ULTIMATE GUIDE TO TRANSFORMATION & INFORMATION SECURITY FOR RETAIL

the cyber leaders' network

Created by Boss Digital

OVERVIEW

The retail market is undergoing a major digital transformation whilst simultaneously defending itself against unprecedented levels of cyber threat.

This whitepaper is designed to help you understand the role of the security function within the broader digital transformation strategy. It is suitable for:

- CIO's
- CISO's
- Heads of change or transformation
- CTO's
- DPO's

the
cyber leaders'
network

PART 1

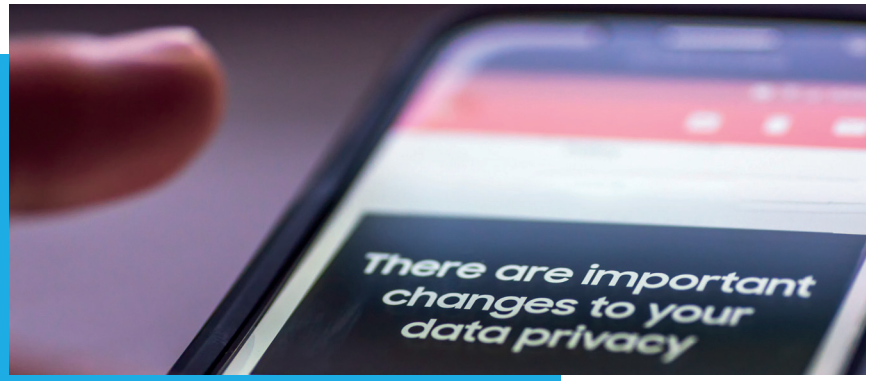
THE CHALLENGES & OPPORTUNITIES OF A RAPIDLY EVOLVING RETAIL MARKET

FROM RETAIL TO E-TAIL

- Every retail brand is now an eCommerce brand. In 2018 alone global eCommerce expanded by over 11%.
- This online experience covers an ever growing array of channels. Each one enables the brand to connect with customers at different moments of the buying journey.
- Online and offline are converging as smart retailers are integrating online tactics into the offline experiences. Each point of contact represents an additional data source, whether that's the website, point of sale systems, mobile apps, cameras, cold storage, shelving and beacons, and every one of these assets is a potential vulnerability.
- The IoT is helping retailers transform their analytics using big data, which in turn can reduce operational costs and drive future purchases. However, using the IoT has risks and retailers need to explore options like Cyber Security Certification Programs in order to ensure all IoT devices in their business are secured.
- The acceleration in this trend has exposed all retailers to cyber threats an order of magnitude greater than they have ever previously known. Few are truly prepared.

EXTERNAL PRESSURES

- As market competition continues to grow, there is a need for retailers to more effectively exploit their data through deeper, data driven customer insights you can better understand consumer sentiment and drive down the cost per acquisition (CPA).
- However, as retailers focus on short-term survival mentality, they often neglect security in order to cut costs.
- Huge volumes of data was rendered useless due to GDPR, and now that a year has passed it's becoming increasingly difficult for CISO's to maintain the board's interest in matters around data privacy.
- Unlike B2B organisations that may only service a handful of large customers, the volume nature of retail means that it only takes one customer with one bad experience to make a complaint, and a company can come under fire.



INTERNAL DIGITAL TRANSFORMATION

- Many retailers have complex legacy systems to overcome as they attempt to integrate new API's.
- Migrations to new ecommerce vendors or payment platforms are fraught with complexity and risk.
- Supply chain and third party product integration can lead to huge operational efficiencies and even an improved customer experience, but also introduce additional vulnerabilities in the process.

EVOLVING CUSTOMER EXPECTATIONS

- Whether they encounter your brand through a google search or via their social feed, customers expect every moment of their journey to be tailored to them as an individual. This requires ever growing pools of data, which means ever growing targets for cyber criminals.
- Online customers don't have the patience they once did. They want frictionless payment and short user journeys, making it harder than ever to enforce the necessary security measures.
- Brand has always been key, but with consumers now having more information than ever and competition fierce, establishing trust between your brand and the audience is critical to survival in most markets. Security breaches can compromise this trust in a heartbeat.

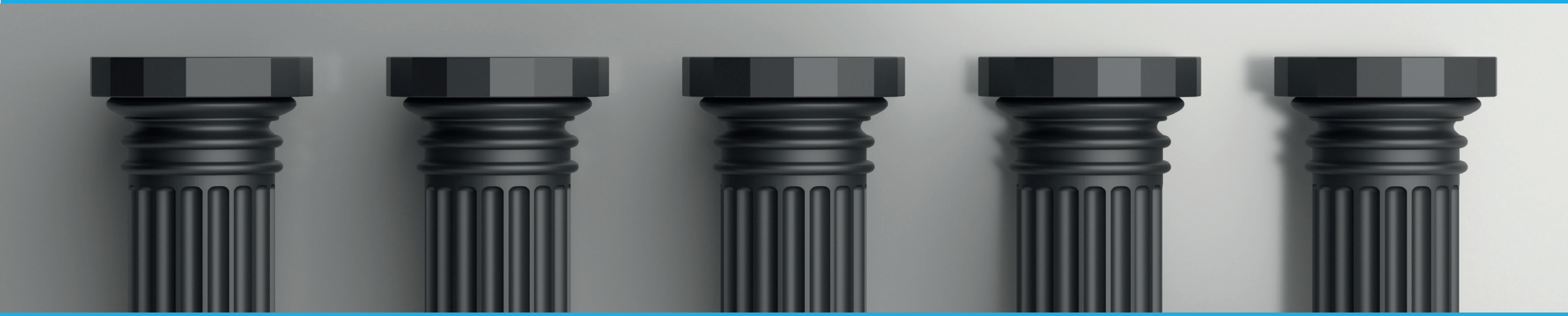
"Security experts tend to focus on what can't be done rather on what can be done. The job of a great security team is not to say no, but rather to facilitate ambitious transformation projects in a secure manner."

- TOR MACLEOD, FOUNDER OF VIA RESOURCE AND THE CYBER LEADER'S NETWORK

the
cyber leaders'
network

PART 2

7 PILLARS OF BUILDING A SECURITY FUNCTION THAT SUPPORTS TRANSFORMATION



1. STOMS - DEFINING YOUR RETAILER'S FUTURE

The first step of building a resilient security function is to develop a Security Target Operating Model (STOM). Your STOM will enable your organisation to:

- Define expectations of the cyber security team with clear goals and results.
- Create and foster consistent communication between your CISO and the boardroom.
- Develop a symbiotic relationship between the security team and core business operations.
- Manage change by mapping out the end goal and steps to get there, negating the traditional short-term survival mentality usually adopted by retailers.
- Align the activities of the security team to that of the broader IT department.

STEPS TO BUILDING YOUR STOM

1 UNDERSTANDING THE CYBER LANDSCAPE

Spend time analysing why these changes are important. If you have clear risks, or recent incidents, use them to understand exactly what changes are needed and how to drive them.

2 DRAWING THE BUSINESS STORYBOARD

Your cyber security team and senior leadership should work together to discuss the different departmental functions and how this relates to governance, risk and compliance.

3 MAPPING YOUR REQUIREMENTS

By having an idea of what you want to get out of your security target operating model, it becomes easy to set expectations, policies and standards.

4 ALIGN THE OBJECTIVES

Work with your key stakeholders to create a mutual understanding of why cyber security can support day-to-day operations and vice-versa.

5 CHOOSE THE TYPE OF MODEL

It's important to make sure the right leadership is in place to deliver a Target Operating Model. Internal teams can help manage the operational procedures, but don't exclude the need for external partners to make sure you don't get too focused on short term changes and neglect the long term goal.

2. ZERO TRUST ARCHITECTURE - A NEW WAY OF THINKING

- Zero Trust architecture is a new way for retailers to ensure complete assurance over their cyber security and information access. Zero`Trust means that every device, user, policy and action must be vetted totally and every user must be approved before access is granted.
- Zero Trust models can restrict access to data for certain users. For retailers with large levels of transactional data, access hierarchies can be invaluable for protecting confidential information.
- Zero Trust mindsets eliminate any potential for human error - which was cited by Shred-It as causing 47% of digital breaches.
- Zero Trust models do create an outstanding level of security internally, but all staff still need to understand the importance of promoting good cyber security in their retail organisation.

3. THINKING COMMERCIALLY

- Understand that info-sec is not simply about reducing risk. It is about helping your organisation make smarter business decisions.
- If you are to get the board members to understand your world, you must begin by understanding theirs.
- Compromises will be necessary. Taking a hard line on nuanced matters will seldom work.

"Engage your board by talking about risk profiles. What is the board or the business willing to accept from from a risk perspective? It's not for security to say what you can and can't do - it's for the business to say or you cannot can't do. Just because something is a high security risk doesn't mean it's a bad business idea, it could be a very valid business move to continue anyway."

- THOM LANGFORD, FORMER CISO OF PUBLICIS GROUP

4. FIND YOUR CHAMPION

- On every board there will be one person who instinctively gets the opportunities and threats of cyber security more than anyone else. Identify this person and build a close relationship as they will be critical in influencing other board members.
- This is particularly important if you're lacking in boardroom experience, as this person will be able to help you shape your content in a way that really resonates with the less technically informed members of the board. They will help you to focus on commercial outcomes, such as reputational damage, operational downtime or large fines.

"It is important to make sure you are talking to the right people. For my business case I put to the board, I was communicating with the owners of the business so I'm talking directly to the decision makers who have the view and the authority to take a decision on what we do with this organisation. As a result, the process is a lot easier and more supportive."

- CHRISTIAN TOON, CISO OF PINSENT MASONS LLP

5. BE CONFIDENT

- The majority of CEOs now consider cyber security a core part of their role, and that is already filtering through to the board agenda.
- It is not as difficult as it once was to get your voice heard, so don't hold back. Your board will be expecting you to speak loudly!
- Don't be afraid to speak up - your board need to hear what's going on with your retailer's cyber security strategy!

"I've noticed a big change in the last five years at board level. Cyber security is not a hard sell anymore."

- STEVE WRIGHT, INTERIM DPO BANK OF ENGLAND

6. BUILDING YOUR TEAM

- When developing your cyber security team, it's important for retailers to create a balanced team with different skills and mentalities.
- Different problems require different ways of thinking. The more diverse the team, the greater the range of problems you will be able to solve.
- Make sure you engage directly with the rest of the business and educate them clearly and concisely on the important of good cyber security, to help build relations and ensure a consistent level of protection across the entire hierarchy of your retailer's business infrastructure.

"We also need people that are younger because the channels and technologies are changing. I don't understand certain media anywhere near as much as my 13 year old daughter, so we need these people to tell us where things are going."

- VICTORIA GUILLOIT, PRIVACY AND CYBER SECURITY EXPERT OF SCHRODERS LLP

7. PRIORTISE DATA PRIVACY

- Data Privacy is now an essential issue for retailers due to GDPR.
- There was a lot of boardroom interest on it prior to 25th May, 2018. The challenge now is to maintain that interest.
- Good privacy practises are becoming a competitive advantage for retailers as more organisations face public scrutiny and penalties for their failure to keep data secure.
- Data privacy must be built into the core operations of retailers transactional activity on a day-to-day basis.

"There's so much value from using personal data but GDPR has raised the bar in terms of compliance, particularly around things such as secondary use, visiblity of privacy notice and transparency into how you use that data. You can't be reactive anymore. You have to actually be proactive and Privacy By Design is a way to doing that."

- JASON KING, GDPR COMPLIANCE MANAGER

the cyber leaders' network

CONTACT US

The Cyber Leader's Network is a research programme to aid in the development and maturity of skills and job roles within the Cyber Security Industry. As the Information Security market grows and evolves – we aim to ensure that organisations stay informed and have a solid skills plan that addresses the challenges of recruitment and retention within cyber security.

The Cyber Leaders' Network
Braywick House West
Windsor Road
Maidenhead
SL6 1DN
United Kingdom

info@cyberleadersnetwork.org

https://cyberleadersnetwork.org