Latest Government cyber report: targeted attacks and impact of the GDPR

April 2019

The Government's latest Cyber Breaches Survey was published this week. It suggests that cyber attackers are targeting fewer businesses, "but may be attacking these [businesses] more frequently or substantively." It also re-affirms that there is still a gap between perceived risk and action when it comes to cyber, and highlights some unintended consequences of the GDPR.

As an organisation, it can be difficult to determine if you are 'doing enough' regarding cyber security. Government reports like this week's Cyber Security Breaches Survey 2019, and last month's FTSE 350 Health Check (see our client briefing on this) can help you benchmark your actions against the wider market and highlight potential risks in your supply chain, particularly where you engage smaller and medium size organisations who may have a different approach to cyber than you.

The latest breaches survey, which is intended to statistically represent UK businesses of all sizes and sectors (and charities – although we focus here on the impact on businesses) has produced some interesting, and in places worrying, results.

Fewer being attacked but more targeting

Cyber attacks are still a persistent threat to businesses – while fewer businesses have identified breaches/attacks than before, the ones that have identified them are typically experiencing more of them.

This trend may be due to a change in attacker targeting / behaviour, meaning that if you are an organisation being targeted you are now likely to face more attacks. 48% of those being attacked, are attacked every month, with 16% being attacked at least once a day. However, it may also be due to the fact that businesses are becoming more cyber secure (and many have increased their planning and defences in some respects, although more work is needed) or that the GDPR has had some unintended consequences.

Unintended consequences of the GDPR?

One suggestion is that this trend may, in part, be explained by a change in the way businesses responded to the survey – either because the GDPR has made them less willing to admit to having breaches or because it has changed the way they view breaches (presumably as they are applying a narrower focus defined only by personal data and GDPR notification thresholds). In our experience, determining whether a breach requires notification outside your organisation (particularly to customers, staff or regulators – not just the ICO) requires a sophisticated approach, specific expertise and legal advice – and it is certainly true that not all breaches will require such notification. However, no need to notify does not mean there has been no attack, and organisations should ensure that all attacks are taken seriously and lessons are learnt.

A narrow GDPR focus can also negatively impact how organisations approach breach prevention. While the GDPR has had a positive impact (with 30% of businesses making changes to their policies or processes as a result of the GDPR) cyber is a broader issue than just the protection of personal data, and "those that did think more holistically about the issue were also typically taking a wider

range of actions, such as implementing more technical rules and controls and managing the risks associated with suppliers' cyber security."

Too narrow a focus generally can also lead to an underestimation of the costs associated with a breach. There is a trend of rising costs. However, the reported average cost is still relatively low (£4180, £22,700 for large businesses) compared to the impact we know large breaches can have. The qualitative findings suggest indirect, long term and intangible costs tend to be overlooked. The nature of breach costs may also mean that they tend to be manageable until a serious breach occurs.

Gap between perceived risk and action taken

Another major finding of the report was a continued gap between the way cyber risk is perceived (with 78% of all businesses and 95% of large businesses rating it as a high priority) and the action they are taking. This is particularly worrying when looking at the statistics regarding smaller and medium sized organisations.

Cyber is not a board level issue: When looking across UK businesses as a whole, cyber does not yet seem to be a board issue, with only 35% of businesses having a board member with specific responsibility for cyber security, only 19% giving monthly updates to the board on cyber and only 16% having a formal cyber security incident management process in place. Just under a quarter of businesses had in place none of the governance measures mentioned in the survey.

Supply chain: The statistics relating to supply chain risk are similarly concerning. Only 18% of businesses required their suppliers to adhere to any cyber security standards, with the report noting that "in qualitative interviews, some had simply not considered suppliers as a potential source of cyber risk before, while some others simply did not consider their suppliers' cyber security to be their responsibility." This supported findings from the FTSE 350 Cyber Health Check, which identified supply chain as a key cyber risk where more action was required. In fact the report found quite a difference in how organisations framed and understood cyber security. This varied by organisation size, sector and region as well as focus, and should be borne in mind when businesses are looking to bring a new organisation into their supply chain.

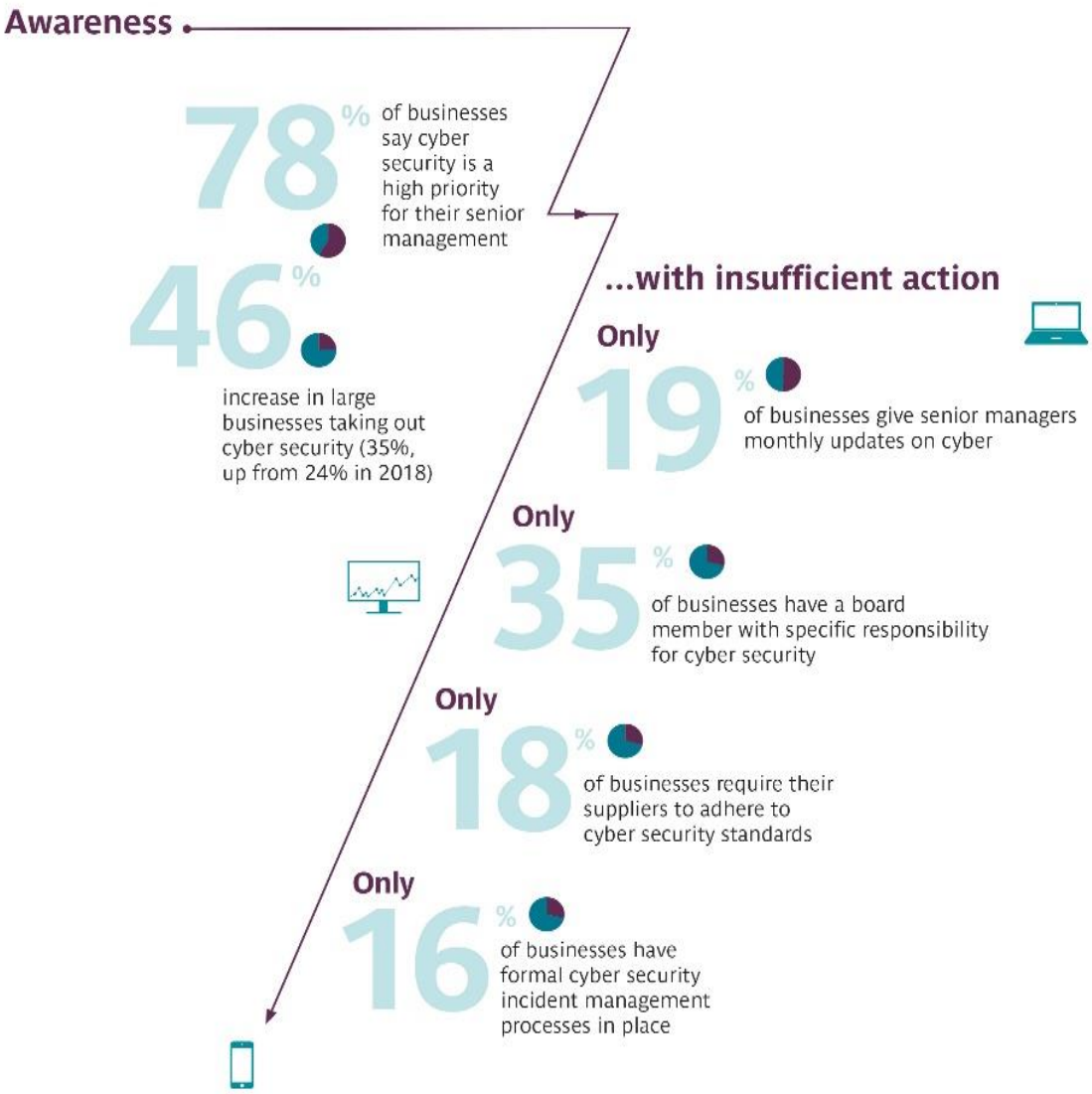
Insurance: Cyber insurance is another area where there has been some increased activity, however uptake overall remains low. Despite a perception that the cyber insurance market has developed, only 11% of all businesses have cyber insurance. The figures are much higher for large businesses (35%, up from 24% last year) with some seeing insurance as a proxy form of accreditation (used in their marketing) or a useful way of accessing breach expertise (IT forensics and breach management teams) even if it does not result in a substantive payment following a claim.

Comment

This survey reveals that in many cases half, if not more, of UK organisations are not following long-standing advice around cyber security and breach management. The survey indicates that the number of businesses taking certain preventative actions is low, despite there being an improvement on last year's statistics. While the picture is more encouraging for large businesses, there is still much room for improvement (for example, over 40% of large organisations still do not allocate responsibility for cyber at board level). The statistics surrounding SMEs should also concern large organisations, many of whom engage smaller businesses in their supply chains. Guidance is available, with many organisations reporting that Government guidance was useful when they did use it (if high level). This report is therefore a timely reminder for directors or senior executives that now is the time to follow that guidance.

Cyber at Slaughter and May

This article was written by Rob Sumroy (Partner) and Natalie Donovan (PSL) from Slaughter and May's Cyber team. At Slaughter and May we recognise that cyber risk is a key concern for our clients. We have developed a range of materials and training sessions that we would be happy to share with you and your boards, including our cyber breach response checklist. For more information on how we can help you with any cyber related matter please contact Rob, Natalie or your usual Slaughter and May contact.



Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Natalie Donovan
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com

Dated April 2019