personnel. This program should include defining performance standards by job function, training personnel to those standards, and then evaluating them against those standards.

- **Educating employees.** Although the WannaCry attack exploited a software vulnerability, many ransomware attacks use emails that appear to be from trusted sources. The most effective line of defense for such threats is an aware user. Depending on the nature of your business and annual employee turnover, training should happen at least once a year, whether in a classroom setting, online, or by email (for example, via awareness reminders or phishing exercises). You may also want to include training in employee onboarding orientation. Training should focus on how to spot potentially dangerous emails and to not open attachments or click on links

Depending on the nature of your business and annual employee turnover, training should happen at least once a year, whether in a classroom setting, online, or by email.

THE DISRUPTIVE CONSEQUENCES OF CYBER-ATTACKS

Cyber-attacks have evolved — and grown in scope and scale — over the past several years. Simultaneously, businesses have become even more reliant on technology for day-to-day operations. As a result, cyber-caused business interruption (cyber BI) has emerged as a very real risk that equals — and sometimes surpasses — data breaches and more familiar disruptions.

In addition to seeking opportunities to steal valuable customer data, cyber-attackers now directly target the operations of the business, looking for ways to damage systems and disrupt or cripple operations for economic gain or in pursuit of other objectives. The WannaCry attack, which affected some 300,000 computers across more than 100 countries in less than a week, is proof of the growing hacker threat.

WannaCry was damaging because it was different from previous attacks. In ransomware scenarios, attackers aim to extort money by installing malware that encrypts the data on a computer and then seeks a fee from the victim to obtain the decryption key necessary to unlock the files. In a typical ransomware scenario, the attack is propagated via email or download, and a user must intervene to start the infection. The required human interaction often results in a gradual rate of infection and allows defenders time to respond. This cyber-attack was different in that it did not require human interaction to replicate, which allowed the malware to spread very quickly from machine to machine.

While the ransom sought was reportedly as little as $300, the virulence of WannaCry led to significant disruption and the economic impact on affected firms was often much greater. Future ransomware attacks may be similarly disruptive. And ransomware remains on the rise because it is cheap, easy, and effective for the criminal.

in unsolicited emails, including ones that appear to be from suppliers, vendors, and other trusted sources. It should also cover how and where to report malicious emails and other forms of cyber-attacks. Furthermore, IT departments should stay informed about the latest tools and techniques that cybercriminals are using, including those that do not rely on user actions to succeed. The investment in training by your organization ultimately will depend on the strength of your technological infrastructure and defenses, including the extent to which potentially dangerous emails are filtered and the need for unsafe workarounds is precluded.

INSURANCE COVERAGE

Networks become more connected every day and businesses more dependent on data-sharing. Every organization relies on technology, which means that every organization should take a fresh look at its insurance policies. In addition to standalone cyber insurance policies as the primary coverage for technology and data-driven perils, property and casualty policies may also address direct loss and liability arising from a cyber event.

While cyber insurance policies have historically been most often associated with data and privacy breaches, the coverage — and the rationale for purchasing it — has evolved. For example, today's cyber policies cover the failure of technology and the resulting interruption or loss of revenue. Insurers are also increasingly recognizing the interdependence of businesses, especially with regard to technology. As such, many cyber policies now contain contingent business interruption (CBI) provisions, including in relation to disruption of an organization's supply chain from a data breach.

A cyber policy can also extend to cover a cyber event that causes property damage. For example, a cyber policy could respond in the event of damage to a computer or server where the cause was malware rather than a physical event — a growing risk as the Internet of Things expands.

Property insurance, meanwhile, has traditionally been triggered by physical perils only. But as organizations increasingly experience business interruptions from ransomware and other forms of cyber-attacks without physical damage, property insurers have been forced to address the issue either by offering a focused grant of coverage or simply excluding losses from cyber events. Some leading property insurers have recently said their policies will affirmatively cover certain specified first-party cyber events. Other property insurers may allow for similar coverage in their policies, usually by endorsement, on a case-by-case basis.

As they seek to address a range of potential cyber risks, especially the growing threat of ransomware, organizations should seek to optimize their cyber insurance programs, coordinating and aligning cyber, property, and casualty insurance coverages. Working with their insurance advisors, risk professionals should review these policies to determine current levels and areas of coverage, identify any gaps or exclusions — with close attention to potential implications of "other insurance" clauses — and tailor insurance solutions to their organization's particular cyber risk profile. Organizations should also update policies as needed to provide coverage for new types of risks, including business interruption and cyber extortion, and reevaluate program limits in the face of catastrophic scenarios.

About This Briefing

This briefing was prepared by Marsh's Cyber Practice and Marsh Risk Consulting's Cybersecurity Consulting and Advisory Practice.

About Marsh

Marsh is a global leader in insurance broking and risk management. Marsh helps clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 30,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. With annual revenue of US$13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a leader in providing risk and reinsurance intermediary services; Mercer, a leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a leader in management consulting. Follow Marsh on Twitter, @MarshGlobal; LinkedIn; Facebook; and YouTube.

MARSH

For more information on this topic, visit marsh.com, contact your Marsh representative, or contact:

THOMAS REAGAN
Cyber Practice Leader
+1 212 345 9452
thomas.reagan@marsh.com

THOMAS FUHRMAN
Cybersecurity Risk Consulting Leader
+1 202 263 7827
thomas.fuhrman@marsh.com

ROBERT PARISI
Cyber Product Leader
+1 212 345 5924
robert.parisi@marsh.com