Don't let peak sales time become peak cybercrime time too!

Black Friday is finally here, ushering in a crucial five week period for retailers through to Christmas and New Year. But while it may be a period of bumper (discounted) sales, the fact is that it can also be a period of bumper cyber-attacks and fraud.

Cyber criminals see opportunities in this and in every facet of increased demand - from launching malicious campaigns while retailers are dealing with increased traffic to online channels and backend payment systems, through to targeting unsuspecting customers with malware and phishing attacks.

Customer trust is hard won but easily lost. Studies regularly show that organisations experiencing a data breach continue to lose customers as a result.

A not so merry Christmas?

In 2018 UK retailers reported a rise in social engineering attacks during holiday periods, with just over a third encountering such a scam. On Black Friday last year, Distributed Denial-of-Service (DDoS) attacks on e-commerce providers - where systems or websites become unavailable due to multiple targeted attack - showed a 70% increase compared with other days in November, while Cyber Monday attacks rose by a massive 109%.

Source: TechRadar - UK retailers boosting cybersecurity for the holidays (2018) https://www.techradar.com/uk/news/uk-retailers-boosting-cybersecurity-for-the-holidays.

But no need to cancel it!

Prevent

Stopping a problem before it occurs is always the best approach…

We can help organisations understand what their actual cyber risk is and then develop a strategy and solutions to manage this.

Transform

Sometimes you will need to think differently about your approach to cyber, perhaps following years of under investment. …

We've helped businesses transform their approach to cyber – designing solutions and implementing them.

Detect

Of course someone is always watching you, so do you know your own vulnerabilities?

Our security specialists work through the eyes of a hacker and will help to find weaknesses and ways into the business before the criminals do.

Respond

But what happens if it still goes wrong and you get hacked?

We can help respond to cyber incidents - providing the right level of support when and where its most needed. Most importantly, getting things working again.

Consistently, we see that the majority of successful cyber-attacks come through exploiting the most common vulnerabilities. A huge amount can therefore be achieved by focusing on the basics.

Below are two examples where we have helped clients who didn't know their systems were insecure, and one who we helped after a Cyber breach.

Detect Case Study: Ethical Hacking

We delivered an ethical hacking exercise at a goods manufacturer, which was designed to identify the risks to their 19 businesses.

Playing the role of hacker, in under 2 hours the team had complete control of the industrial systems key to production across their entire business, along with access to the payroll system, and pricing and budget planning systems. The CFO then understood the real Cyber risks to his business. This resulted in a remediation programme that encompassed cultural change, technology change and a remediation programme to fix the immediate issues.

Respond Case Study: Incident Response

One of our clients IT systems was infected with a complex malware strain. It stopped their business from running day-to-day operations, they were losing money and didn't have the right skills in-house to respond.

We were onsite within 4 hours of the call to help manage the incident. We contained the malware, stopped any further infection, and were able to restore business operations within 48 hours.

Our team then provided forensic post-incident support to determine the root cause of how the malware had managed to infect the network. This allowed our client to make changes and stop this type of attack occurring in future.

Finally…. another analogy to better understand how we can best support our clients

I want you to imagine that I am holding a large box in front of you, the sort that you get Black Friday Deals delivered in, over your desk. The box represents one of your clients.

Inside that box are hundreds of ping pong balls, each representing a system or piece of sensitive data, also inside the box we have employees, third parties and contractors, all of whom have access to the data. The box is constantly under attack from hackers, organised crime syndicates, nation states and even employees. If the box were to be broken into, then the balls will drop onto your desk and scatter everywhere, at this point your client enters crisis mode, battling with the fallout, and trying to catch and contain the data loss.

In Cyber we help clients to keep the box intact and the data from leaking out. But just as important, we help them to respond and clean-up should they have a Cyber breach.

Why KPMG?

Cyber relevant to your needs. Our experts have practical experience gained across public and private sectors in all aspects of cyber. Our staff hold all the major qualifications you'd expect (e.g. CISSP, CIPP/E, CREST, CHECK). We are also a UKAS accredited certification body for the international standards ISO 22301 and ISO 27001.

Track record of delivery. We are an award winning cyber security consultancy and take great pride in being recognised by Forrester as a leader in the market.

i4. We own the world-leading i-4 organisation, which focusses on trusted collaboration for CISOs and equivalents. We have access to market-leading, cross sector-insights which we can bring to our delivery.

Contact us

Want to see how we can make a difference?

Martin Tyley
Partner

T: +44 7748 111484
E: martin.tyley@kpmg.co.uk

Del Heppenstall
Partner

T: +44 7467 339438
E: del.heppenstall@kpmg.co.uk

kpmg.com/uk