OPTIMISING DATA SECURITY

Glenn Warwick *weighs up whether an apparent obsession with compliance in the UK is having a positive or negative impact on cyber security*

With ever-increasing legislation governing business operations, it's clear that organisations are shifting focus to fall in line with these standards. Ensuring compliance is no longer a 'nice to have', instead it's essential in maintaining reputation, building consumer trust and safeguarding long-term continuity. But it must also be regarded as more than just a tick-box exercise.

Is legislation actually having a negative impact in some cases? As businesses become more and more obsessed with being fully compliant, there is an emerging culture of investing huge volumes of money in security controls that may not be needed. For many organisations stuck in this compliance mindset, this approach can create a short-sighted desire to simply display compliance credentials, rather than work strategically to ensure that the right practices are put in place – and, as a result, they are likely to be missing real opportunities to increase their overall cyber maturity.

Following the introduction of GDPR, businesses undertook urgent reviews of their security measures

So, the question remains: are businesses genuinely working to uphold higher levels of industry best-practice, or has this laser-focus on legislative compliance led UK organisations to become a nation of 'compliance chasers'?

Organisations have long been expected to run in line with legislative requirements, and this reached a pinnacle with the introduction of GDPR in May 2018. As part of this legislative change, organisations were closely policed on their data security, with significant fines imposed for data breaches – and as a result, many businesses undertook urgent reviews of their security measures, with many deciding to implement security standards such as ISO 27001.

This increased incentive to achieve compliance forced many businesses to attain a level of certification against these standards. But without true organisational buy-in, simply achieving certification is no guarantee of genuine cyber-security. In the first quarter of 2020 alone, at least 68 GDPR fines were issued totalling nearly €50 million. Clearly, it isn't enough just to go through the motions of compliance; businesses must commit to ongoing workforce education and invest in the right resources to truly reap the benefits of upholding these standards.

GETTING IT RIGHT

The first step in improving cyber security is to implement the correct standards. According to Risk Based Security research published in the 2019 MidYear QuickView Data Breach Report, the first six months of 2019 saw more than 3,800 publicly disclosed breaches, with 4.1 billion compromised records. As such, it's clear that there is still a long way to go in terms of improving security standards. But if organisations don't maintain a healthy cyber security culture or implement the right dedicated resources to manage their security on a daily basis, widespread adoption of these operational security practices is unlikely.

To achieve true, long-lasting cyber security, organisations must continually assess and reassess risks, educate employees and make sure that they're investing in the right resources. By ensuring that their security controls are keeping pace with the changing threat landscape, companies can continually deploy the latest and greatest techniques to combat exposure. In turn, this will allow them to avoid breaches, as well as any heavy associated fines.

Assuming that a security certificate alone will provide adequate data protection is the riskiest part of the UK's current 'compliance culture'. If businesses focus on simply achieving certifications, then there is a risk of breeding a culture where employees do not feel accountable or responsible for upholding best practice. This, in turn, is likely to result in reactivity rather than proactivity; where companies only invest time and effort when renewing their certifications. Any subsequent staff awareness campaigns are then likely to be geared towards passing an audit, rather than genuinely raising awareness or educating staff about cyber security. While this approach can satisfy the desire for compliance, simply going through the motions won't keep the company secure. So, while organisations must follow industry standards, it's clear that the key to success comes when they are adopted into daily business operations.

When it comes to data security, one of the weakest links is the risk of human error. If the workforce is not operating in a secure way, the risks of a data breach increase exponentially. According to recent analysis of data from the UK Information Commissioner's Office (ICO), 90 percent of data breaches that occurred in 2019 were caused by user error. The data also showed an increase in breaches caused by user error in 2019 over 2017 and 2018, which is when GDPR came into effect.

By running phishing campaigns, regularly updating antivirus software and implementing mandatory password updates and multi-factor authentication, businesses can start putting best practice in place. However, it's essential to educate staff about the importance of upholding these processes to ensure they fully understand the risks of non-compliance, even if it is time consuming or inconvenient to do so. This will help achieve widespread organisational buy-in for utilising best-practice security measures, and most importantly, will mitigate against attempts to circumvent the processes in place.

IT ESSENTIAL TO IDENTIFY THE CORRECT LEVEL OF SECURITY FOR EACH ORGANISATION

Security needs are ever changing, and never more so than in the current climate. The Coronavirus pandemic has forced many businesses into new ways of working with increased reliance on technology and connectivity, meaning that there has been little choice for those businesses but to accelerate digital transformation.

As part of that transformation driven by the pandemic, organisations have had no choice but to reassess their security software and processes. This is largely driven by the large-scale global shift to working remotely. With millions of employees now working from home, workforces have been forced away from using their secure on-site servers and are instead reliant on users' home networks. Allowing access to business networks through those home networks creates more risk as security is a lot harder to monitor.

It's no surprise, therefore, that almost half of organisations have suffered a cyber security incident as a result of the sudden shift to remote working, according to a survey undertaken by Barracuda Networks. It was discovered that 46 percent of organisations across the UK, US, France and Germany have suffered at least one "cybersecurity scare" since the lockdown began, suggesting that scammers are taking advantage of the unprecedented situation to infiltrate organisations' newly vulnerable security systems.

With the combined consequences of a weakened set of operational security resources, reduced revenue, furloughed staff and redundancies, a lot of companies have been hit hard by the pandemic. As

such, the resulting financial and logistical issues have meant that these businesses are not necessarily able to operate with the same level of security as before the pandemic – and now, more than ever, this makes it important for businesses to make sure they maintain the strongest possible levels of security resilience within their organisations. Another potential from the pandemic could be an increase in insider threats with heightened levels of redundancies and layoffs causing concern that disgruntled employees may try and retaliate via security attacks.

TO ACHIEVE TRUE, LONG-LASTING CYBER SECURITY ORGANISATIONS MUST CONTINUALLY ASSESS RISKS

By keeping abreast of the various different attack methods that businesses may face, vulnerabilities can be better identified, monitored and managed to prevent any adversaries or malicious attackers from exploiting software or process-based weaknesses. This is a continued threat; and as such, it's essential that organisations can promptly and proactively mitigate against any vulnerabilities as soon as they are identified. Typically, this can be achieved through maintaining basic cyber security hygiene practices. This can be accomplished through software patching, via alternative mitigating strategies such as the hardening of an operating system or additional security measures such as firewalls and antivirus software.

It's also essential to identify the correct level of security for each organisation. By working as a community, different sectors can capitalise on a central service from a competent authority; using a baseline cyber assessment framework against which they can measure their own security practices and identify areas of improvement.

Of course, as previously discussed, simply complying with this baseline is not enough. Without considering an organisation's individual needs, it is likely that they will end up with inappropriate, ill thought-through security controls that have been put in place simply to meet arbitrary security requirements. Compliance is one part but adhering rigidly to a prescriptive set of requirements is quite another. Working with a security expert can help businesses pinpoint their own specific needs within the restrictions of legislative compliance; determining the security controls that they need and supporting them to make the right decisions.

Above all, working to implement the right security in the right places will reduce the organisational culture of 'compliance showcasing'. Rather than scrambling to pass an annual audit or achieve the latest ISO accreditation, businesses can move away from blind legislative compliance to truly focus on the 'why' – helping them to navigate the uncharted waters of lockdown, keeping their reputation intact and staying secure for the future ●

Glenn Warwick is Principal Cyber Security Consultant, Bridewell Consulting.

In October 2020, British Airways was fined £20-million for data breaches by the ICO