



CYBER RESILIENCE TOOLKIT FOR RETAIL



FOREWORD	4	THE CYBER RESILIENCE LIFECYCLE	33
TOP TAKEAWAYS FOR CHIEF EXECUTIVES IN COMPANIES LARGE AND SMALL	8	Prevent	34
Cyber Resilience Strategy	8	Physical to Digital	35
Where Could the Threat Come From?	9	Resources for Prevent	36
What Sort of Threats?	9	Prevent - Covid 19 Security Support Guidance	40
So What Can Be Done?	10	Prepare	41
The Board –The Key Role and Responsibility	11	What to Do?	42
THE BRC TOOLKIT	12	Resources for Prepare	43
Introduction	12	Respond	44
RETAIL AND CYBER RESILIENCE	14	What to Do?	45
Retail in Flux	15	Resources for Respond	46
Personalisation	15	Recover	47
Omnichannel Retailing	16	What to Do?	48
Cyber Security- Why Have It	17	Review	49
WORKING WITH CUSTOMERS AND THE PUBLIC	18	What to Do?	49
TOOLS FOR RETAILERS 20		THE HUMAN ELEMENT IN IT AND CYBER SECURITY	51
For Smes	23	How People Build It Systems	53
RESPONSIBILITIES IN A BUSINESS	24	How People Keep It Systems up-to-Date	53
The Board and The Communications Team	25	How People Use It Systems	54
The Other Main Operational Roles	26	QUICK GUIDE	55
CYBER RESILIENCE – THE ROLE OF BOARDS	27	Public Bodies	56
The Key Messages	29	Relevant Legislation	57
Risk Management and The Board	31	GLOSSARY	58

FOREWORD



HELEN DICKINSON OBE
CHIEF EXECUTIVE,
BRITISH RETAIL CONSORTIUM

The UK is a world leader in digital retail; but as online shopping has blossomed, so too have the threats it faces. Consumers have access to a fantastic range of products with the click of a button, yet criminals are only a few clicks away. And it is not just e-commerce that is affected. From shift patterns and working from home to payroll, from procurement to marketing, processes have been digitised and automated.

It is estimated that every household will have around 15 products connected to the internet in the early 2020s – the Internet of Things – and retailers are being given legal responsibility for helping to make sure these are safe from cyber criminals who can use them as an entry point to the whole system. As the technology evolves, so do the threats; as they evolve, so must our cyber resilience. Every day NCSC is warning businesses of a cyber threat – often just in time.

The move to online retailing either by pure players or omnichannel retailers is not new – but the experience of the coronavirus lockdown brought many more people of all ages to online shopping. This is true for food and essential products and for non-food products where year on year growth rates are around 40-50%.

The reputational risk from a cyber breach and potential loss of personal data is high and can take years to recover: the financial penalty and loss of trust and sales can be daunting. The risk is not confined to large businesses – just as apparently innocent products such as children's toys connected to the internet have proven to present real opportunities to criminals, so too are criminals targeting the information held by smaller retailers perhaps insecurely.

Retailers need to keep their systems and people, whether staff or customers, secure. Our latest figures show that annual spending on cyber-crime prevention, which was £41 million in 2015/16, is now over £186 million. New threats are emerging, and it is essential that retailers, no matter their size, understand cyber security and the measures that can be implemented in order to build resilience.

To help inform, educate and make the industry more secure, we had support from the NCSC to create this toolkit which we hope will assist not only practitioners - but also will help those who are not experts but are responsible at Board and Director level to understand what is necessary to keep their business secure.

This guide is not just about better cyber resilience, it is about better retail; it will support retailers in innovating, competing and exploring new ways of engaging customers. With the industry in a revolution driven by changing consumer expectations and experiences as much as technology, I could not think of a better time to publish this revised toolkit.



IAN LEVY
NCSC TECHNICAL
DIRECTOR

The National Cyber Security Centre's mission is an ambitious one to help make the UK the safest place to live and work online. To achieve this, we work across a spectrum of industries and sectors significant to the UK economy, in particular the retail sector and the multitude of important businesses within it. I am therefore delighted to be able to support the British Retail Consortium (BRC) in the publishing of this updated cyber security toolkit.

As for many industries, the landscape in retail has changed substantially as a result of the COVID-19 pandemic. Throughout this period, NCSC and the retail industry worked together to protect supply and service provision as many retailers and their staff were pivotal to the national efforts to support citizens during the lockdown. I cannot stress how important and vital the retail industry has been throughout the pandemic, whether that has been in rising to the growth of online shopping for food or consumables or in making changes to their business models and finding ways to work differently to reach existing customers and new markets when the ability to trade face to face has been minimal.

We at NCSC are proud to have been able to play our part in supporting this important service. As well as continuing to provide the industry with advice and guidance and access to our tools and services, we have worked closely with BRC and key retail partners to enhance retailer business ability to protect themselves against cyber threats and help to uphold the reputation of the retail industry during the pandemic. We have been helping companies effectively to manage cyber attacks, to build and increase their cyber maturity and knowledge and to become more cyber resilient. We seek to carry on that work as we look to the future and towards a new way of living and working. Examples of some of the bespoke material crafted by NCSC during this period are our homeworking guide, advice on moving your business from physical to digital and on how to use video conference facilities safely. These accessible and actionable products are contained within this toolkit to benefit your business right now and into the future.

As we move forward together, NCSC is committed not only to helping the high street but also online business, small traders and other retail bodies - the whole sector continues to be a primary focus for us. We are keen to provide advice, tools and support, but also to build mutual partnerships, share information and increase collaboration across the retail industry. The more we can work together and support each other, the stronger the sector can be in defending against cyber attacks and in having the right strategies, policies and procedures in place to manage cyber risk appropriately.

We all want to keep customers' data, identity and privacy as safe as can be, and for everyone to be able to continue shopping and browsing online with confidence. This means working together, sharing our knowledge and experience to ensure that the retail sector is well equipped to face the cyber challenges associated with an ever increasing digital world.

Cyber security need not be daunting. There are a number of straightforward best practice measures you can put in place to ensure you are protecting yourself and your customers. For example, using or advocating strong passwords based on three random words, having good staff training and awareness programmes in place, backing up your data regularly and ensuring you know what to do before - and after - a cyber attack happens, as well as who to call when you need help.

The NCSC knows that creating products that are easy to use, with clear and concise guidance for businesses and consumers requires a pioneering approach. This is why this revised BRC toolkit has been written for *retail* specialists and is not aimed at those with a cyber specialism. However, it is also aimed at key decision-makers in the industry to enable them to understand enough about cyber security to be able to make a contribution, to ask the right questions, to articulate the right challenges and to oversee the right responses.

The predecessor to this toolkit represented a major milestone in the development of our partnership work with the retail industry. We are now bringing material up-to-date and broadening our thinking, with new sections on the role of the Board, the human element and detail on the new tools created by NCSC in response to the needs we have heard from the retail industry.

We know that, since it was published in 2017, the last toolkit has been downloaded many thousands of times and has made a hugely valuable contribution, so much so that its concept has been adopted and applied across numerous other sectors. I am sure that this new version will achieve even more success and help you, and the BRC, to ensure that the retail sector continues to make a valuable contribution to keeping our nation cyber secure.

TOP TAKEAWAYS FOR CHIEF EXECUTIVES IN COMPANIES LARGE AND SMALL

The British Retail Consortium (BRC) has developed this Toolkit with the support of the National Cyber Security Centre (NCSC), the UK Government's technical authority on cyber security.

It is primarily for retailers who are non-specialists in cyber security. Deliberately non-technical, our goal is to help you understand cyber security and the practical cyber security measures that are available.

Accountability for implementing strong cyber strategies - which should cover technical, policy and procedural aspects - needs to be driven by the Board in a large company or the CEO in SMEs.

Cyber security is not a luxury: it is a necessity. E-commerce, consumer expectations and data are changing retail and opening up new opportunities for cyber criminals every day. Indeed, the general view is not whether a business will suffer an attack but when - so it needs the best possible protections but also the best possible plan for recovery. In the event of a successful breach share prices can collapse by over 7% on average - sometimes much more - but far less when early appropriate action is taken. The cost of prevention is less than the reputational and financial cost of recovery - so the fewer the occasions on which recovery is necessary the better.

Through the BRC and NCSC, retailers are increasingly collaborating to manage the risks better and at lower cost. Transformational change will be quicker and more effective if we work together as an industry on this shared challenge.

CYBER RESILIENCE STRATEGY

All retailers should have a cyber resilience strategy, which must take account of business and operational imperatives. They must understand the systems and processes that are crucial for the business to function and which data is their most valuable asset, and use that to inform their approach. The strategy must not be limited to IT but expanded to cover issues such as - if there were a breach who would talk to customers and the media; how would the financial position be kept healthy; who would engage with the regulators; and what could the longer term effect be on the business?

WHERE COULD THE THREAT COME FROM?

There are many sources for a potential threat, some are not immediately as obvious as others. They include:

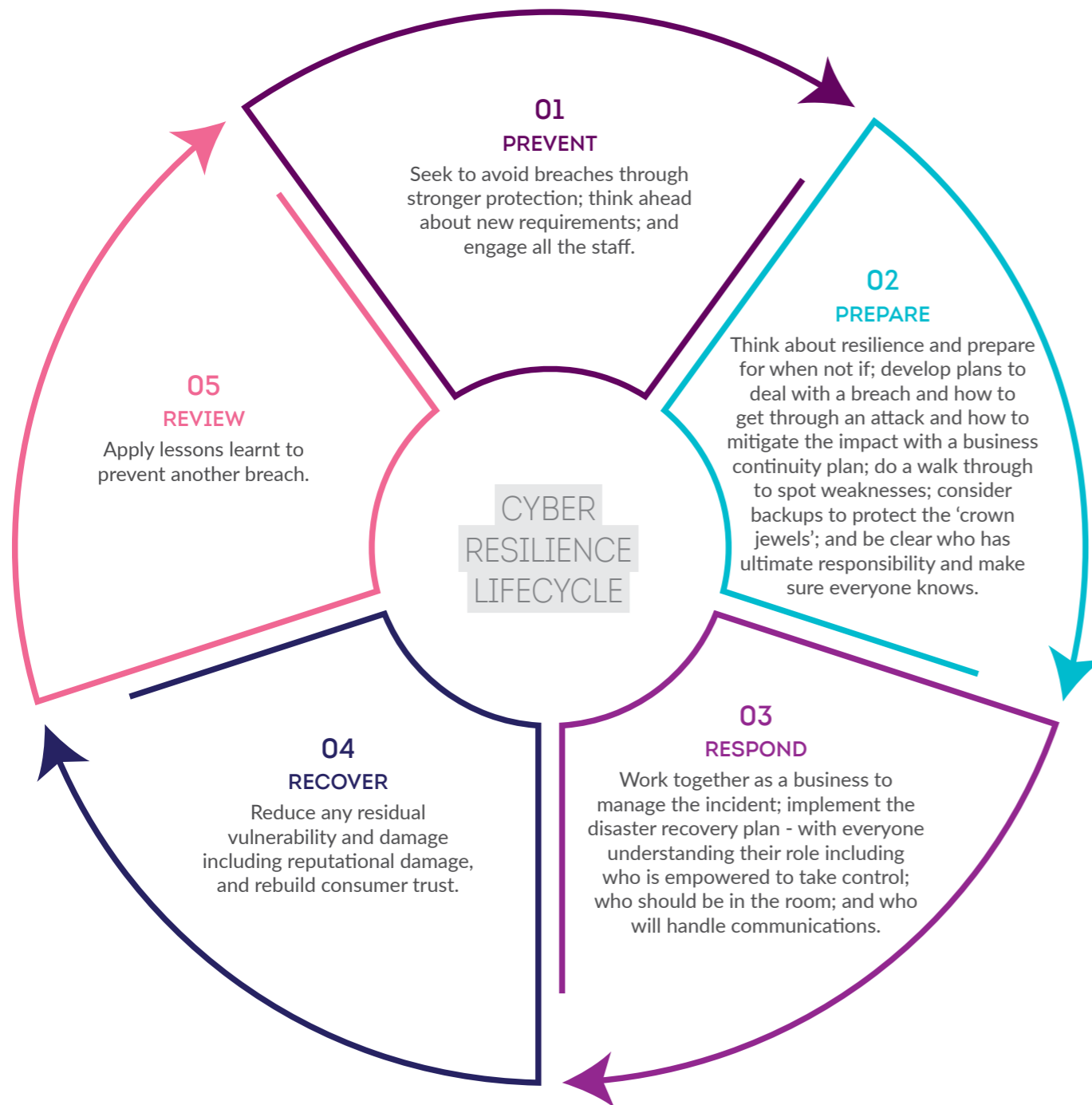
-  People working differently from usual such as at home without the office systems and possibly with IT devices plugged into their wifi
-  Budgets under too much stress to maintain up to date technology and security systems
-  Phishing emails
-  Legacy systems that are not updated and do not have security at their core
-  People with a grievance who become careless and distracted or act maliciously
-  Failure to invest in talent with cyber security capability
-  Third party risks from the weakest link in the supply chain possibly, a small business or one that is new to online that does not see itself as a risk
-  Lack of cyber awareness by everyone in the business - everyone has a responsibility

WHAT SORT OF THREATS?

The main threats today are

-  Ransomware
-  Phishing emails
-  Credential stuffing
-  Planting a virus
-  Denial of service
-  Hacking (e.g. for credit card details of customers via a third party)

SO WHAT CAN BE DONE?



THE BOARD -THE KEY ROLE AND RESPONSIBILITY

The role of the Board – or in a very small company the CEO - is central at all stages. It must work with technical specialists to own and constantly drive improvements in security and develop a culture of secure by design. It should appoint someone to take overall responsibility and report to every meeting – and that person should be recognised throughout the business and be empowered to take decisions. The non-Executive role is one way of bringing in strategic experience of cyber security if necessary.

In particular, the Board should:

- Embed cyber security into the business objectives, structure and culture;**
- Strengthen and develop cyber security expertise;**
- Develop a positive cyber resilience culture;**
- Establish the crown jewels of the business that need protecting at any cost;**
- Understand the specific threats posed to the business;**
- Monitor and manage cyber risk actively;**
- Implement effective cyber security measures;**
- Collaborate with suppliers and partners who may potentially be the weak point through which criminals can gain access;**
- Plan, refine, constantly update and practise the response of the business to cyber incidents;**
- Identify the systems to have in place to function after an attack. These systems may not be the largest or involve the most expensive equipment, but they will be at the heart of the operations;**
- Adopt a 'no blame' culture so that everyone feels free to report potential issues.**

THE BRC TOOLKIT

INTRODUCTION

"Retailers spend record amounts on cyber security, deploying cutting edge systems to keep their customers safe. But attackers are getting more sophisticated, and across a range of industries we see that coming together sensibly gives us all better protection. With the BRC and NCSC, we at the John Lewis Partnership are at the heart of bringing the industry together to be even safer and better prepared, irrespective of size or sector. This toolkit is an excellent starting point for all, although the detail of your approach will depend on your business needs and estate."

Carole Drape, CISO, John Lewis Partnership

This guide has been prepared by the British Retail Consortium (BRC), with support from the National Cyber Security Centre (NCSC) to help the industry become more secure. It is primarily aimed at two groups:

- those, particularly in more strategic or Director level roles, who are not technical experts but whose role and responsibilities increasingly incorporate cyber security strategy or practice. Cyber security is, and must be, a task for everyone in the organisation and should be a key item for every Board of Directors meeting
- newer retailers, such as start-ups, which are now thinking more about how digital commerce or systems can support the next phases of growth.

It is a 'plain English' guide to the cyber security landscape, including

the potential threats

responsibilities

the resources available to explore the issues further

the protections to consider

how to recover



RETAIL AND CYBER RESILIENCE



Retail is placing an increasing premium on digital systems and use of data;



Retailers of all sizes and sectors must be robust in their approach to cyber resilience



Retailers are increasingly collaborating on cyber security through the BRC and NCSC

RETAIL IN FLUX

"All retailers are using data to improve their offer to consumers. Whether it's for to-the-minute predictive distribution networks, which save time and cost and reduce environmental impacts, or giving consumers personalised offers, retailers want to give their customers what they want, when they want. That makes the role of cyber security more important than ever as there's more reliance on more data than ever before, and that trend will only get stronger."

Luke Fairless, Technology Director - Security and Capability, Tesco

Retail is an industry that is evolving quickly not least in the use of and, in some cases, reliance upon, digital tools. The rise of online platforms, marketplaces and proprietary e-commerce sites where large and small companies can sell their own products, has profoundly altered the industry. There are impacts from systems which are widely used across the retail industry, such as e-payment services for e-commerce and cutting-edge AI (Artificial Intelligence) which drives personalisation of alternative product suggestions. There are also technologies used to support the business, such as HR systems and information management systems. Every retailer (even those which do not sell online) is reliant to some degree on connected technology.

PERSONALISATION

Irrespective of sector, business model, size or stage of development, every retailer is reliant on cyber technologies and thus cyber security is a key concern. One major trend in UK retailing has been growing personalisation. This can be seen most clearly in marketing, where a better understanding of what consumers of different types, or even individual consumers themselves, want and how best to make them aware of the available products has revolutionised the industry.

Digital platforms are also driving greater personalisation of the goods being sold, which requires seamless links to the manufacturing and distribution processes. For example, some well-known watch manufacturers now enable those buying certain products to inscribe a name and message onto the strap of their children's watches.

On the whole, an increasingly bespoke offer, whether of products or marketing means the retailer holds more detailed personal information about its customers. This increasingly brings retailers within the scope of the UK Data Protection Act 2018 which implements the EU General Data Protection Regulation (GDPR) as well as making the impact of a breach potentially more severe.

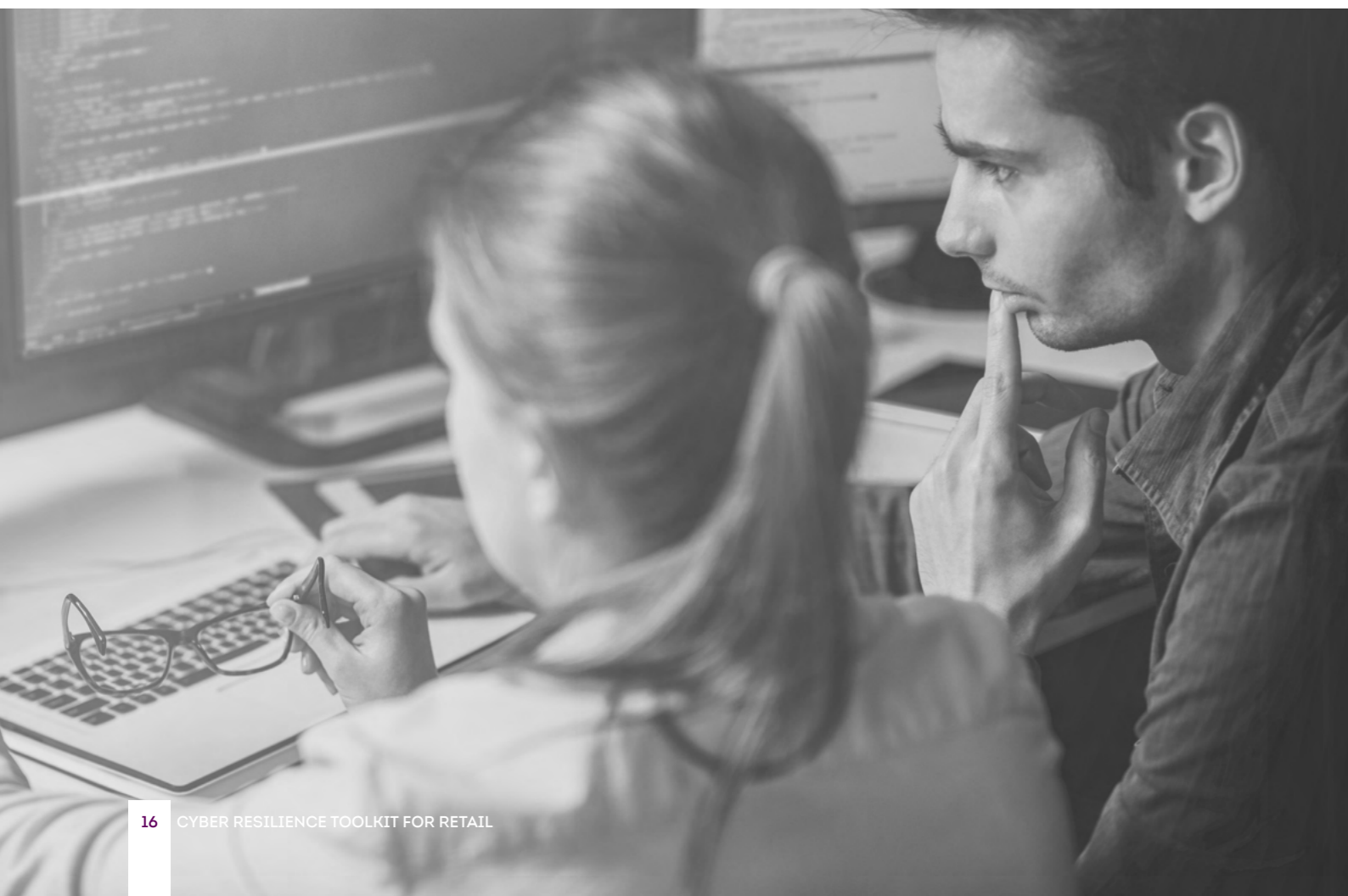
OMNICHANNEL RETAILING

Another major trend is the move towards omnichannel retailing with a mix and match approach. A website may, for example, allow customers to check whether specific products are available in specific stores, minimising wasted trips.

Accurate, comprehensive and available data, often personal data, is at the heart of these improvements. Consumers can consent to provide that data or choose not to and, under the relevant legislation, now have more ways than ever to seek to get that data back. Unless they trust the retailer to hold their data safely, and use it sensibly for their benefit, they will simply take their business elsewhere to someone they do trust.

This reliance on trust is only going to grow, with digital capabilities moving from 'nice to have' to 'business critical'. Without effective cyber security, retailers will lose that trust and the 'licence to innovate' which rich, accurate and complete data can support. Even already in 2017, a PWC survey had found that consumers stated they would take their business elsewhere if they did not believe an organisation was handling their data responsibly.

Retailers should always remember that without effective strategies and techniques they can become 'collateral damage'. Even where they are not targeted themselves, retailers may be caught up unwittingly in a cyber attack on other retailers, their suppliers or other sectors of the economy, which will either undermine confidence generally, or will have a direct impact on the business.



CYBER SECURITY- WHY HAVE IT

Surveys of retailers indicate:

- Across the industry, Chief Information Security Officers (CISOs) report that they are seeing between 400% and 500% growth in the number of cyber attacks compared with a year ago;
- Spending on cyber security has grown considerably: from just over £41 million in 2015/16 to £186 million in 2018/19;
- Among the various main types of cyber attacks, industry experts see credential stuffing and phishing attacks as significant with ransomware a growing concern.

So retailers place a substantial premium on their cyber security work.

- The investment need not always be massive. A few sensible and fairly simple precautions can help to mitigate or reduce the most serious risks substantially.
- Many experts believe strong cyber security and the reputational benefits which go with it are a competitive advantage. For example, The Harvard Business Review, has argued that cyber security should be shifted away from a technical question into a strategic level one, with the role of the CISO also elevated, to drive improved commercial performance.
- There are legal requirements to do so, particularly when personal data is in question or the retailer is operating online.
- Data protection laws can add significantly to the costs of a breach which, if it includes significant loss of personal data, can see a retailer fined up to 4% of global turnover or nearly £20 million, whichever is greater. The wider costs of rectifying the issue - lost trading, legal advice, communications and, most crucially, supporting customers who are affected - can also become very expensive, very quickly, in both monetary and reputational terms.
- In recent cyber attacks there has been a clear and significant upsurge during peak trading periods, such as late December. Recovery from an attack which takes down systems for weeks during those periods might be very difficult.
- There is also a growing imperative around finance. Many institutions require a level of cyber security maturity of their customers. Failure to meet those standards, whether in terms of a level of proactive protection or preparedness to respond if there is a significant breach, can impair the retailer's creditworthiness, significantly increasing the costs of doing business or the ability to recover when there has been a breach.
- A successful attack might easily see highly sensitive commercial information removed and posted for the world at large to see or use to harm a business. The criminal may, for example, rewrite large swathes of data held in critical systems so that it is incorrect, severely hampering a business for a considerable period after the breach.

Where it is in the best interests of their customers, retailers are used to collaborating lawfully to maximise choice, value and safety. Cyber security is an area where retailers are increasingly applying the values of collaboration, working with the BRC and NCSC, to help ensure that the customers they serve are even more secure.

WORKING WITH CUSTOMERS AND THE PUBLIC

“An embedded and sustainable approach is needed where citizens, industry and other partners in society and government, play their full part in securing our networks, services and data”

- UK Cyber Security Strategy -

The retail sector also has a role to play in helping the public keep themselves secure online. An online account with a retailer needs to be protected by the customer as well as the retailer through the use of strong and separate passwords.

Customers can be empowered through the provision of clear, easily understood and easily implemented cyber security advice. By promoting consistent NCSC advice to their customers, a business can be assured that the messages are technically accurate, actionable and timely. They must also be consistent across all online platforms. It will help the public become less confused by cyber security advice if all retailers provide the same information.

Thus the aim should be to:

- Proactively promote cyber security advice to customers, using the National Cyber Security Centre's advice as the template. This advice underpins the government's public awareness campaign on cyber security – Cyber Aware.
 - » Cyber aware is the UK government's national campaign on cyber security led by the NCSC. The campaign provides timely and accessible advice so that individuals and organisations feel confident and empowered to take the necessary actions to protect themselves online. The advice has been developed by technical experts at the NCSC and focuses on the most important and practical steps for individuals to take to improve online security. More details are available at cyberaware.gov.uk

- Provide cyber security advice to customers at relevant points in their buying journey – both online and offline.
- Ensure customers can implement the Cyber Aware advice on an online platform. For example, ensure the business password policy allows customers to use the Three Random Words advice to set their online password for their account.
- Provide a clear and accessible link on the website to report fraud and cyber crime. Customers living in England, Wales or Northern Ireland should report to Action Fraud at actionfraud.police.uk or by calling 0300 123 2020. Customers living in Scotland should report to Police Scotland by calling 101.

In the case of the Internet of Things – consumer products connected to the internet – retailers are to be required to ensure products they sell are secure by design with passwords that are unique. It is estimated that every household will have around 15 such products by the end of 2020 – and even apparently innocent articles like toys can be subject to cyber attacks. With people at home using workplace computers connected to the same network such attacks may have broader implications for a business.



TOOLS FOR RETAILERS

The NCSC and its partners produce and share a wide range of free resources that help retailers of all shapes and sizes make themselves safer, many on nsc.gov.uk. They include:

Board Toolkit

Cyber security is central to an organisation's health and resilience and this responsibility sits with the board.

nsc.gov.uk/collection/board-toolkit

Risk Management Guidance

Guidance to help organisations, regardless of size, make decisions about cyber security risk.

nsc.gov.uk/collection/risk-management-collection

Exercise in a Box

An online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment. It is completely free and you don't have to be an expert to use it.

nsc.gov.uk/information/exercise-in-a-box

Small Business Guide

Five quick and easy steps that small- to medium-sized organisations can implement to significantly reduce the chances of becoming a victim of cyber crime.

nsc.gov.uk/collection/small-business-guide

Small Business Guide: Response & Recovery

Provides small- to medium-sized organisations with guidance about how to prepare their response and plan their recovery from a cyber incident.

nsc.gov.uk/collection/small-business-guidance--response-and-recovery

10 Steps to Cyber Security

A concise summary of NCSC's advice aimed at medium to large organisations. It is designed to help organisations protect themselves in cyberspace. It breaks down the task of defending your networks, systems and information into its essential components, providing advice on how to achieve the best possible security in each of these areas.

nsc.gov.uk/collection/10-steps-to-cyber-security

Top Tips for Staff

A free and easy to use e-learning training package which explains why cyber security is important, how attacks happen and four key areas to focus on.

nsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

Cyber Essentials

A simple but effective, Government-backed certification scheme that will help to protect an organisation, whatever its size, against a whole range of the most common cyber attacks.

There are two levels to the scheme:

Cyber Essentials – a self-assessment option which provides protection against a wide variety of the most common cyber attacks. The certification process has been designed to be lightweight and easy to follow.

Cyber Essentials Plus - Cyber Essentials Plus Certification still has the trademark simplicity approach. The protections you need to have in place are the same, but this time the verification of your cyber security is carried out independently by a Certification Body.

cyberessentials.ncsc.gov.uk/

Cyber Security Information Sharing Partnership (CiSP)

A joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

nsc.gov.uk/information/cyber-security-information-sharing-partnership--cisp-

Reporting an Incident

NCSC provides a 24/7 cyber security incident reporting mechanism. report.ncsc.gov.uk/ Further guidance on Incident Management and how to effectively detect, respond to and resolve cyber incidents can be found at

nsc.gov.uk/collection/incident-management

Cyber Incident Response (CIR)

The NCSC set up the CIR scheme to certify companies which can help organisations which have been the victim of a significant cyber attack.

nsc.gov.uk/information/cir-cyber-incident-response

Cyber Incident Insurance

A guide for organisations of all sizes who are considering purchasing cyber insurance. It is not intended to be a comprehensive cyber insurance buyers guide, but instead focuses on the cyber security aspects of cyber insurance. If you are considering cyber insurance, these questions can be used to frame your discussions. This guidance focuses on standalone cyber insurance policies, but many of these questions may be relevant to cyber insurance where it is included in other policies

nsc.gov.uk/guidance/cyber-insurance-guidance

Cyber Aware

Cyber Aware is the UK government's national campaign on cyber security led by the NCSC.

The campaign provides timely and accessible advice so that individuals and organisations feel confident and empowered to take the necessary actions to protect themselves online.

The advice has been developed by technical experts at the NCSC and focuses on the most important and practical steps that individuals can take. Retailers are encouraged to promote the advice to customers, with campaign assets available at

cyberaware.gov.uk

Supply chain security guidance

A series of 12 principles, designed to help you establish effective control and oversight of your supply chain.

ncsc.gov.uk/collection/supply-chain-security

Logging Made Easy

(LME) A practical way to set up basic end-to-end Windows monitoring of your IT estate.

ncsc.gov.uk/blog-post/logging-made-easy

Business Email Compromise

Guidance to help you spot the signs of targeted phishing emails and steps on how to make yourself a harder target.

Cloud computing

A framework to help you evaluate the security of any cloud service.

ncsc.gov.uk/collection/cloud-security

Email Security & DMARC

NCSC has produced a collection of guides that will enable you to combat the threats to email security, using readily available technology.

ncsc.gov.uk/collection/email-security-and-anti-spoofing

DMARC has also been developed as a collaborative effort to fight phishing and other dangerous email scams.

Secure Business – operating securely with overseas parties

Designed to encourage leaders to think about security and risk management up front when entering into international partnerships.

ncsc.gov.uk/blog-post/thinking-securely-about-international-business

FOR SMEs



SMEs sometimes think they are immune from attack – too small for anyone to care. That is not the case. They can sometimes be used as the entry point for an attack on a larger business they supply or deal with or to steal customer information such as credit card details.



Companies that are at the very start of the pathway that require practical cyber security controls should start off with the NCSC's Small Business Guide and the Small Business Guide: Actions List as they provide quick and easy steps that could save time, money and even a business's reputation.



Just as for larger businesses, alongside essential cyber security controls, small businesses need to be prepared for how to cope and deal with a cyber breach or attack. When something happens, such as a cyber incident, it can be difficult to know how to react. The best way to help limit the impact of a cyber breach on a business is for the business to be prepared. The NCSC understand you will want to resolve the problem and get back to business as soon as possible.



The NCSC have launched the Small Business Guide: Response & Recovery – a simple, easy to use guide to help small businesses prepare their response and plan their recovery to a cyber incident. It is a five-step guide which takes users through the process from preparing for incidents through to learning lessons from them.

More information:

ncsc.gov.uk/small-business-guide

ncsc.gov.uk/small-business-guide-actions

ncsc.gov.uk/small-business-guidance--response-and-recovery

RESPONSIBILITIES IN A BUSINESS

Cyber security is not a matter that can be addressed by the IT security department alone, nor is there a 'magic bullet' for achieving digital resilience. It is a cross-cutting corporate issue that demands a collective response, and it is vital in this context that all business functions understand, and implement, their respective roles in achieving the necessary levels of protection, and in dealing with any response to a breach.

THE BOARD AND THE COMMUNICATIONS TEAM

A Board member should be responsible for the operational aspects of the Board's responsibilities – and it should be clear to everyone in the business who that person is. That person should be empowered to act on behalf of the Board.

The Board and the Communications team each have crucial roles.

They should be asking themselves some key questions.

Board	Communications Team
Are we aware of, and content with, our Information Security Strategy, including representation on our Cyber Steering Committee?	Do we have a dedicated Communication Strategy for the incident response plan, focused on supporting customers and handling the Media?
Underpinning the strategy, have we completed a cyber security risk assessment for our company, and do we keep it under regular review?	What is our policy on the details we will publicise in the event of a data breach, when we will do this, and with whom will we communicate?
<p>Do we have an Incident Management Plan in place and is it regularly reviewed?</p> <p>Is this plan integrated into our wider Business Continuity plans?</p> <p>Have we invested sufficiently in Cyber Protection?</p> <ul style="list-style-type: none"> Do we have sufficiently qualified staff? Have we invested in the appropriate technology (Penetration Testing, etc.)? Do we have appropriate cyber security training and an exercising regime across the business? 	<p>Have we arranged cyber security-related media training for a nominated Board Member and/or the CEO?</p> <p>Have we developed a strategy to maintain ongoing communications with customers?</p>
Is our company engaged in relevant external initiatives (e.g. CiSP, BRC IT Community)	Have we implemented an internal communications plan to promote cyber security amongst staff?
Have we made preparations to report any incident to the appropriate authorities, and conducted a post-incident review?	Have we liaised with communications teams across our supply chain to mitigate vulnerabilities?

THE OTHER MAIN OPERATIONAL ROLES

Beyond the Board, every organisation will manage its cyber security differently, and there is no 'one size fits all' model that will work for everyone. But there are some roles and responsibilities which may be used within a retailer to manage its cyber security. Some or all may be part of a bought-in service or may be employed by the software provider themselves.

- Chief Information Officers (CIO) will usually be the most senior people within a retailer directly responsible for the use and, with the CISO, protection of information and data. Increasingly on the Board themselves and reporting directly to the Chief Executive Officer, they have oversight of using and keeping information secure.
- Chief Information Security Officers (CISO) will usually be the most senior people within a retailer directly responsible for the protection of information and data. Usually reporting to the CIO, the CISO should have a degree of ownership of implementation of the overarching cyber resilience strategy. Increasingly, having a CISO operate at the strategic level is seen as a key driver of improved commercial performance.
- Data Protection Officers (DPO) have a leadership role within a retailer with responsibility for overseeing that retailer's data protection strategy and implementation to ensure compliance with the Data Protection Act. This role is a requirement for retailers which carry out certain types of processing, such as collecting information from individuals on a large or systematic basis. There is substantial guidance on the ICO's website, and if there is any doubt as to whether a DPO is required, proper legal advice should be sought. Several retailers can come together to appoint a single DPO.
 - » DPOs must be independent, properly qualified and report to the highest levels of management. They must also be appropriately resourced to discharge their duties.
 - » DPOs are the lead executive looking at Data Protection Act compliance and the contact point for engagement with the ICO. The role includes advising on and assisting projects that make use of personal data to ensure high (and lawful) standards are maintained.
 - » Even when not required by law to do so, it may be good practice to appoint a DPO where, for example, the retailer holds a considerable amount of personal data about its customers or staff.
- Non Executive Directors (NEDs) are members of the Board of Directors and, as people without executive responsibilities, can have a wider view and provide an objective challenge function. As people with a background in a particular specialist area they can be an important source of knowledge. Increasingly it is thought that cyber security is a specialism for which NEDs might be recruited.
- Network Defenders specialise in recognising, preventing and neutralising threats to a computer network. They are usually charged with understanding a retailer's network (and advising on its design from a security perspective), installing and managing security controls and devices and creating and implementing the security policies.
- Penetration Testers use known techniques to probe an IT system for weaknesses and vulnerabilities without causing harm or loss, or corrupting data. They will then provide support and guidance to the host retailer, allowing them to close any gaps and fill in any weaknesses in their system before criminals exploit them.
- Security Architects are the individuals responsible for designing, building and maintaining the security structures for a retailer's computing systems, usually reporting to a CISO.

CYBER RESILIENCE – THE ROLE OF BOARDS



Cyber Resilience must be a Board level subject



Boards should work through the nine key messages and 'own' overall risk management.



Boards might look to the Non-Executive Director role to bring in key experience.

"Cyber security is not an I.T. issue, it is a boardroom issue"

- Elizabeth Denham, Information Commissioner -

“Research feedback from board directors often reveals that all too often they struggle to obtain the kind of meaningful information necessary for making informed decisions about their organisational resilience to growing cyber-attacks. They want to understand the potential impact for their strategic goals and the risks to business continuity and hard-won reputations.

This means cyber risks and vulnerabilities need to be communicated in boardroom language and related to the critical business ambitions of the organisation. In the event of an attack any retail organisation needs to have a tried and tested response plan - make sure you know who will take the tough decisions and how and when these will be communicated. Who will reassure customers? Who will talk to and manage the media? Who will keep staff updated and who will be leading and co-ordinating any response? All critical questions that can't wait to be answered when it's too late.”

Nick Wilding, General Manager of Cyber Resilience, Axelos

In retail, as in other industries, cyber security has long since stopped being a topic which can be managed and overseen without the Board's oversight. It is, a substantial risk that can have extremely serious implications. It can easily wipe out a whole organisation virtually overnight, with the potential to destroy value, reputation, growth and jobs.

To tackle this effectively, boards need to get a “little bit technical”. To assist with this, the NCSC has designed the Cyber Security Toolkit for Boards. The toolkit encourages essential discussions about cyber security to take place between the Board and their technical experts. It is based on extensive consultation with industry and the NCSC's unique insights into cyber security.

It aims to equip boards with the questions they need to ask to understand the cyber risk to their business, what they care about and how to defend it. Asking these questions and understanding what answers Boards may receive will help them protect their business.

The NCSC toolkit is freely available on the NCSC's website at

ncsc.gov.uk/collection/board-toolkit

The guidance contains nine sections, each one containing straightforward guidance and helpful questions that board members can ask.

THE KEY MESSAGES

1. Embedding cyber security into your structure and objectives

Cyber security should not be left to just one member of the Board. A cyber security incident will affect the whole organisation – not just the IT department. All board members should have an understanding of how cyber security relates to their area of responsibility, and also any broad implications for the organisation as a whole. It may be good to have an expert on the board and increasingly Non-Executive Directors with specialist knowledge of this area are being retained to assist.

2. Growing cyber security expertise

Everyone on the board should understand what cyber expertise the organisation has and what it needs.

3. Developing a positive cyber security culture

A positive security culture where people feel safe to raise security concerns and challenge ineffective security practices will help you build security that works for your organisation.

4. Establishing your baseline and identifying what you care about most

Work out what you care about the most. This is vital, as no company can protect against all of the risks all of the time.

5. Understanding the cyber security threat

Understand the threats that are relevant to your organisation. Not everyone faces the same level or type of risk, so try to understand yours thoroughly and plan and react accordingly.

6. Risk management for cyber security

Make sure that cyber security risk is integrated with the company's approach to managing other business risks. Cyber security decisions should not be made in isolation, they have to work for the business.

7. Implementing effective cyber security measures

Implement defences that will protect the company's critical assets against the biggest threats, tailoring defences to mitigate against the highest priority risks. Then test for effectiveness and take action on the results.

8. Collaborating with suppliers and partners

Build cyber security into relationships with partners and suppliers. Understand what they have access to, set clear expectations for how they protect your data, and build security into all agreements from the outset.

9. Planning your response to cyber incidents

Have an incident management plan, test it and learn from it. Make sure your plan covers all the main topics and includes all the necessary people. So, for example, how are you going to manage your public communications, and what are you going to say with a journalist's microphone under your nose? Who at your bank will you talk to if you need to organise additional lines of credit quickly?

RISK MANAGEMENT AND THE BOARD

The risk assessment should be owned by someone on the board.

The threat of cyber attacks and online criminality is here to stay, and retailers should be realistic that no business can protect itself 100 per cent against all risks. Not only are e-commerce systems potential targets, but also wider business systems, such as payroll and staff information records. Cyber security in the retail industry can however be improved by implementing effective risk management processes. Understanding the nature of the cyber risks to a business on an ongoing basis is a central component of an effective approach; it forms the baseline understanding against which appropriate measures can be installed to protect digital assets.

In completing a cyber security risk assessment, retailers should consider the various types of risks facing their companies, their potential range and scale and the whole-organisation response that may be needed when tackling them. Prepared and practised teams can deal with unanticipated much more easily problems than those for whom everything in the situation is new.

While ownership of the assessment is for someone on the Board, it must draw on the expertise of functional areas across the business to address questions including



What would be the impact of a cyber security incident to your business?



What are your sensitive and / or business' critical digital assets (e.g. customer data / payment systems)?



Where do your sensitive and / or business' critical digital assets reside?



Who has access to these assets, and how is this being controlled and monitored?



Who might want to access these assets and why?



Do you have an Incident Management Plan in place with responsibilities understood across the business, overseen by a cross-functional committee?



What are the access pathways to your systems (e.g. points of sale / wireless / USBs)?



What (if any) cyber vulnerabilities are introduced to your business through its supply chain?



Who holds the customer data you are processing (e.g. third-party supplier, cloud services)?



What proportion of your sales are conducted online?



Are you aware of the existence of legacy IT systems within the business, and are sufficient steps being taken to protect them?



What level of investment has your company made in cyber security systems and processes to date?



What access (if any) does your business have to cyber / information resilience skills?



Are any proposed new cyber security measures proportionate?



How regularly does your business review (i.e. testing plans and processes in a structured, robust and independent manner) its cyber security preparedness through exercises such as 'red teaming' or the NCSC Exercise in a Box Tool?



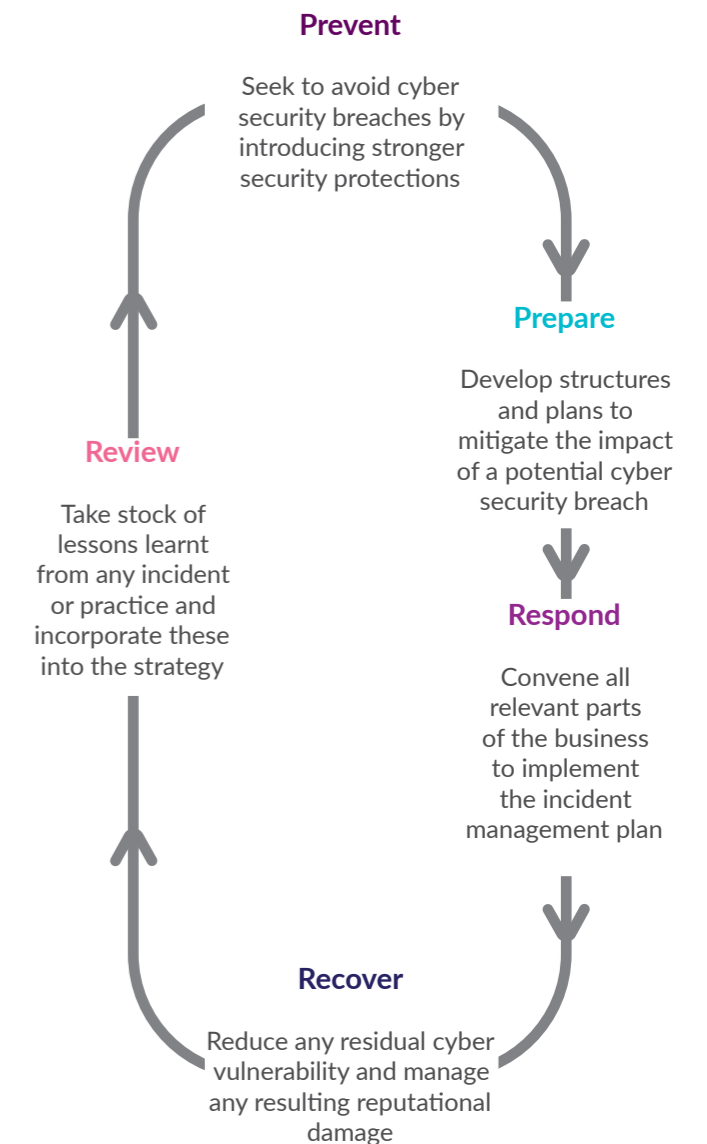
Does your business routinely invest in cyber security exercising and awareness training across the business.

It is important to stress that the process of cyber security risk management is not a one-off exercise. Any company's assessment of the risk should be kept under constant review.

Further information on effective cyber security risk management processes is set out in the NCSC's 10 Steps to Cyber Security guidance: [ncsc.gov.uk/guidance/10-steps-cyber-security](https://www.ncsc.gov.uk/guidance/10-steps-cyber-security)

THE CYBER RESILIENCE LIFECYCLE

Having assessed the cyber security risks facing the business, retailers are encouraged to consider adopting a full lifecycle approach to cyber security incident management within the company's overarching information security strategy, every aspect of which should be overseen by a nominated member of the board. To achieve this, companies could make use of the cyber resilience lifecycle for retailers comprising the following five streams of activity (P-P-R-R-R):



PREVENT

Recommended Roles and Responsibilities for PREVENT:

Nominated Board Member	Ultimate ownership of Information Security Strategy. Facilitate regular discussions on cyber security strategy at board level. Ensure company completes (and regularly reviews) a risk assessment
Finance Director	Ownership of ensuring company invests in cyber security
Communications	Promotion of cyber hygiene across business through internal communications
Human Resources Director	Ensuring cyber security awareness is driven across the business through training and development activity
CISO	Operational implementation of all technical cyber security aspects. Responsibility for signing up to Cyber Essentials
Data Controllers	Responsibility for ensuring awareness of DPA/ GDPR requirements across business and associated reporting

A basic minimum level of protection can be achieved by ensuring that all staff develop basic cyber security awareness and competence through training, and by companies gaining certification through Cyber Essentials.

A retailer should place a strong emphasis on installing and embedding a preventative cyber security culture all the way across its business, and ideally throughout its supply chain.

In practice, this means introducing strong cyber security protections as well as encouraging, through training and exercising, practical cyber security measures among employees, contractors and customers. Often small changes in behaviour can lead to tangible benefits for corporate cyber resilience.

One relatively new area is connected devices, including 'BYOD' – Bring Your Own Device to Work. Retailers now regularly allow (or encourage) colleagues to use their own devices for work purposes, such as dealing with (non-confidential) email on their personal mobile phone through an App. This can be very sensible and boost productivity but may require a slightly refined approach to cyber security than other, more traditional, approaches. Certainly, it is worth any retailer going down this path developing specific guidelines and controls for this kind of approach and, for example, thinking about which systems and data should be isolated from connected devices, stopping the use of default passwords and taking action when devices stop being supported.

PHYSICAL TO DIGITAL

Many businesses have moved from the physical to the digital world. Doing this securely can not only help them grow confidently and sustainably, but also help to uphold their reputation with their customers.

For SMEs who have moved to include delivery of the business online, answering the questions below should help establish a baseline of their security status to identify areas which may need attention:

What technology do you already use?

Are you using cloud services?

Do you have access to IT support?

What cyber security measures do you have in place?

Are there any regulations you need to follow?

Do you have cyber insurance?

Finally, it is important to make sure that all devices and applications are kept up to date. Applying software updates is one of the most important things anyone can do to protect themselves online. All the apps (and the device's operating system) should be updated whenever prompted. It will add new features and immediately improve its security.



RESOURCES FOR PREVENT

<p>CYBER SECURITY TOOLKIT FOR BOARDS</p> <p>Cyber security is central to an organisation's health and resilience and this responsibility sits with the board</p>	<p>Value The toolkit aims to equip Boards with the questions they need to ask to understand the cyber risk to their business and to understand what they care about and how to defend it. Asking these questions and understanding what answers Boards may receive will help them protect their business.</p> <p>More Information ncsc.gov.uk/collection/board-toolkit</p>
<p>SMALL BUSINESS GUIDE</p> <p>Five quick and easy steps that small-to medium-sized organisations can implement to significantly reduce the chance of becoming a victim of cyber crime.</p>	<p>Value Following the five quick and easy steps outlined in the guide could save time, money and even your business's reputation. The guide cannot guarantee protection from all types of cyber attack, but the steps outlined in the guide can significantly reduce the chances of a business becoming a victim of cyber crime.</p> <p>More Information ncsc.gov.uk/blog-post/cyber-security-small-business-guide</p>
<p>SMALL BUSINESS GUIDE: RESPONSE AND RECOVERY</p> <p>Provides small to medium sized organisations with guidance about how to prepare their response and plan their recovery from a cyber incident.</p>	<p>Value Should the worst happen, you will know how to react, as the guide takes you through the process from preparing for incidents, to resolving plural incidents and learning from them.</p> <p>More Information ncsc.gov.uk/collection/small-business-guidance--response-and-recovery</p>
<p>ISO 27001</p> <p>The ISO 27000 family of standards helps organisations keep information assets secure. Using this standard will help your organisation manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.</p>	<p>Value ISO/IEC 27001 is a well-known, basic standard providing requirements for an information security management system.</p> <p>More Information iso.org/iso/home/standards/management-standards/iso27001.htm</p>

<p>SECURITY TRAINING</p> <p>Free introductory courses that help retailers and their staff understand cyber security.</p>	<p>Value Access free online training for you and your staff.</p> <p>NCSC Top Tips for Staff Training – A free and easy to use e-learning training package which explains why cyber security is important, how attacks happen and four key areas to focus on: ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available</p> <p>Cyber security training for business: gov.uk/government/collections/cyber-security-training-for-business</p> <p>Introduction to Cyber Security course offers a comprehensive introduction to cyber security and how to protect your digital life online: futurelearn.com/courses/introduction-to-cyber-security</p>
<p>CYBER ESSENTIALS</p> <p>Cyber Essentials is a simple but effective, Government-backed scheme that will help you to protect your organisation whatever its size, against a whole range of the most common cyber attacks.</p> <p>There are three levels of engagement aligned to the level of commitment your organisation is able to sustain:</p> <ol style="list-style-type: none"> 1. Cyber Security terminology familiarisations to gain enough knowledge to begin securing your IT. 2. If you need more certainty in your cyber security, you can go for basic, or entry level Cyber Essentials certification. 3. For those who want to take cyber security further, you can go for Cyber Essentials Plus certification. 	<p>Value</p> <p>Cyber Essentials – the NCSC self-assessment option gives protection against a wide variety of the most common cyber attacks. Certification gives you peace of mind that your defences will protect against the vast majority of common cyber attacks.</p> <p>Cyber Essentials Plus - still has the Cyber Essentials trademark simplicity of approach, and the protections needed to put in place are the same, but this time the verification of your cyber security is carried out independently by your Certification Body.</p> <p>More information cyberessentials.ncsc.gov.uk/</p>

10 STEPS TO CYBER SECURITY

A summary of NCSC's cyber security advice for medium to large organisations, which also directs people to more in-depth advice.

Value

Though not retail-specific, NCSC offers this free guidance on how organisations can manage their security risks.

More information

[ncsc.gov.uk/guidance/10-steps-cyber-security](https://www.ncsc.gov.uk/guidance/10-steps-cyber-security)

EMAIL SECURITY & DMARC

Email is a core business tool that is vital to many business processes whatever the size of an organisation. Email spoofing as such is often the focus of criminal activity, both as the initial route to attack an organisation or as the channel to facilitate fraudulent activity. Various organisations have come together to find ways to combat this threat at internet level as well as at an organisational level. Domain-based Message Authentication, Reporting and Conformance (DMARC) has been developed to fight phishing and other dangerous email scams.

Value

DMARC allows you to set a policy for how receiving email servers should handle email which doesn't pass other spoofing checks. DMARC also generates reports, which can be used to understand how emails are being handled.

The NCSC has also produced a collection of guides that will enable you to combat these threats using readily available technology.

More information

[ncsc.gov.uk/collection/email-security-and-anti-spoofing](https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing)

CYBER SECURITY INFORMATION SHARING PARTNERSHIP

The Cyber Security Information Sharing Partnership (CiSP), part of the NCSC, is a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.

Value

Retail participants of CiSP benefit from access to the retail group on the platform, which is populated with additional material, content and discussion points. Joining CiSP will also provide retailers with access to other tools which will help to protect an organisations resilience. Working together in this way, businesses are helping to protect each other on an industry-wide basis.

More information and to register

<https://www.ncsc.gov.uk/section/keep-up-to-date/cisp>

RISK MANAGEMENT GUIDANCE

Guidance to help organisations, regardless of size, make decisions about cyber security risk.

Exploring techniques of looking at risk, the core concepts behind each technique and the types of problems each is suitable (or not) to apply to.

Value

To manage cyber risk effectively, we need to apply a variety of different techniques. Therefore having an understanding of the strengths and weaknesses of the techniques can help to select and apply appropriate alternatives.

More Information

<https://www.ncsc.gov.uk/collection/risk-management-collection>

SUPPLY CHAIN SECURITY GUIDANCE

A series of 12 principles, designed to help you establish effective control and oversight of your supply chain.

Value

The guidance will provide organisations with an improved awareness of supply chain security, as well as helping to raise the baseline level of competence in this regard, through the continued adoption of good practice.

More Information

[ncsc.gov.uk/collection/supply-chain-security](https://www.ncsc.gov.uk/collection/supply-chain-security)



PREVENT - COVID 19 SECURITY SUPPORT GUIDANCE

Covid-19 has resulted in many businesses altering their ways of working often for the long term. Businesses reacted quickly to imposed constraints by increasing reliance on IT and digital technology to keep their business active.

The NCSC has created the Covid-19 SME support package to specifically support businesses who have had to increase their digital working. These documents were released as part of its COVID support work but remain important and relevant as businesses transition to a new way of working.

The support package consists of the following guidance documents:

Home working: preparing your organisation and staff;

Video conferencing services: security guidance for organisations; and

Moving your business from the physical to the digital

By working through the support pack, businesses can gain a clearer understanding of their current cyber security arrangement and know how to implement security controls where needed. This should give them the confidence that the business and operations are secure online.

Home working

For various reasons including Covid-19 many businesses have encouraged more of their staff to work from home. While home working may not be new to many organisations and employees, many have been forced to adopt remote working at a greater scale and with speed. This presents new risks and security challenges which need to be addressed.

Businesses should consider the increased risks which come from homeworking where staff may need to use personal devices or removable media to continue their work. This includes assessing the access staff have to corporate systems and whether staff require new accounts to be set up to manage their workload.

Organisations should also consider the security of the additional services required so teams can continue to collaborate including, for example, video conferencing services which provide chat rooms, teleconferencing and document sharing.

Video Conferencing Services

While these services provide greater flexibility for staff working, businesses need to consider the security controls when using these services.

Only software from trusted sources should be downloaded and privacy settings should be checked before installing. There are several video teleconferencing platforms, so the features available should be understood before deciding which service is right for the business. Once installed, the video conferencing account should be protected with a strong password.

It is also important to control who joins a video conferencing call. For specific instructions, refer to the support website of the service. But more generally, NCSC advises not to make the call public, know who is joining the call and that people consider their surroundings when using video functionality.

PREPARE

WHO DOES WHAT?

Recommended Roles and Responsibilities on **PREPARE**:

Nominated Board Member	<p>Ensure creation of Incident Management Plan by the Leadership Team</p> <p>Ensure cyber training / exercising takes place across the business</p>
Finance Director	<p>Allocate funding to cyber security skills, training and exercising in business</p>
Communications	<p>Integrate cyber security awareness in customer engagement strategy</p> <p>Lead work on what information will be shared and when during an incident</p>
CISO	<p>Advise Board on internal capability / need to appoint external support</p> <p>Allocate staff to contribute to CiSP</p> <p>Encrypt and back up business critical data</p>
Data Controllers	<p>Ensure Board are aware of responsibilities arising from DPA/GDPR</p>

This section outlines guidance for retailers on how to prepare for serious cyber security incidents such as data breaches.

The following information draws upon, and seeks to elaborate in a more retail-specific manner, a wide range of existing 'best practice' incident management guidance, including the relevant aspects of the NCSC's '10 Steps to Cyber Security'.

WHAT TO DO?

INCIDENT RESPONSE PLAN

Create an Incident response plan, drawing on all elements of the incident management section of the '10 Steps to Cyber Security'. The plan should include, amongst other issues:



An indication of senior management approval and backing for the plan



An overview of what information will be shared, when, and with whom



An overview of the specialist training that underpins the response



Guidance on the collection and analysis of post-incident evidence



An outline of the roles and responsibilities across the organisation, including lines of internal communication



A commitment to conduct a lessons learned review (see 'Review' below)



Details on the company's data recovery capability



A plan for educating users and maintaining their awareness



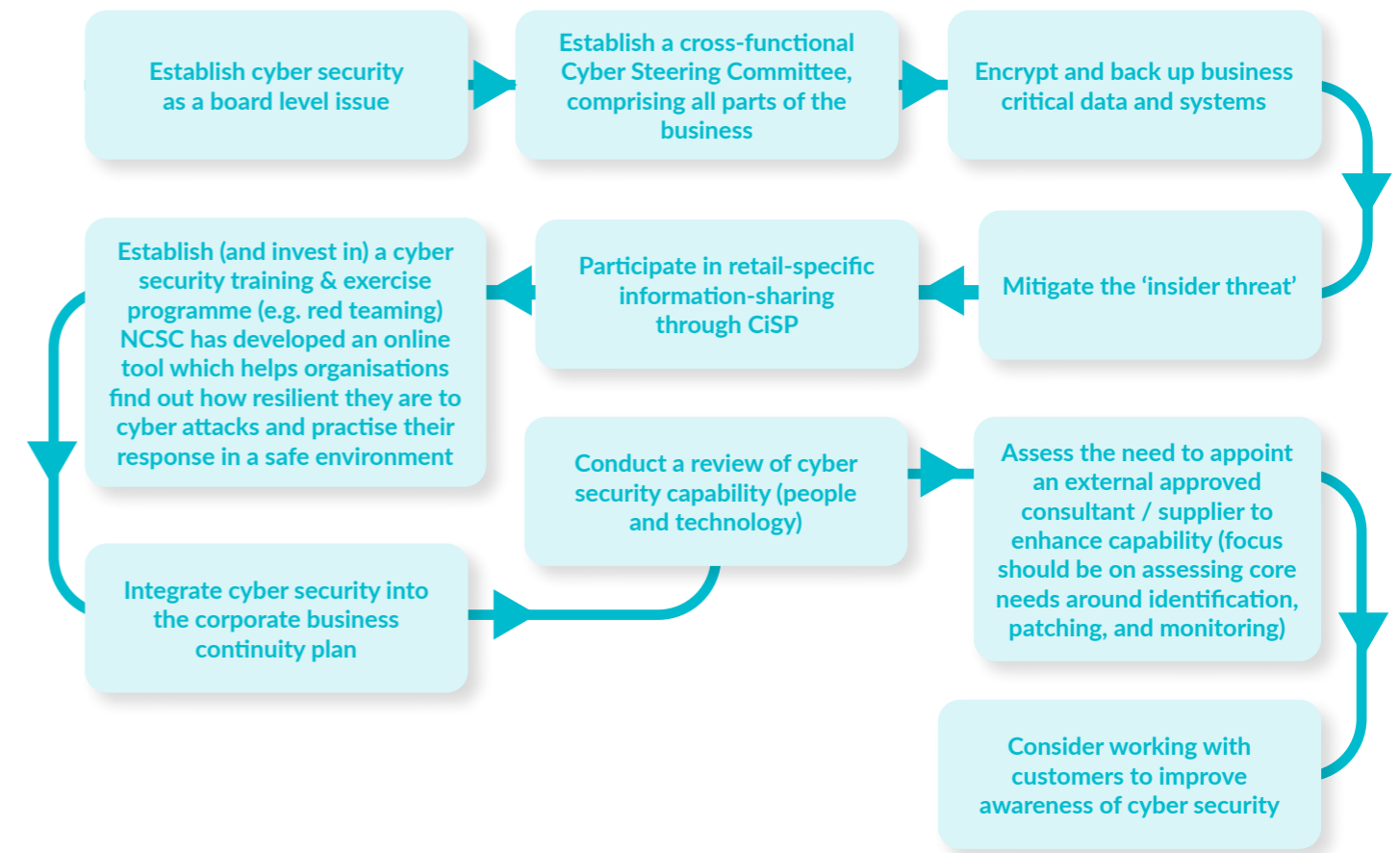
Overview of company's strategy for monitoring all ICT systems



A stated commitment to report criminal incidents to Law Enforcement (see 'Respond' below)



A schedule on regular testing of the incident management plans



RESOURCES FOR PREPARE

EXERCISE IN A BOX

An online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment.

Value

The tool provides exercises, based around the main cyber threats, which organisations can do in their own time, in a safe environment, as many times as they want. It includes everything needed for setting up, planning, delivery, and post-exercise activity, all in one place.

It is completely free, and does not require expertise.

More information

ncsc.gov.uk/information/exercise-in-a-box

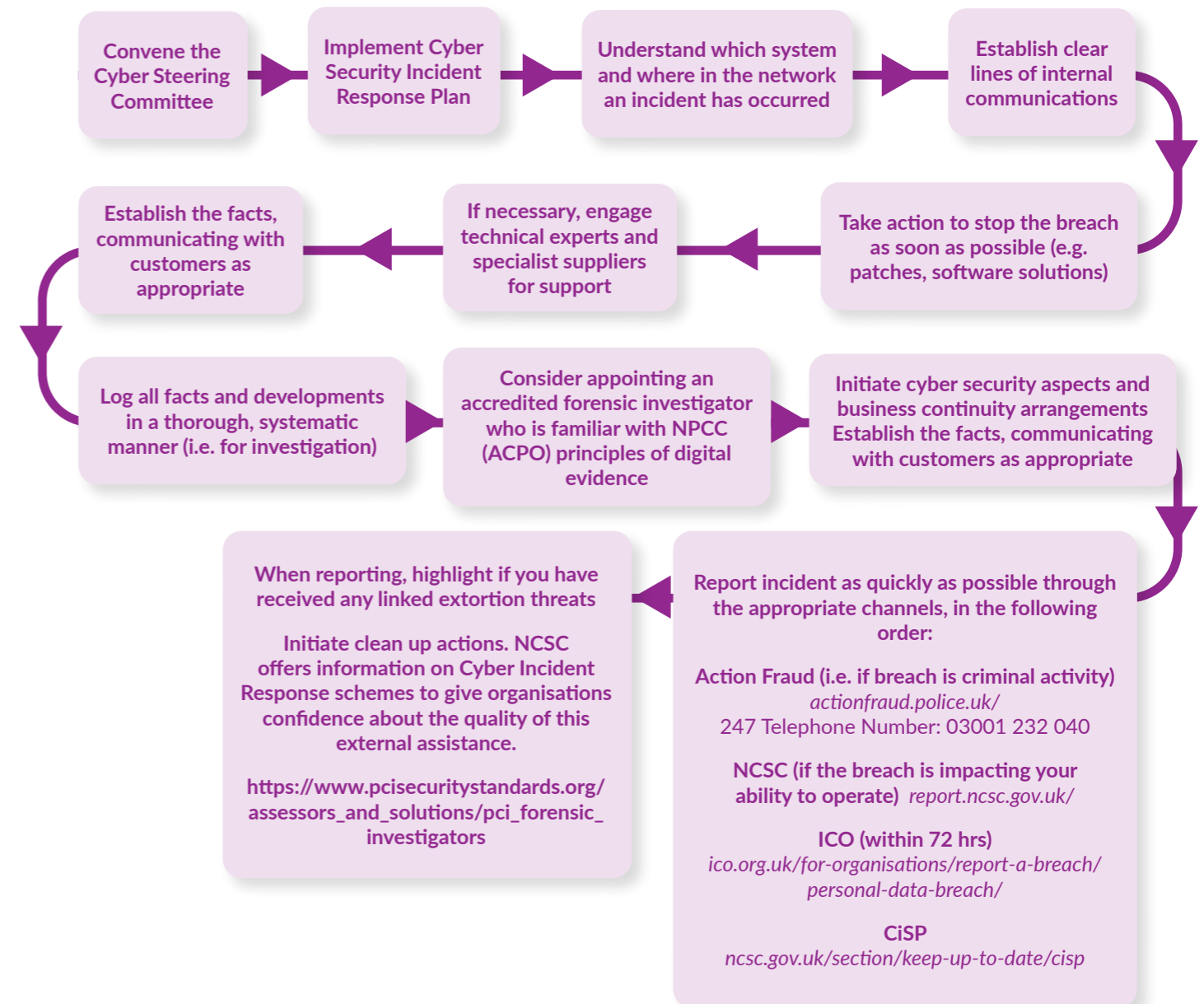
RESPOND

WHO DOES WHAT?

Recommended Roles and Responsibilities on **RESPOND**:

Nominated Board Member	<ul style="list-style-type: none"> Convene Steering Committee Oversight of implementation of Incident Management Plan Appoint additional support as required (working with CISO)
Finance Director	<ul style="list-style-type: none"> Make additional cyber security funding available as may be necessary
Communications	<ul style="list-style-type: none"> Inform customers of facts in line with strategy agreed in the Incident Management Plan Communicate with staff on type and impact of breach
CISO	<ul style="list-style-type: none"> Take technical measures to stop breach Source external support as necessary - the NCSC's 'Marketplace' is a useful source of certified advice and products: nsc.gov.uk/section/products-services/introduction Identify technical aspects of breach and assess potential impacts Report relevant aspects to Action Fraud / NCSC / CiSP (in consultation with Director of Security)
Data Controllers	<ul style="list-style-type: none"> Submit report of breach to the ICO

WHAT TO DO?



RESOURCES FOR RESPOND

SECURITY INCIDENT RESPONSE SERVICES

The skills required to effectively respond to a cyber security incident need to be regularly updated and in many circumstances, organisations will not have them in-house.

The CREST Guide is designed to help companies of any sector determine what a cyber security incident means to the organisation, build a suitable cyber security incident response capability and learn about where and how to get help.

Value

CREST offer a detailed, 56-page incident management guide covering how to handle cyber security incidents. It provides expert advice on how to prepare for, respond to and follow up an incident in a fast and effective manner.

NCSC's guidance will help you plan, build, develop and maintain an effective cyber incident response capability, as well as providing you with an understanding of how to effectively use an incident response company.

More information

crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

nsc.gov.uk/collection/incident-management

nsc.gov.uk/information/cir-cyber-incident-response

RECOVER

WHO DOES WHAT?

Recommended Roles and Responsibilities on **RECOVER**:

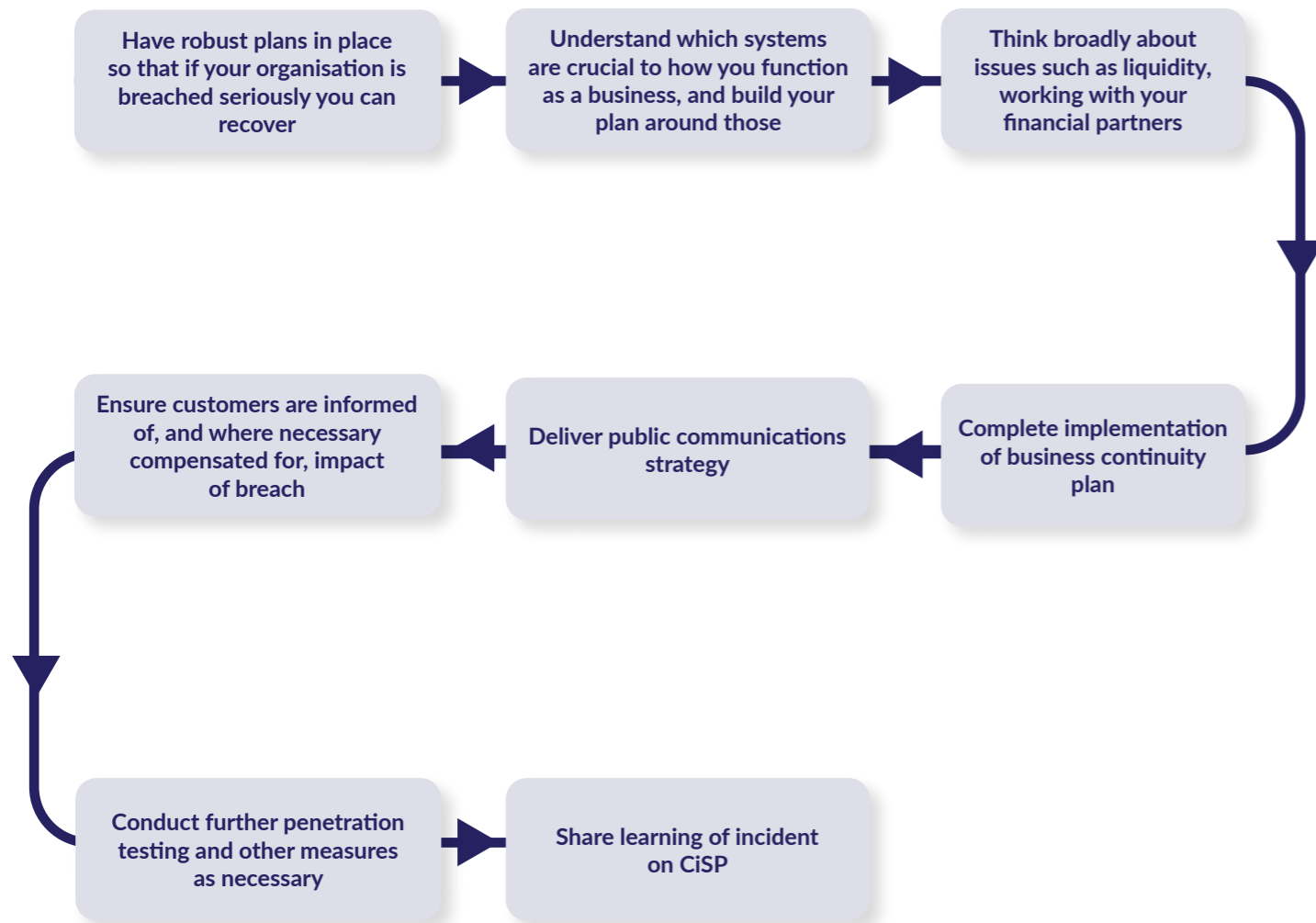
Nominated Board Member	Oversight of business continuity arrangements Spokesperson for company in communicating arrangements
Finance Director	Responsibility for customer compensation as may be required
Communications	Recommend what should be said to journalists and the public Highlight corporate cyber security citizenship
CISO	Further technical testing e.g. penetration testing (specialist vulnerability tests)
Data Controllers	Liaise across business around ICO follow-up and implications

"Failure to realise that an incident has occurred and manage it effectively may compound the impact of the incident, leading to a long term outage, serious financial loss and erosion of customer confidence"

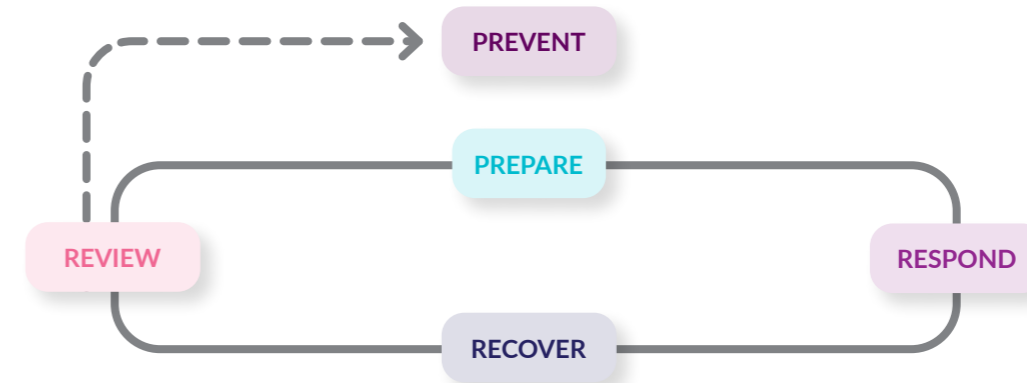
NCSC, 10 Steps to Cyber Security



WHAT TO DO?

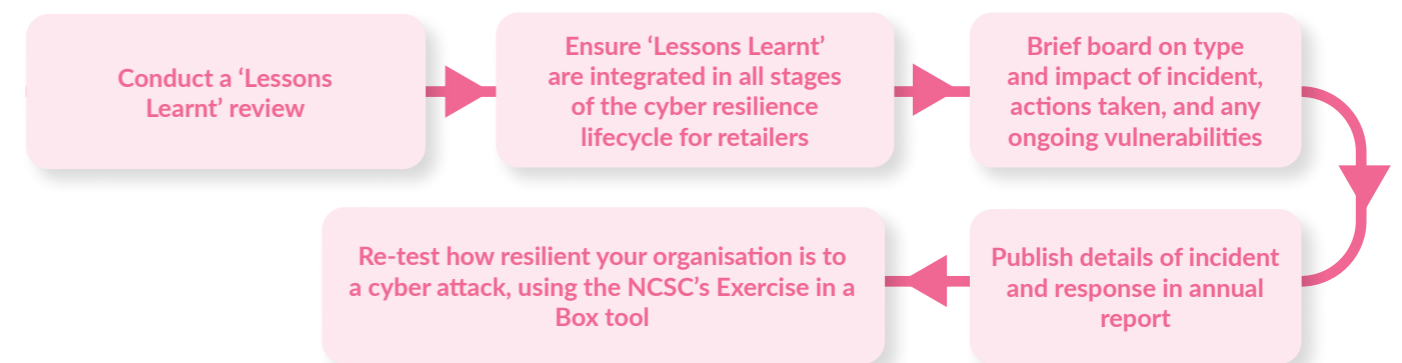


REVIEW



WHAT TO DO?

In the aftermath of an incident, or after a practice, it is recommended that a nominated board member oversees the following activity in close cooperation with all members of the Cyber Steering Committee:



More information:

Cyber security is not an end in itself, but a way to continue as a business. While prevention is always better than cure, it is still crucial that the retailer thinks about how it will survive an attack and recover from it as a functioning business.

This is one of the easiest areas to overlook, but it may be the most important. For non-specialists it may also be one of the easiest to grasp. In the same way that Boards will be planning for how to manage the business if a distribution centre goes down because of a traditional risk factor, they should think about how to manage an outage because of a breakdown in their cyber systems.

There are some pre-emptive steps that can be taken, such as creating parallel systems that can be switched on if the primaries are breached and backing up significant amounts of data in separate centres. But these can be expensive, and the business case should be considered carefully, certainly if it is not possible to have secondaries and back ups for everything.

Planning should always include a way to take the company back into a full operational phase, meaning that plans should take account of what is operationally most important for the retailer and its fiscal needs. That, as with other areas, requires the cyber strategy to closely align with the wider business strategy – there is no sense if the final system to be rebooted is the most important in terms of generating cashflow, even if technically that makes sense.

Those plans should be updated regularly. As networks and systems evolve and priorities shift, resilience plans should remain accurate. There is no point in a retailer thinking it can rely on the existence of a particular capability if a technology refresh renders it redundant. Part of the answer to the question of, 'what happens if a virus takes out our smartphones?' might well be using desk-based landlines, but not if moving to flexible working has seen landlines removed from the desks that need them.

That highlights another point: that planning for resilience needs to be business-centric and really quite granular. The appreciation of how cyber capabilities drive business processes needs to have a high level of detail, including of legal and contractual requirements. It is easy to think of massive HR and distribution systems, but simple things like printers can be just as important. How are you going to sell anything if you can't print receipts?

It is not the breach which kills the business, or the loss of reputation or negative press coverage. Ultimately, as with all businesses, bankruptcy is a possible financial outcome. One of the early and most important conversations a retailer that has suffered a major attack should have is with their financial partners. Liquidity requirements may actually increase as income falls to zero, as there are new demands around media management, additional service provision, legal fees and similar. A strong relationship with lenders and the right Treasury advice can be the difference between survival in the medium term and not surviving at all.

"Treasury teams are as much a part of being prepared for a cyber-security event as any other part of a retailer and are integral to the response and recovery. We work alongside our clients to help them understand the strength of their systems and protections, while also supporting them with their crisis financial planning."

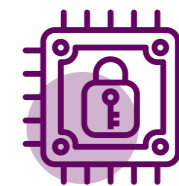
Giles Taylor, Head of Data & Cyber Security, Data Services, Lloyd's Bank

As with everything in this guide, perhaps the most important point here is to be realistic. Bringing IT systems back online can easily take months unless there has been significant investment in secondary systems, as can checking and assuring data, even once it has been unencrypted. It is better to prepare for the worst and deal with something much less challenging than to tell oneself that it will be 'alright on the night'.

THE HUMAN ELEMENT IN IT AND CYBER SECURITY



Cyber resilience isn't just a tech issue, a focus on people can often be very valuable



Improving employees' basic cyber hygiene can make an organisation significantly more secure



Never forget how people operate in the real world when thinking about cyber security

"Cyber security is sometimes viewed as 'just a tech issue' but that couldn't be further from the truth. At ASOS, we've found that a balanced approach that encompasses improving processes and employee awareness, as well as continuing to invest in the technology that we use, has returned far greater benefits than focusing on new tech alone."

George Mudie, CISO, Asos

The human element plays out in dozens of ways, from hiring the right CISO for a massive multi-national to an employee who has not been given the right training accidentally plugging an apparently discarded memory stick they found into a networked computer in case they can see who dropped it.

A 2014 report by IBM Global Technology Services found that human error was a contributory factor in over 95% of all successful cyber attacks analysed. The most commonly reported issues were system misconfiguration; poor patch management; use of default user names and/or passwords, or easy-to-guess passwords. A more recent report might point to the decision by an organisation to only rely on passwords, and not apply multi-factor authentication in the most critical systems; lost laptops or mobile devices; and disclosing information to the wrong email address. But the most common point identified was clicking on an unsafe link, perhaps in an email. In short: how people build IT systems, how people keep IT systems up-to-date (or don't) and how people use IT systems is crucial. There is one key principle to identify when designing any system that humans will use.

- always design your systems with a proper understanding of human nature as a starting point. This is sometimes known as 'User Experience Design'. Put very simply, it is much better to design your systems in a way that 'goes with the grain' of how people feel natural in doing things than try to force them to do something unnatural.

A good example from the field of cyber resilience is passwords: if you force someone to use a really complicated password, they may respond quite naturally by writing it on a post-it stuck to their monitor, by forgetting it regularly or by making it really simple for them to use and for a criminal to guess (Password1!, for example).

It is much easier to teach people a sensible system to build a password that is simple for them to use and very difficult for a criminal to crack. The NCSC's ThinkRandom advice is to use three random words which are not easy to guess (so not "password"). For example, "coffeetrainfish" would both be easy to remember and very difficult to guess. Up-to-date advice is that passwords should not necessarily expire after a period of time.

A second point is that in terms of user authentication (how someone proves they are who they say they are, and so should have access to the relevant systems) passwords may no longer be adequate. Retailers are increasingly using services that are directly connected to the Internet, for example to make remote working easier. These services are commonly hosted in the 'cloud' (computing resources available to many users over the internet which are, typically, not directly controlled by the user but by the cloud provider). In those cases, authentication often becomes the main decision point for whether a user, or attacker, can gain access to a service.

In those cases, retailers should very carefully consider services that offer a form of multi-factor authentication ('MFA'), such as a password and a thumbprint. But even there the main point remains: when building those systems, build them with the human who will use them, good and bad points alike in mind.

HOW PEOPLE BUILD IT SYSTEMS

In retail the IT systems used are incredibly complicated, often using a mix of the retailer's own systems and third parties'. Taken together, these form a complicated and highly tempting 'attack surface' (the number of points that a hacker can try to enter a retailer's systems).

The systems develop and grow through conscious decisions. If the base is wrong everything that relies on it will also be wrong. Moreover, the decisions do not always take sufficient account of security. This is a human issue – the people integrating and evolving are thinking about efficiency, or highly technical architecture issues. But are they paying enough attention to the security implications of what they are doing?

The short answer to this, as in other areas, is to make sure that people have the right skills, knowledge and incentives to prioritise building a secure, efficient and stable system - not just an efficient and stable one. Secure by design is the key.

Where mistakes are found, accountability is important, but as a path to improvement. Employees must feel that they can highlight problems to get them resolved and learn how to avoid them in future. A blame culture can actively work against that.

HOW PEOPLE KEEP IT SYSTEMS UP-TO-DATE

Software providers to business (and personal) users will regularly release updates and 'patches', which the user or the people who manage the network have to accept and allow to be applied. Some of these will be to improve performance, or even allow the systems to do new things. Others will be to fix a security issue which has been identified, perhaps a relatively simple thing for a hacker to exploit.

There are certainly technical aspects to developing a patching strategy that works. At the very least, you need to know the in-house systems you rely on and test them. In case of unacceptable problems with the patches, have systems that allow you to 'rollback' (take the systems back to a point before the update) in place.

But the human side is certainly as important. Where users have an element of control over patching, such as where the retailer is on a very small scale, they should be encouraged to accept updates as soon as they become available.

In very much the same way as it is sensible to do for a home computer, it can take up a little bit of time, but people need to be encouraged to see it as a task worth doing and worthy of being a high priority.

Where the patching is less remote, cyber teams should see it as part of their function not only to respond to the latest intrusions, or read up on cutting-edge viruses, but to work with colleagues so that their voice is heard in discussions over the patching strategy and the importance of keeping systems secure, efficient and stable.

Really successful cyber security requires proactivity on the part of cyber security teams. They have to be plugged into a wide range of developments, constantly looking for new threats and opportunities and mitigating or taking advantage of them, working across the whole organisation to deliver the best possible balance.

HOW PEOPLE USE IT SYSTEMS

The policies and processes around how people interface and engage with the IT systems provided to them can be a critical way of protecting a system from cyber attacks. Never lose sight of the user and consumer and the crucial role that they have in making your organisation more or less secure.

Any policy you develop should be easy for people to follow and implement, so that you create a secure operating culture in practice, as well as theory. That means people should naturally follow it.

Passwords are, perhaps, the most obvious area. Have a policy which gives you the most secure possible system, not the one way that, in theory, could give you the most secure passwords. Although highly complicated, people might forget those, and resort to insecure ways to remember them (it may also be sensible to be open-minded about workers using secure password managers).

Similarly, think about access controls. Who is allowed to access certain systems and what are they allowed to do there? Not just in a narrow sense, but more broadly. Make sure colleagues know not to plug USB memory sticks into systems. This well-intentioned move is a favourite exploit of penetration testers and is successful more often than you might hope.

Thirdly, a growing area (particularly in HQ roles) is 'bring your device to work'. Essentially, people use their personal web-enabled devices for business purposes, such as work email on a personal mobile phone. If used properly this can be a very sensible approach, but it creates a series of technical and human challenges. For example, on the human side you, will need to find a way to encourage people to never leave their devices easily accessible and/or unlocked in exactly the same way as you would a work desktop PC.

As you do encourage them to use their own devices sensibly, make sure you are working with human nature, and not against it.

QUICK GUIDE

"Cyber crime is one of our strategic priorities at the City of London Police and is something we, and all our colleagues across the country, take extremely seriously. We are committed to training our officers and staff so they are able to offer the best and most up-to-date advice on prevention, and we have a range of dedicated resources to assist with investigating cyber crimes from across the country and beyond."

Ian Dyson QPM, Commissioner of the City of London Police

PUBLIC BODIES

One of the first things anyone new to cyber security practice might notice is the sheer number and range of acronyms, and organisations. Here are some of the main bodies who are involved in retail cyber security and their roles.

Wider Public Sector/Law Enforcement

There are a number of key organisations within the public sector generally, and law enforcement specifically, which have a role in building the UK's cyber security capacity and who may become involved if a retailer is breached. In addition, many are good sources of documents providing help and information.

Law Enforcement and Regulatory

Action Fraud – managed by the City of London Police - is the single online reporting portal for cyber crimes and fraud in UK law enforcement. In the event of a breach, this is the first place to report the potential crime to UK law enforcement.

If the incident also involves a qualifying loss of personal data, a report will have to be made to the ICO in parallel.

City of London Police – the City of London Police force is the national lead police force for economic crime and it is in this capacity that it manages Action Fraud, and the National Fraud Intelligence Bureau, which analyses Action Fraud reports and sends them to relevant police forces for investigation.

The Information Commissioner's Office (ICO) is the lead body for and regulator of information rights within the UK, with a strong cross-border work programme. Notably, the ICO has an enforcement function under the Data Protection Act, the NIS Directive and PECR for which there may be mandatory reporting requirements.

The National Crime Agency (NCA) leads the UK law enforcement response to tackle serious and organised crime and reduce its impact on the UK. The NCA holds a number of specialist capabilities, including the National Cyber Crime Unit (NCCU).

The NCCU is the UK law enforcement lead for tackling the cyber-crime threat, working closely with a range of partners including UK Police, Regional Organised Crime Units and international law enforcement partners, such as Europol and the FBI. The NCCU also works in close partnership with the private and third sectors, sharing information and expertise that helps companies protect themselves from cyber criminals.

WIDER PUBLIC SECTOR

The Department for Digital, Culture Media and Sport (DCMS) is the lead Government department for, amongst other things, supporting economic growth within the UK through the better use of technology.

The National Cyber Security Centre (NCSC) is the public sector organisation whose vision is to make the UK the safest place to live and work online. The NCSC supports the most critical organisations in the UK, the wider public sector, industry and SMEs, as well as the general public. The NCSC is not a regulator.

More specifically, the NCSC:

Understands cyber security, and distils this knowledge into practical guidance that is made available to all

Responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK

Uses industry and academic expertise to nurture the UK's cyber security capability

Reduces risks to the UK by securing public and private sector networks

The NCSC also works collaboratively with other law enforcement bodies, defence, the UK's intelligence and security agencies and international partners. They can be contacted here: nsc.gov.uk/section/about-this-website/contact-us

RELEVANT LEGISLATION

The UK has some of the most protective legislation governing cyber security for retailers in the world, providing a strong level of some of the key pieces of legislation to think about are:

Data Protection Act

The Information Commissioner's Office (ICO) has provided detailed guidance on the Act, which is an accessible starting point. The DPA applies to any processing of 'personal data', with processing covering a broad range of uses by human or automated means, such as collecting payroll information, sharing CCTV footage or using data for marketing campaigns. 'Personal data' means information relating to an identifiable natural person, potentially a very broad category.

In general terms, the DPA requires retailers or, in many circumstances, their business partners to abide by the six data protection principles. The sixth principle is that the data be processed securely, applying effective data security processes and systems. A breach of personal data may become a serious breach under the DPA.

Enforcement is the responsibility of the ICO. The DPA significantly increased the potential penalties available, including a maximum of 4% of global turnover or €20 million, whichever is the greater for certain categories of breaches. This has already led to fines in the first instance of in excess of £100 million accompanied by considerable media interest.

Under the DPA retailers are also responsible for the compliance of their data processors with the DPA. For example, where a retailer holds personal data and passes it to a business partner, such as a data science company, the retailer, as data controller, may remain liable for the security failures of that data science company in relation to the personal data it is processing for the retailer. This creates an additional, and significant, supply chain liability risk.

Privacy and Electronic Communications Regulations 2003

The Privacy and Electronic Communications Regulations ('PECR') operate alongside the DPA to give people specific privacy rights over certain types of electronic communications, such as marketing emails, webpage cookies and itemised billing information. If applicable, this section is likely to be of most interest to marketers (as well as data and privacy teams). As of early 2020, consideration is being given to updating PECR.

The requirements and standards under PECR depend on the type of communication being used, and for some there are built in exemptions. For some areas, PECR requires taking appropriate security measures, this is security which is proportionate to the risks they guard against.

In some cases you may have to inform users of the nature of the risks and the safeguards. Breaches must be notified to the ICO.






Notably, breaches of PECR can see both the retailer and Directors fined, potentially up to £500,000.







Computer Misuse Act 1990

This 1990 piece of legislation, which has actually been updated many times since, carries the major criminal offences with which a cyber criminal may be charged.

The Act outlaws a number of specified offences, including unauthorised access to a computer (hacking), unauthorised access to a computer with intent to facilitate commission of further offences (e.g. hacking to steal money), unauthorised acts with intent to impair the operation of a computer (e.g. Distributed Denial-of-Service (DDoS) attacks to take down a retail website) and making or supplying articles to commit an offence under the Act (e.g. selling an exploit kit). Most seriously, there is an offence of unauthorised access which creates a risk of serious damage, which can include damage to the economy of a country or the supply of food.

GLOSSARY

 <p>BLACK HAT HACKER A computer hacker who breaks into an information system or digital network with the purpose of inflicting malicious intent.</p>	 <p>DATA BREACH The ICO defines a personal data breach as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service”.</p>	 <p>DENIAL OF SERVICE ATTACK (DOS) A method of taking a website out of action by overloading or ‘flooding’ the server.</p>	 <p>DOXING Discovering and publishing the identity of an internet user, obtained by tracing their digital footprint.</p>
 <p>HACTIVIST A combination of ‘hacker’ and ‘activist’, someone who uses computers and computer networks to promote a political agenda.</p>	 <p>LOCKED ACCOUNTS Where customers are (usually temporarily) unable to log into their accounts as a result of criminal activity on systems such as, for example, DOS attacks.</p>	 <p>MALWARE A program or malicious software that consists of programming, for example code or scripts, designed to disrupt the performance of PCs, laptops, handheld devices, etc.</p>	 <p>PHISHING A method of accessing valuable personal details, such as usernames and passwords, often through bogus communications such as emails, letters, instant messages or text messages.</p>
 <p>PORT SCANNING A technique employed to identify open ports and services on a network, potentially with a view to exploiting weaknesses illegally.</p>	 <p>PHARMING A method of deceiving an individual into ending up at a fake website, even though the correct URL has been entered.</p>	 <p>RANSOMWARE A type of malware that prevents the use of a system, either by locking the system’s screen or by locking the users’ files unless a ransom is paid.</p>	

 <p>SOCIAL ENGINEERING In a cyber security context, the general art of manipulating people online so they give up confidential information.</p>	 <p>SPEAR PHISHING As per phishing, except that it is a directed attack against a specific target.</p>	 <p>SPOOFING Masquerading as another individual or entity by falsifying data, thereby gaining an illegitimate advantage.</p>	 <p>SQLI SQL injection attacks are a common way of trying to penetrate websites, through which attackers steal large volumes of information from underpinning databases.</p>
 <p>THEFT OF DATA Stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information.</p>	 <p>WHALING A type of spear phishing (i.e. specifically directed) attack, such as an e-mail spoofing attempt, that targets senior members ('big fish') of a specific organisation, seeking unauthorised access to confidential data.</p>		

KEY ORGANISATIONS

<p>NCSC Established in October 2016, the National Cyber Security Centre (NCSC) aims to be the authoritative voice on information security in the UK.</p> <p>CISP The Cyber-security Information Sharing Partnership is a joint industry/government initiative designed to facilitate the sharing of cyber threat and vulnerability information to reduce the impact on UK business.</p>	<p>NCCU The National Crime Agency's National Cyber Crime Unit (NCCU) leads the UK law enforcement response to cyber-crime, including by coordinating the national response to the most serious threats.</p>	<p>ICO The Information Commissioners Office (ICO) is the UK's independent body set up to uphold information rights. The organisation takes action to change the behaviour of organisations and individuals that collect, use and keep personal information.</p>
---	--	--





THE BRITISH RETAIL CONSORTIUM

The BRC's purpose is to make a positive difference to the retail industry and the customers it serves, today and in the future.

Retail is an exciting, dynamic and diverse industry which is going through a period of profound change. Technology is transforming how people shop; costs are increasing; and growth in consumer spending is slow.

The BRC is committed to ensuring the industry thrives through this period of transformation. We tell the story of retail, work with our members to drive positive change and use our expertise and influence to create an economic and policy environment that enables retail businesses to thrive and consumers to benefit. Our membership comprises over 5,000 businesses delivering £180bn of retail sales and employing over one and half million employees.



BRITISH RETAIL CONSORTIUM

Suite 60, 4 Spring Bridge Road, Ealing, W5 2AA.
+44 (0)20 7854 8900 | info@brc.org.uk | brc.org.uk

British Retail Consortium - a company limited by guarantee
Registered in England and Wales No. 405720

registered office: 100 Avebury Boulevard, Central Milton Keynes, MK9 1FH