Market Insight: Retail Branch Security

Big Challenges; Big Effort; Continued Concerns

Hewlett Packard Enterprise | zynstra

Hewlett Packard Enterprise (HPE) and Zynstra are working together to address the IT needs of the retail branch. Our recent conversations with IT professionals responsible for retail branch office infrastructure have shown a massive focus on retail branch IT security, with many feeling that they are "running to stand still", and that, despite their best efforts, potential security breaches remain a significant concern.

We wanted to understand this trend in more detail and get a view of the challenges and responses to IT security in branch retail in 2017, so we commissioned research to analyse the topic. We surveyed 300 Retail IT managers and C-level executives from the UK and US to better gauge the state of the industry.

Most of the public commentary on security breaches has focused on the issues in the datacenter, and on the individual devices used by employees. But our research suggests that retail branches and their server infrastructure are also subject to significant levels of attacks. And if branch IT is vulnerable, this provides a way in to the total IT estate, with obvious consequences in terms of business continuity and, most importantly, customer confidence. We believe that nothing can impact customer loyalty as much as a lack of confidence that retailers are doing everything they can to keep personal data secure.

"Our research shows that IT teams are responding to security threats, to the best of their ability. Yet despite this, significant threats remain. We believe that this calls for a new approach to retail branch security – one that takes the load off IT teams and increases confidence through the intelligent automation of the processes required to keep distributed branches secure."

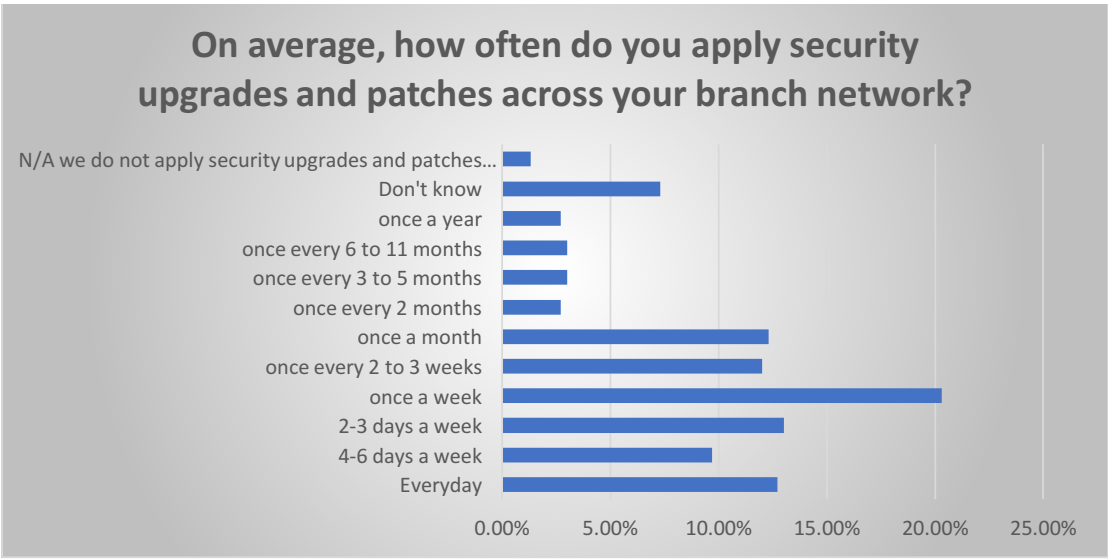
Nick East, CEO, Zynstra.

The branch threat level is high

Firstly, we wanted to assess the scale of security threat retail branches are facing, so we asked Retail IT professionals how often they responded to breaches or attempted breaches of security. The results were startling. Over 45% of retail IT professionals say they respond to security breaches or attempted breaches at least once a week, with the average (mean) number of threats standing at 2.2 per week. In other words, the threat is constant, unrelenting and alarmingly frequent.

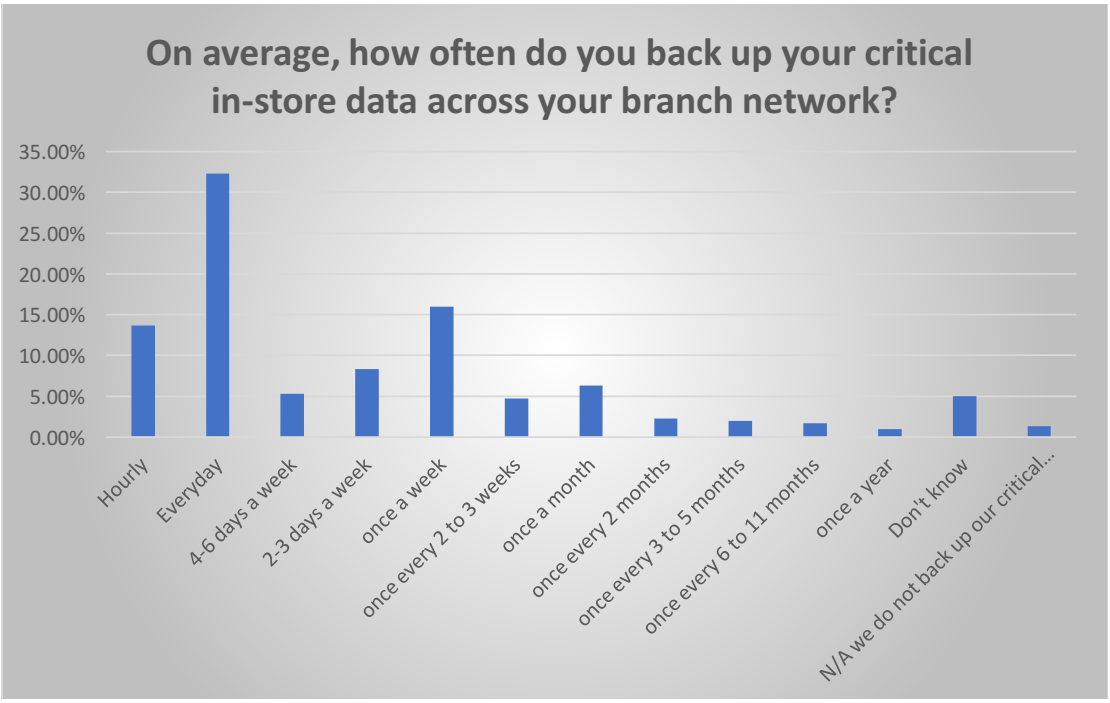
16% of respondents experienced breaches or attempted breaches every day, with the number being even higher at 29% in the Grocery Sector. Other notable retail verticals that said they had to deal with security breaches once a week at the very least were 64.7% of Sports & Outdoor Retailers, 48.5% of Fashion stores, 40% of Department stores and 40% of DIY outlets.

These results show the scale and breadth of attacks across the retail industry. The question for the industry is, perhaps, how long they can cope with this threat level without a fundamental change to the way in which such risks are managed. Are the best efforts of strained IT teams enough when business continuity, revenue, and reputation are subject to this constant and unremitting challenge, or is a new approach required?



IT teams are responding

Our research showed that IT teams are making valiant efforts to respond to the scale of the challenge. 55% of respondents said that they apply security upgrades and patches across their branch network at least once a week, with 12% acting daily, and 77% limiting upgrades and patches to once a month.



This represents a massive workload for IT teams. We all know that keeping software up to date with the latest security patches and upgrades is a real challenge. And this challenge is multiplied significantly when it applies to a distributed, and disparate retail branch estate.

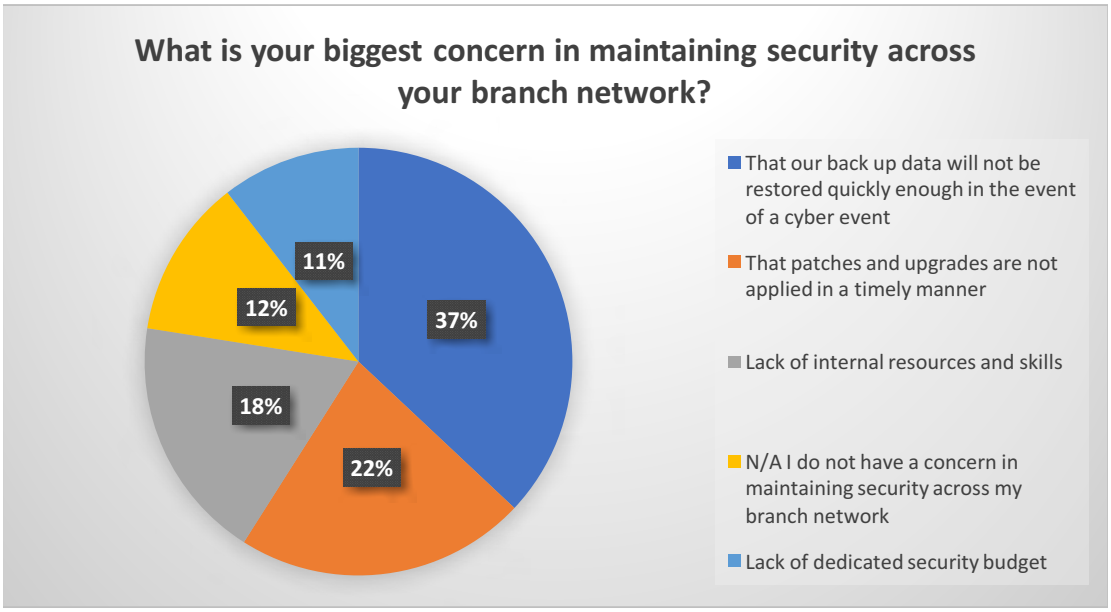
And when it comes to backing up, 46% of respondents back up critical in-store data across their branch network daily, and 75% do it at least once a week.

The pattern is similar across a range of retail industries. 79% of Sports and Outdoor retailers, 70% of Department stores, 69% of DIY outlets and 61% of Grocers reported backing up branch data at least once a week. And, of course, this level of effort is being applied as a protection against ransomware. The more frequently you back up, and the easier you can restore, the quicker you can get back in business.

Both of these pictures highlight the scale of the challenge facing IT teams. In our experience, not only does dealing with this level of threat place great strain on overstretched IT resources, but stops IT efforts being focused on new, revenue-generating business initiatives. If a vast swathe of time is spent dealing with the enemy at the gate, there's little left to build exciting, and creative innovations.

Concerns remain

Despite this workload, only 33% of those we asked stated that they are very confident that their branch network is secure, with confidence highest in the Grocery Sector at 40%, and lowest in Electrical Retailing at 19%. Major concerns expressed were that backup data will not be restored quickly enough in the event of a cyber event (37%), and that patches and upgrades are not applied in a timely manner (22%). So, despite the herculean efforts of IT teams described above, confidence isn't as high as it should be, and the major concerns remain on keeping systems up to date and quickly restoring back up data.



From our conversations with retail IT professionals on both sides of the Atlantic, there is a growing realisation of the scale of the challenge. The traditional in-store infrastructure of PCs, servers and device components assembled over time can present real operational issues. Multiple computing appliances running multiple applications, each with their own operating, management and security system, lead to operational nightmares for the IT team, and raise justifiable concerns over ongoing security, compliance and reliability – in the very location where the revenue rubber hits the road.

If threats are high, resource needs high, and confidence low, then a new approach is needed.

"The retail branch is a unique environment, and the challenges of managing hundreds or thousands of distributed and disparate systems needs fresh thinking."

Nick East, CEO, Zynstra.

A new approach is required

Security threats at the edge, where retailers meet their customers face to face, are high and the compliance requirements onerous. It's our view that the IT industry must respond to the security challenge and deliver retail branch IT that is designed with security at its core; built-in from the ground up, not bolted on. And this needs to be easily and cost effectively applied at scale across hundreds, or thousands of sites. This means it needs to be centrally controlled and – most importantly – automated to lift the IT burden and diminish the human error factor.

Up to 70%* of security breaches occur because systems are not kept up to date with the latest patches and updates. Automation is required to keep branch edge solutions always up to date, secure and compliant. Historically, many retailers have had to put up with frustratingly inefficient processes that rely on the best efforts of their IT team to maintain keep current and security. The way forward is to automate these processes, and drastically reduce the level of human intervention and increase process resilience.

* https://www.itgovernance.co.uk/blog/more-than-70-of-cyber-attacks-exploit-patchable-vulnerabilities/

The Partnership

HPE and Zynstra are working together to transform workplaces across the globe.
If you're interested in moving to a simpler, more agile and cost-effective IT infrastructure **get in touch today.**

About Zynstra

Zynstra is transforming edge computing for retailers. Its intelligent infrastructure is purpose built for the edge, delivering high reliability and managing risk in every store. With Zynstra, powerful automation capabilities centrally manage thousands of distributed sites at a fraction of the cost and enable retailers to launch new store services faster. As a result of a close working relationship and global agreement with Hewlett Packard Enterprise (HPE), Zynstra's virtualization and cloud management software is packaged by HPE as a key part of its new ProLiant Easy Connect portfolio.

Zynstra is backed by Octopus Ventures, one of Europe's leading investors in fast-growth companies, focused on backing unusually talented entrepreneurs.

About the research

In July 2017, HPE and Zynstra commissioned independent research company Censuswide to conduct an online survey of 300 Retail IT managers and C-level professionals. Respondents were drawn from retailers across the US and UK, from companies of all sizes.

For more information on our solutions **click here**

Hewlett Packard Enterprise | zynstra