The Financial Conduct Authority accused TSB's leadership of failing to make external stakeholders aware of the extent of the issue to the public

Picture credit: Getty

SIZE MATTERS

Andy Barrat *explains why there's no economy of scale when it comes to cyber security*

It seems barely a week goes by without another story breaking about a high-profile organisation being affected by a major cyber security incident. Recently, we've seen CEOs fall on their swords, the value of shares plummet and hundreds of thousands of people told to update passwords and security procedures for online accounts.

The current cyber threat landscape means that no business is safe – either from external threat or from internal malpractice. The IT saga that engulfed TSB this summer, and ultimately cost the bank's CEO Paul Pester his job, is a perfect example of a big business simply getting it wrong and causing itself major issues through poor risk management.

The papers were filled with stories of bank customers left without access to their digital accounts for weeks as TSB tried to migrate client data from its existing IT platform to that of its new Spanish owner, Sabadell. When IBM was called in to restore order, it quickly became apparent that insufficient testing had been carried out in advance to ensure the transfer process would run smoothly.

MPs, journalists and customers have since accused TSB of having its head in the sand over the incident, failing to get to the root of the issue quickly enough and not communicating effectively to key stakeholders. So how could this happen to a business with presumably vast security resources?

The answer is that behind the curtain – and contrary to accepted wisdom on cyber security – large organisations are often not the best prepared to protect themselves against cyber risk, despite having greater resources than most.

IDENTIFYING WEAK SPOTS

Coalfire recently conducted its inaugural Penetration Risk Report, which tested the cyber defences of enterprises of various sizes across sectors including financial services, retail, healthcare and tech and cloud services. The research involved simulating planned cyber attacks against the businesses – a practice known as penetration testing – to identify weak spots in their security armour.

We found that large enterprises were not the most secure, despite having the most substantial cyber security budgets. Instead, it was mid-sized firms that found the sweet spot in terms of protecting their assets and mitigating their security risks. We also found that the complexity and presence of legacy, often outdated IT infrastructure was causing serious security issues in larger organisations. Consequently, smaller, leaner businesses were far more effective at defending themselves.

It's worth noting at this point that TSB's issue was not caused by malicious intent or outside interference. However, the incident highlighted a disturbing lack of understanding running throughout the business that is indicative of how large corporations expose themselves to risk.

Business leaders need to get comfortable hearing about IT problems and technical risk. Often in large companies, there is a mindset that the board doesn't want to know about a problem, so risks are constantly re-framed and cracks painted over. As a result, senior decisions makers often don't have sight of the full picture when they sign off on a project. This can mean that deep-rooted issues aren't factored in and risks go unaccounted for.

THE BLAME GAME

This 'yes' culture that often leaves boards in the dark usually occurs in organisations where blame is prevalent. Corporates must adopt an environment where employees are comfortable raising issues to senior management rather than patching them up for fear of being accused of making a mistake – when they could actually be preventing a significantly detrimental event from taking place.

In the worst-case scenario, this disconnect between boardroom and shop floor can leave CEOs and directors weathering a media storm with little understanding of the issues that have led them there.

In contrast, British Airways' chief executive Alex Cruz demonstrated how it should be done. The airline boss was quick off the mark to publicly communicate what had happened after the airline discovered a malicious breach in September, coming across as both knowledgeable and proactive.

Immediately after TSB's IT failure, the Financial Conduct Authority accused the bank's leadership of "portraying an optimistic view" and failing to make external stakeholders aware of the extent of the issue to the public. The bank apologised unreservedly, but it arguably took too long and wasn't backed up by a clear plan of action (not publicly at least). As a result, questions remained about its competence and whether TSB's leadership understood or was on top of the job at hand.

While it would be unreasonable to expect the CEO of every UK bank or FTSE 100 business to be an expert on IT and cyber security, ultimately they have to take responsibility for a fault. Given the reputational impact and potential disruption to operations, there are a lot of lessons senior leaders can learn from the case of TSB.

Large businesses can also be put at risk by the complexities of their supply chain, particularly if their security measures don't account for the shortcomings of their partners.

> HUMAN ERROR REMAINS A COMPANY'S BIGGEST WEAKNESS – ACROSS ALL SIZES AND SECTORS

This was a major factor when Ticketmaster was subject to a supply chain attack earlier this year. In this example, cyber criminals used code from Ticketmaster's third-party chatbot operator to extract payment information from its website after the code in question was incorrectly repurposed by Ticketmaster's own IT team.

THE BIGGER THEY ARE...

Similar activity could be partly to blame for British Airways' data breach, where data was lifted live from its website most likely via third-party code. BA is a regular participant in industry forums and best practice initiatives, and yet has still been affected, highlighting the risk that large organisations face through their extended network of partners.

Like most big businesses, airlines are particularly at risk of attack because they frequently rely on complex infrastructure and shared services – provided by airports, booking agents, aggregators and global distribution systems – many of which don't meet the security compliance rules we set here in the UK.

For businesses of this size, resilience in the face of an attack is the modern approach. Always assume that someone will find a way in. Responding to that quickly will enable you to minimise loss.

It's also important to acknowledge that some element of human error is unavoidable – the larger an organisation gets, the bigger the risk due to the number of people employed. It also goes without saying that the potential for human error increases exponentially the bigger a work force is.

Our Penetration Risk Report found that human

▶

error remains a company's biggest weakness – across all sizes and sectors. Whether through human error or creating opportunities for social engineering hacks, the chances are that your staff will be your cyber security Achilles heel.

Accountancy giant Deloitte was hit last year as cyber criminals got hold of confidential data via an administrator's account, which had only single-factor authentication in place. In this case, it's likely that phishing – where hackers pose as a trustworthy entity (usually via email) to obtain sensitive information – was used to expose the password.

LARGE ENTERPRISES ARE NOT THE MOST SECURE, DESPITE SUBSTANTIAL CYBER SECURITY BUDGETS

Tesco Bank was recently fined £16.4 million following the breach it suffered the year prior to Deloitte. In what was a largely avoidable attack, cyber criminals were able to secure £2.26 million of customer money during the 48-hour incident. Tesco Bank has already paid £2.5 million in compensation to the nine million customers whose accounts were compromised. Initial reports suggested that the FCA was considering imposing fines of over £30 million had Tesco not provided them with such high levels of cooperation and agreed to an early settlement.

GDPR GAME CHANGER

Fortunately for Tesco, and for most of the businesses mentioned here, the breaches and failures they suffered fell before the arrival of the EU's new data protection regulation – GDPR. British Airways, however, is the first high-profile business to experience a major data breach since new rules came into action in earlier this year. The new rules give data regulators – in the UK's case, the ICO – the power to issue fines of up to four percent of a business's global turnover if it is deemed not to have taken necessary technical precautions to protect its customers' data. In BA's case this could mean a fine totalling £489 million.

GDPR gives real teeth to data protection enforcement. Though it will ultimately have a positive impact on data safety around the world, it does mean that, more than ever, cyber security is an issue big businesses can't afford to get wrong ●

Andy Barratt – UK managing director of Coalfire – has almost 20 years' experience working in IT infrastructure, information security and assurance services. He is actively involved in supporting security with a number of technology companies, software suppliers, payment processors, acquiring banks, insurance underwriters and other complex service providers.

BA's chief executive was quick to publicly communicate what had happened after the airline discovered a malicious breach

Picture credit: Getty