TANIUM

Cybersecurity for retail: Prevention is better than the cure

Foreword

Will 2022 be the worst year on record for cybersecurity? Almost three quarters (74 percent) of IT, security and business leaders in the retail sector certainly think so.

Behind this gloomy statistic there are reasons to be optimistic about retailers' ability to cope with the evolving threat landscape. To empower cyber teams and senior executives with contextual, cross-industry data, Tanium commissioned a research project called 'Cybersecurity: Prevention is Better Than The Cure', the findings of which are revealed here.

Do security personnel have the strategic and financial support from business leaders to tackle the unprecedented growth in attacks? Is security spending expected to increase over the next 12 months? How proactive or reactive is the retail sector when it comes to cyber? Read on to understand what's in store for the remainder of 2022.

Has the horse bolted?

Many security practitioners we heard from feel their work is ignored or undermined until it's too late. In fact, the research is quite conclusive that IT and security teams believe a cyber event has to occur before they can receive higher cybersecurity investments. More two thirds of respondents (68 percent) agree, which sets a foundational question at the heart of the report: Is 2022 turning into a perfect storm for cybersecurity?

A common feature of large and growing organisations is the value they place in being faster and more agile. Resilience, on the other hand, is a less glamorous quality – one that often floats under the radar until it's needed. Eight in 10 (79 percent) professionals we surveyed across retail and other vertical sectors said that more cybersecurity budget would likely be assigned following a data breach, not ahead of one. This is an acknowledgment that some senior leaders don't fully appreciate the preventative role that cybersecurity plays in protecting the business.

Lack of proactive investment can cause problems when it comes to preventing security incidents and data breaches. Almost three quarters (71 percent) of our survey sample claim to have a "preventative" approach to cybersecurity, yet more than half (61 percent) have suffered an attack that was "avoidable", begging the question regarding just what types of preventive investments are being made?

These statistics highlight that there is ample scope for retailers' cyber teams to make improvements in many areas that are under their influence and control. As an illustration, around a third of professionals surveyed (35 percent) said they intend to invest more in "employee awareness training". However, this significantly lags behind other sectors, including telecoms (75 percent) and public service orgs (63 percent). This prevention-first approach is one way to reduce vulnerabilities that are often caused by human error or lack of education on cyber matters.

How will new technology spend be allocated? Retailers say:

#1 Threat detection (74 percent)

#2 New endpoint devices (50 percent)

#3 Data recovery and back-up (47 percent)

#4 Endpoint security (38 percent)

#5 Employee awareness training (35 percent)

"Given that retail is a heavily regulated sector, the cost of overcoming avoidable cyber attack can be extremely detrimental. Economic fines and greater industry oversight is one thing, but retailers will also be hypersensitive to the brand and reputational damage caused. Prevention is always better than the cure.

Vulnerabilities occur where there are gaps in understanding and inconsistent compliance across an organisation. It's common, for example, for large retail networks with multiple sites to know how many endpoints even exist. This lack of visibility will heavily compromise cyber teams in their ability to keep on top of the growing threat landscape and maintain compliance with far-reaching standards such as PCI."

Erik Gaston
VP Global and Industries, Tanium

Fear of the known

So far, we've determined that the threat landscape is approaching "worst year" levels of concern. We've also learned that organisations will 'find the money' for cybersecurity, but often only after a problem has occurred. But what specifically are grocers, department stores and other retailers fearful of should the firewalls be breached? The answer is inconclusive with a broad spread of equally-weighted concerns – until, that is, we look deeper into the data.

The largest number of survey respondents (59 percent) speculates that "loss of productivity" would have the biggest post-breach impact, followed by "loss of clients and/or revenue" (53 percent). However, it's worth noting that these two answers have a mutual association – downtime. Following two years of pandemic disruption, organisations are naturally sensitive to anything that interferes with business as usual.

Other listed concerns include: ""reputational damage" (50 percent), financial damage from ransom payments" (47 percent), "staff hours to recover from the incident" (47 percent) and "loss of IP/data" (44 percent). These answers are all the more interesting when we ask our respondents what they think concerns their senior leaders. Again, we get a fairly even spread of results, but with one significant discrepancy: just 29 percent believe that the "staff hours to recover" would raise significant alarm in the boardroom.

Given these potential issues, it's not surprising that IT security professionals feel overstretched and underfunded. Exactly half (50 percent) believe they don't have enough staff to "focus sufficiently on cybersecurity preventative measures".

Ultimately, however, there is a strong feeling that prevention is better than the cure. 81 percent of organisations (retail and other vertical sectors) believe that more spending on preventative measures to stop cyberattacks and data breaches would "minimise" the impact of "avoidable incidents".

What are retailers' biggest cyberattack concerns? Senior executives say:

#1 Reputational damage to my organisation (62 percent)

#1 The immediate loss of clients and/or revenue because of downtime (62 percent)

#3 Financial damage to my organisation associated with ransom payments (56 percent)

#4 The loss of productivity because of downtime (50 percent)

#5 Loss of intellectual property or owned data (41 percent)

"Attitudes towards cybersecurity vary between industries, just as they do within organisational hierarchies. However, our data shows that management and cyber teams in retail organisations have a common concern: the lost of client revenue from downtime. This shows that IT and security teams are fully conversant with the main business-level concerns - they are not detached from them.

Nonetheless, cyber professionals need to redouble their efforts in educating senior executives about the merits of a prevention-first strategy – and to set invest levels appropriately. That's best achieved through contextual reporting of the threat landscape using insights that business leaders can interpret and act upon decisively."

Erik Gaston
VP Global and Industries, Tanium

An under-policed crime wave

Returning to our headline statistic that this could be the worst year on record for cybersecurity, let's put some context around the claim. In 2021 alone, cyberattacks increased by 31 percent, including distributed denial of service (+11 percent) and phishing (+36 percent).* Looking ahead, is there anything to suggest an abatement of this worsening trend?

50 percent of retailers taking part in our research say they will spend more on new devices—which translates to more endpoints—over the next financial year. In contrast, just 12 percent forecast fewer devices being added to the fleet of hardware joining company networks. Indeed, only the telecoms industry is more convinced about the proliferation of endpoints with 75 percent expecting to spend more on mobiles, laptops and printers.

Consequently, more three quarters of professionals we surveyed (78 percent) said that they "carry a higher level of accountability" for cyberattacks and data breaches, compared to before the COVID-19 outbreak. Almost two thirds (65 percent) of retailers also claim that their cybersecurity team is struggling to keep up with the volume and variety of cyber attacks. In truth, the burden of responsibility falls on the entire cybersecurity industry to come together and help organisations overcome these threats.

This leads us to an examination of the favoured tools and techniques of the cybersecurity function. Do these teams have the right toolboxes in place to tackle cyber threats and criminals effectively?

As expected, protective measures such as firewalls and antivirus tools are used extensively across all industries, and, in most cases, have been used for a long time. However, some of the more sophisticated techniques for combating bad actors are still not widely adopted.

Almost half of those surveyed (50 percent) said that there's a "lack of software in place" to prevent avoidable cyberattacks. Despite this, security professionals recognise that the solutions exist on the open market. More than two thirds of respondents (68 percent) believe that the evolution of risk analysis tools is "making it easier" for organisations to prevent cyber threats.

Which avoidable incidents are most likely to cause a breach? Retailers say:

#1 Employees clicking on phishing links (68 percent)

#2 Lack of software in place to prevent an attack (50 percent)

#3 Sensitive data being stored incorrectly (47 percent)

Tanium says...

"IT and security teams are fairly confident that their business will invest more in new devices for outlets, offices and employees. But they're equally convinced that they don't have enough staff and software to protect against new cyber attacks.

The scale and nature of threats on enterprises demand that retailers become much more proactive in their approach. IT and security teams say they are more accountable for attacks, since the Covid outbreak, so they need to ensure they have the right tools, processes and funding in place to do what they're being asked to do: protect the business against the loss of customers, productivity and reputation."

Source: TechTarget (15 March 2022)

Final thoughts

Retail is coming through a particularly testing time with the effects of the pandemic and an ever-strengthening compliance landscape. This is placing unique demands on supermarkets and retail chains, in particular, due to their large physical footprint and widely distributed endpoints. The infrastructure supporting this is being tested to the limit and overdue investment to upgrade key systems – including cybersecurity.

The retail sector lives and dies on the basis of the customer experience which demands high levels of data integrity, system uptime and compliance. This makes the work of IT and security professionals all the more important. Our research shows that cyber teams understand the threat landscape and how to manage it effectively, but don't have the resources at hand to prevent the avoidable.

Given that 76 percent of organisations think that the majority of attacks are, indeed, avoidable, firms are clearly paying a high price for being reactive. But it's an expense that senior retail executives are seemingly prepared to write off with the vast majority (92 percent) likely to sign off more budget "when a data breach has happened", not before. To cyber teams this is deeply illogical, but to senior management it's simply a question of dealing with finite resources and a long list of priorities.

Against this backdrop, it's easy to see why many retailers feel that this could be the "worst year" for cybersecurity. But that's too simplistic, too reactionary, and altogether too pessimistic. Forward-thinking IT and security teams will already be acting to upgrade and integrate back-end systems that have been overwhelmed by device proliferation and a growing front-end tech stack.

The good news is that it doesn't necessarily require more tech and more spend to modernise cybersecurity performance. It can mean quite opposite - more rationalisation of the IT estate to lower the overall risk profile. That's an enticing proposition that can unite IT, security and business leaders around a common goal: prevention.

Research recap

300 survey participants from organisations with over 250 employees across banking, finance, education, healthcare, manufacturing, retail and telecoms. 23 percent have a C-suite and/or board level role with 77 percent dedicated to IT and IT security.

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.