Scientific Publications

Universal Journal of Computer Sciences and Communications, 2019, 1, 1253
www.scipublications.com/journal/index.php/ujcsc
DOI: 10.31586/ujcsc.2019.1253

Review Article

A Comprehensive Study of Proactive Cybersecurity Models in Cloud-Driven Retail Technology Architectures

Chandrashekar Pandugula [1*], Zakera Yasmeen[2]

[1] Big Data Engineer, USA

[2] Big Data Support Engineer, USA

*Correspondence: Chandrashekar Pandugula (chandrashekar.pandugula.de@gmail.com)

Abstract: This is a comprehensive, multi-year study designed to explore proactive security technologies implemented in cloud-driven retail technology architectures. Deploying cloud technologies in the retail environment creates a need for more comprehensive and proactive security technologies that protect both the psychological estate and fiscal estate. This work contributes to cloud-driven retail research by investigating anticipatory security technologies across numerous case studies. These case studies offer best practice models for elevating proactive cybersecurity in retail environments. The academic and professional communities currently lack security information and practices that apply to the retail environment. It is anticipated that the final results of this project will have value in shaping the next set of research in cybersecurity in retail environments. Many retail organizations are restricted to reactive security operations. Advanced security technologies operate on piloted activations that require the intervention of security analysts. In actuality, basic security products and security operations are now piloted by automation and machine learning. In one case study, a retail CTO shares a forensics example using a proactive security technology aimed at both psychological estate and fiscal estate. In another case study, direct discussions provide a retail university lecturer with insight into the use of driven intelligence for inventory management. The use of card technology for a model is used as an example that can be implemented as security technology which can be offered as a service to retail organizations.

Keywords: Proactive Security Technologies, Cloud-Driven Retail, Retail Technology Architectures, Anticipatory Security, Case Studies, Best Practice Models, Proactive Cybersecurity, Retail Environments, Security Information, Reactive Security Operations, Advanced Security Technologies, Security Automation, Machine Learning, Retail CTO Forensics, Psychological Estate, Fiscal Estate, Driven Intelligence, Inventory Management, Card Technology, Security-as-a-Service

How to cite this paper: Pandugula, C., & Yasmeen, Z. (2019). A Comprehensive Study of Proactive Cybersecurity Models in Cloud-Driven Retail Technology Architectures. *Universal Journal of Computer Sciences and Communications*, *1*(1), 1253. Retrieved from https://www.scipublications.com/journal/index.php/ujcsc/article/view/1253

Received: October 16, 2019
Revised: November 23, 2019
Accepted: December 17, 2019
Published: December 27, 2019

1. Introduction

Currently, retail enterprises operating in several countries are heavily dependent on technology and prefer to avail themselves of cloud service models. Every single large and small event in the retail technology environment is captured, consolidated, categorized, analyzed, and stored in the cloud to enhance a customer's experience by personalizing products and services to analyze demand-based data. Each piece of event data posted in the cloud increases its storage; thus, the need for scalable cloud computing solutions is present in retail, offering better performance at lower expense. For the computational needs of various sizes of retail enterprises, organizations are shifting towards the efficient and cost-effective use of an integrated cloud-computing environment. As cloud computing solutions are rapidly growing and show an intrinsic appeal for retailers, they have grown in astronomical proportions. There is a standardized approach in cloud technology for more than 75% of world retailing organizations that they have adopted.

With the exponential increase in digital retail activities comes the challenge associated with the security of these technologies. As cloud computing technologies are growing in complexity, the difficulty in accurately managing cybersecurity is increasing. A retail technology environment possesses a large attack surface and is besieged by many potential threats. In various computing environments, to some extent, cloud users bear some level of security responsibility.

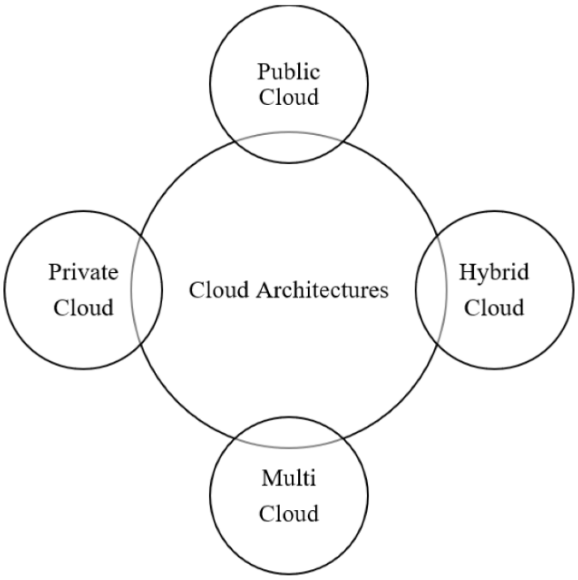

Figure 1. Cyber Security in IoT-Based Cloud Computing.

Cloud technology comes with shared responsibility when it comes to security practices. Organizations should adopt proactive, pragmatic, precise, and coherent protection strategies and practices in retail environments that are in sync with their business aims and threat assessment. A proactive cybersecurity component is missing in the retail and cloud business domain. As a result, the adaptive-tolerant cybersecurity weakness will increase the susceptibility and exploitability of the retail ecosystem. In the cloud environment, a one-size-fits-all security mechanism doesn't ensure complete security. The main objectives are to investigate how cloud-driven world-class retail organizations are currently protecting their applications, data, and other assets; additionally, to propose improvements to current security application practices in different areas of the retail world.

Equation 1: Proactive Cybersecurity Efficiency (PCE):

$$PCE = \frac{(D + R + A)}{T}$$

where:

D = Detection speed of threats

R = Response effectiveness

A = Automation of threat mitigation

T = Total system latency

1.1. Background and Rationale

Background Retail has changed; a once simple trade of goods for money is now a sophisticated series of interactions engineered to extract the maximum value per customer engagement opportunity. As cloud computing matured, it arrived at retail organizations, driving new and evolving trading opportunities that encompass new business models such as subscription-based consumption and the ever-narrowing circle of social media-powered engagement. These novel trading opportunities come with an intrinsic aggravation of new cyber threats that retailers must seek to mitigate or defend themselves against.

Background and Rationale Consumers have more money than time; they also have a multitude of options to choose from when allocating the former to the causes that are important to them. With these thoughts, many retailers are enjoying a boom of possibilities; they have the potential to move large customer markets towards their products and services from previously unknown or untapped sources with a single campaign. The irony, however, is that by doing so, they are also tapping into large databases of potential personal and financial information - cherry-flavored cyber bait that is now within snuffling reach of threat actors [1].

This following assertion may sound like gratuitous fear; however, answers can be found with a simple query in any public database: Retail cybersecurity is in dangerous abeyance. A historical lack of effective regulation to encourage the hardening of security mechanisms known collectively as "compliance" has caused a widespread conflagration of retail data breaches. At the time of writing, this extends to over 90 breaches involving organizations such as Sears, Adidas, Saks, Lord and Taylor, Macy's, and Under Armour, in addition to examples such as the female period subscription service and working in tangent. Many of these attacks lived inside the IT architecture of the retailers' cloud estate for several months, undetected, before discovery, posing a distinct security threat to large customer databases and associated organizational infrastructure. In the face of regulatory numbness, the only solution is proactivity; in the context of the cybersecurity threat landscape, this has created the theoretical context for this research. The stable document on cloud security explains, "Cloud computing has the same threats as traditional IT environments, but their responses are different." This means that the opportunity to be breached exists in the long list of technical configurations, data and applications, and subcomponents that together create the "cloud" approach.

1.2. Research Objectives

Retail cybersecurity has traditionally been a concern in most early-phase papers, working papers, studies, and industry practices with after-the-fact attack models. However, as discussed in the previous section, there is an ever-increasing consensus that cybersecurity ought to be proactive in its strategies, especially in sectors where the damage from a single large breach might cripple any company, causing serious economic disruption not only to such an entity but to that entity's entire operating ecosystem. Leading the urgency of the notion of a necessity for proactive cybersecurity are findings indicating the force of denial of inventory attacks, with reports indicating that 580 such attacks were first researched in 2016 and 800 were similarly first observed in 2017. The value of studying attacks that have just emerged is useful in proactively analyzing future vulnerabilities that might be exploited in the same way or exactly as perhaps in a similar entwined component's supply chain, as often occurs in retail.

This full research paper accordingly identifies retail's unique threats and its technology environment, lays out in a literature review how those have been addressed so far in the existing technical and behavioral research literature, and projects findings and insights into both academic critique and retail executive approaches to organizing these infrastructures and implications for infrastructural design. Our project here accordingly presents two essential objectives: First, to ascertain the ERM apps, we interview and survey 170 executives who make decisions about ERM at 87 companies in these infrastructural ecosystems. Second, we aim theoretically to critique the current academic and managerial emphasis on ERM and compliance activity. Our research findings show that cybersecurity is increasingly seen not as an issue that the firm needs skilled individuals to manage for threats that the executives see as having unpredictable evolutionary elements.

2. Cloud-Driven Retail Technology Architectures

The emerging trend of adopting cloud-driven technology infrastructures has revolutionized the retail sector. With the novel offerings, retailers experience an efficient optimization of their resources without acquisition and maintenance costs and have to pay only for utilized resources. For example, cloud computing can provide a scalable e-commerce architecture that can manage heavy traffic when a retailer offers cost-saving deals to customers. Apart from this, Big Data brings new commercial insights into the retail sector to understand consumer preferences through their activities online and the geographical distribution of customers. Cloud computing, as a service delivery platform, has facilitated the integration of advanced retail technologies such as radio frequency identification, sensors, and handheld devices in the form of mobile apps and social network apps, further fueling customer engagement to a large extent. The architecture of cloud-based retail systems discusses multi-tier system architecture, including customers, organization services, partner services, ERP tier, software and hardware services, and facilities. Business benefits of cloud-based retail systems include enhanced customer engagement, simplified supply chain systems, reduced cost of ownership services, redundancy services, and data; online sales and marketing trend management; automated organization management; and integration of web, partner, and organization services through the integration tier.

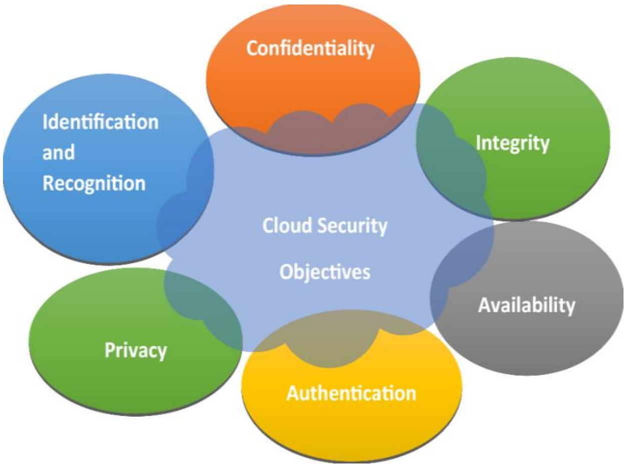

Figure 2. Securing data and preserving privacy in cloud IoT-based technologies

The emerging retail technology infrastructures managed by cloud service providers provide retail services by using an array of services, ranging from Infrastructure as a Service to Software as a Service. Cloud service providers use the essence of inter-cloud, multi-clouds, and federation clouds for merging infrastructures, resources, and services, and for creating an advanced technology retail architecture. Cloud service providers being integrated and utilizing multi-tier technology systems provide online and social network applications of commercially designed IoT-enabled retail services. Besides the retained cloud services of IaaS, PaaS, and SaaS, in the cloud-driven retail architecture, the software as a platform service provides resources for running the software at the application layer offered as per industry needs. Often, such services are used to operate the software, run scripted applications, share platform information in Enterprise 2.0 formats, offer platform-hosted services, and bill directly for application usage. Integration of cloud services includes those services provided by the retailer from the application as a service layer [2].

2.1. Overview of Cloud Computing in Retail

The growing use of cloud solutions by retailers helps to build extensive business analytics to acquire a better understanding of customer preferences and behavior. The data collected is then analyzed to help provide operational advice to clients, predict trends, and improve customer satisfaction. At the most basic level, cloud technology significantly reduces costs by allowing retailers to trade capital investments for operating costs, while at the same time only paying for actual usage. Availability and instant scalability are particularly interesting due to agility in the retail sector, where there are frequent and unpredictable peaks in orders. Customers are also drawn by the promise associated with omnichannel retail. In the realm of omnichannel retail, processes intended to deliver a consistent shopping experience, whether in-store or online, across a variety of connected devices are more important than the products purchased themselves. The omnichannel approach has become a necessity given that a significant number of customers use multiple devices when shopping, while a large percentage expect in-store prices to be as low as online, and many expect that they will be lower. Nevertheless, there are still some outstanding issues with the mainframe systems in which cloud technology is used. E-commerce can now consistently share large files between different cloud-based systems, control and view data, and execute the required tasks on cloud servers, providing more rapid and cost-effective interaction across the board.

2.2. Key Components and Features of Retail Technology Architectures

Retail technology architectures require the latest technology components that have emerged as essential tools for business operations. The integration of these components has enabled features such as tool portability, interoperability, and plug-and-play for the successive expansion and acquisition of new and advanced business systems. In today's progress, any institution that wants to succeed in the retail trade must integrate state-of-the-art components into its infrastructure. Sales or point-of-sale systems are designed to capture customer transactions and aid in large amounts of checkouts. POS systems come with a variety of features, including a customer display, cash drawer, receipt printer, barcode scanner, and more. Inventory management is another key area for any retail business where businesses track items from manufacturer to warehouse to store and finally to the point of sale.

Another key facet is customer relationship management systems that allow businesses to develop relationships with their customers - previous, current, and potential - more effectively. Powerful in-store CRMs enable sales associates to create agents and customers on behalf of loyalty programs, access receipt and preference information of check customers, register customers for events and product seminars, and provide alerts to others. At the same time, web-based in-store orders can be presented in a consolidated view by a single agent, graphically identify the client's merchandise assortment, and ensure accurate pricing and preparation for deliveries. Intelligent payment and checkout systems are deployed in stores that leverage AI to enhance consumer buying processes. The implementation of the decentralized, hybrid store will expand the currently deployed cloud-driven retail ecosystem uniformly. Machine learning and AI are employed to get accurate predictive data regarding transactions and customer demands. They play an important role in avoiding customer dissatisfaction, reducing inventory, and making real-time business judgments. Real-time processing and analysis of large volumes of complex data, such as transactions, customer information, and products, can produce efficient and helpful business outcomes.

Application Programming Interfaces have been used to provide interfaces that connect to existing hardware, rather than rewriting specialized and platform-specific drivers that run the peripherals. Thus, the use of APIs would ensure backward compatibility for extension and acquisition in any modular POS device. The customdeveloped components are plug-and-play for current and future POS devices, such as printers and displays, and the entire process is plug-and-play. The current method for component devices is a step to prevent downtime for POS devices running on common operating systems. To sum up, the above technological capabilities have integrated different retail sectors and are harnessing the benefits. The discussion clearly shows how different facilities could be used to offer a competitive advantage in the retail sector. The careful understanding of these technologies also clears the use of advanced threat models at every stage. The advancements are towards offering a secure environment by integrating networked and embedded systems for optimizing different services deployed across the different retail sectors.

3. Cybersecurity in Retail Technology

Retail technology environments facilitate transactions between vendors and customers. The digital currency and sensitive information processed by these systems pose unique security concerns; every time a payment is processed or consumer information is exchanged, vital data becomes susceptible to cyber threats. As a result, partners and clients of cloud service providers have feelings of unease regarding full cloud migration. Increased menu selections of cloud-driven technologies heighten the chances of data insecurity and call for robust defense methods to retain customer and system trust. The regular exposure of personal and payment information, session IDs, analytics, and any other data passed to cyber attackers is as constant as the danger arising from consumer and staff comfort through the internet. Detrimental consequences typically entail litigation from banking institutions, customer retaliation, and sometimes the closure of retail companies.

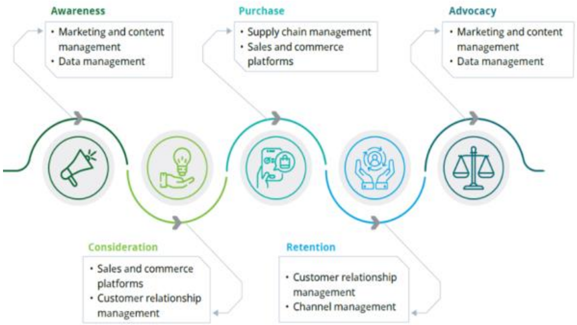
Awareness
• Marketing and content management
• Data management
Purchase
• Supply chain management
• Sales and commerce platforms
Advocacy
• Marketing and content management
• Data management
Consideration
• Sales and commerce platforms
• Customer relationship management
Retention
• Customer relationship management
• Channel management

Figure 3. Transforming Retail Through Technology

In the retail technology business, the protection of personal data is monitored by guidelines and rules to follow. In the U.S., many retailers have implemented compliance requirements from data security standards, as well as individual state laws that require businesses to report unauthorized access to personal information. In Europe, regulations further extend the management and protection of individuals' personal information. In Australia, laws enforce numerous safety requirements that companies must meet or face penalties. To sum up, the e-commerce sector represents a significant proportion of global cyber threats. These attackers exploit financial motivation, impersonation of legitimate retailers, blackmail and fraud, imposition of insider threats, credit card compromises, identity theft, and others. Cyber threats are common across most retail and e-commerce (online and offline) companies and vary across businesses of different sizes. Within e-commerce and e-business organizations, cyber threats include the interception of sensitive customer and transaction data; the trading of stolen payment card data; phishing scams, malware, and spyware; ransomware and denial of service attacks; and more. Phishing and card skimmers have had a significant impact on the retail business.

3.1. Importance of Cybersecurity in Retail

The retail sector currently relies extensively on technology to manage sales, inventory, and customer relationship databases. Due to the widespread use of skills and technological know-how, it is a viable avenue for cyberattacks to jeopardize customer accounts. A direct consumer account belonging to a major retailer can be used to harvest large quantities of personally identifiable information in one place. The results of a breach within this industry can lead to enormous financial penalties and litigation costs if a company has breached a law to protect its customers' rights. A significant percentage of all suspicious cyber incidents were related to espionage or spyware, most likely instances of state-backed attackers.

The retail sector also bears the financial brunt of both ransomware and distributed denial of service attacks, such as downtime and costs to alleviate these issues. Companies that have faced ransomware attacks in the retail sector witnessed a significant increase in necessary downtime. However, this sector is likely to attract more cybersecurity threats as its digital infrastructure rapidly develops. To protect customer and company information, cybersecurity measures are continuously developing. They are being developed in the form of antivirus and malware programs. In the digital world, retailers may also protect technology on a wider basis by continuously educating their employees. National agencies have developed guidelines for establishing a solid cybersecurity culture. The retail sector is also particularly vulnerable to cyber threats. Retailers typically manage inventories, workplace information, customer databases, invoicing details, and payroll among other customer data. Some statistics show that a supermarket operator will normally lose tens of thousands of dollars a minute in the middle of the day if systems are down. This can swell to hundreds of thousands by contractor agreements and additional personnel required [3].

3.2. Common Cybersecurity Threats in Retail

Retailers are traditionally targeted by attackers because the potential gains are higher, as well as the fact that transactions occur online, which can amplify attacks. The most common attack vector is phishing – attackers have consistently utilized phishing attacks to target customers’ personally identifiable information (PII) by capturing bank account details, credentials, and passwords from customers. Another attack vector is malware, which is used to gain unauthorized access to computer systems to steal or corrupt customer details. An additional threat vector used against retail systems is distributed denial-of-service (DDoS) attacks, especially as a diversionary tactic. These attacks are utilized to distract IT and security staff from the main target of the attacker’s activities occurring on the system. DDoS attacks disrupt network traffic by dominating the network with a large amount of internet traffic, so user requests cannot get through, which can cause system outages and thereby prevent customers from purchasing goods or services.

Retailer networks are also attractive to attackers because they generally lack robust security practices or efforts and have in essence the posture of “soft targets.” The retail sector, as a result, is subjected to a high rate of computer breaches. The greatest concern with retail security is that customer financial information is the actual target for attackers. The storing of customer login credentials, personally identifiable information, and financial information is prevalent at many retailers. A data breach at a retailer can be very expensive and can be large, impacting thousands to millions of customers. A major security breach also can harm the company’s reputation and stock value. Retailers are responsible for the scrutiny of customer and business data due to local, national, and international data privacy laws. Some of the most damaging retail security breaches have further highlighted security issues and have had a chilling effect on e-commerce by driving consumers away from internet purchases. Major retail incidents include breaches at various points of sale and payment systems, which resulted in the loss of millions of customer payment card details. This, in turn, led to a significant drop in stock value.

Equation 2: Threat Prevention Index (TPI):

$$TPI = \frac{(S \times P)}{V}$$

where:

S = Security infrastructure strength

P = Proactive threat prevention measures

V = Vulnerability exposure reduction

4. Proactive Cybersecurity Models

The proactive architecture, which will be specialized for the retail sector and is also expressed as zero trust-based models, is at the center of interest in terms of PSU. Proactive cybersecurity has a unique approach that distinguishes it from reactive approaches. While traditional cybersecurity methods were based on reactions to threats, the fundamental idea of zero trust-based, bluntly proactive approaches is rooted in the prediction and prevention of threats. To paraphrase, proactivity means having plans, methods, and approaches designed for the anticipation of threats before they occur and preventing them from the beginning [4].

A strong risk assessment and evaluation are extremely important to address the traditional reactive cyber capabilities of the retail sector, with the increasingly digitized retail sector and even the highly digitalized cloud-driven retail technologies. For adaptive, modern, and up-to-date solutions, zero trust-based proactive architecture that the digitalized cloud drives should embody could offer the following main advantages to the business: First of all, a high level of security posture can be offered to the resources used in the cloud, and critical data is continuously safeguarded in the face of threats. Employee training on how these models would be defined, the crisis and scenario methods that could be brought to the fore before an incident occurs, and the resources and resource sacrifices that might receive the attack should be scheduled within the institution.

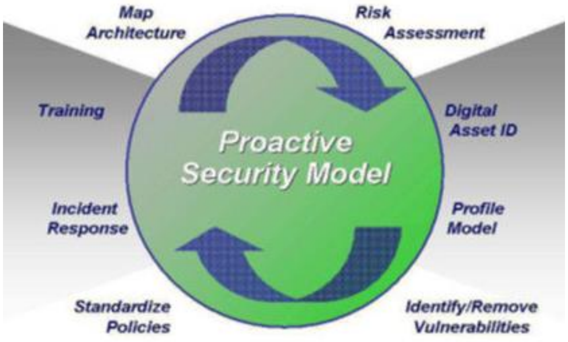

Figure 4. Proactive security models

4.1. Definition and Principles of Proactive Cybersecurity

In simple terms, when taking a proactive approach, an action is performed in anticipation of a future threat or potential incident that could occur. Time is invested in recognizing incoming threats so that responses are not initiated from scratch when an incident or potential disaster approaches. Recognizing, identifying, or preventing a security incident or privacy violation just before the incident occurs is the best practice to deliver more networking availability and reduce the value of risk. A proactive security control management process includes three main principles. First, proactive cybersecurity includes continuous risk assessment, fueled by an open-minded and consultancy-based business engagement attitude. In translating risk findings into tangible impacts, a clear business discussion about agreed-on decisions is necessary. Second, the principles of a proactive approach include investing in secure technologies and creating good security hygiene or practices. It ensures high resilience, but all practices are utterly meaningless if they are not perfectly performed. This is where the skill and awareness of a human cyberdefender come into play. Finally, threat intelligence plays an enormous role. It is a key asset that can magnify and enable other proactive controls to function more effectively. Companies should not rely entirely on their devices and appliances to update and scan traffic with new threat intelligence, specifically if the threat is tailor-made to escape detection. It can take weeks or months for firewalls and anti-malware systems to be updated; humans should, therefore, have a better chance of receiving news faster and sharing it back with the community. In consumer retail contexts, security practitioners adopt the reactive model traditionally. By preventing incidents from occurring, proactive models shift the focus to security. It places a strong emphasis on recognizing and avoiding disturbances or weak points until they are exploited. A proactive model reduces the amount of time, money, and effort invested in comparing models after attackers have already made their move. In addition, security efforts tend to have a wider influence when following proactive policies. To implement a proactive security model, businesses have a responsibility to expand their knowledge and abilities. This duty does not definitively extend to knowledge, but it covers other existing technologies or services that can better prevent attacks. One of the higher-tier rules is having a way to get advice from a cybersecurity specialist to fill in the skill gaps if anything is unclear. Provided appropriate access to current security best practices, a business can take pride in its duty to diligently gain insight. Whether a company generates security-related information or infrastructures through third-party commercial cybersecurity advisors, the business can take a stand and take proper measures to safeguard those offerings. Businesses are also more successful if they exchange security data and threats with peers. Cybersecurity experts can provide a new business with the latest news and information on potential threats collected from various enterprises. By sharing their experiences and estimating the probable damage of threats, they should work together with those companies to come up with a plan to approach the threat if it has already shown up. These are the four paradigms of essential security principles for trains. These paradigms are anticipated to provide a holistic, realistic, and relevant analysis of emerging technologies. Shifting approaches to active hazards, performing risk assessments at all overlaps, and active monitoring can be a crucial attack mentality. There is a new, viable option for widespread retail protection in the future. The proposed mechanism depends on this. To stop malicious commands and obviate adverse activities, it visually examines artificial intelligence anomalies in retail business data that prompt a supervisor's method.

4.2. Benefits of Proactive Cybersecurity in Retail

Ensuring the security of personally identifiable information (PII) can result in substantial competitive advantages. Modern consumers prefer to engage with retailers that they trust and that can show they are trustworthy. To foster this trust, retailers must be seen as taking every precaution to protect customers and record their sensitive data. By implementing proactive cybersecurity measures, they can demonstrate that they are safeguarding their customers' data to the best of their ability. This, in turn, results in brand loyalty. Forecasts indicate that worldwide cyber incidents may cost retailers significantly. Given that threat actors often target retailers for their large customer databases, reducing the number of incidents is a solid step towards preventing those potential costs. Research also shows that proactive cybersecurity measures could result in a savings rate much higher than investing in reactive cybersecurity measures about potential losses.

Retail businesses are required to comply with a variety of federal, state, and even local regulations and laws. Proactive cybersecurity measures can ensure compliance with many of these laws and regulations by making them an integrated part of operations. A proactive cybersecurity model will enable the quickest response to and prevention of unusual behaviors or activities associated with new threats. By adopting proactive cybersecurity measures, the organization will establish a more secure technological playing field internally and externally, resulting in a more resilient retail ecosystem. In addition to the above-mentioned strategic imperatives, a proactive cybersecurity model will have cultural benefits. It will promote good security habits among staff by increasing employee understanding of the dangers of not proactively practicing cybersecurity. As a result, the proactive implementation of cybersecurity within the retail ecosystem leads to increased organizational infrastructure security. This, in turn, fosters robust consumer and investor confidence in the underlying technology processes.

5. Case Studies and Best Practices

This section provides an analysis of reports and case studies produced by leading Internet security vendors and combines this analysis with a best practices survey of retail to provide some current case studies of retailers actively trying to protect their computer networks to give real-world examples of how retailers are currently addressing these issues. As such, the aim is to offer commentary on retailers' efforts with a view to inspiring confidence and innovation in retail about intruders and protection measures. The report draws on several vendor sources that provided discussion articles based on survey interviews in these publications.

This section will present the significant findings of any reports considered in the results of previous reviews, and case studies, an outline of common findings and practices, and final considerations or conclusions. A problem of scale: The message is clear. These best practices show the effectiveness of proactive security and great promise but also illustrate some of the challenges facing retailers. Larger retail organizations with large staffs of security specialists, particularly in the US, have higher budgets and organizational maturity and resilience to be able to proactively mitigate threats. The following sections provide details from the results of industry reports and survey materials that were examined. Each section includes the pertinent practices exhibited by visionary retailers.

5.1. Real-World Examples of Proactive Cybersecurity Implementation in Retail

Walmart Standardizes Cloud Security Strategy - Utilizing a dedicated cloud security hub, Walmart employs a multitude of tactics to prevent, detect, and combat data breaches and cybersecurity threats. Their cybersecurity hub actively scans for potential threats or issues and performs thousands of tests to uncover vulnerabilities in systems and software that would encourage unwanted attention. Walmart also uses both physical and virtual firewalls to create layers of protection throughout the network, continuously monitors for any malicious behavior from vendors, and has an incident response team on standby to manage and minimize the impact of any attempted cyber attack.

The Gap Adds Cybersecurity to In-Store Experience - For stores utilizing networks for applications and services like online order collection, categorized as a store of the future, robust cybersecurity becomes an essential integration. The Gap has achieved this through installing distributed denial of service shields, along with malware and antivirus software on in-store servers to safeguard customer and employee data. As with Walmart, a dedicated team is in place to respond to any cybersecurity threats, and employees are part of the cybersecurity solution at The Gap, where staff are trained to spot a potential phishing email. Employees who successfully identify a scam email are then rewarded with a cash bonus [5].

The Home Depot Prevents Point-of-Sale Captures - Only in cybersecurity for the past 7-8 years, The Home Depot has begun to prioritize information security following breaches in recent years that affected millions of customers. Striking a balance between security and functionality, the retailer has designed a PCI DSS environment: a collection of secure computing, storage, and networking components capable of preventing Point-of-Sale terminals from being hijacked. This environment has facilitated the creation of a secure mainframe, helping to target the deduction of vulnerabilities and assisting in preventing cyber attackers from moving laterally across Home Depot's systems.

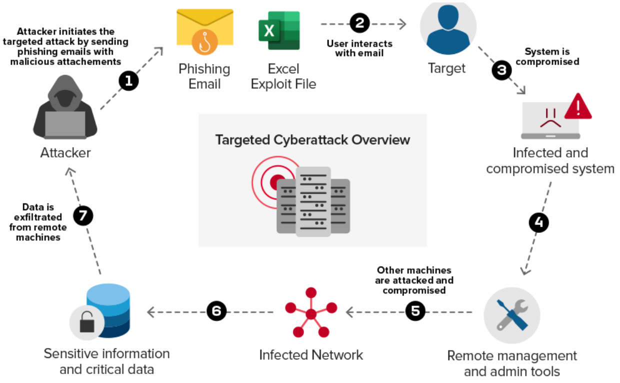
Attacker initiates the targeted attack by sending phishing emails with malicious attachements
1
Phishing Email
Excel Exploit File
2
User interacts with email
Target
3
System is compromised
Attacker
Targeted Cyberattack Overview
Infected and compromised system
4
Data is exfiltrated from remote machines
7
Other machines are attacked and compromised
5
6
Sensitive information and critical data
Infected Network
Remote management and admin tools

Figure 5. Proactive Cybersecurity Overview

6. Conclusion

In this paper, we analyzed a proactive cybersecurity model in the context of the cloud-driven retail technology architecture. Key findings of the study imply that proactive cybersecurity models within the retail architecture are essential for the enhancement of better security, which can control and minimize any potential risks against a complex set of cyber threats. Findings also revealed that no security model system in use can proactively secure the cloud-driven retail technology architecture, as this space has received comparatively little attention and has not been explored before. The innovation and complexity of IT service provisioning within a dynamic environment, together with the increasing threats, trends, and vulnerabilities found in cyber issues, make this area highly sophisticated. The integration of retail technology together with cybersecurity issues will be evident in shaping the future of retail operations and business as a whole. This study is original in comparison to other cybersecurity studies in artificial intelligence, anomaly detection, and deep learning—primarily because this study is based on cloud-driven retail technologies.

Overall, one of the main goals of cyber risk management practice is to avoid or minimize disruptions to supply chain activities and interruptions in the delivery of goods and services and their timely delivery to the end users. Cyber theory offers critical contributions to a better understanding of cybersecurity, the use of external event and threat information, and external attribution of the economic effects of cyber risk and security. Retail cybersecurity focuses on maintaining suitable governance, risk management, and compliance processes, including thorough planning, establishment, documentation, communication, monitoring, review, and audits. Moreover, although the proactive cybersecurity model as presented in this study provides a comprehensive perspective on cybersecurity for the future of retail architecture, more research studies are needed to adapt and extend the model system from other cloud-driven architecture points of view for further comparison with the retail sector as a whole. It is anticipated that more businesses in cloud-driven sectors, dominated by the retail chain environment, could evaluate and find this solution as a starting point in their endeavor to secure the overall operations and services provided to the end users. Overall, the capabilities within the conceptual proactive model ensure that security controls become more predictive, thus eliminating security breaches before they occur and thereby reducing both the cost and complexity of operations.

Equation 3: Cyber Resilience Score (CRS):

$$CRS = \frac{(M \times A)}{L}$$

where:

M = Monitoring system robustness

A = Automation level in threat handling

L = Latency in threat detection and response

6.1. Summary of Key Findings

Executive and Assisting Director. The research findings in this study point to the fact that, traditionally, cybersecurity has often been a reactive measure; organizations are solving or preventing one problem at a time. Organizations are waking up to the fact that an appropriate risk management approach is not merely designed to reduce the likelihood and magnitude of future incidents but also enhances business performance and trust in, and reliance on, networks. We found that a proactive approach to cybersecurity is associated with improved security postures. This is illustrated by the increasing use of risk assessments, of which 82% of organizations carry these out at least once a year. These agencies also use real-time or continuous monitoring of the security of their systems. A statistically significant upward trend in the number of organizations that have largely converted to real-time continuous monitoring may also be observed. These strategies are coupled with a cultural push inside the organization to encourage a culture of security. Up to 94% of security leaders feel that their staff understands the importance of cybersecurity.

We have concluded that proactive cybersecurity is largely associated with preventing and reducing incidents in an organization. These range from high-level outcomes, such as a reduction in priority incidents, to longer-term benefits such as improved compliance. In our case studies, one respondent estimated that he had reduced the number of incidents faced annually by 20%, which statistically has a large effect on outcomes. Moreover, 38% of organizations in our survey noticed improved public trust flowing from active brand protection and 35% noticed increased digital services from their security operations. On top of this, new processes have been implemented across preventive organizations. For instance, risk assessments and continuous monitoring are likely to lead to improved patch management, the data on which was largely collected in this study. Finally, organizations are taking high-insight approaches to properly understand the risks that they face. Therefore, ensuring cybersecurity reflects the commitment to succeed. And in retail, success is measured by the tangible benefits that come by way of a sale. Our findings reveal the beneficial returns from investment in a proactive cybersecurity approach.

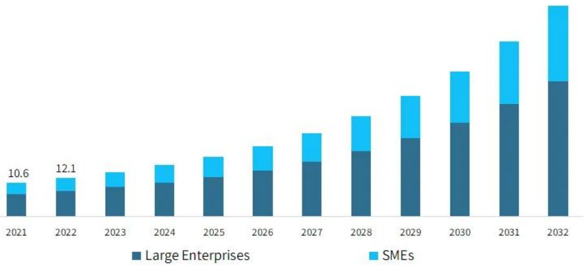

Figure 6. Retail Cybersecurity Market Size

6.2. Implications for Future Research

The implications we have articulated in the preceding subsection challenge the researchers and expose the need for future research in the domain of proactive enterprise security models that can withstand the pressures of time, i.e., the constantly changing nature of contemporary retail environments, which requires new solutions as digital transformation capabilities in the retail industry keep expanding. Among the numerous opportunities for future research in the areas of proactive cybersecurity and threat intelligence ubiquitous across digital society and cybercrime operations are six essential contexts that inevitably require elaboration for comprehensive boundary review and subsequent contribution to the well-described nexus between the four disciplines. Fundamental future research domains include exploration of the protections possible with knowledge extracted from social networks that are inherent to innovations and their ability to thwart retail crime; gaining insights into how risk can be mediated by embracing technology as a driver in retail to create commerce resilience; and the combined sophistication of developing live electronic hoarding at scale.

Future research tasks begin with investing in exploring the retail workforce to measure awareness and resilience against social engineering as accepted norms of online behavior become subtly intruded upon, such as supply chain breaches. Equally significant is assessing data mediums under the helm of behavioral security to discover if they reduce attack capabilities. Pivotal to future proactive retail security research is, naturally, the induction of emerging ICTs and the potential threats they pose. In tandem is the requirement for longitudinal studies and wider inclusion of retail industry expertise to ensure that insights obtained can inform academic practice and, conversely, that awareness of academic theory will cascade into newer best practice models of co-opting emerging threats. Such endeavor must delve deeper into the threat level so the natural frequency of emerging retail technologies that inspire attitudinal despair can provide a feasible cycle of robust retail futures. The shared competence of academia and industry will also form models of the digital retail footprint, seamlessly integrating the field of information system management and technology innovation in an analytical and collaborative forum. By raising these future research domains of potential benefit to the retail innovation dilemma, it is evident that the six derived from enhanced analyses propose a nursery of future channel opportunities.

References

[1] Vankayalapati, R. K., & Rao Nampalli, R. C. (2019). Explainable Analytics in Multi-Cloud Environments: A Framework for Transparent Decision-Making. Journal of Artificial Intelligence and Big Data, 1(1), 1228. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1228

[2] Dilip Kumar Vaka. (2019). Cloud-Driven Excellence: A Comprehensive Evaluation of SAP S/4HANA ERP. Journal of Scientific and Engineering Research. https://doi.org/10.5281/ZENODO.11219959

[3] Chintale, P., Korada, L., Ranjan, P., & Malviya, R. K. (2019). Adopting Infrastructure as Code (IaC) for Efficient Financial Cloud Management. ISSN: 2096-3246, 51(04).

[4] Syed, S. (2019). Roadmap For Enterprise Information Management: Strategies And Approaches In 2019. International Journal Of Engineering And Computer Science, 8(12), 24907-24917.

[5] Mandala, V. (2019). Optimizing Fleet Performance: A Deep Learning Approach on AWS IoT and Kafka Streams for Predictive Maintenance of Heavy - Duty Engines. International Journal of Science and Research (IJSR), 8(10), 1860–1864. https://doi.org/10.21275/es24516094655