DigitalXRAID
CYBER SECURITY EXPERTS

FOCUS ON RETAIL

Top 5 Cyber Security Challenges for Retail Organisations:

Protecting Your Business in the Digital Age

The retail industry is one of the largest and most important sectors in the global economy.

In recent years, the retail industry has undergone a rapid digital transformation, with the adoption of new technologies and platforms to improve the customer experience.

Retail organisations have now become increasingly reliant on technology to run their operations.

From online stores to point of sale systems, technology has streamlined many of the day-to-day tasks that retailers need to manage. While this has brought many benefits, with the increasing reliance on technology comes an increased risk of cyberattacks.

Retail organisations are now among the most targeted by cyber criminals due to the vast amounts of sensitive data they hold, including customer information, financial data, and intellectual property.

This ebook will explore the top cyber security challenges faced by the retail industry and provide recommendations to address these challenges.

Phishing Attacks

Phishing attacks are one of the most common methods used by cyber criminals to target retail organisations.

These attacks involve sending fraudulent emails that appear to be from a trusted source, such as a bank or a supplier.

The emails often contain links to malicious websites or attachments that contain malware. Once the recipient clicks on the link or opens the attachment, the cybercriminal can gain access to the retailer's network.

Phishing attacks are a significant threat to the retail industry, with a report from the Anti-Phishing Working Group (APWG) revealing that the retail sector was the most targeted by phishing attacks, accounting for 30.4% of attacks, in just a 12 month period.

Addressing the Challenge

To address the threat of phishing attacks, retail organisations should invest in employee training to help staff identify fraudulent emails.

Regular phishing simulations can also be used to test employee awareness and identify areas for improvement. According to a report by Verizon, 85% of ransomware attacks are delivered via email, highlighting the importance of educating employees on how to identify and avoid phishing emails.

Additionally, penetration testing can be used to identify vulnerabilities in the retailer's network and help to prevent cyberattacks.

Point of Sale System Vulnerabilities

Point of sale (POS) systems are a critical component of retail operations, but they also represent a significant security risk.

Cyber criminals can exploit vulnerabilities in these systems to gain access to sensitive customer data, such as credit card details.

The risk of POS system vulnerabilities was highlighted in the well publicised breach of Target, where cyber criminals were able to gain access to the retailer's POS systems and steal the payment card details of millions of customers.

The breach resulted in significant financial losses for the company, with estimates suggesting that the total cost of the breach could be as much as $1.1 billion.

Addressing the Challenge

To address these vulnerabilities, retail organisations should invest in regular penetration testing to identify weaknesses in their POS systems.

It is also important for retail and ecommerce businesses to ensure that all software and firmware is kept up to date with the latest security patches.

Additionally, retailers can deploy encryption technologies to protect the sensitive data processed by these systems.

Third-Party Security Risks

Retail organisations often work with a wide range of third-party vendors, such as logistics suppliers and payment processors. These third-party vendors can represent a significant security risk, as cyber criminals can exploit vulnerabilities in their systems to gain access to the retailer's network.

According to an industry survey, 56% of companies experienced a data breach that was caused by a third-party vendor.

This highlights the importance of conducting regular vendor risk assessments to ensure that all third-party vendors have appropriate security measures in place.

It is also important to ensure that all third-party vendors are contractually obligated to notify the retailer in the event of a security breach.

Addressing the Challenge

To address these risks, retail organisations should conduct regular vendor risk assessments to ensure that all third-party vendors have appropriate security measures in place.

It is also important to ensure that all third-party vendors are contractually obligated to notify the retailer in the event of a security breach.

Beyond regular vendor risk assessments, retailers should establish stringent cybersecurity standards for all third-party partnerships. This includes requiring vendors to adhere to specific security protocols and regular audits to verify compliance.

Additionally, implementing a robust incident response plan that involves third-party vendors is essential. This plan should detail procedures for rapid communication and coordinated response in the event of a breach. By taking these proactive steps, retailers can significantly mitigate the risks posed by third-party associations, safeguarding their networks and customer data effectively.

Mobile Device Security

Mobile devices have become an essential tool for retail organisations, but they also represent a significant security risk.

Cyber criminals can exploit vulnerabilities in mobile devices to gain access to sensitive customer data.

According to a report by Verizon, 43% of data breaches in the retail industry were caused by device hacking, with mobile devices being a primary target.

This highlights the need for retailers to implement robust mobile device security policies and protocols.

Addressing the Challenge

Retailers should ensure that all mobile devices used by employees are equipped with strong passwords and biometric authentication features.

Mobile devices should also be equipped with anti-malware and anti-virus software.

Additionally, retailers should implement mobile device management (MDM) solutions to ensure that all devices are up to date with the latest security patches and that sensitive data is encrypted.

Insider Threats

While cyber criminals represent a significant threat to retail organisations, insider threats also pose a significant risk.

Employees can intentionally or unintentionally compromise the security of the retailer's network.

According to a report, insider threats account for 34% of all data breaches in the retail industry.

This highlights the importance of implementing robust security policies and procedures to minimise the risk of insider threats.

Addressing the Challenge

Retailers should implement access controls to ensure that employees only have access to the data and systems that are necessary to perform their duties.

Regular employee training and awareness programmes should also be implemented to educate employees about the importance of cyber security and how to identify and report suspicious activity.

Ransomware Attacks

Ransomware attacks have become increasingly common in recent years, with cyber criminals using this type of malware to encrypt retailers' data and demand payment in exchange for the decryption key.

The frequency of ransomware attacks on retailers has surged, with several high-profile breaches in the UK in just the last 12 months.

One such attack happened to WH Smith, the second successful cyberattack on the company, following one which also targeted the company's online bookshop.

With this attack being the latest in a string of breaches that the retail industry has suffered, it's clear the sector has become a key target for cybercriminals.

And the more successful breaches that occur, the more these businesses will be exploited by hackers.

Addressing the Challenge

Retail organisations should invest in a Security Operations Centre (SOC) service to monitor their network for signs of a cyberattack.

Regular penetration testing can also be used to identify vulnerabilities in the retailer's network and help to prevent ransomware attacks.

Retailers should implement a robust backup and recovery system. This can help to mitigate the impact of a ransomware attack by allowing retailers to restore their data from a backup if it becomes encrypted.

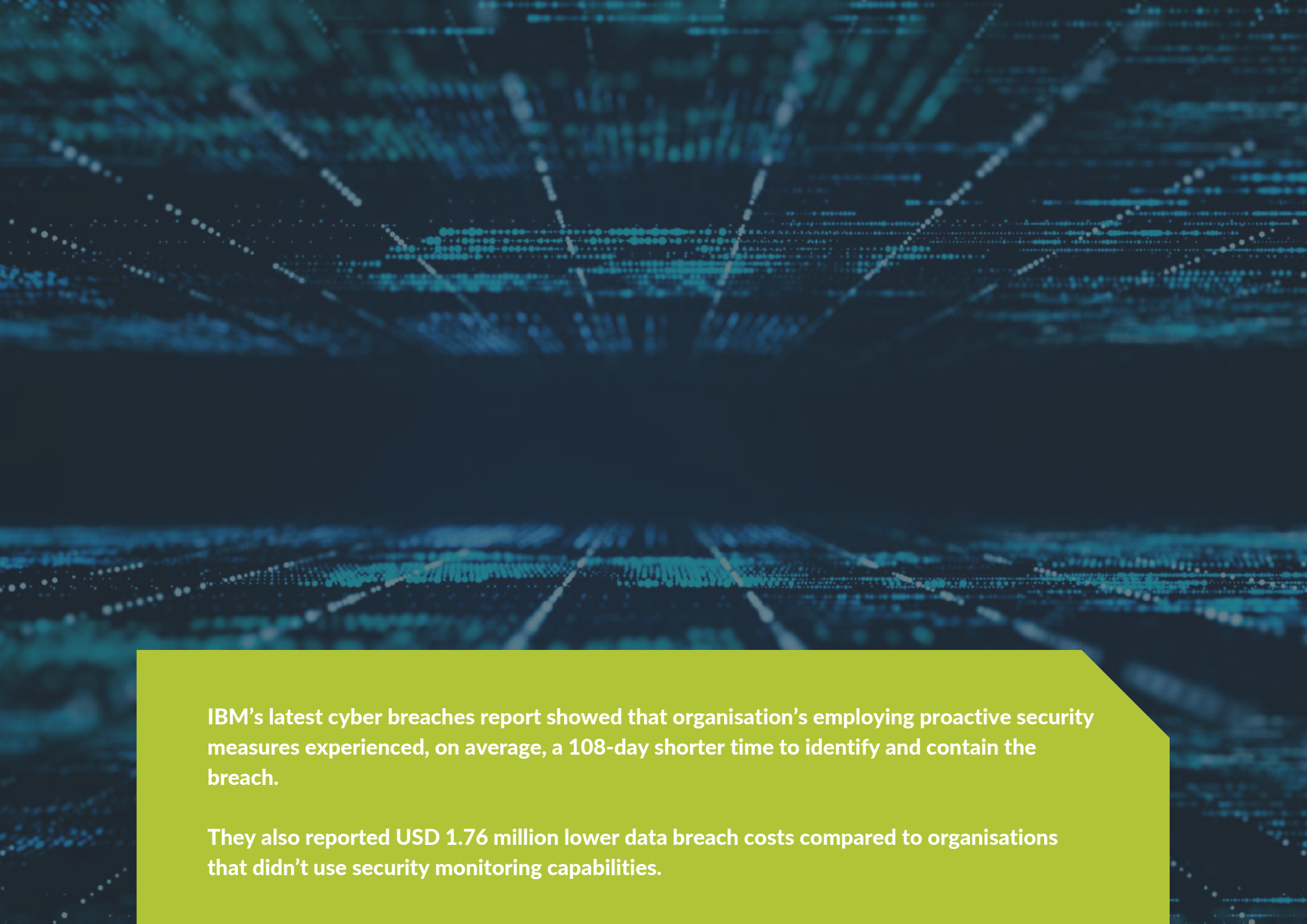
Never pay the ransom. This not only incentivises cyber criminals to continue their attacks, but there is also no guarantee that paying the ransom will result in the data being restored. Instead, retailers should report the attack to law enforcement and work with a cyber security service provider to restore their data and prevent future attacks.

A SOC service will monitor your network 24/7/365 for signs of a ransomware attack

In today's digital age, cyber security is a critical concern for retail organisations. Cyber criminals are constantly evolving their tactics to exploit vulnerabilities in retailer's systems and networks.

To protect their businesses, retailers need to invest in robust cyber security measures, including regular penetration testing and Security Operations Centre (SOC) services.

At DigitalXRAID, we offer a full spectrum of cyber security services, including penetration testing, SOC services, and vulnerability assessments. Our services are backed by CREST and CHECK accreditations, ensuring that our clients receive the highest standard of service.



IBM's latest cyber breaches report showed that organisation's employing proactive security measures experienced, on average, a 108-day shorter time to identify and contain the breach.

They also reported USD 1.76 million lower data breach costs compared to organisations that didn't use security monitoring capabilities.

DigitalXRAID's Security Operations Centre (SOC) service

DigitalXRAID's 24/7 Security Operations Centre (SOC) is a leading cyber security service that analyses, manages, and responds to all aspects of your IT infrastructure's security every day of the year.

DigitalXRAID's CREST accredited Security Operations Centre operates on a 24/7/365 basis, with a dedicated team of analysts monitoring networks, systems and applications, keeping them secure and responding to security events in real time.

The flagship managed SOC service helps customers understand and reduce risk. Our security services operate as an extension of your own team, working seamlessly to provide world-class threat detection and response.

The service uniquely supplies the complete spectrum of advanced threat detection and response capabilities, more recently coined as XDR (extended detection and response).

Services include vulnerability management, IDS & IPS, threat mining, SOAR (Secure Orchestration and Response), SIEM & log management, endpoint D&R, file integrity monitoring, dark web monitoring and full compliance reporting.

Our world-leading, CREST accredited Security Operations Centre can identify and neutralise threats in under six minutes, which protects your retail business 24/7 to avoid any operational downtime.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence
Against Cyber Threats?
Call us now on 0800 090 3734

info@digitalxraid.com digitalxraid.com