FENDING OFF A CYBERSECURITY ATTACK

Shani Latif *examines the long-term damage that can be done to a business in the event of a cyber attack*

Picture credit: Anna Shvets

Almost half of UK businesses suffered a cyber security breach or attack during the past 12 months – rising to 68 percent of medium-sized firms and 75 percent of large enterprises – according to the Department for Digital, Culture, Media and Sport (DCMS).

As our reliance on connectivity and devices grows in both our professional and private lives, society's relationship with technology broadens and becomes more complex. Unless businesses take significant preventative measures against these attacks, the figures reported by governments and analysts are likely to rise.

Cybersecurity issues are something that businesses cannot afford to rectify retrospectively. The financial, reputational and personal effects these attacks have are profound. For companies with operations or interests in the public domain, attacks are destined to spill into the public consciousness and influence consumer habits. Equally, an organisation's reputation in their industry could be irreversibly damaged.

In recent years airlines have been a constant target for cybersecurity attacks. Most recently, the details of 9-million EasyJet customers were accessed in a hacking of the airline's data including over 2,000 credit and debit card details. In 2018, at least 185,000 people may have had payment card details stolen because of a British Airways data breach. Victims' details were left exposed due to a website compromise that had gone undetected for months.

Airlines, of course, aren't the only victims. Already this year, many household consumer names have revealed similar flaws or attacks. Both Tesco and Boots reported security breaches to their respective loyalty card schemes – in the same week. The former was forced to reissue some 620,000 cards, while 14-million Boots customers were affected.

Not all compromises are caused by bad actors, however. In March, Virgin Media admitted its database containing the personal details of 900,000 people was left unsecured and accessible online for 10 months. The problem was, fortunately, identified thanks to a flagging from a security researcher rather than an exposure by opportunistic cybercriminals.

It is not just the big names falling victim. Small businesses in the United Kingdom are the targets of repeated cyberattacks with around 10,000 attacks occurring every day, according to the Federation of Small Businesses.

The ramifications of attacks like these are widespread and damaging. As well as the personal effect on customers, businesses can expect a drop in share prices, fines, and, frankly, a sense of mistrust from the general public – irrelevant of whether an attack could've been prevented or better defended against.

Financially, in the UK the average cost of a data breach has grown to nearly £2.7-million, according to IBM research. British Airways faced a record £183-million fine alone for its data breach in 2018.

The reputational damage to a brand can prove hard to restore. Forty-four percent of UK consumers claim they will stop spending with a business temporarily after

MALWARE ATTACKS CAN BE COMBATED BY PUTTING IN PLACE A STRICT SECURITY COMPLIANCE

a security breach, and 41 percent claim they will never return to a business post-breach. Thirty-three percent of UK organisations say they lost customers after a data breach. A Forrester study of UK and US companies found 38 percent had lost business because of security issues. Businesses operating further away from the public eye are likely to face damage to their standing or integrity in the industry they operate in.

The occurrence of these breaches shows no signs of slowing, as businesses continue to migrate their operations to cloud-based systems, increasing the number of associated risks to tackle.

And as if the need to be vigilant wasn't urgent enough before lockdown, research by Deloitte shows that cyber criminals around the world are capitalising on the COVID-19 pandemic crisis. Their research has tracked a spike in phishing attacks, malspam and ransomware attacks as attackers use COVID-19 as bait to impersonate brands and mislead employees and customers.

In addition to businesses being targeted, end-users who download COVID-19 related applications are being tricked into downloading ransomware disguised as legitimate applications. Already, Zoom – the platform opened up by millions to virtually replicate work meetings and family get togethers – has had its security flaws laid bare across a timeline of issues and been

With more employees forced to work from home the need for adequate security defences is greater than ever before

forced up ramp up its security capabilities. As the trends that have sprung from working from home – such as the increased adoption of smart home devices and employees connecting to company servers and networks – look set to continue after the lockdown to varying degrees, businesses will need to be extra vigilant looking to the future.

But before considering how businesses can better shield themselves from cyberattacks, it is important to identify and understand how breaches can present themselves.

UNDERSTANDING THE RISKS

Despite cyber threats being among the primary concerns for' management teams, a lack of understanding of where to prioritise investment to prevent or identify threats is a notable problem. Before considering how we can better prevent our businesses and organisations from attacks, it is important then to understand how these attacks manifest.

Communication networks, for example – a vital part of the UK's critical infrastructure – are a key target for malicious cyberattacks. The availability of voice, data and internet infrastructure underpins much of the economic and social activity in the UK. Most sectors and the businesses that operate in them are dependent on the connectivity provided by telecoms, the services it enables and the activities it supports.

These networks however, especially when connected to the internet, are increasingly vulnerable to a range of malicious cyber threats. Distributed Denial of Service (DDoS) attacks – malicious attempts to damage a service, sometimes by traffic overload, sometimes by the transmission of malware – are a major threat to these networks. Malware such as viruses, worms and Trojans and hacking, including attempts to subvert the proper operation of the billing system in networks, also need to be rigorously protected against.

Malware attacks are another cause for concern, and this can be caused by not having the right internet security software in place. One way to combat this directly is to put in place a strict security compliance. Additionally, selecting the right cloud provider can go a long way in preventing malicious data breaches and managing an organisation's data effectively so it can make sure it can pinpoint what data has been stolen and ensure the weaknesses are addressed.

One key risk which businesses are keen to mitigate is hacking. More often than not, hackers will be able to

access a network through people sharing credentials and password details. To overcome this, businesses must look at placing restrictions on sharing information while also monitoring employees to ensure they are not sharing data, either unwittingly or deliberately. Additionally, businesses must educate employees to ensure they are aware of the ever-evolving challenges of cyberattacks and how they can identify cyber threats.

When assessing these risks, it is no longer a case of if an organisation will be attacked, but when.

Good cyber security is now considered an essential requirement of today's businesses, but there are still challenges emerging as attacks continue to escalate and evolve. Issues such as lack of investment, awareness and training need to be addressed.

The average UK cybersecurity budget is around $900,000, compared with an average of $1.46-million globally, according to insurance company Hiscox. Coupled with this is the cyber security workforce shortage, expected to reach 1.8-million by 2022.

DCMS says that there is work to be done in areas such as internal and external security audits. Only half of businesses have done these in the past 12 months and the quality of auditing varies wildly. The prevalence of insurance against security incidents, which is held by just 32 percent of businesses, is another concern.

As the technology we adopt gets more complex, so do the attacks that need to be shielded against. The mismanagement of cloud data can be rife in these circumstances. The amount of information that an organisation is required to digest and base investment decisions on is growing, impacting the level of resources and skills required from the internal IT team and increasing vulnerabilities. Many organisations have, and will continue to, find themselves unintentionally exposing sensitive personal data – presenting the opportune environment for a cyberattack or accidental data breach.

While attacks are becoming more sophisticated and complex, at the same time regulation, legislation and industry compliance requirements are also becoming more onerous. From General Data Protection Regulation (GDPR) to PCI compliance, to added international standards, the landscape is complex for any business to navigate. Although compliance improves practice across the industry, it doesn't leave an organisation immune to attacks by any means. The constant changes in regulations also require current, adaptable knowledge and skills within a business' IT department.

Cyber Security Maturity (CSM) benchmarking is emerging as a solution which can provide organisations with the intelligence to transform the quality and value of short, medium and long-term planning and decision making.

Achieving CSM enables the IT security team within an organisation to report on the status of their organisation's security status via consistent monitoring and risk analysis. A high level of CSM is also proven to reduce overall cybersecurity spend.

To keep a business' data safe, companies must be prepared to constantly be on the lookout for potential risks. At telent, we believe in not only optimising the full potential of technology, but also combining this with the people that have the right expertise to deploy the most-effective services possible can keep your data and your business protected.

The potential damages of a cyber-attack can no longer be ignored, but they can be mitigated. With the right solution in place, organisations can improve their business resilience, all while adapting to emerging business objectives and the changing technology and evolving threat landscape.

Businesses therefore need to identify their vulnerabilities and how they can protect their assets from attacks before their name is attached to the latest data breach story we read about ●

Shani Latif is the Sales Director at telent Technology Services Ltd, focussing on the service provider, emergency services, higher education and public sector areas of the business, which includes helping to develop customers' IT security strategies.

185,000 British Airways customers had credit card details stolen in a data breach in 2018