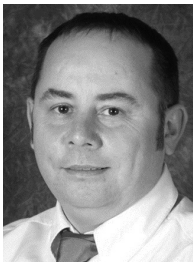
Mark Flegg

GDPR: Cyber security issues abound

Mark Flegg, of CSC, gives insight into the General Data Protection Regulation, what this means in terms of cyber security, and how to protect yourself and your business from cyber criminals.

Frequently used (and somewhat tedious) acronyms such as LOL, BRB, BTW, TBH, for example, have been popularized by our abbreviation-obsessed culture in the digital age. The acronym on the lips of in-house lawyers at the moment is GDPR – or General Data Protection Regulation – and it trumps the entire list.

But in all seriousness, the GDPR is nothing to LOL about. What was first announced in May of 2016 is now a very real standard that businesses in the European Union (EU) – and any company around the world doing business in the EU – will be required to comply with as of 25 May 2018. If businesses fall victim to a cyber security attack, and a data breach occurs, they may face a heavy fine of up to 4% of their total global annual revenue or €20 million **(whichever is greater).**

For those unfamiliar, the GDPR is a new measure intended to strengthen and unify data protection, thus giving control back to consumers in the EU. By introducing the GDPR, the EU sets the standard, and also holds businesses accountable for security breaches.

Many organizations are up to speed and well-versed on legal compliance with the regulation. However, far more may have failed to consider one of the driving forces behind the regulation: increased cyber security at a foundational level to ward off data breaches – be they through hacking, phishing, or malware attacks – before they gain steam.

It's important for businesses to understand the cyber security element of the GDPR, as well as the solutions to the issues they may face, and how to divide and conquer those issues by working closely with key departments like IT, legal, marketing, and security.

"While the risks of being non-compliant are significant, this is also an exciting opportunity for companies to really understand how they deal with data – what personal data they collect, what they do with it, and how long they hold it for – and to improve their processes," said Salma Daneshmand, associate general counsel for CSC, a global leader in digital asset management, online brand protection, and cyber security.

"Being able to demonstrate GDPR compliance will also enable companies to inspire trust amongst their customers, suppliers, and employees," Daneshmand continued. "If you can show how you're protecting your data from unauthorized access, people are going to want to work with you and trust you."

Cyber criminals never sleep

The digital landscape is littered with cyber criminals willing to jump at every chance to take down your website and steal your business from any corner of the globe. Motivated cyber criminals are planning attacks and outages that could cost as much as $100,000 per hour[1] due to lost revenues and lost productivity.

Early in 2017, another cyberattack was committed via the WannaCry ransomware, which affected more than 200,000 victims. Additionally, the Anti-Phishing Work Group, an international consortium that monitors businesses affected by phishing attacks, reported that phishing activity rose from 2015 to 2016 to a total of 1,220,523 attacks, a nearly 65%[2] increase year over year.

The steady uptick in distributed denial-of-service (DDoS) and phishing attacks to steal sensitive information and disrupt a business's website means it's of the utmost importance to partner with a cyber security provider that's trusted, reliable, and – above all else – secure. Because, when the GDPR comes into effect, you'll want to be protected against the many risks that exist.

"The data protection landscape has been constantly evolving and we will now have a unified law across the EU on data protection," said Daneshmand. "Hopefully, this will lead to more consistent decisions amongst data protection authorities, and it will be easier for companies to achieve compliance across the globe."

[1] http://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/

[2] http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

Résumé

Mark Flegg, Global Product Director of Domains and Security, CSC

In his role at CSC, Mark is responsible for advising a global client base on digital risk and the preventative measures brands can take to safeguard their digital assets.

During his 16-year career, Mark has acquired a wealth of experience in cyber security technology, focusing on DNS, SSL, and DDoS protection software. In order to further raise awareness of the digital threats to businesses, Mark regularly presents at leading industry events.

Cyber criminals, naturally, pose the biggest risk to your digital assets, because more than 76%[3] of all attacks start with organizations or individuals looking to exploit a system through various avenues. Hacktivists – be they socially or politically motivated – can also have a significant financial or reputational impact on a brand. Both parties use DDoS attacks, malware, phishing, and even SQL injection to get what they want, leaving companies exposed and damaged.

Lower the risk, reduce the impact

Ask yourself: What are your business's most important and sensitive items or entities? Would you include data and revenue? How about the security of the machines – both stationary and mobile – your employees use? What about the brand you've worked so hard to build and perfect, and the reputation and goodwill that accompanies it?

All of the above are susceptible to theft and attack in the online world. Below is just a sample of the types of attacks, the symptoms they present, and the risks they carry:

- **"Zero Day" Malware:** Also referred to as a "zero hour" virus, this undisclosed and publicly unreported virus is released on computer software, infecting systems and machines. The results include data breach, data loss, and compromised desktops, laptops, and mobile devices.
- **DDoS Attack:** This attack essentially makes a network resource unavailable by indefinitely disrupting the service of a host connected to the Internet, rendering a company's email and website useless, but open to ransomware demands. The results include data breach, a disruption in business, and lost revenues.
- **Phishing/Email Fraud:** A direct hit on the email accounts of a business and its clients, phishing and email fraud work by misdirecting or redirecting messages, sending phony emails, and causing other social engineering issues. The results include loss of customer confidence and trust, unfavorable press and online reviews, and lost revenues.
- **Domain Infringement:** By spoofing a website, hackers can run sales on products, offer services that normally aren't offered, and generally present their business under the guise of the affected brand. The results include lost revenues and loss of customer confidence and trust.
- **Domain Hijacking:** Cyber criminals can also completely hijack a domain instead of setting up their own, which can lead to customers volunteering information on what they believe to be a genuine site, only to find out later that they handed their sensitive materials over to an unknown third party. The results include lost reputation, theft of credentials, and an unfavorable effect on the brand's reputation.

In the last two years, cyber attacks of all forms have hit the newswire every other day, if not every day. In 2015, an attack on TalkTalk left the telecommunications company subject to a hefty fine of £400,000 by the UK Information Commissioner's Office. Sources suggest that if TalkTalk was fined under the GDPR, the penalty would have been much more significant at roughly £70m[4] (i.e., 4% of TalkTalk's global annual turnover).

Additionally, EU financial institutions could face fines of up to €4.7 billion in the first three years under the GDPR, according to a study conducted by Consult Hyperion[5]. Daneshmand says that both European financial institutions and those abroad working with European companies and clients should take note.

"The financial sanctions resulting from cyber attacks and data breaches should incentivize corporations to comply with data protection legislation," said Daneshmand. "Under the GDPR, companies risk facing even higher fines for non-compliance, and EU Member States will have a unified stance on how to approach financial penalties."

Solving the problem requires a team effort

Cyber security is no longer simply the responsibility of the IT department as it may have been 10 or 20 years ago. With every department, desktop, and mobile device a potential victim, it's up to each company to unite the forces of IT, legal, marketing, and security to stop cyber criminals in their tracks.

The process may seem like a major undertaking, but it's important to partner with expert providers that ensure data is protected and secure as part of data protection law compliance, which involves more than just a tick-box approach.

Figuring out exactly how many different digital assets your company maintains – and finding out where they're located, if they're secure, and who looks after them – requires a multipronged effort. There are four ways to begin the process:

- **Audit and Consolidate:** Ideally, you want to set out all your digital assets in one comprehensive view, which should include domain names, DNS, SSL, and social media usernames.
- **Use and Secure:** Check to make sure your digital IP resolves to relevant content and directs traffic to your sites, then ensure they're properly safeguarded with security measures like SSL Certificates, Multilock, and Two-Factor Authentication.
- **Optimize and Promote:** Analyze which of your domains can be safely divested based on their relevance to your company and the business they conduct. Only then can you identify the gaps related to available domain names, including brand and social media usernames.
- **Monitor and Enforce:** Search for GDPR infringements across your assets. Once you've identified them, prioritize violations by importance, so you can ensure compliance on a case-by-case basis.

You could have a belt-and-braces privacy policy, but if you don't abide by its provisions, you will be penalized by data protection authorities in the event of a security breach. Get out of your comfort zone and form your multidisciplinary team. It's the best way to devise a defense plan and research which approach you want to take, including which third parties may be able to help you with compliance. GDPR may be a terrifying acronym, but embracing the change now will save you time, money, and quite possibly your brand's reputation.

[3] https://www.infosecurity-magazine.com/news/76-of-ransomware-attacks-strike/

[4] http://www.decisionmarketing.co.uk/news/talktalk-could-have-faced-70m-fine-under-gdpr

[5] https://www.finextra.com/newsarticle/30698/eu-banks-could-face-fines-totalling-47-billion-in-the-first-three-years-under-gdpr