RETAIL CISO'S COMPLETE GUIDE TO CYBER RISK PROTECTION

How to Automate, Accelerate, and Orchestrate the Threat Defense Lifecycle

Approach Note

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Overview

The aim of this guide is to shift our focus to the most fundamental and immediate need of the digital world. Cyber Security has been a major concern for a while now and is a constant constraint for retail organizations that want to push their limits by exploring advancements in technology. A few months ago, The World Economic Forum ranked Cyber Attacks among the top 10 most significant risks worldwide in their Global Risks report. It is not surprising as the global Cyber Crime Market has reached worth 100's of billions in the recent few years. Cybercriminals have shifted their focus from traditional financial markets, to targeting the retail sector. Retail organizations experienced nearly three times as many cyberattacks as those in the finance sector which was top of the list of cyberattacks on organizations in the 2015 report. The Global Threat Intelligence Report GTIR 2017 NTT Security reveals that retail is one among the four major industry sectors which gets affected by ransomware attacks with a whopping 15% detected attacks in an year. Increasing instances of cyber attacks like Ransomware attacks are a serious concern for the retail industry which handles vast amount of customer data including Personal Identifiable Information and credit card information and other financial transaction data.

The internet has revolutionized the way we live, work and interact with each other. With the astounding growth and reach of the internet and ecommerce, the technology is redefining the way we conduct business, be it in the form of Cloud, Mobility, IoT or Big Data. On one side the breadth and depth of technology growth are making businesses smart and more connected and customers closer to business. However, on the flipside, these technology advancements also expose businesses to more risks, including some of which are unheard of too. Cyber-attacks are now becoming more innovative and sophisticated in achieving their motives and the number of organized attacks across retail space has increased tremendously in the recent years. In this age of Omnichannel customer engagement, POS transactions, NFC payments, Mobile wallets and Beacon technology enablement, consumers leave their valuable data including credit card information across various channels. With limited amount of IT resources and massive amount of customer data across multiple channels, it is not an easy task for small to medium retail industry players to effectively devise a cyber security strategy and implementing it. Retail organizations have a serious imperative to take utmost care and caution of the customer data when storing, transferring and authenticating it.

Cyber risks affect every class of business and no organization can consider themselves completely immune to these rising number of cyber-attacks. In spite of the usage of effective control measures, attackers are day by day identifying novel methods including advanced social engineering strategies, sophisticated malware techniques including ransomware attacks, advanced persistent threats and innovative evading techniques, to penetrate into an organization's defense barriers. The presence of vulnerabilities in end point and perimeter security controls provide a fertile ground to penetrate into the existing defense and wreak the havoc to the organization. Apart from this, the existing security tools and approaches that work in silos, target only certain type of threats while ignoring the other issues or fail to connect and share data with the other existing tools in the system. This makes it challenging for organizations to get a bird’s eye view of the organizational risk posture, thereby exposing them to cyber risks.

The time is up to rethink our traditional approaches and adopt an integrated approach to handle cyber security in an organizational landscape. The integrated way of handling cyber risks enables organizations to be more confident in effectively identifying and responding to new age cyber risks and concentrate more on their core business.

This integrated approach should be capable of employing multiple tools and technologies in an automated system, governed by analytics with relevant insights. These features will work together to effectively make a strong, end to end cyber security platform that will manage the entire lifecycle of security, from protection, detection to triage, to response, and remediation.

In this guide, let us analyse the key challenges in organizational cyber security space, the existing solutions or approaches for defense and mitigation, their effectiveness, the need for an integrated approach and how an integrated solution can address the current challenges in the retail cyber security space.

The Emerging Cyber Risks

One of the biggest challenges organizations is facing when it comes to cyber risk management is in gaining an end to end visibility of their environment. Some of the key obstacles cited as contributing to lack of visibility are:

- Lack of proper understanding about the organization's risk posture
- Lack of skilled and trained resources to perform the risk analysis
- Lack of knowledge about contextualizing key information across multiple areas/tools
- Lack of basic security controls such as vulnerability management, back ups and restore controls, periodic patch management etc.

A holistic approach for cyber risk management which covers the policies, infrastructure, applications, network devices and resources is the need of the hour.

The Existing Challenges In Organizational Cyber Security Environment

Security measures that work in siloes

Retail organizations still rely on traditional security technologies like Firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, Anti-virus etc. to combat the cyber security threats. The challenges with these traditional security measures which works in siloes, include delayed detection of root cause, delayed resolving and failure in providing a complete integrated view of what's going on around in the threat landscape. It remains passive and blind to broader threats and reacts too slowly to emerging sophisticated threats like ransomware attacks and other malware threats.

Over dependence on the third party consultative expertise

Many retail organizations rely on third party security consultants to periodically review and assess the organization's security posture. However, in such cases the experience and expertise of the consultant along with the trust they build decide the effectiveness of the risk assessment/ management. The organization has to closely work with the third parties to keep the work in tact since the lack of focus or understanding in any of the areas that can compromise the security posture.

Traditional technologies, frameworks, and practices

Many players in the retail space still depend on traditional technologies, frameworks, and practices and which makes it challenging for them to address the cyber threats associated with new gen technologies like IoT/M2M., In most of the instances, the lack of timely review and updating, makes the tools, technologies, frameworks and best practices turn obsolete. This may have a significant impact in a retail organizational cyber security posture.

Increasing data privacy challenges

Retail is a sector which generates massive amount of data each fraction of a second. The exponential growth of data also contributes to cyber security risks. Improper handling of these data would create serious implications in terms of cyber security.

Need For An Integrated Cyber Security Solution

We have seen the current approaches that organizations follow while addressing the cyber risks and also the challenges associated with these approaches. It is highly significant for any retail organization to maintain a 'defense in depth' strategy for controlling and protecting their risk and security posture. For this, a well-integrated, automated and orchestrated threat defense life cycle is key. Let us take a look on how an efficient Threat Defense Life Cycle must work in an organization, ideally.

STEP 1

Organizations must have a clear understanding of their risk & compliance posture at any point of time.

STEP 2

Leverage consultative expertise for cyber risk management.

STEP 3

Integrate new age security technologies and operate as an ecosystem.

STEP 4

Break the silos and be part of an integrated system and leverage analytics to gain better insights and build proactive threat defenses & intelligence.

STEP 5

Incorporate efficient automation and orchestration to drive faster response throughout the Incident management lifecycle.

An integrated approach to cyber security defense enables retail organizations of any size to defend the unpredictable threats including ransomware attacks presented by the prolific growth of data and devices, cloud infrastructure and consumerization, changing technologies, Omnichannel approach and highly motivated threat actors.

The integrated Cyber protection coordinates analysis to action by providing complete visibility to risk, exposure and enhancing the team performance. This is achieved with an integrated design approach for our customers to perform faster detection and response.

1 Identification

It gives a holistic view of the security risks that is targeting a retail organization. Faster aggregated detection of the cyber-attacks helps an organization to be better prepared to face the adversities.

2 Analysis

The identification and analysis will be followed by blocking the vulnerabilities in the affected systems or network and updating it in the intelligence records for further reference.

3 Blocking

The identification and analysis will be followed by blocking the compromise of affected systems or network and informing the concerned parties about it or giving the intelligence updates.

4 Countermeasures

After blocking the system vulnerabilities, trace the path of the attack and counter measures should be taken based on intelligence and analytics.

5 Protection View

The final step in the work flow involves compiling all the information and providing an integrated dashboard with visual representations of the attack lifecycle and the mitigation steps to be shared with the organization. These dashboards will help organizations in gaining complete visibility into the cyber security posture and also help in remediating security gaps quickly.

The systematic cyber threat mitigation approach enhances customer confidence, brand protection, and cyber loss protection.

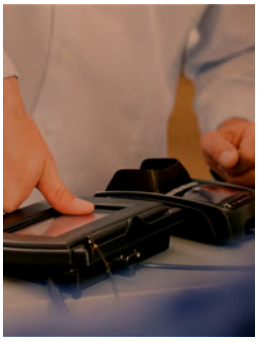
Some of the Sample use cases which can be addressed effectively by an integrated approach includes:

Visibility into User Behavior

The correlation of user information from sources like IDAM, DHCP, DC help in quickly detecting compromised accounts and gain full visibility into threats associated with privileged accounts and threats and anomalies for users and entities within the organization.

Advanced Network Threats and Data Loss

Ability to detect and remediate cyber-attacks and gain visibility into threat behavior movement with automated threat modeling and identifying evidence of data exfiltration from assets or users within an organization. Streamline the threat workflow to review anomalies and perform analysis on the hidden threat patterns to respond and prevent data loss.



New Pattern of Risk Activities

The self-learning and workflow understanding from network, users, assets and traffic patterns enable faster detection of the risks .The cross reference with policies and incident data helps in arriving faster at the risk channels.

PCI DSS Compliance Handling

Most of the ecommerce and retail players are integrating third party payment gateways to fulfill their payment process. However, in many instances it has found that cyber-attacks are compromising the data security of the card holder. To avoid this, PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. Here, CRPP application will secure customer cardholder data with PCI DSS guideline by Building and maintaining a secure network and systems, Protecting cardholder data, Maintaining a Vulnerability Management Program, Implementing strong access control measures, regularly monitoring and testing networks and Maintaining an information security policy.

Defense against zero-day attacks such as Ransomware

Unlike traditional signature based systems, integrated cyber security defense systems detect anomalous behavior in users and enterprise systems across multiple behavioral vectors such as connectivity, bandwidth and user activities. AI & ML integrated cyber defense systems provide deeper visibility into the enterprise IT. They perform real time analysis to detect zero-day attacks and enable rapid response.

For example: The Indicators of Compromise (IOCs) for ransomware (WannaCry) can be detected by an AI enabled cyber defense system through behavioral anomalies such as Spikes in network traffic from processes connecting to the same domain, Excessive data access usage on end-points specifically network / data shares, Processes making connections to unexpected external hosts, Connections made to unusual listening ports etc. These will trigger proactive alerts in case of ransomware attack thus enabling an enterprise to deploy a rapid incident response.

1

How we helped a Leading IT Outsourcing Company achieved overall 30% IT cost reduction

2

How we helped a huge Gaming Corporation build a centralized view of security events for applications across infrastructure

3

How a Fortune 500 Conglomerate Overcame Skills & Resource limitations to set up a robust risk management platform

4

How we enabled a Digital Transaction Management company ready for ISO27001 compliance

5

How we helped a leading large scale retail chain in India with integrated security solution for faster incident detection and response capabilities, with centralized security view and compliance reporting

Reach out to us if you want to know more about CRPP applications and our case studies

Cyber Risk Protection Platform (CRPP)
An Integrated Cyber Security Solution

Happiest Minds Technologies integrated Cyber Risk Protection Platform (CRPP) helps organizations to automate, accelerate and orchestrate the threat defense lifecycle. With this platform organizations can leverage on multiple security technologies including SIEM, advanced and next generation network, endpoint security and DLP provider, deeper analytics and insights, providing you a unified approach to handling your overall threat lifecycle and address security holistically.

Why Cyber Risk Protection Platform?

Integrated Threat detection and response across multiple layers of enterprise IT, removing siloed approach to security

Enhanced visibility and situational awareness across network, end points and cloud

Leverage best of the breed technologies and security best practices

Tiered approach to address security needs based on threat/risk profile of organization

Analytics- driven framework for better contextualization

Automated, adaptable for continuous monitoring and response

Features & Benefits

1. Integrated strategy and plans across functions to consciously mature your organization's security capabilities
2. Consolidated internal and external intelligence to contextualize and prioritize
3. Tighter integration between data, processes, and products to improve visibility, enable more effective analytics, and action
4. Detect, interpret, and respond to events effectively & comprehensively
5. Enable cost reduction of incident response and compliance despite an increasing volume of events, incidents, and regulatory actions
6. Real time visibility, to effectively detect, investigate, and adapt to future attacks and remediate
7. Comprehensive security and management that narrows the time to detection and resolution from days, weeks, or months to hours, minutes, or even seconds
8. Defense against zero-day attacks (ransomwares) and provisions for rapid incident response

Check out the video on Cyber Risk Protection Platform (CRPP)

Watch Now

“U.S. companies and government agencies suffered a record 1,093 data breaches last year, a 40 percent increase from 2015, according to the Identity Theft Resource Center.”

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Conclusion

The overall risk management which includes the steps- Protect, Detect, Mitigate, and Adapt is undergoing a deep transformation from an organizational point of view. The key executives of retail organizations are viewing cyber risk management as an influential factor in business decision, making capable of delivering more value to business. Since cyber risk is the business risk itself, addressing it effectively is the top most priority for any organization. At a time when attack models are getting more and more sophisticated and the current defensive measures fail to provide the required coverage when it comes to the case of incidents like ransomware attacks, it is high time for retail organizations to explore and adopt efficient and integrated frameworks like Cyber Risk Protection Platform (CRPP), developed by Happiest Minds.

For More Information
Write to us:
business@happiestminds.com