Securing a digital retail enterprise: Recommendations for reducing risk

Andy Rowland, Head of Customer Innovation and Tom Breteler, Innovation Associate

Introduction: the complex security landscape

Security is an ever-growing concern for retailers, with breaches resulting in loss of customer confidence and onerous data protection fines.

Security has the power to make or break an organisation's efforts at digital transformation. It is the number one enabler, allowing you to run at speed, build customer trust and investor confidence. Conversely, poor security is a disabler and will ultimately undermine plans for a digital future.

We live in a world where technology is all-pervasive, and as businesses roll out ever more sophisticated and ambitious digital strategies, ruthless criminal entrepreneurs are seizing the opportunity to exploit and monetise vulnerable systems.

Their attacks are supported by a vast, well-resourced and hugely profitable black market in which constantly evolving attack tools can be easily bought and hired. A recent example is the rise in ransomware as a service, often bought by criminals without the skills to restore your files, but who will take your money nonetheless!

But digital risk and digital opportunity are two sides of the same coin. Build security into your digital strategy and this can help your customer experience if you get it right. Regardless of what digital transformation means for your business, whether it be a move to a new cloud-centric services model or an increasingly mobile workforce, you'll need security to achieve your objectives.

'92% of companies see digital as a security opportunity and 73% say digital security is on the board agenda.[1]*'*

For the retail sector specifically, some of the key threats to watch out for include:

- Insider threats via email-based spear phishing
- Attacks on Internet of Things (IoT) devices and platforms used in retail outlets
- New mobile payment devices, which may have unknown vulnerabilities

Retail is increasingly about loyalty and trust. More and more, customers allow retailers to collect personal data in exchange for the benefits of a personalised experience. Cyber-attacks can therefore be more emotional, so there's a great opportunity for retailers to differentiate themselves by offering the most secure service on the market.

As a result the focus is very much on compliance (e.g. GDPR, PCI-DSS) and preventing attacks aimed at sales activity. Retail execs will also be questioning how secure supplier IT systems are, as well as how to counter the increasing vulnerabilities around IoT and multiple IP devices.

In this paper we'll explore the security risks that come with being a digital retailer in a world where becoming increasingly digital is a necessity for business survival.

We'll share our view on some of the new risks CIOs and CSOs need to be aware of, many of which revolve around technologies like Blockchain and biometric identity verification, and recommend what's needed to do it right so that you gain the most from your digital transformation.

General Data Protection Regulation (GDPR):

In May 2018 GDPR becomes law. The core implication of this regulation is that companies must design data protection into their business processes. In fact, GDPR makes explicit reference to this point. Companies must demonstrate that they have the necessary capability and controls in place to protect personal data.

Managing risk is, more than ever, a process; it is a task without an end-point. Companies obviously must embrace digital innovation, but at the same time they should address upfront all security and privacy questions related to any new initiative. Unfortunately, many companies still struggle with this.

Payment Card Industry Data Security Standards (PCI-DSS):

PCI-DSS protect customer card information and prevent agent fraud. These standards must be met by any merchant dealing with card details, and it's crucial that all agents and systems that routinely use card data are fully compliant.

PCI-DSS compliance is a complex on-going process that can be time consuming, expensive, and can sometimes limit business agility. However, non-compliance with these standards could damage your reputation, credibility, and customer loyalty, and expose you to legal issues.

[1] BT KPMG Taking the Offensive - working together to disrupt digital crime report 2016

Security developments within the retail sector

Retailers are an attractive target for cyber-attacks due to the large amount of customer data held.

Retailers are an attractive target

Retailers have been an attractive target for cyber-attacks for years as they have access to large amount of customer data (e.g. credit card details and customers personal information) that can be exploited by criminals to commit identity theft, fraudulent buying, and even corporate espionage.

A number of technologies have opened up new risks, which we'll delve into in more detail:

1. Point-of-Sale (PoS) malware specifically targets the memory where this data is stored in a process called 'RAM scraping'.
2. New payment methods
3. Biometric identify verification
4. Internet of Things (IoT)

1. The security implications of PoS

By finding lapses in the security (e.g. default login credentials or compromised partner systems), PoS malware can use its backdoors and command-and-control features to decide which data to steal and upload to a remote server.

Alternatively, ransomware can hold your systems hostage for financial gain (as heavily publicised by the recent WannaCry ransomware attack on the NHS and Telefonica). Ransomware attacks can have dramatic consequences across your company if unaddressed.

One of the most popular ways to introduce PoS malware has been via social engineering, which is the use of deception to manipulate individuals into divulging confidential or personal information, and phishing emails. Since retail as an industry is characterised by a large proportion of sales employees with little technical experience, education of staff to adhere to your security policy should be a prime concern.

Although the adoption of EMV (Europay, MasterCard and Visa) chip-enabled PoS systems and widespread implementation of PCI-DSS standards have contributed to a sharp decline in PoS malware attacks (88% reduction in new malware variants according to SonicWall[2]), it does not mean the threat is gone, as exemplified by the recent cyber-attacks on Kmart and Chipotle[3]. Unfortunately the progress that was made against PoS malware might have led to an increase of ransomware, which grew by a factor of 167 in 2016[4].

Retailers, and especially e-commerce companies, are vulnerable to ransomware attacks as downtime of their websites is directly linked to profits, making it more likely for cyber criminals to try and profit. Considering the international and technologically complex landscape retailers find themselves in (especially when running both physical and digital environments), a 360-degree view of security is necessary.

This only increases when engaging with third parties, so it is important to consider your network segmentation and segregation strategy, specifically regarding the availability of sensitive payment information. For instance, it is suspected that the major hack into Target's PoS systems in 2013[5] originated from a third party supplier that had more access than strictly necessary, leading to the theft of data for about 40 million debit and credit cards.

Protection against PoS malware and ransomware

In general, protecting yourself against PoS malware and ransomware should be part of your standard security policy. Unfortunately, it seems that the retail industry may be particularly overconfident in their security ability, especially regarding data breaches. As according to research from Tripwire[6] 90 per cent of retailers interviewed said they could detect a critical data breach within a week, and 75 per cent claimed to do it in just 48 hours.

In contrast only 55 per cent of IT professionals interviewed at companies with over $100 million in revenue said that they checked security compliance 'at least weekly'.

Implementation of breach detection tools did not increase over the last year, where 50% of the respondents reported that antivirus tools, intrusion detection systems, and whitelisting solutions were 'only partially or marginally implemented'.

These numbers taken together show that the retail industry still has work to do when it comes to basic security implementation. As a starting point, the guidelines provided by the PCI-DSS should be adhered to at all times (and updated regularly), and some questions to consider are:

- Do you have firewalls, even between networks?
- Are all endpoints secured?
- Is all data doubly encrypted (encrypting and then using SSL)?
- Do you have file integrity and monitoring software in place?

[2] https://blog.sonicwall.com/2017/02/sonicwall-threat-report-reveals-cybersecurity-arms-race/

[3] http://money.cnn.com/2017/05/28/technology/chipotle-credit-card-hack/index.html

[4] https://blog.sonicwall.com/2017/02/sonicwall-threat-report-reveals-cybersecurity-arms-race/

[5] http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html

[6] https://www.tripwire.com/company/press-releases/2016/11/tripwire-study-retailers-overconfident-in-endpoint-cyber-security-despite-point-o/

- Do you use two-factor authentication for all entry points and system configuration changes to the CDE (Cardholder Data Environment)?
- Do you monitor all network and data access?
- Have you ensured only specific whitelisted apps are able to run in the system?
- And lastly, have you developed your segmentation strategy, with regard to third parties you are working with?

As mentioned, a particular emphasis should be put on the education of staff in order to prevent social engineering and phishing attacks, especially when employing many unexperienced staff.

2. New payment methods

With the rise of new and nimble fintech companies, there have been rapid developments in area of payments. These innovations lead to an increase in convenience, accessibility and speed, but also uncertainty. Your understanding of the risks inherent in these new payment methods, and how to mitigate them, should be a prominent component of your security strategy.

Some new methods you will need to consider include:

- Digital Wallets (e.g. PayPal, Google Wallet)
- Mobile Wallets (Android Pay, Apple Pay)
- Mobile Credit Card Payments (CC readers with mobile app)
- P2P mobile payments
- Wireless card payments in supermarkets, hotels, restaurants, vending machines, etc.
- Connected cars that make the car a payment device to allow pay at pump, pay at drive thru for food, remote order/pick-up, and payment for parking meters.

Securing your payment methods

For any payment method that allows digital transactions (e.g. mobile and internet payments), the potential anonymity of not requiring face-to-face contact makes it more attractive for fraud and other criminal activity, as it is harder to verify identity and trace the transactions.

Other risks are related to incomplete or fabricated information, structured or recurring non-reportable transactions, the ability to reload, and a higher velocity and/or frequency of transactions.

Although these problems are not necessarily new, with these new methods they might occur quicker and on a larger scale. In general, the more international (i.e. the less geographical restrictions on use) the payment method, the larger the risk – especially if transactions can occur in jurisdictions with a higher risk for money laundering or terrorist financing[7]. Additionally, risk is increased if there is limited control on user activity and user identity, especially when combined with high frequencies.

The possibility for fraud or other criminal activity is increased where:

a) Value-transfers are possible between two unrelated individuals (online)
b) There is no maximum load value
c) There is no expiry date for the service.

Luckily there are also new ways of verifying the identity of the user, making it easier to manage and mitigate the risk by engaging appropriate service features and control.

The newness of these technologies means that there are still a few regulatory gaps, and in some cases the security of these methods still needs development. In general, these fintech-related developments are hard to regulate, as they are often based on a decentralized model (instead of nodes in the system, which is what regulators are typically familiar with).

Recommendations

To mitigate some of the risks associated with new payments, organisations should, at a minimum, consider implementing controls such as placing specific limits on funding, specifying the parties and methods authorised to fund the accounts, and specifying the nature of the legal tender used to fund the accounts.

Depending on the judged risk of the proposition, stricter identity verification of the service user might be necessary, with screening of users before and throughout the service lifetime. For instance, do you know your users' name and address, which location they will use the service from, their date of birth, and phone number? If not, how can you confirm that they are legitimate users?

Additionally, we recommend you undertake additional security steps and due diligence for any third parties you are working with. Ask whether they adhere to the same (international) standards as your company, check in which jurisdiction are they domiciled, and confirm that there are clear lines of accountability and oversight, and when you can you control whether they actually comply in practice (and not only on paper)? As with PoS systems, proper segmentation and segregation of your network is key here, as it ensures sensitive data is not available to unauthorised parties.

Transaction monitoring is a useful tool here, as it will allow your company to keep track of unusual transactions in terms of frequency, value/volume, location (e.g. high risk countries), and help identify patterns related to typologies (and exceptions to those patterns).

It is also important to record transaction records, especially when concerning suspicious transactions. Aim to be proactive towards the (dynamic) regulatory landscape, not only for compliance's sake, but also to be quicker than your competitors.

[7] http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

3. Biometric identity verification

Biometric identity verification is quickly emerging as a way to ensure security and user-friendliness at the same time.

A key aspect of any biometric technology is that it is stable and shouldn't change significantly over a period of time. As examples, physical biometrics solutions include fingerprint scans, geometry (e.g. finger length), iris and retina scans (using standard video cameras), and vein/vascular patterns (using near infrared light).

Also, there are solutions that rely on behavioural aspects such as voice recognition, computer mouse signature (shape, speed, pressure, timing), gait recognition (how you walk - currently at an experimental stage), and keystroke dynamics (speed and timing).

Security implications

For the retail sector, biometric verification increases inclusion, security and convenience (especially for elderly users that have trouble using chip and PIN systems), and can simplify online and mobile shopping. By establishing the user's integrity you can remove many of the problems related with anonymity, significantly increasing the level of security.

Unfortunately, some of these new techniques are not invulnerable yet, and are in need of more development. For example, in recent news the voice recognition software for HSBC was 'hacked' by a twin to copy his brother's voice[8], and the Samsung Galaxy S8 iris scan[9] was fooled by just printing out a picture of the iris in question and holding it behind a contact lens. Still, it is possible these are teething problems in the road towards a more secure (and convenient) future.

Another consideration is the privacy and storage of biometric data. Anyone implementing this type of system needs to consider who has access to that database, how they access it, what security is in place to avoid it being hacked into, and how users feel about handing over their biometric data and having it stored centrally.

Luckily there are some techniques available to you, like biometric cryptosystems (matching takes place in encrypted domain), private or cancellable biometrics (one-way transformation only), differential privacy systems (biometric data and personal information always stored separately), and smart-card secured templates.

For the latter technique, control is handed over to the card holder, and it removes the uncertainty of matching via a network-connected device, an external server, or a database. There are even new methods being developed to associate a digital identity to an individual while using a token that does not store any data whatsoever (and is therefore useless when lost).

Tokens can be programmed to recognise your biometric data, and generate a unique key that is then sent to the server, to interface with the current authentication portal. Because there is no actual physical data stored, your identity is secure while still allowing the other party to verify that it's really you on the other side.

Although these types of methods are costly, they are developing rapidly, and promise a future where there is no longer a trade-off between security, privacy and ease-of-use.

Recommendations for biometric technology

Biometric identity verification is becoming increasingly popular, and although elements are still being developed it provides definite benefits over traditional usernames and passwords. Still, until the accuracy of biometric technologies can be guaranteed, it is important to have alternatives. A blended approach is advised where traditional and biometric verification support each other.

To determine which method of verification you want to use, two factors are important:

1. FAR (False Acceptance Rate), which gives opportunity for fraud
2. FRR (False Rejection Rate), which results in large consumer inconvenience and frustration.

Companies will generally consider to have a threshold of recognition which allows for a certain amount of false acceptance (fraud) in order to reduce consumer frustration resulting from being falsely rejected. You should consider:

- Would using biometric identity verification add significant value, simplicity and/or ease-of-use to your company, employees or customers?
- Could it solve any security problems you are having now with passwords or verification?
- If so, which method would fit best with your business needs, your existing verification controls, and how would it relate to your FAR-FRR balance?

The adoption of biometrics should be a long-term strategy instead of a short-term upgrade, and that the level of risk should warrant the cost (both of purchase and change), since at least for the near future, installing the necessary biometric solutions still carries a hefty price tag.

[8] http://www.dailymail.co.uk/sciencetech/article-4522062/Brothers-trick-HSBC-voice-recognition-software.html

[9] http://www.mirror.co.uk/tech/samsung-galaxy-s8-hacked-tricksters-10488353

4. Security implications for IoT

Beyond cost savings, businesses are beginning to tap into the IoT for new revenue models, often from products, platforms, and services that enable automated homes, connected cars, and increasingly smart cities.

For the retail industry specifically, common devices and applications include: in-store mobile functions, interactive information hubs in stores, and credit/debit cards that use sensing technology to monitor and take action on behalf of the consumer.

Other potential applications in retail include near field communications sensors that track your instore browsing habits (e.g. items you've picked up and put back) and a raft of radio-frequency identification (RFID) and camera-based tracking technologies, many of which store highly personal customer data.

Regardless of how they're used, many organisations are deploying IoT devices without proper security measures.

This shortcoming is in partly due to many vehicles, shop-floor equipment, and other increasingly IoT-enabled devices not being built with internet connectivity or the requisite security in mind.

The IoT attack surface is magnified by scale, distribution, and the broad spectrum of IoT endpoints, from the very simple to the highly sophisticated. It's possible that some of these devices are not even being monitored.

Many IoT deployments will require real-time analysis and response, which necessitates automated processes that have little or no human involvement.

With IoT devices, however, risks can be transferred from the digital world (e.g. databases) and into the physical realm. Target retail experienced theft of 40 million credit card details through the air conditioning supplier being hacked[10], which gave access to the PoS network. Modern IoT-based building management systems could provide similar means of intrusion if not segregated.

Although there are many sophisticated methods to defend your business from attacks, there are some basic recommendations that will make life harder for would-be attackers. Basic requirements for devices are the ability to system reset to its original manufactured state, disable default passwords (but rather use ones that are unique and reasonably secure), exclude ancillary services that are not required to support its core functions, exclude the possibility of any backdoors, ensure clear availability of device support (online manuals, access to updates, updated instructions, clear contact information), and include a basic support label on every device to help the authorised operator identify it and offer support information.

Specifically for the software/firmware update capability, every network-connected device should have a means for authorised operators to update the device's software and firmware (e.g. software-over-the-air/SOTA and firmware-over-the-air/FOTA). Ideally, the updating process will be highly automated while still providing cryptographic checks to allow updates from an authorised source.

These measures will strengthen the defence of your IT perimeter, leaving you to focus on the prevention of more sophisticated attacks.

[10] https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

The importance of regulatory awareness

In today's increasingly globalised and interrelated environment, companies are subject to a wide variety of laws, standards and regulations.

Regulatory awareness

Being in a highly competitive industry, retailers are under pressure to bring innovation, offers and campaigns to market as quickly as possible. However, balance is key. Businesses should not rush at the expense of security; it needs to be always kept front of mind and be built in from the ground up.

Although providing a full view of all the legislation for retail companies is beyond the scope and scale of this paper, we will briefly discuss two of the largest regulatory developments that will affect most retail companies in Europe (if not across the world): GDPR and PSD2.

More on General Data Protection Regulation (GDPR)

Set to be enforced in May 2018, GDPR covers all automated processing and all processing of personal data which forms or is intended to form part of a filing system. It applies to any organisation:

- With an "establishment" within the EU whether processing takes place within the EU or not
- That offers goods or services to people in the EU
- That monitors people in the EU.

Sanctions for a breach of data are severe; any breach has to be reported within 72 hours, and a two-tiered sanctions regime could lead to fines of up to €20 million or 4% of global annual turnover for the preceding financial year (whichever is the greater) being levied by data watchdogs. For other breaches, the authorities could impose fines on companies of up to €10m or 2% of global annual turnover, again whichever is greater.

In order to not fall behind (and face the considerable penalties), companies should ask themselves:

- Are all decision makers aware of GDPRs impact?
- Are you certain that you are aware of all personal data you hold, how it is communicated, and know whether you should be holding it at all?
- Do you have the proper procedures in check to detect, report and investigate a data breach?
- Have you designated a Data Protection Officer?
- Are you aware of how data travels across your value chain?

These questions and more (and being able to answer them) will help not only avoid reprimands, but also strengthen the amount of trust between you and your customers.

Payment Services Directive 2 (PSD2)

Due to be implemented by early 2018 (but not confirmed), the PSD2 is designed to increase consumer protection, and increase competition and innovation in payments. At the core of PSD2 is the requirement for banks to grant third parties access to a customer's online account/payment services in a regulated and secure way (as if permitted by the customer). In order to provide this access to accounts, banks must also allow for customer identity verification and authentication via APIs.

Access to customer accounts via APIs enables the provision of entirely new types of service that are regulated under PSD2—namely third party payment initiation (provided by Payment Initiation Service Providers or PISPs) and third party account access (provided by Account Information Service Providers or AISPs), that could make the consumer experience far better in the end. In short, this directive clearly benefits new entrants into the market, but can provide a chance for traditional banks as well to gain new customers and provide better service to their existing clientele.

For retailers, this new directive will directly impact how consumers give retailers' permission to access their money, without an intermediary. In a sense this will make life easier for retailers when customers have more than one bank account, but also raises issues when it comes to safeguarding individuals' payment and purchase data. In order to safeguard the system, there will be strong consumer authentication, and an unconditional right to a refund should something go wrong.

It is recommended to approach this regulation proactively and get involved with its current development (there is still uncertainty regarding the technical standards and local variations), rather than waiting to see when exactly it will come into action. We're recommending you ask yourself:

- How does this affect your business' strategy?
- Can you start experimenting now to test your thinking, and maybe even discover any faults before they harm your company?
- Is your infrastructure prepared for the use of open APIs (even if the definitive technical standards are not defined yet)?

Consider how this regulation affects you, whether any parts of your business need to be re-examined, and seriously investigate how responding to the new regulatory landscape quicker than your competitors might benefit you in the long run.

Embedding security as good practice

A practical guide to addressing the challenges.

Don't skip the basics

Many retailers are trying to implement the latest security tools in order to protect themselves against sophisticated attacks. However, many attacks these days still focus on existing hardware and software vulnerabilities.

Based on the challenges outlined, here is where the digital security opportunity lies.

1. Protect what matters most. In other words protect your data regardless of where it is stored or traveling.
2. Harness big data - security, network, and user devices now produce vast quantities of data. The modern challenge is to rapidly make sense of that data; in real-time, to detect and prevent internal and external threats.
3. Comply with regulation - you need to look at your entire security landscape, because it underpins your efforts to comply and protect data.

Organisations can eliminate a large portion of the threat by applying some simple best practice to the way security is managed. For example, at BT we have a dedicated security policy across our business, with centralised patch control and device management[11]. However, good practice isn't just about technology, and it's key to create a distinction between the technical/physical requirements and the people/process, and for each there are some questions you can ask yourself.

Technical considerations

- Do you have an inventory of all authorised devices, so you can block unauthorised ones?
- Are you in control of all the software that is used?
- Do you use anti-virus, anti-spyware, and anti-malware programmes, and are they (consistently) up to date?
- Is your data encrypted properly, both in transit and at rest?

People and process considerations

In addition to raising awareness of regulation and the handling of personal data to ensure compliance, your employees are also key to directly thwarting cyber-attacks, as the 'inadvertent actor' (insiders that commit errors unintentionally or fail to adhere to process and policies) is a major catalyst for these types of attacks.

So ensure you, and they, can answer the following:

- Is there a data breach / incident response plan?
- Do you monitor user activity, especially privileged users?
- Do you have clear roles and responsibilities defined for each employee, with regards to security permissions and responsibilities?
- What kind of training programmes and communication do you have in place to educate your staff?
- Do you conduct penetration tests / ethical hacking (e.g. spear phishing, whaling) to check if your employees act according to policy?

These practices may be familiar to you, but we know they are still being missed in large organisations. We continue to see cyber vulnerabilities (and resulting attacks such as WannaCry) which could have easily been avoided by using simple and known solutions.

But where should we start?

Given the development and, potential threats mentioned, we know it can be a daunting challenge to get started on the 'so what now'.

BT has 70 years of experience in cyber security and over 2500 security personal located in 14 security operating centres globally. Based on our own experience we recommend you start by taking the following steps:

1. Identity your "crown jewels"

Start with identifying your top fifty or hundred business assets that are critical to the successful running of your business. This might include ICT assets (e.g. WANs, LANs, and computers), physical assets like specific buildings, and human assets such as high value individuals, or privileged users like system administrators and data base administrators.

Once you have your list, see if you can answer these questions:

1. What is your most important infrastructure, information, or asset and why?
2. What are your most critical applications and what do you do to test and check them?
3. What are you monitoring proactively, how do you baseline normal and what do you do when you pick up an abnormality?
4. What Distributed Denial of Service (DDOS) protection do you have in place?
5. Do you audit or control the access your partners and third parties have to your critical data?

2. Carry out a risk analysis

- Review all risks and vulnerabilities across the threat landscape. Do a gap analysis, and write a tactical plan to address the most pressing needs.
- Get somebody independent to undertake ethical hacking, e.g. code reviews, penetration testing, red team and social engineering, firewall and host configuration reviews, and network testing both fixed and mobile.

3. Address the gaps

- Review your processes and whether they are actually being applied in your organisation.
- Don't buy lots of new technology, optimise what you have first – e.g. companies are buying advanced big data analytics, but not carrying out basic virus patching.
- Keep rethinking the risks, undertake horizon scanning for new threat vectors, ensure you are proactive not reactive.

4. Consider how technology can help monitor emerging threats

The increasing sophistication and tenacity of cyber criminals mean that no organisation can be 100 per cent assured that its systems are secure. However, businesses can take steps to make successful attacks more difficult, more costly and ultimately much less profitable.

Harnessing big data by applying threat intelligence tools can bring many positives for security, for instance by identifying attackers before they hit; finding previously unknown attacks (e.g. zero days); finding attacks that are in

[11] https://www.cisecurity.org/controls/

progress quicker; and by understanding the impact of a successful attack.

Data analysis and visualisation tools are based on intelligent and self-organising software algorithms, and are applicable to structured and unstructured data feeds. They radically simplify the analysis of complex associations, and enable the user to interact with and enhance the data during the analysis process.

In fact, 48% of companies find it somewhat difficult, and 26% find it very difficult, to assess the quality of threat intelligence feeds[12].

So to ensure that big data is leveraged to get the best effect, and not just used for the sake of using it, there are two basic things to get right from the start.

Make sure you are collecting all the relevant data you need: people, process and technology all need to be taken into account, and stealthier (and more persistent) attacks require more data to discover.

Use visual analysis tools in order to make sense of this mountain of data. By turning threat data into threat intelligence, there is a good chance to learn and improve, which is also increasingly required by regulation.

One way to collect the kind of data you want, but exclude the risk for false positives, is by employing honeypot software, which attracts would-be attackers to systems likely to be of interest; e.g. the computers of executives, and central servers that control user access.

The use of big data and threat intelligence tools can give you a definite edge in the arms race between cybersecurity and cyber-attackers. If you decide (after setting up the basic security measures for your company) that you are ready for the next step, you should consider asking yourself:

- Which software do I choose?
- Which data sources will I use?
- Do I have the necessary skills in-house to work with and interpret the results of the threat analysis?

As long as the security measure fits with your business and weighs up against the cost, there are many options to explore to increase your chances of seeing would-be attackers coming, and even 'trapping' them. After all, as was already stated long ago by the famous warrior poet Sun Tzu; "There can never be enough deception".

Conclusion

Looking forward, the implications of cyber-attack for retailers will become more serious. The pressure will not tail off. The volume of cyber-attacks continues to grow and criminals will exploit soft targets and share intelligence on them with their peers.

With the increased regulation of GDPR, there will be significant fines for businesses failing to protect personal data of any EU citizen. The role of the CIO will change because of the additional pressure of monetary consequences, and demand for CSOs may rise as CIOs look to share the burden.

At the heart of this is getting the basic housekeeping right in terms of people, processes and technology, and having necessary threat intelligence tools to deal with new attack as they will undoubtedly emerge.

The opportunity for retailers' lies in transforming your stores into a truly digital business. It is now possible to combine the best of online and instore to create a joined up customer experience. New payment, authentication and IoT technologies only serve to enrich the customer experience, providing they are implemented securely.

BT is uniquely placed to help you on this journey. We recognise that although our customers often need to address a number of common challenges, in practice individual circumstances mean that a 'one size fits all' approach does not deliver against your needs and expectations.

Our approach, although firmly based on industry best practices, allows our capabilities to be tailored to the individual customer's requirements. We draw upon the wealth of experience and knowledge of prevailing regulation, vertical market requirements and experience of implementing complex solutions.

We can help you:

1. **See the technology in action:** book a visit to see product demonstrations, expertise and process in action at our world-class Security Operations Centre Showcase, or your local showcase.
2. **Develop your strategy:** our BT Security professional services consultants can help you plan, develop and implement your digital transformation strategy.
3. **Get started:** our choice of security assessments are the starting points for building your transformational roadmap and business case.

[12] https://www.youtube.com/watch?v=xnJ_hzmlklg

Find out more: www.bt.com/security

Offices worldwide
The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

Registered office: 81 Newgate Street, London EC1A 7AJ. Registered in England No: 1800000.