CUSTOMER EXPERIENCE AND CYBER SECURITY: GAINING BOARD ALIGNMENT

RICHARD HOLMES
HEAD OF CYBER SECURITY SERVICES
CGI UK

IN TODAY'S DIGITAL WORLD, HERE'S WHY THE BOARD NEEDS TO PUT CYBER SECURITY ON ITS AGENDA. RETAILERS AROUND THE WORLD ARE TRANSFORMING RELATIONSHIPS WITH THEIR CUSTOMERS BY OFFERING AN OMNI-CHANNEL SHOPPING EXPERIENCE, WHERE CUSTOMERS CAN MOVE BETWEEN CHANNELS WITH EASE. THIS GIVES CUSTOMERS MORE WAYS TO SHOP AND INTERACT, MORE INFORMATION ABOUT PRODUCTS/ SERVICES, AND GREATER PRODUCT AVAILABILITY.

Omni-channel gives rise to increased information about customers, bringing with it the opportunity to target product recommendations and promotional campaigns directly to individuals. Big Data profiling gives retailers the ability to target the illusive 'market of one'.

> BIG DATA PROFILING GIVES RETAILERS THE ABILITY TO TARGET THE ILLUSIVE 'MARKET OF ONE'

Information harvested from payments, loyalty schemes, mobile apps, connected cars, smart TVs and other platforms will enable sellers to design compelling offers that the targeted individual will be unable to resist. In the future, it may be that customers are far more receptive to what's now perceived as spam. This will be as a result of retail communications being designed to be of such strong interest that they could even eclipse standard messages received from family and friends.

As a result, retailers are rewarded with stronger relationships with their customers and a deeper understanding of their behaviour and preferences. However, with this personalisation across omni-channels comes rising concerns over privacy. As customers realise the extent that their behaviours can be profiled, many people may want to resist the retail 'Big Brother' watching them.

Many digital platforms, including social networks, are already providing ever more fine-grained control over the personal information individuals share. However, it is not clear whether consumers pay attention to these controls. So while legislation such as the General Data Protection Regulation (GDPR) is designed to put the power back in the consumer's hands over their personal information, it's not yet clear to what extent consumers will exercise this new control.

It's still early days for the regulation, which only came into force in May 2018. The question therefore remains: will consumers start to understand the value of the data they are giving away in return for special offers? And, furthermore, will this drive a new wave of change in the omni-channel targeted approach?

Another point to consider when it comes to increased personalisation within retail service is logistics. Where omni-channel, Big Data and personalisation are pervasive, the future of retail will centre on the customer experience. With customers making choices in stores, the next step is surely to ensure rapid fulfilment so their goods are delivered to their homes before they return from shopping.

The amount of information that this technology chain requires is formidable. It necessarily includes data detailing customers' historical shopping behaviour, influences, trends, location, logistical preferences and so on. Safeguarding information of such a personal nature is important, if not vital, in order to maintain trust in a brand.

Good cyber security is a fundamental part of this process and must be justified through an understanding of the cost of getting it wrong. CGI and Oxford Economics' recent Cyber-Value Connection study identified that the average impact on company valuation was a drop of 1.8 per cent in share price following a severe cyber incident becoming publicly known. For the average FTSE 100 company, this represents a drop in value of some £120 million.

Good cyber security comes from the top — every company needs to communicate to its employees and suppliers that, in the digital world we live in, everyone has a responsibility to keep their company and their customers safe. Many organisations direct their focus on cyber security solely to the technical parts of the organisation without understanding the need for leadership, governance, planning and culture change as part of their cyber-security strategy. CGI recommends the following steps to ensure board alignment for cyber security:

- Accountability. Ensure a senior executive is responsible, at board level, for cyber security — and that they have the authority and know-how to address the risks
- Board agenda. Put cyber security on every board agenda. As a minimum, this should include reporting on: risk to the business, the nature of sensitive data and the mitigation progress
- Risk management. Treat cyber security as a company-wide business risk, assessed as you would other key business risks, encouraging a discussion about risk appetite, risk avoidance, risk mitigation and cyber-security insurance
- Legislation. Understand the legal landscape that applies to cyber risk, including European legislation in the form of the GDPR and the Network and Information Security Directive (NISD)
- Advice. Ask if the company has access to specialist expertise to advise and inform the board, whether from internal teams or external advisors
- Plans. Ensure the company has an effective programme of work to manage cyber risk, allowing a realistic timeframe and budget for this
- Response. Make sure the company routinely demands improved security from IT suppliers, including products, systems and services.

Retailers, through omni-channel, are becoming ever more digital in nature. From capturing customer sales to taking orders, managing supply chains, analysing Big Data, overseeing delivery logistics, reviewing/improving back office systems, analysing markets and many other aspects of retail operations — it's all becoming increasingly digitally enabled.

While many organisations are well aware of the benefits of this, few are equally aware of the damage which can be caused by a cyber breach. Cyber security underpins every aspect of this new digital world. If your organisation doesn't pay attention to this at every level, your company will not only be vulnerable to being out-marketed by a more secure customer centric retailer — it will also be vulnerable to a potentially devastating cyber attack.

CGI has partnered with the BRC to deliver the recent 'Gaining board alignment on cyber security' webinar. Recording available now: https://brc.org.uk/events/past-events/gaining-board-alignment-on-cyber-security.

RICHARD HOLMES
// cyber@cgi.com
// cgi-group.co.uk/retail

CGI

> "GOOD CYBER SECURITY COMES FROM THE TOP – COMMUNICATING TO EMPLOYEES AND SUPPLIERS THEIR RESPONSIBILITY TO KEEP CUSTOMERS SAFE."