

Economic crime and cybercrime

It is clear that the digital landscape, often termed cyberspace, is a man-made environment, in which human behaviour dominates and where technology both influences and aids our role in it — through the internet, telecoms and networked computer systems, which are often interdependent. The extent to which any organisation is potentially vulnerable to cyber-attack depends on how well these elements are aligned.

18 October 2022

This article is taken from October's public matters newsletter. [Click here](#) to view more articles from this issue.

It is clear that the digital landscape, often termed cyberspace, is a man-made environment, in which human behaviour dominates and where technology both influences and aids our role in it - through the internet, telecoms and networked computer systems, which are often interdependent. The extent to which any organisation is potentially vulnerable to cyber-attack depends on how well these elements are aligned.

This article explores recent experience and seeks to navigate through the latest Government policy reviews around cybercrime and offer some insight into the way organisations should be thinking when addressing these issues.

Background

The Government, as part of its [National Cyber Strategy 2022](#), published by the Cabinet Office earlier this year, has emphasised the crucial role the digital economy has as part of its wider agenda - not least the development of education and skills, but also the long-term plan for digital transformation of the economy to aid growth.

Part of this accepts the presence of online and digital vulnerabilities and therefore, whilst the digital 'growth' strategy is rightly front and centre, building resilience and beating crime in this arena is crucial; without them, confidence in the strategy will be seriously undermined.

Where we are now?

Firstly, the good news. According to the [PWC Global Economic Crime Survey 2021](#), in the past two years, three of the top five types of fraud reported by UK respondents — cybercrime, customer fraud and payroll fraud — have all fallen since 2020. Promising start...but:

- 64% of all UK respondents had experienced fraud, corruption or other economic crime;
- 51% of those fraud activities were perpetrated from outside the organisation — by customers, hackers or vendor suppliers; and
- whilst technology helped, the most effective detection method of the most serious cases was existing internal fraud risk management including activity monitoring, internal monitoring, and security.

The tension between empowering people or implementing technology in the fight against cybercrime has long been at the centre of the debate around best practice.

The people risk

Worryingly, reporting through whistleblowing, tip-offs or internal staff changes were the least effective in detecting the criminal activity. One explanation, perhaps, is that organisations are trusting more in process and technology than in training their people to spot and detect fraud both from inside and outside the business. For all organisations, it is a careful balance of resources, particularly where staff and their time are at a premium. So, one take-away from the survey is that training and raising awareness with employees pays dividends.

Another concerning trend identified by PWC is the linked increase in the amount of external fraud which has targeted organisations. In part, this is an indication of the rise in risk in supply chains and also in the virtual customer base.

Procurement of services and confidence in suppliers, therefore, is a particular area of weakness. It is clear that artificial intelligence solutions for onboarding and customer management do not appear to be a reliable solution on their own yet. Demand for certain materials in the current economic cycle, where sanctions affect supply, and the search for cheaper, more readily available alternatives are putting pressure on businesses and organisations to take greater risks with credit, and also often causes their supply chains to lengthen. Where those risks are not managed, and where ID verification processes and supplier security might be less rigorous, organisations may be exposed to greater risk of fraud, data theft and economic crime.

To that end, whilst businesses generally understand the need for greater transparency in supplier relationships necessitated by KYC and AML processes or for ESG reasons, the increased burden on the management of relationships becomes a decisive factor in combatting cybercrime. In economically challenging times, due diligence takes on even greater significance but, inevitably, is sometimes overlooked, intentionally or otherwise, and such shortcuts may lead to greater vulnerability and potential harm.

One positive on the horizon is the planned [Economic Crime and Corporate Transparency Bill](#), which provides for greater ID verification of directors and persons of significant control. If the Bill is approved into law, it is hoped that the related Act will stop the abuse of the Companies House registration process which has seen many instances of bogus directorships or phoenix companies set up for criminal purposes. As an online public repository of data, accessible to all, this would be a good starting point.

The technological risks

With 90% of businesses and 80% of charities (including schools and universities) having a digital footprint (such as ability to pay online, using networked devices or storing information electronically), the potential for increased cyber victimisation is understandably higher now than ever before.

It is worth noting, though, that the move to online or remote working during the pandemic did not lead to a rapid spike in cybercrime, although it certainly has risen. Surprisingly, volume is not the issue, with overall crime numbers falling. There has been an evolution in cyber-criminals' technical sophistication, which is the marked feature of cyber-enabled fraud over the past 12 months.

The [Cyber Security Breaches Survey 2022](#) identifies phishing attempts as the most common threat, with 83% of UK organisations (including charities and education institutions) who were attacked suffering disruption as a result. Staff being duped by fraudulent spoof emails linking to malware-infected documents or fake websites remains a big issue for most organisations. One in five victims also identified malware, DDoS (denial of service) and ransomware attacks, demonstrating a much higher level of ingenuity and a change in attack vector by the so-called bad actors.

The larger organisations (with incomes >£5 million), with their greater capability and more comprehensive cyber security, experienced more than one of these types of attack in the past year, meaning the variety of methods being adopted and the frequency of these attacks is increasing.

In response, the resilience of organisations to defend themselves against cybercrime depends upon their IT resource and security, as well as measures in place and ability to respond. The survey confirms that, although rarer than phishing, these multifaceted attacks have a much more substantial impact on the victim organisation. The scale, and severity of the impact of such multi-faceted attacks lead to greater recovery times, higher potential costs (and losses) and greater damage to reputation and staff morale.

Although aware of the need for vigilance and prevention policies, most organisations are, however, reactive and rely on some form of loosely drafted response plan. Crucially, fewer have proactive measures and written guidance. The latter should form part of a holistic approach to dealing with incidents — allowing clear lines of reporting, early engagement with insurers or cyber specialists, notifications to regulators, and communications to stakeholders and with the public where required.

Technology vs people

It is not surprising, in the face of the increased technological challenges, that the [DCMS report on cyber security breaches](#), which surveyed 10 organisations who had experienced a cyber breach, confirmed their greater reliance on technology over people. Whilst their experiences of these breaches were distressing and disruptive, few truly understood or had, in fact, measured the financial impact on their businesses — such as management time and investigation and remediation costs. A review of the themes of this study is helpful in explaining the challenges facing many organisations.

Many organisations' focus seemed to be on remedial steps, such as informing trustees/directors, assessing the scale, and identifying the source of the breach, including (where the budget allowed) and placing reliance on cyber security. Small and medium sized businesses were particularly affected where outsourced managed service providers, (for email and data storage) which the organisation relied upon, were at arm's length and the organisation could not properly benchmark their performance, which led to mixed (often negative) responses in the face of an incident. Whilst technological remedies and minimising disruption forms part of any response, few truly understood the scale of the problem their organisations had to meet.

In many ways the seriousness with which an organisation treats these issues is fundamental to their ability to bounce back. Some of the respondents saw cyber security as a Board issue, but ironically, only after a breach was 'real' leadership shown. Even then few organisations took the time to properly analyse the true financial impact and understand, address and adopt learning outcomes in order to improve their security going forward.

It is evident that inconsistencies in approach leads to a mixed response overall. Drafting and implementing a coherent cyber security strategy is the responsibility of senior management. Given the ever-increasing risks and importance the strategy plays in protecting the organisation against these, it should be a regular topic of discussion at board meetings – with actions taken to address any issues, or gaps in the policy that might arise.

Prepare and learn

And therein lies the challenge. The DCMS-surveyed organisations indicated that people and culture were more of an issue and weak spots in their response to cyber risk than the technology, whilst accepting that there was an increased vulnerability at all levels.

Fortunately, while it is no panacea, if your organisation is reviewing this issue, there is a starting point solution which marries the two apparently divergent areas of vulnerability.

The Government's National Cyber Security Strategy provides some practical guidance in its '[10 Steps to Cyber Security](#)'. It is a simple set of rules, not only providing organisations with broad principles to build good governance and corporate policy, but to detect fraud and also build resilience. Board engagement, better governance, risk management of suppliers, risk and asset management and investment in skills, cyber awareness and culture, including a written emergency response plan, should be at the forefront of any policy.

Of these 10 steps, staff engagement and training stand out as the quickest and easiest win. Investing in your people, validating them and their credentials on appointment and promotion, then embedding an anti-fraud culture in a cybercrime-aware workforce will, no doubt, save your organisation money.

If you would like to discuss any of the issues raised in this article, please contact us.

Contact

Paul Wainwright

Partner

paul.wainwright@brownejacobson.com

+44 (0)121 237 4577

Related expertise

Services

Counter fraud for insurance

Cyber liability and data security
insurance

Data protection and privacy