Cybersecurity and the in-house lawyer in 2017

09/01/2017

In-house analysis: Iohann Le Frapper, general counsel at Paris-based ChetWode, chair of the Association of Corporate Counsel (ACC) board of directors, and vice-chair of the International Chamber of Commerce (ICC) Commission on Corporate Responsibility and Anti-corruption considers the challenges organisations and in-house lawyers are facing in relation to cybersecurity.

What data and analytics topic do you expect to pose the biggest challenge to an organisation's cybersecurity in 2017?

Dealing with the dual threats of breach preparedness and compliance with cybersecurity laws is complex—it's no wonder that data security is one of the leading issues keeping in-house lawyers up at night.

Under the umbrella of breach preparedness, ransomware and managing threats to cloud storage will both be huge challenges. In its recently published report, 2017 Threats Predictions, McAfee Labs wrote that use of ransomware will continue to grow in 2017, until reaching record highs, then subside slightly as the year comes to a close. Notably, in Europe, companies have already been exposed to ransomware attacks more commonly than other parts of the globe. According to the ACC Foundation: The State of Cybersecurity Report, a survey of more than 1,000 in-house lawyers in 30 countries, ransomware/malware attacks were the second most common cause of a breach in Europe. This is compared to the sixth most common reason in the US.

The proliferation of cloud storage introduces another challenge for companies in 2017. As organisations become more comfortable with moving sensitive data to the cloud, hackers will be increasingly drawn to target these platforms. Companies will have to focus more attention on thwarting this type of attack.

An additional challenge comes with the new regulations that companies will have to navigate. The coming year marks the time when EU-based organisations must prepare for the European Union General Data Protection Regulation (GDPR), to be enforced starting in 2018. This will be a major overhaul of current data protection rules, and will require that companies completely reassess their data safety programs.

In the UK, the government has announced that a national scheme will be set up to retrain 'high-aptitude professionals' as cybersecurity experts. What challenges do in-house lawyers face in making people aware and taking seriously cybersecurity issues?

The challenge with cybersecurity is that the area is constantly, and quickly, evolving. Even at companies with robust data security programs, the fast pace of change necessitates constant retraining. This is true both for those closely involved in data breach prevention/response and for all other employees. In fact, most data breaches originate with employees, rather than hackers.

Employee error is the most common reason for a breach to occur, according to the ACC Foundation's report, which found that nearly one in three in-house counsel have experienced a data breach at their organisation. Yet only 45% of companies have mandatory cybersecurity training for all employees. Those companies with the highest revenues, most employees, and largest law departments are more likely to hold mandatory training. Thus, company size and budget are additional challenges to overcome when spreading awareness about cybersecurity. Even with mandatory training, there may also be a lack of follow up regarding confirmation that employees attended sessions and understood all material.

Cyber issues also span business, IT, and legal, so there are multiple stakeholders. As a result, achieving consensus and implementing solutions can be more difficult. Working across multiple departments means navigating separate budgets, varied priorities, and different approaches. A lack of centralisation can also mean a lack of direction, though many in-house lawyers are stepping in to solve the problem. Most in-house counsel see their roles in the direction of their company's cybersecurity strategies increasing. In fact, 59% of general counsel (GC) or chief legal officers (CLOs) stated in the aforementioned ACC Foundation survey that they expect their role in cybersecurity to increase. Today's legal department takes an active role in corporate cyber challenges.

What should organisations be setting out in their contracts with regards to cybersecurity? Is there anything which is commonly overlooked?

Threats to an organisation's information security are as varied as they are dangerous, but contracts with third parties are one of the biggest risk areas for companies today. Only 7% of in-house counsel are 'very confident' that their third-party vendors and affiliates are protecting the company from cybersecurity risks (ACC Foundation: The State of Cybersecurity Report). A slightly higher percentage, 22%, are very confident that outside service providers are managing the security of client data.

For example, press reports for 2016 brought to light quite a few cyberattacks such as the one against the Mossack Fonseca law firm in Panama that led to the Panama Papers or against several New York-based law firms that resulted in insider trading by Chinese cyberhackers who got access to strategic information about M&A deals. No doubt this is the tip of the iceberg and one may assume that not every service provider has dared for short-term commercial reasons, notifying their customers of the theft of data.

One of the most crucial things is to require in a contract that a third party notify you in the event of a breach. It seems obvious, but only 61% of in-house counsel worldwide confirmed that they require notification. This startling figure is even worse among in-house lawyers in Europe, Middle East and Africa (EMEA), at only 40%, so there is definitively room for improvement.

Do you have any best practice tips for 'futureproofing' the security of data and analytics made available on mobile platforms or stored in cloud based technologies?

More and more, data storage has moved to the cloud. When coupled with the fact that consumers use mobile devices to access sensitive data, the combination gives hackers additional opportunities to steal personal information. With hacking efforts growing more sophisticated each year, preparedness is the key element in 'futureproofing' data security.

My recommendation is that corporate counsel should recommend to their senior management to leverage the recently-released ISO/IEC 19086-1 international standard. The latter establishes a set of common cloud service level agreements (SLA) building blocks (concepts, terms, definitions, contexts) that can be used to create cloud SLAs. Therefore, this standard can be used as a due diligence tool to evaluate if current or potential cloud services providers can meet ISO/IEC 19086-1 and negotiate SLAs with the short-listed cloud provider.

When it comes to mobile access, companies are in a position to set policies about passwords, and in some situations, 'bring your own device' (BYOD) policies. Currently, 81% of companies have password policies, while only 42% have BYOD policies. The ACC Foundation tracked that in both cases, these are more common among respondents who said their companies have had a breach. It's likely then, that in hindsight, these policies would have proved helpful in preventing the incident. Thus, preparing these policies in advance is certainly a best practice.

Setting aside additional budget is another best practice. Cybersecurity preparation and response is costly. 31% of EMEA-based respondents to the ACC Foundation: The State of Cybersecurity Survey reported their law department spend had increased as a result of the company's approach to cybersecurity—leading all regions worldwide. This makes sense, as in 2015, the Ponemon Institute published that the 'average consolidated total cost' of a data breach rose 23% as compared to 2013. Indeed, even preparation is more costly, as the number of platforms needing protection (ie new cloud technology) has increased and as solutions need to grow more sophisticated to outpace pioneering hackers.

What impact do you envisage the new GDPR having on cybersecurity?

With the GDPR coming into effect in May 2018, companies will use 2017 to prepare for its enforcement, especially the requirements regarding 72-hour data breach reporting and the hiring of a data protection officer at most organisations.

With stringent reporting requirements and the threat of heavy fines, the regulation will ensure that all companies take cybersecurity even more seriously. The comprehensive law will streamline the various data privacy regulations currently enacted across the EU. This harmonisation, although short of uniformisation of the framework, will be beneficial to in-house lawyers seeking to provide clear guidance to their companies that operate in multiple EU member countries.

In-house lawyers working in Europe today already consider complying with these laws to be challenging. The 2015 ACC Global Census of more than 5,000 in-house counsel in 73 countries found that in-house counsel considered privacy concerns and cybersecurity to be the two greatest challenges in complying with laws inside their jurisdiction. With the GDPR, complying with cybersecurity and privacy rules will become clearer for in-house lawyers and their client organisations, but penalties for noncompliance will escalate.

Interviewed by Diana Bentley.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor