SOPHOS
Cybersecurity delivered.

Industry Secrets: Cyber security for retail

The retail sector is one of the most highly targeted verticals in terms of cyber and social engineering attacks. Millions are lost annually as a result of ransomware attacks as retail employees are duped via increasingly ingenious methods into providing access to critical systems and data.

We caught up with Christopher Salgado, CEO, All Points Investigations, and Kostandino Kustas, Cyber Security Consultant, Sophos, to find out how organisations are being targeted and what they can do to protect themselves.

A Sophos Whitepaper. July 2022

Q – What exactly is social engineering?

CS - Social engineering is the use of deception through manipulation of human behaviour to target a person into divulging confidential or personal information. Put simply, it is getting someone to do something that they otherwise would not do if they knew the true identity of the person asking for it. What's particularly dangerous about social engineering is you don't need any technical skills to be successful. It has been identified as being a precursor to between 95-98% of all cyber-attacks.

There are basically three different approaches taken in social engineering. Digital or non-physical attacks, physical attacks and hybrid attacks.

With regards to digital or non-physical, we're talking about classic phishing either via a voice call or electronically via email. Smishing is the term used to describe SMS attacks. Then there is spear phishing, which takes a very targeted approach.

Social engineers know that if they personalise their attack, their rate of return goes through the roof. They'll find out as much about the intended target and tailor their engagement. The victim's guard comes down because they think they're talking to somebody with authority.

Physical attacks include face-to-face engagements, which could be engineered as "chance" encounters or even scheduled meetings. They also include physical mail that encourages individuals to call or post back a response, or go to a website and fill in an online form.

The hybrid approach is arguably the most dangerous/effective. A classic hybrid attack could be a "vendor" invoice being emailed, and not long after that someone emails and/or calls to say "hey, I just sent you an updated invoice. Just wanted to let you know that we switched banks. Can you go ahead and let us know how we can get that payment from you? It's nine days overdue." Imagine you're working in payments with a long list of urgent tasks and very similar genuine requests like this from real suppliers. People fall for this one all the time.

In 2021 there were several "loss prevention agents" of a large retailer that called cashiers at the stores to activate numerous and large denominations of gift cards as part of an "active investigation". They were bad actors, and they were not in fact loss prevention agents. There was no active investigation. And in chasing down these bad actors, we identified they're located somewhere in Eastern Europe.

Retailers are also falling foul of social engineering by smartphone. Not just by their use as a communication channel via calls, texts and on mobile browsers, but also via apps. Retail organisations are increasingly enabling mobile or contactless payments. Bad actors have identified this trend and have developed rogue apps that people are encouraged to use.

Q – How prone to attack is the retail sector?

KK - The retail sector is unfortunately very heavily targeted. In the UK, retailers face one cyber-attack every eight days. These may not be very large scale, they may just be very early indicators of compromise or somebody who has tried their luck to get into these environments. But for them to happen at such a high frequency means that realistically the retail sector should take this as seriously as possible, whether they are direct attacks on infrastructures, or whether they are social engineering attacks.

Two recent examples stand out from 2021, UK grocers Spar and Sainsbury's were both attacked via their supply chain. Spar lost access to payment card systems and Sainsbury's lost access to their payroll systems. Both attacks were very damaging to the organisations.

According to our own data, the retail sector was second in terms of the number of organisations that had been hit by ransomware in the last year. The average was 66%, retail stood at 77%. Sophos operates something called Rapid Response. These don't have to be Sophos customers, in fact most of the time they're an organisation that's going through a security incident that has led to a breach, or maybe they have an active adversary in their environment that they're unable to contain or neutralise, so they engage our Rapid Response service. Retail is second only to manufacturing in all the cases that the Rapid Response team deal with.

Q – How can you assess your exposure to risk?

CS - You've got to look at your exposure points. It could be social media, personal websites, blogs, clubs or other groups. On average, every single one of us is exposed on approximately 70 different databases. And most of them we don't know about, which is very concerning because those databases allow bad actors to pay as little as $5 to find information about us such as our postal address, email, telephone number etc.

There's a concern that once something is online it is memorialised forever. In some cases, it is true, but in most cases you can hunt it down and delete this information, it might just take a bit of work. Our data as individuals is more valuable than gold today, so companies that own the data do not want to give it up, but you can and should delete it because doing so will reduce your exposure level.

One classic example I see time and again is that of a retiring employee who posts a photo on LinkedIn of their work badge saying, "it's been a great 20 years I'm off to another party," it's all in good spirit. But they are essentially providing a blueprint to the bad guys on how to copy that company badge.

Q – Once we've assessed our risk, how do we protect ourselves?

CS - Unfortunately, there is no prevention for every single social engineering attack out there. However, you can install efforts to prevent and mitigate damage. A good strategy would be to identify the number one worst case scenario that would cripple your business, maybe it's a client data leak or sensitive corporate documents like patents or business plans.

You then need to invest in a robust cybersecurity operation with layered defences that include anti-social engineering tactics. A lot of companies invest resources into impressive software that looks good on paper and makes people feel secure, but doesn't do anything about the human element, which has been identified time and again as the weakest link in a security chain.

Organisations need to train all employees, contractors and vendors on the do's and don'ts of how to be cyberly responsible. This should include social engineering and how and when to report suspicious cyber and physical actions or behaviour.

Companies need to implement retrains, and make sure that their policies come with teeth. I've seen corporations build a policy stipulating that people need to take training. And then the employees just hit the 'remind me later' button. Weeks might pass without the training having been taken and there are no repercussions.

Furthermore, your supply chain should be incorporated into this programme. Your suppliers' security might not be as tight as yours, but they could have access to your systems and therefore represent a huge point of weakness.

Organisations today also need to protect corporate mobile phones just as rigorously as they do laptops or desktops.

In retail in particular, organisations need to consider POS systems and upgrading security and operational systems. In today's world, POS systems need to be fully updated 24/7, 365.

When you're rolling out software/system updates you should consider taking a tiered approach, it could be regional, or per system. Taking a tiered approach allows for more control than a big bang implementation.

A final consideration is insurance. It is important to remember you can't just buy insurance and rely on that for cover. Insurers will insist on certain levels of security and your premium will be affected by how proactive you are. Also, the insurance cover might not be as much a ransom demand. But having some insurance is better than having none.

KK - At Sophos we have identified the following six points that organisations should address when developing a protection plan:

- Ensure you have high-quality defences at all points in your environment.
- Hunt for potential threats and investigate them.
- Harden your IT environment, use alarms and tools to identify points of weakness.
- Have a cyber-incident report plan. The ability to be able to respond, even if it is just to pick up the phone to somebody like our Rapid Response service, cannot be underestimated.
- Make sure you back everything up and practice restoring files periodically.
- Finally, remember the essentials like employee education, policies for access and authentication, and patching critical bugs.

At Sophos we base everything around what we call the adaptive cybersecurity ecosystem strategy. This is effectively a single pane of glass called Sophos Central where we manage all of our security products from that same management console, and we offer XDR security operations which can be used to conduct proactive threat hunting.

We also offer a Sophos Managed Threat Response service. This is our 24/7 Security Operations Centre that provides incident response and takes a proactive approach to looking for indicators of compromised attack.

Q – When it comes to social engineering who has ownership?

CS - The answer is, it depends. And that's the answer that we never want to hear. It depends because it's about the makeup of the company. We've engaged companies standing up support for anti-social engineering measures and the makeup can differ immensely. It often comes down from the CFO because ultimately it is a cost. It will be the tech folks that stand up the cyber portion of the security apparatus. But the physical security could be a front desk or security guard. Ultimately, with social engineering, everyone needs to take some responsibility.

Q – How can technology help organisations protect themselves against social engineering and credential phishing?

KK - One very obvious piece of technology is an email security filter. An effective modern filter will use AI to analyse natural language and email addresses to work out if they match certain patterns.

Organisations can also use training technology such as phishing simulation software to help employees identify when they're being phished and what to do when it happens.

At the end of the day, it's all about making sure you've got layered defence in place. Crucially, you need to ensure it's very easy for employees. The more barriers that are created, the more likely employees are to find shortcuts that render your security ineffective.

Q – How can organisations protect themselves from their supply chain being socially engineered by an attacker?

CS - Unfortunately, this is a huge risk, because you have a large variance of security apparatus and security infrastructure from one vendor to the next. You can only go so far injecting yourself into a supplier, partnership or the supply chain, but you as the customer can demand certain actions be taken or at least demand they have certain understandings of social engineering and the current tactics being used in cyber-attacks.

You want to make sure that you incorporate an audit process through your entire supply chain. You want to make sure that you have an understanding and get documentation from your supply chain partners to outline your expectations. You should make sure it goes through your legal team to ensure you're not overstepping legal boundaries.

Q – If an attack happens, how long does it typically take to recover?

KK - Ransomware recovery can typically take up to a month. There are some organisations that are taking longer and in some cases it's years and beyond. In retail, if your POS goes offline, it would be catastrophic, it would not be feasible to take as much as a week off, let alone a month.

The average ransomware recovery cost according to our data was £1.12 million. This isn't all the ransom payment, it covers downtime, investment in tools or maybe forensic services and solutions to be able to truly recover from ransomware threats.

While a third of organisations we surveyed paid the ransom, the majority of those cases didn't get all their data back. Cyber criminals are not out to make the world's best encryption product that can be recovered, they're out just to get that encryption to work from an impact perspective, they're not too bothered about recovery.

In conclusion, organisations need to invest today to avoid tomorrow's problem. A social engineering attack can quickly lead to infiltration, loss and/or negative brand while the cost of breaches is going through the roof. We cannot consider social engineering problems exclusive to security teams, bad actors are going after everybody.

To learn more about the Sophos MTR service visit our website or read our case studies and research.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2022-07-26 (WP-NP)

SOPHOS