Information Security at the Heart of the Retail Supply Chain[1]

Authors
Katherine Woods, MSc (Royal Holloway, 2014)
Chez Ciechanowicz, ISG, Royal Holloway

Overview

Distribution centres (DCs) lie at the heart of the retail supply chain. They are a high availability and business critical environment. Any impact to the availability of a DC or the services it provides will reverberate throughout the supply chain and ultimately impact the business. This article discusses particular challenges to secure the retail supply chain and how they may be overcome.

Introduction

The retail industry is changing. Technological advances have facilitated the rise of multi- and omni-channel environments. Traditional visits to a store have been replaced by a growth in online sales, with consumers demanding a seamless shopping experience. This, combined with participation in large trading events, such as Black Friday and Cyber Monday, have seen retail supply chains buckling under the strain.

While the majority of customers believe that their interaction is simply with the retailer, behind the scenes the reality is more complex. Retailers are dependent on a supply chain network of numerous manufacturers and suppliers. There is an ever increasing pressure on the supply chain to maintain high availability of products, a limitless inventory and fast deliveries, as well as free-of-charge returns, while keeping prices low.

To help meet these demands, a number of retailers are investing in automated distribution centres (DCs). DCs lie at the heart of the retail supply chain. Any disruption to their operation will have a knock-on effect upstream and downstream, resulting in potential delays to orders, a loss of sales, reductions in profits and subsequently damage to brand reputation. In recent years a number of such examples have been highlighted in the media.

DCs are a high availability and business critical environment. In an environment of this nature security controls may suffer as a consequence. This places an even greater emphasis on the human factor. People and processes are an important aspect of information security for any industry. However the nature of a DC makes this a particularly interesting and challenging area due to the number and variety of employees and suppliers, the automated systems and the potential threats to which the environment is exposed.

The 2014 Verizon Data Breach Investigation Report (DBIR) found that the main threats to the retail industry were denial of service (DoS) attacks, point of sale (PoS) attacks and web application attacks. Combined, these threats accounted for 74% of recorded security events, with DoS attacks responsible for 33% of incidents. In addition, a rise in sophisticated spear phishing campaigns has

[1] This article is to be published online by Computer Weekly as part of the 2015 Royal Holloway info security thesis series.

seen people increasingly targeted by social engineering as a means to compromise a network. By clicking on a fake link or email attachment a user can unknowingly provide an attacker with a backdoor, used later to gain credentials, perform operations and steal or alter data.

Threat Actors

Cybercriminals / Organised crime: Motivated by financial gain, access to the corporate network may be the ultimate target of an attack on a DC. It contains a wealth of valuable information, including customers' personal identifiable information (PII) and payment card information. Alternative attacks may include a denial of service (DoS) attack against DC systems, with the intention to blackmail; or the compromise of shipping data, in order to track specific containers.

Hacktivist: A hacktivist's motivation is normally reprisal for a moral issue and/or a lack of corporate responsibility. The intention is to cause reputational and operational damage. The 2014 DBIR found activists to be responsible for two thirds of the web application attacks recorded against retailers. Other potential attacks may include altering the integrity of shipping data, causing disruption and blocking shipments to, or products from, certain countries that are involved in a political or moral issue that they oppose.

Skilled hackers: Skilled hackers may be motivated by financial gain and hired by a criminal organisation or hacktivist group. They have expert system knowledge and the ability to identify unpublished vulnerabilities.

Script kiddies: Motivation is not likely to be financial gain. The media coverage following a cyber-attack on a major retailer's DC would provide the desired recognition. Vulnerability exploit kits and malware tools are widely available for their use.

Competitors: Competitors may target an organisation for industrial espionage. There is a wealth of intellectual property within a retail organisation, such as new designs, expansion plans, sales strategies and sales forecasts.

Government agencies: Government agencies are not a likely threat actor in the case of a retail DC. However, if it was deemed to be in the interest of a country to obtain certain information, or disrupt operations, then the capabilities to attack would exist.

Insiders: An insider may act maliciously because they are seeking revenge against their employer. For some of the other actors above, applying for a role as an employee will enable them to access the systems, gather intelligence and/or upload malware. It is also possible that a non-malicious insider may cause unintentional damage due to carelessness, or through a lack of knowledge and suitable training.

A Lack of Traditional IT Security Controls

Attackers will be searching for the weakest link and this may be the very systems used to increase efficiency and productivity. The automated applications and components are managed, operated and monitored by industrial control systems (ICS), most commonly supervisory control data and acquisition (SCADA) systems. ICS components have evolved from industrial engineering technologies. These were designed to be operated as standalone systems, on isolated networks. However, business requirements for access to accurate real time data has led to connected networks. The need for end-to-end automation, as well as remote control and supervision, has led to the integration of a wide range of software and hardware, including mobile devices. The benefits of increased access and mobility are therefore accompanied by new entry points and potential attack pathways.

ICS components have an inherent lack of native security. They do not incorporate modern IT requirements, such as operating system (O/S) hardening, regular patching updates, the use of anti-virus software, secure communication protocols and suitable access controls. This affects their ability to protect themselves against threats and to monitor, alert and report on malicious activity. Although vendors are working to increase the security of ICS protocols and devices, this will take time and years for systems to be swapped out. In the meantime threats against ICS systems are increasing.

The implementation of appropriate technical controls is therefore required to counteract this and to reduce the exposure level. This includes the deployment of access controls as well as the use of devices which provide the capability to monitor, log and generate alerts. Measures to provide network segmentation must also be in place, to ensure that the rest of the retail estate is not exposed.

The Human Factor

> "You can't hold firewalls and intrusion detection systems accountable. You can only hold people accountable" *(Daryl White, Former Chief Information Officer for the US Department of Interior)*

In a high availability environment, if vulnerabilities and risks are not properly understood, this is a risk in itself. Combined with no requirement to adhere to mandatory compliance regulations, this may present an additional challenge when getting the buy-in to both implement and finance information security projects. There is a need for skilled security professionals, with the ability and knowledge to carry out thorough risk reviews and to implement effective security controls and operations, focusing not only on the technology aspects, but also the people and processes.

Although largely automated, humans still have a significant role to play in the running of DCs. These large warehousing facilities are often run by third party suppliers and employ hundreds of permanent, temporary, contract and agency staff. Within the retail industry, there is a high turnover of staff and the DC is no exception, with a large number of temporary staff recruited quickly for peak periods. Many employees are responsible for storing, picking, packing and shipping goods; work which is both labour intensive and pressurised. Within a DC there are a large number of people to manage, each with access to the building and potentially the systems, Wi-Fi

and data.

Security Policies: A process to manage risks and to reduce exposure level

Policies provide employees with a framework and high level guidelines on how to manage information security in different situations. In addition, they may help to reduce an organisation's liability in the case of an incident, or support disciplinary action for non-compliance. It is therefore essential that these documents are written with the users, technology and an organisation's culture in mind. They should be clear, up to date, easy to use and understood by a range of employees with varied abilities. Otherwise they may be mistrusted, less likely to be followed and therefore ineffective. Policies and standards need to be stored in a place that is accessible to all employees. Not all staff within a DC will have regular access to a computer and this should be taken into consideration.

There may be a resistance to following new security policies if employees are poorly motivated in their role, or do not plan to work at an organisation for long, therefore do not see the need to invest in its future. There may be concerns that new processes will have a negative impact on personal targets, or system efficiency and performance. Security processes may also be neglected if deemed not necessary. This may specifically apply to an automated DC environment, where a number of employees/suppliers may have worked with legacy equipment for many years and never witnessed a breach.

Employee Training and Awareness: Understanding roles, responsibilities and security measures

To be effective, the organisation's stance on security and policy guidelines should be reinforced though a training and awareness program, supported by executive management. Employees are often unaware of the risks that they may encounter in their roles and are not adequately armed with the basic skills to mitigate these. Information security is also viewed by many as a technical or specialist area and as more emphasis is put on the individual, some employees may find this a daunting task. Despite this, there remains a lack of information security training in many organisations.

> "The most essential part of any security defence is the human element and staff must be trained to recognise and respond to problems appropriately". (*S. Purser, A practical guide to managing information security, Artech House, Boston, London, 2004)*

Training and awareness campaigns should focus on the current and impending threats, areas that are not working well, or areas that staff are concerned about. To be effective they should include regular updates. This is an ongoing cycle and new policies need to be communicated to suppliers and training materials updated to reflect this. The variety of employees within a DC and their different working patterns may mean that standard training methods and follow-up campaigns are more difficult to organise, leading to an inconsistent approach. It may be beneficial to work with suppliers to identify training requirements and facilitate training. Mandatory training may also be required prior to suppliers being given access to resources and sensitive data.

Supply Chain Security: Maintaining the confidentiality and integrity of data

Within the retail industry, accurate data allows for an increased visibility of demand and leads to a reduction in levels of stock sitting in storage. This creates a need for collaboration and connected networks. Successful supply chains share information, some of which will be highly sensitive, with a number of partners. This exchange of data flows in all directions and is transferred across organisational boundaries via a number of mediums, from paper-based to email, internet interfaces and the integration of cross organisation data streams.

> "Organisations go to great lengths to secure intellectual property and other sensitive information internally, yet when that information is shared across the supply chain, security is only as strong as the weakest link".(*Information Security Forum, Securing the Supply Chain – Executive Summary, 2014).*

A retailer is responsible for managing the movement of information; however their suppliers' ability to protect the data will vary greatly. Although a particular retailer may not be the target of an attack, an attack on one of their suppliers can still impact the availability of the retailer's products and systems, as well as compromise the integrity and confidentiality of their data. Such an attack could have a negative brand impact and most probably result in financial loss. Additionally, suppliers will have their own suppliers and subcontractors with whom they communicate and share information. A retailer has a lack of visibility into these companies, making them an unknown risk to the organisation.

Collaboration: Working with suppliers

Although collaboration is essential, a number of concerns exist: How does the retailer ensure that their data is only being shared with the right people? How do they ensure that this transfer is taking place via a secure method? How do they ensure that their suppliers' suppliers or subcontractors (and their suppliers) have appropriate security controls in place? Reputational damage is not transferrable, but to mitigate the effect of any impact experienced as a result of a supplier failure, legal contracts are essential. In addition, confidentiality agreements are necessary to ensure that any confidential information shared with a supplier, their employees or sub-contractors is subject to the terms of this agreement.

When selecting suppliers, it is not uncommon for the commercial side of a business to dictate the organisations they wish to use. Issues raised by security may be seen as a barrier to business progress, especially where only a limited number of specialised suppliers exist, such as those that offer automation systems. It is questionable how much influence the security team will have if the business wishes to work with a supplier, who is offering state of the art equipment, increased efficiency and a reduction in costs. In addition, if selected by the business, how effective will the security team be in enforcing policy requirements on this supplier, if they are not stated upfront in the initial agreement/contract?

A retailer needs to be confident that their chosen suppliers are following recognised information security best practice and that their security policies are being effectively communicated to and followed by their staff. Without security involvement from the outset, there is a danger that any security issues raised later may be signed off as a business risk by someone who does not fully understand the risks to which they are exposing their organisation. Involving security during the selection process empowers the business to better understand the role of security and feel

confident that their chosen supplier will meet the business needs, as well as reducing the risk of retrospective controls needing to be incorporated to address security deficiencies.

Supplier assessments may be used to assess the suitability of each new or existing supplier. Answers to specific questions, accompanied by supporting documentation, provide an understanding of the service provided, the supplier's security posture and the controls they have in place to protect data. This process also enables any vulnerabilities or risks to be identified and addressed. Aligning controls to a recognised industry management standard such as ISO27001 will provide insight into a number of security areas within the supplier organisation.

Two key areas covered by the standard are Human Resources (HR) and Business Continuity Planning. HR is especially of interest due to the sheer number and variety of employees on site at a DC and the quick turnaround of temporary staff. Details regarding HR processes will identify whether new hire background checks are taking place and also what security processes exist for when staff join, move roles, or leave the organisation. Business continuity planning is another key area; suppliers should be able to demonstrate that they have contingency plans in place to maintain their service in the event of a disaster or a breach. Without appropriate plans in place, events will have a far greater impact on the speed at which a DC can get up and running again in the aftermath of a security incident or attack.

Conclusion

It is anticipated that more retailers will invest in automated distribution centres to help meet their demands. These may range from fully owned DCs, to outsourced and even shared facilities. They may include a range of new technologies, such as those to enhance data access and remote management, each aspect introducing a host of new variables for consideration. Any impact to the availability of a DC, or the services it provides will reverberate throughout the supply chain and ultimately impact the business.

Within a DC, the combination of legacy systems and modern business requirements has created new vulnerabilities and attack pathways ready to be exploited. Although largely automated, humans still have a significant role to play in the running of a DC and the number, variety and turnover of staff creates extra challenges. In addition, the importance of supplier risk management has been emphasised by recent attacks, which highlight the potential weaknesses of the retail supply chain.

When threats, vulnerabilities and risks are not properly understood and managed, this is a risk in itself. Information security within a DC environment requires experience in the challenges of ICS systems, as well as the ability to review processes and operations from a personnel point of view. Only by combining these can thorough risk reviews and mitigation strategies be provided.

Biographies

Katherine Woods is an Information Security Consultant at Verizon Enterprise Solutions, focusing on Governance, Risk and Compliance. She has a BSc (Hons) in Psychology, 2002 and an MSc in Information Security, 2014, both obtained from Royal Holloway, University of London.

Chez Ciechanowicz received his PhD in Pure Mathematics in 1980. He then worked at the NPL specialising in compiler validation and in digital signatures. From 84 to 89 he lectured in the Computer Science Department of Royal Holloway. From 89 to 96 he was a consultant at Zergo focussing on risk

analysis. He was editor of the Elsevier Information Security Technical Report for 10 years. He was a founding member of the BCS ISEB Information Security Management Certificate Board. He returned to Royal Holloway in 96 as Programme Director of the Information Security MSc. At Royal Holloway he has performed high profile consultancy assignments for TfL's Oyster Card, the Dutch Government's OV-Chipkaart, and the ITSO scheme.