Cyberint

Securing the Customers' Digital Journey

Threat-Centric View of the Customer Experience

December 2019

TABLE OF CONTENTS

INTRODUCTION

In a world where a competitor's offer is only one click away, customer trust is a valuable asset that directly affects Customer Lifetime Value for eCommerce and online retail businesses. Mutual trust is an essential component in acquiring new customers, and it is even more crucial for developing and maintaining customer loyalty. Arguably, it is the most significant asset any retailer (both on-and-offline) can have - loyal customers are also the most profitable in the long run. With each additional year of a relationship, loyal customers not only become less costly to serve, but buy more and pay premium prices. They also become brand-builders and bring in new customers through referrals, online reviews and testimonials, and social media.

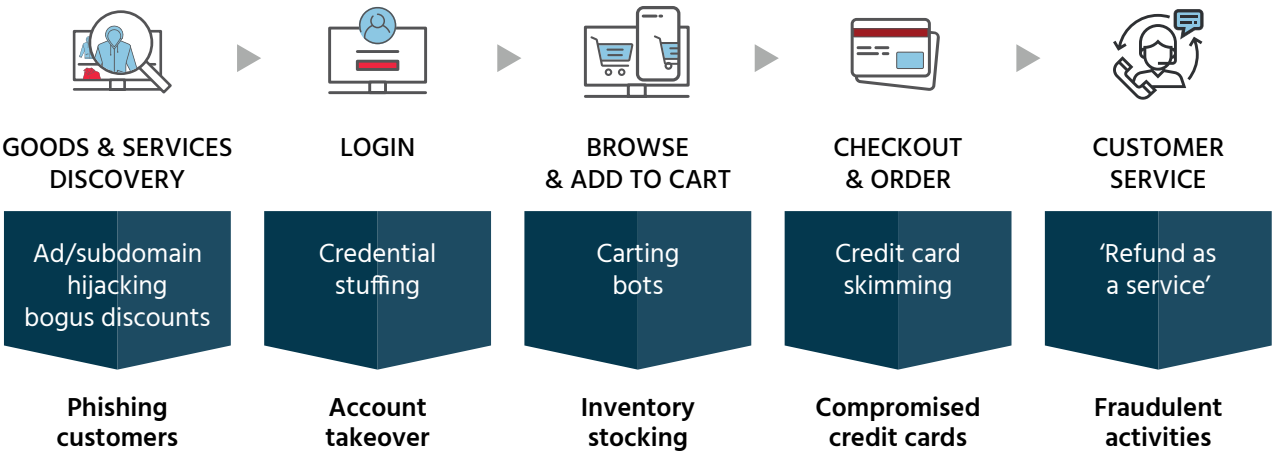
Nowadays data is a tremendously valuable commodity and consumers are becoming increasingly careful with whom they entrust their personal data. In fact, poor data security is a deal-breaker for a growing number of consumers; 78% would stop engaging with a brand online if it had experienced a breach. Moreover, 54% of consumers are more concerned with protecting their personal information today than they were in 2018.

Online retailers and eCommerce players have a responsibility to be aware of the threats throughout the customer journey and keep it secure. This eBook provides clear and actionable guidelines on how to achieve that.

PROTECTING THE CUSTOMERS' DIGITAL JOURNEY

Customer journeys are becoming increasingly complex. Brands today use more touchpoints than ever to interact with their customers. Customer journeys span multiple channels, assets, and involve various departments and business processes across the entire organization. As a result, securing the end-to-end journey becomes increasingly challenging.

Threat actors thrive on this complexity, targeting every stage of the customer journey; from goods and services discovery, to post-purchase customer service with targeted attacks.



The road to maintaining cyber resilience throughout each point of the customer journey begins with an understanding of how customer and business processes interact with an increasing number of touchpoints. Potential cyber threats are lurking at each point of a customer's journey and can be exploited by threat actors to obtain any sensitive data and personal information they can monetize. Online retailers need to be aware of what they are faced with if they are to take necessary steps to secure their business and protect their customers.

FOCUSING ON THE BIG THREE

Customers

Customer data is a highly valued commodity that is often targeted by threat actors. PII and payment data are obvious targets, but auxiliary information related to the customer journey such as login credentials, shopping preferences, and club membership details are often targeted as well.

Customer data:

- PII, payment data
- Login credentials
- Shopping preferences
- Club membership details

Employees

Employees hold the keys to their business environment. Employee login credentials, VPN access, and email mailboxes can all be leveraged by threat actors to launch attacks on their customers, partners, and business.

To do their jobs, many employees require access to payment information and discount benefits; yet another touchpoint that can potentially be abused. Employee endpoint devices such as mobile devices, laptops, and desktops must also be protected.

Employee Data:

- Login credentials
- VPN access
- Corporate mailboxes
- Endpoint devices

Brand and Business

Successful brand management must be actively pursued and maintained. Brand elements encompass multiple online and offline assets and business processes, including the customer journey and how it is supported and protected from abuse at multiple stages through a multitude of platforms and devices. Each online retailer has a unique brand footprint comprising among other elements the specific promotions, the pricing of goods, and even supplier networks, including contracts with 3rd party partners. The greater the investment in marketing and promotional activities, the greater the law for threat actor activities.

- **Online assets:** websites, domain names, social media channels, online platforms, images, videos, and software applications
- **Physical assets:** proprietary merchandise, physical locations such as stores and distribution centers, and IT infrastructure
- **Business processes:** threat actors can exploit refunds, shipping, pricing, and other processes and policies

TAKING THE THREAT-CENTRIC APPROACH

Retailers of all sizes are facing richer customers' digital journeys. Every touchpoint presents an opportunity for would-be-attackers to launch a targeted attack.

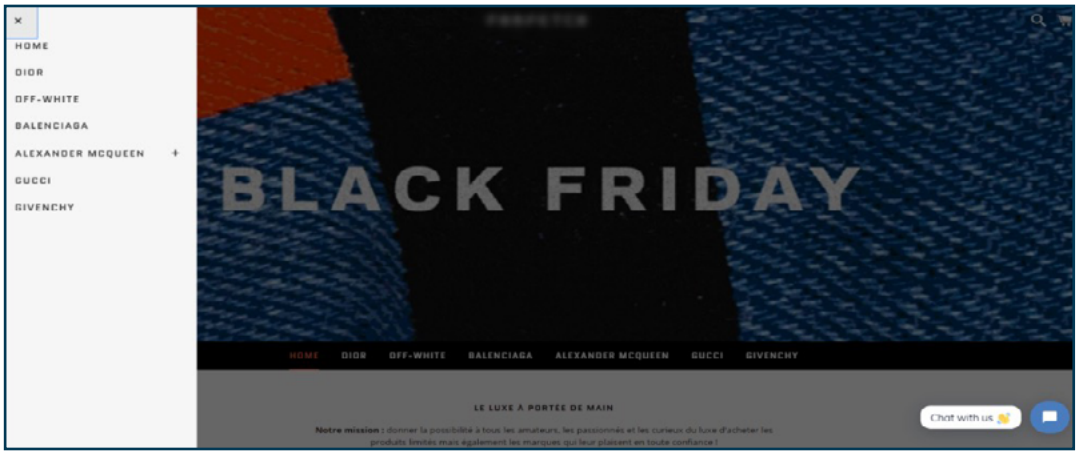
Customer Journey Stage	Business Process at Risk	Top Threats	Risks
Goods & services discovery	Marketing campaigns, merchandise display	Ad hijacking, scam promotions & bogus discounts, phishing, abandoned subdomains	Compromised PII, spamming, brand abuse
Login	Authentication, authorization and access	Phishing, data skimming, credential stuffing	Account takeover, brand abuse
Browse & Add to Cart	Marketing campaigns, pricing and digital commerce	Carting bots, IP data compromise, cart abuse	Fraudulent orders, artificial “out of stock” notifications, price & inventory manipulation
Checkout & Order	Transaction, warehouse management, fulfillment, shipping	Payment data compromise, customer data (PII, preferences e..g address of delivery, type of delivery)	Fraudulent payments, revenue loss, fraudulent operations
Customer Service	Refunds, returns	Refund fraud, phishing customer care representatives	Fraudulent activities, revenue loss

Customer Journey Stage: Goods and Services Discovery

Business processes	Threats	Risks
Marketing campaigns, merchandise display	Ad hijacking, scam promotions & bogus discounts, phishing, abandoned subdomains	Compromised PII, spamming, brand abuse

Real-life example:
Phishing Campaign - Targeting European retailer

- Fully impersonate major eCommerce brand's website using the Shopify platform.
- Collections of that brand items, and photos.
- Targeting retailer's audience with "Black Friday" promotion



Argos™ Detection: phishing site potentially compromising Black Friday event for a large European retailer

CyberInt Mitigation:

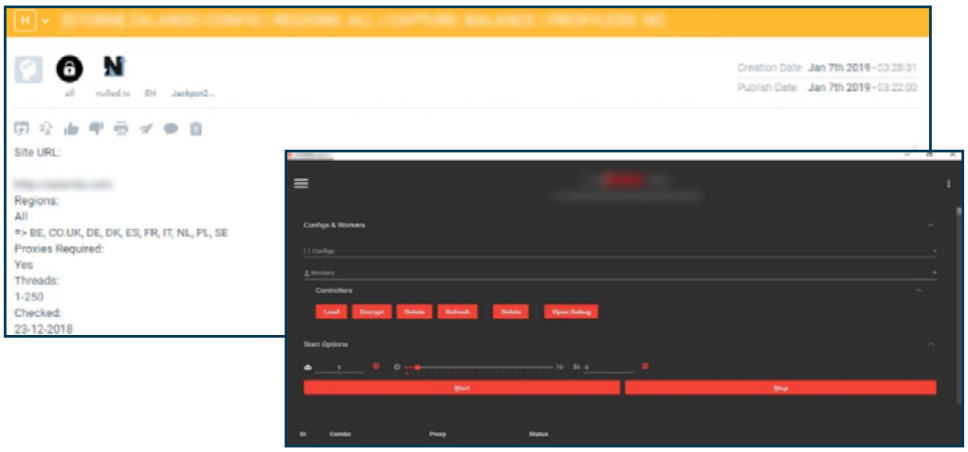
1. Phishing site takedown
2. Drive awareness of customers

Customer Journey Stage: Login

Business processes	Threats	Risks
Authentication, authorization and access	Phishing, data skimming, credential stuffing	Account takeover, brand abuse

Real-life example:
Credential Stuffing For Sale - Brute force attack on targeted brands

- Tailored CONFIG FILE for use against specific e-commerce websites
- Leveraging stolen credentials and technology
- Enabling takeover of users' accounts
- Execute fraudulent activity / or sell comprised data in the Dark Web
- May go undetected in existing security



Config file includes IP addresses to execute the brute force attack

CyberInt Mitigation:

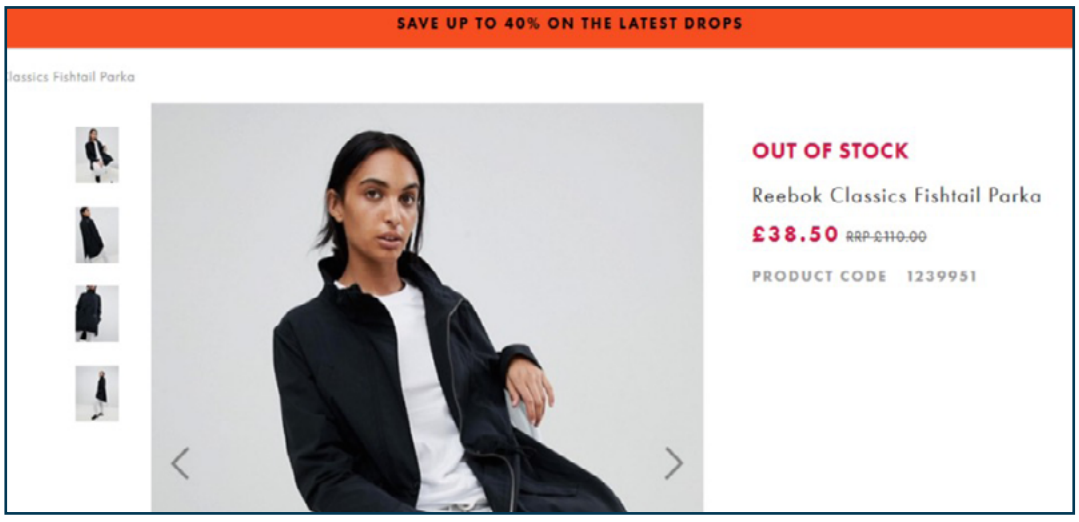
1. Configure the SIEM to alert and block the attack
2. Blacklist the rotating IPs
3. Investigate the current accounts and credentials validity

Customer Journey Stage: Browse & Add to Cart

Business processes	Threats	Risks
Marketing campaigns, pricing and digital commerce	Carting bots, IP data compromise, cart abuse	Fraudulent orders, artificial "out of stock" notifications, price & inventory manipulation

Real-life example:
Carting' Bots: Automated Stocking of Goods - Cart/Bag abuse & price manipulation

- Automation bots renewing "add to cart"
- Customers not purchasing due to experiencing "unavailable" or "out of stock" message
- Lack of purchasing manipulates price down
- Critical issue on specific shopping events resulting in loss of customers, loss of revenues



Config file includes IP addresses to execute the brute force attack

CyberInt Mitigation:

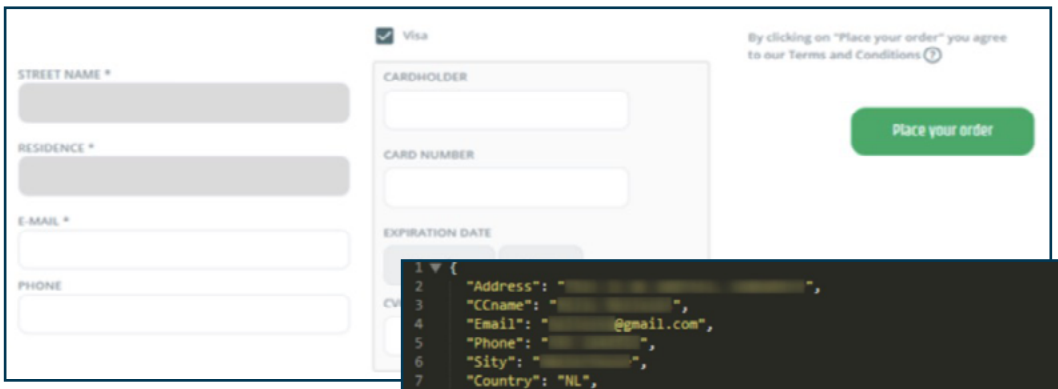
1. Investigate threat – identify accounts used to do the carting
2. Configure existing security control to block bot activity

Customer Journey Stage: Checkout & Order

Business processes	Threats	Risks
Transaction, warehouse management, fulfillment, shipping	Payment data compromise, customer data (PII, preferences e..g address of delivery, type of delivery)	Fraudulent payments, revenue loss, fraudulent operations

Real-life example:
'Magecart' Data Skimmers - Malicious script in the 'checkout' pages

- Injected JavaScript payload allows payment and personal data to be scraped
- This data is encoded and sent to the threat actor' command and control server
- Leveraging a vulnerability in the digital commerce platform
- Data theft exposes brands to GDPR fines



Personal data and payment card form example

JSON data for exfiltration (expanded for ease of reading)

CyberInt Mitigation:

1. Configure the SIEM system to alert and block the bruteforce attack
2. Blacklist the rotating IPs

Customer Journey Stage: Customer Service

Business processes	Threats	Risks
Refunds, returns	Refund fraud, phishing customer care representatives	Fraudulent activities, revenue loss

Real-life example:
Fraud: 'Refund as a Service' - Malicious script in the 'checkout' pages

Threat actors exploiting retailer's 'return policy' to get goods without paying for them
5-step operation:

- Threat actor reaches out on deep web forums
- Buyer reaches out to the threat actor: gets proof and refund requirements
- Threat actor executes refund process with retailer
- Buyer receives the refund, and goods
- Threat actor receives payment for service

- Retailers suffer revenue loss; business process abuse


Amazon/Google/Apple Service!

You received your order already? What are you waiting for?! Fill out the form now!

Current recommended limits (always updated):

Amazon.DE - max 350 EUR (1 item only)
- max 200 EUR if your acc has no previous orders

Microsoft - max 15.000 EUR (max 10 items)
Google (USA/CA) - max $6000
Google (EU) - max 4000 EUR (max 10 items; buy one cheap item, so we can do a particular refund - REQUIRED)
Apple (USA/CA) - max $5000 (1 item only !!)
Hollister (GER/USA/CA) - max 400 EUR (max 10 items)
Asos (EU/USA/CA) - max 400 EUR (max 10 items)
Abercrombie & Fitch (GER/USA/CA) - max 400 EUR (max 10 items)

EU = Europe (incl. UK)
USA = UNITED STATES OF TRUMP
CA = CANADA
GER = GERMANY
Amazon.de/Microsoft =Worldwide

Limits are changing really often, these limits are recommended limits by me, since I do tons of refunds every single day so I am 99% aware of the current limits.
Keep in mind, the minimum I charge for a refund is 35 EUR.

Argos™ Detection: fraudulent refund ad posted in the deep web

CyberInt Mitigation:

1. Reveal the identity of the threat actor, attack vector and potential accomplices
2. Refund policy change; detect accounts used for the fraud
3. Detect accounts taken over for fraud

SECURE CUSTOMER EXPERIENCE IN 3 STEPS

Step 1:
Threat-Centric Detection

- Know which are the common threats to your customers
- Leverage technology tools to search for threat actors' techniques
- Apply continuous monitoring of different assets, forums to detect threat actors' campaigns in the making
- Execute periodic threat hunting to identify insider threats and potential reconnaissance activities of unknown and undetected incidents

Step 2:
Mitigate Threats on Your Customers' Journey

- Configure existing security controls, e.g. SIEM, EDR to alert and block the attack
- Carry out investigations and leverage virtual HUMINT services to reveal the full scope and scenarios of attacks
- Reveal the identity of a threat actor, threat vector, potential accomplices
- Identify insider employees
- Blacklist rotating IPs and take down phishing sites
- Secure payment systems and transactions apps
- Review and adopt refund policy change
- Drive customer awareness

Step 3:
Data Breach Response Plan

For most organizations, the question isn't "if" but "when" a data breach will occur. That is why it is extremely important to have an updated Data Breach Response Plan (DBRP) that delineates the roles and responsibilities of all the relevant stakeholders involved, both internal and external.

The DBRP should cover the following:

- Who is responsible for notifying the internal stakeholders and making sure that the patch is available and released quickly?
- Who will alert the law enforcement and data privacy agencies in a timely manner?
- Who will be handling public, investor and customer communications?
- Which support agents will be manning the phones and incoming customer inquiries? What are they supposed to be saying regarding the breach?
- Who is responsible for root cause analysis and making sure that the same problem doesn't arise ever again?

CYBERINT RETAIL PROTECTION SECURES THE CUSTOMERS' DIGITAL JOURNEY

- Bring business centricity and customer experience into focus
- Obtain visibility and monitor the digital presence
- Provide actionable insights
- Combine cyber & fraud
- Include industry's seasonality addressed in risk prioritization

The need for a clear approach to securing the customer journey rather than the individual touchpoints is made apparent by the fact that the retail industry is one of the slowest when it comes to detecting and responding to data breaches, with the average time to identify a data breach reaching 206 days. Securing the end-to-end customer journey in online retail and eCommerce means that security teams require better tools that empower them to look at the customer journey as a whole within the relevant business and threat-landscape context.

The customers' digital journey should be secured end-to-end to protect employees, customers, and business processes. The key to achieving this lies in the continuous monitoring and analysis of the organization's digital environment, including social media accounts, hashtags, websites, brands, domains, and other company assets. Advanced threat intelligence empowers your team to look at your brand assets and business processes through the eyes of a threat actor, helping them secure vulnerable touchpoints across the customer journey.

CyberInt Retail Protection ensures that no stone is left unturned when it comes to securing the entire customer journey. This modular offering provides visibility into the digital footprint and potential attack surface, to help address threats across organizational and digital environment and understanding your company's risk profile.

GET CYBERINT RETAIL PROTECTION »

We believe cyber security is a business opportunity
to drive growth, customer loyalty, and brand value

MANAGED TARGETED
DETECTION & RESPONSE

SINGLE PLATFORM;
PRODUCTS & SERVICES

MULTILINGUAL
CYBER INTELLIGENCE
ANALYSTS

HQ: ISRAEL
USA, UK
LATAM, APAC

Cyberint

sales@cyberint.com

ISRAEL
Tel: +972-3-7286777 | Fax: +972-3-7286777
Ha-Mefaslim 17 St | 4951447 | Kiryat Aryeh Petah-Tikva | Israel

USA
Tel: +1-646-568-7813
214 W 29th Street, Suite 06A-104 | New York, NY, 10001 | USA

UNITED KINGDOM
Tel: +44-203-514-1515
14 Grays Inn Rd, Holborn | London | WC1X 8HN | Suite 2068

SINGAPORE
Tel: +65-3163-5760
10 Anson Road | #33-04A International Plaza 079903 | Singapore