CYBER SECURITY TOOLKIT

A GUIDE FOR RETAILERS

<< RETAILERS WHO PRIORITISE THE PEOPLE, PROCESS AND TECHNOLOGY ASPECTS OF CYBER SECURITY WHILST MAXIMISING THE OPPORTUNITIES OF INNOVATION WILL BE THE MARKET LEADERS OF THE FUTURE. >>

FACTS AND FIGURES

CYBER CRIME REPRESENTS AT LEAST **5%** OF THE TOTAL DIRECT COST OF CRIME TO RETAIL BUSINESSES

ESTIMATED **5.8M** FRAUD AND COMPUTER MISUSE INCIDENTS IN YEAR ENDING 2016

3.8M OF THESE WERE FRAUD INCIDENTS

2M WERE COMPUTER MISUSE INCIDENTS[2]

£1.9BN GOVERNMENT INVESTMENT IN CYBER SECURITY OVER FIVE YEARS[3]

= **120%** INCREASE

RISING FROM £860M BETWEEN 2011-16[4]

IN 2015, THE AVERAGE AGE OF SUSPECTED CYBER CRIMINALS FEATURED IN INVESTIGATIONS INVOLVING THE NCA WAS **17** YEARS OLD[5]

ACCORDING TO THE UK CYBER BREACHES SURVEY, 25% OF LARGE FIRMS BREACHED ARE ATTACKED AT LEAST ONCE PER MONTH[7]

ALMOST HALF OF THE TOP FTSE 350 BUSINESSES REGARDED CYBER-ATTACKS AS THE BIGGEST THREAT TO THEIR BUSINESS

WHEN COMPARED WITH OTHER KEY RISKS - UP FROM 29 PER CENT IN 2014[6]

ACCORDING TO THE UK GOVERNMENT,

4 OUT OF 5

UK CITIZENS BOUGHT SOMETHING ONLINE IN THE PAST YEAR[1].

A QUARTER (24%) OF ALL BUSINESSES DETECTED ONE OR MORE CYBER SECURITY BREACHES IN THE LAST 12 MONTHS[8]

1 Matt Hancock, Minister for Digital and Culture addresses CBI conference, 14 September 2016, Via: https://www.gov.uk/government/speeches/minister-for-digital-and-culture-addresses-cbi-conference

2 'Crime in England and Wales: year ending Mar 2016', Statistical Bulletin, 21 July 2016, Via: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2016#new-estimate-of-58-million-csew-fraud-and-computer-misuse-offences

3 'Chancellor's speech to GCHQ on cyber security', 17 November 2015, Via: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

4 'The UK Cyber Security Strategy 2011-2016: annual report', Via: https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report

5 National Crime Agency, 'Campaign targets UK's youngest cyber criminals', 8 December 2015, Via: http://www.nationalcrimeagency.gov.uk/news/765-campaign-targets-uk-s-youngest-cyber-criminals

6 'Two thirds of large UK businesses hit by cyber breach or attack in past year', 8 May 2016, Via: https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year

7 'Cyber Breaches Survey 2016', Via: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016'

8 'Cyber Breaches Survey 2016', p.4

£4,110=

AVERAGE INVESTMENT IN CYBER SECURITY BY RETAIL/WHOLESALE/ TRANSPORT SECTOR IN LAST FINANCIAL YEAR[9]

THE TOTAL GLOBAL CYBER MARKET IN 2015 HAS BEEN ESTIMATED AT

£419.2BN[12]

ACCORDING TO INSTITUTE OF CUSTOMER SERVICE DATA;

30% SAID THEY WOULD CHANGE SUPPLIERS IF THE COMPANY THEY ARE USING BECOMES A VICTIM OF A CYBER-ATTACK[11]

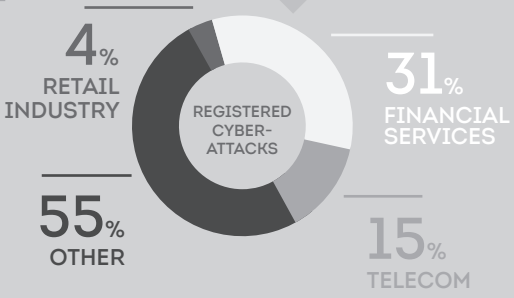
70% OF FRAUD REPORTED TO POLICE IS CYBER ENABLED[10]

IN 2015, RETAIL AND CONSUMER PRODUCT COMPANIES DETECTED

154%

MORE INCIDENTS THAN THE YEAR BEFORE[15]

AVERAGE INFORMATION SECURITY SPENDING IN THE RETAIL INDUSTRY SOARED **67%** IN 2015[16]



IT HAS BEEN ESTIMATED THAT 4% OF REGISTERED CYBER-ATTACKS LEVELLED AGAINST RETAIL INDUSTRY[13]

GCHQ ESTIMATES

80%

OF ATTACKS COULD BE PREVENTED IF FIRMS INTRODUCED BASIC PROTECTIONS[17].

ONLY **37%** OF ORGANISATIONS HAVE A CYBER INCIDENT RESPONSE PLAN IN PLACE[14]

9 'Cyber Breaches Survey 2016', p.19

10 'What is fraud and cyber crime?', Action Fraud Website, Via: http://www.actionfraud.police.uk/what-is-fraud
The BRC's 2016 Annual Crime Survey Report highlighted that an estimated 53% of all fraud levelled against the retail industry was cyber-enabled.

11 'British business not to be trusted with our data, say consumers', 25 November 2015, Via: https://www.instituteofcustomerservice.com/media-centre/press-releases/article/british-business-not-to-be-trusted-with-our-data-say-consumers

12 UKTI, 'Security Export Figures for 2015', Via: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545242/Additional_Statistics_-_Global_Security_Market_2015.pdf

13 Centre for Risk Studies, 'Integrated Infrastructure: Cyber Resiliency in Society', Via: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Integrated_Infrastructure_Cyber_Resiliency_in_Society_8_Apr_2016.pdf, p.8

14 PWC, 'Global Economic Crime Survey 2016', Via: http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf, p.16

15 PWC, 'Turnaround and transformation in cybersecurity: Retail and consumer ', Via: http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/pwc-gsiss-2016-retail-consumer.pdf

16 PWC, 'Turnaround and transformation in cybersecurity'.

17 Cyber Security Strategy, 2011. Via: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

08 FOREWORD

09 ACKNOWLEDGEMENTS

10 SECTION A: INTRODUCTION

14 SECTION B: CYBER SECURITY LANDSCAPE

15 UNDERSTANDING THE RISKS TO RETAIL

16 ROLES OF GOVERNMENT, POLICE & OTHER PUBLIC AGENCIES

19 SECTION C: TACKLING CYBER SECURITY

20 RISK MANAGEMENT

20 CYBER RESILIENCE LIFECYCLE

22 PREVENT

27 PREPARE

28 RESPOND

29 RECOVER

30 REVIEW

31 SECTION D: CYBER SECURITY CHECKLISTS

32 QUESTIONS FOR THE BOARD

32 QUESTIONS FOR COMMUNICATIONS DIRECTORS

32 GUIDANCE FOR SMES

33 SECTION E: OPTIONS FOR WORKING WITH STAFF AND CUSTOMERS

35 SECTION F: USEFUL RESOURCES

38 SECTION G: GLOSSARY

39 COMMON THREATS AND TERMINOLOGY

40 KEY ORGANISATIONS

41 SECTION H: CYBER SECURITY AT THE BRC

FOREWORD

Strong cyber security means strong commercial competitiveness. In our digitised economy, with its ever-increasing reliance on technology, and online retail sales increasing by around 10-15 per cent annually, the most successful businesses are those that view information security as an enabler for growth, not a financial burden. Cyber security and e-commerce therefore go hand in hand in a digital age. Retailers who prioritise the people, process and technology aspects of cyber security whilst maximising the opportunities of innovation will be the market leaders of the future.

The case for cyber security is not only driven by opportunity - customers are rightly placing demands on companies to protect their personal information against criminals and other malicious actors. The onset of cyber crime is a major risk to the UK economy in general, and the retail industry in particular. The Office for National Statistics estimates that 5.8 million incidents were experienced by adults in England and Wales in 2015/2016 (3.8 million of these were fraud incidents and 2.0 million were computer misuse incidents).

Measuring the exact cost of cyber crime presents several methodological challenges, and its overall impact is not easy to measure or limited to financial harm. However, according to the latest BRC Annual Crime Survey, it represents five per cent of the total direct cost of crime to retail businesses. This conservative estimate amounts to a direct financial loss of £36 million per annum. Separately, the latest survey asked retailers to estimate the cost of fraud levelled against them that was conducted online/internet enabled. This was estimated at 53 per cent, representing a total direct cost of cyber-enabled fraud to the retail industry of around £100 million.

In my regular meetings with retailers, I have been struck by how cyber security has quickly risen to the top of the list of strategic risks facing our industry. Speaking with CEOs and board members across the country, the growing challenge they face from online fraud and cyber crime is now starkly apparent. The types of attacks they face on a weekly basis and covered in this guide are varied and include, amongst many others, Data Breaches and Denial of Service attacks.

The importance of effective cyber security for the industry is therefore self-evident. It is a serious issue for our members, with 91 per cent of those responding to our crime survey stating that the overall number of cyber breaches is either increasing or remaining the same.

Cyber-attacks on the retail industry are doubly damaging in that there are two sets of victims in crime of this nature - both the customers (whose data is hacked or money stolen), and the retailers themselves. Calls for companies to 'do more' to protect their customers, whilst well intentioned, often fail to recognise that retailers are themselves the victims of this type of crime.

Against this backdrop, the BRC and its members are prioritising strengthening the public-private cooperation that is needed to improve the UK's cyber resilience. In our approach to working with law enforcement to seek enhancements to the UK's online fraud reporting system, Action Fraud, or informing and supporting the development of the UK's new National Cyber Security Centre, we agree that neither Government nor industry can achieve cyber security on their own.

A huge amount of work has been done to strengthen the UK retail industry's cyber security: but there is more we need to do. It is in this context that BRC members tasked us to develop, as an urgent priority and in cooperation with partners, a set of industry-specific guidelines for cyber security that would have broad utility across the industry. This document and its associated implementation plan that we will deliver in 2017 is the fruit of that labour.

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. This cyber security toolkit for retailers is intended as a practical, step-by-step guide for all parts of the industry that have a large and growing stake in implementing cyber security.

HELEN DICKINSON OBE
Chief Executive, British Retail Consortium

ACKNOWLEDGMENTS

This toolkit has been developed under the auspices of the Fraud and Cyber Security Member Group of the BRC to provide retailers with an introductory guide on how to set about implementing an effective approach to cyber security.

This toolkit has benefitted from formal and informal consultation with many individuals and key organisations operating in the UK security sector, to whom the BRC is immensely grateful, including:

- Centre for the Protection of National Infrastructure
- City of London Police
- Department for Culture, Media and Sport (Cyber Essentials)
- Getsafeonline
- Home Office (Cyber Aware)
- Home Office (Strategic Centre for Organised Crime)
- Home Office (Tackling Crime Unit)
- London Digital Security Centre
- Metropolitan Police Service (Falcon)
- Mayor's Office for Policing and Crime
- National Crime Agency (National Cyber Crime Unit)
- National Cyber Security Centre

The BRC would like to thank all of the contributors who attended the BRC's Cyber Security Incident Management event in Association with AON on 27 October 2016, whose discussions helped to inform this document.

The BRC would also like to pay particular thanks to Allie Andrews, Amrit Bhabra, Dave Clemente, Sam Crome, Georgie Barnard, Laura Penfold, Shetal Bhatt and Simon Dukes for their assistance at various stages throughout this project.

Any errors or omissions in the pages that follow are the responsibility of the authors, not any of those named above.

Whilst this document seeks to assist retailers of all sizes, the differing types and sizes of retailers in the UK means that there can never be a one size-fits-all solution.

Therefore, the toolkit does not claim to be exhaustive - it deliberately provides 'signposts' to other existing sources of other freely-available guidance. The document has no legal status and the BRC, its members nor any of its supporters accept any legal responsibility for any advice or guidance provided.

"THE STEP-BY-STEP, PRACTICAL GUIDANCE CONTAINED IN THIS CYBER SECURITY TOOLKIT DESERVES TO BE ADOPTED BY INDIVIDUAL BUSINESSES, AND ACROSS THE WHOLE RETAIL SUPPLY CHAIN. THE CYBER THREAT FOR RETAILERS IS NOW SELF-EVIDENT AND THE TIME FOR ACTION IS NOW."

- John MacBrayne QPM, Group Security and Resilience Director, Tesco, and Chairman, BRC Fraud and Cyber Security Member Group -

"'THIS IS A PRACTICAL TOOLKIT – MORE, IN FACT AN ARMOURY OF WEAPONS TO HELP DEFEND AGAINST THE MANY AND VARIOUS CYBER THREATS TO RETAILERS"

- Mike Wyeth, Security Director, Shop Direct (Holdings) Limited -

"WE ARE CURRENTLY SEEING A SIGNIFICANT SHIFT FROM CONVENTIONAL ACQUISITIVE CRIME TO CYBER-CRIME AND CYBER-ENABLED FRAUD. THIS DOCUMENT IS TIMELY AND WILL GIVE BUSINESSES, BOTH LARGE AND SMALL, VALUABLE INFORMATION BOTH ON REDUCING THEIR VULNERABILITIES, OR, IF THE WORSE HAPPENS, THE KNOWLEDGE TO MORE EFFECTIVELY DEAL WITH THE CRISIS. READERS, I RECOMMEND YOU ACT UPON THE WISDOM WITHIN WITHOUT DELAY"

– Phillip C Hagon QPM, Recently Senior Security Advisor, J Sainsbury PLC -

"RETAILERS HAVE AND WILL ALWAYS BE ONE OF THE MOST ATTRACTIVE TARGETS FOR THE CYBERCRIMINALS OUT THERE – DON'T MAKE YOURSELF AN EASY ONE!"

- Tarun Samtani, Group Cyber Security Advisor, Findel Plc. -

10

SECTION A

INTRODUCTION

AIM OF THIS TOOLKIT

This cyber security toolkit has been developed by the British Retail Consortium (BRC) to help retailers of all sizes, prevent, prepare for, respond to, and recover from major cyber-attacks and other forms of online criminal activity. It has been designed to introduce the issues in clear English, and provide practical, step-by-step guidance for retailers on how to set about handling sophisticated cyber-attacks such as data breaches, and how to report and address common issues such as fraudulent scams.

The toolkit resembles other existing BRC guidance in the security field, such as our work on Reducing Violence in the Workplace, by taking account of the specific characteristics and requirements of the retail industry. Whilst drawing upon, and providing signposts to, existing guidance where applicable and relevant, it is the first toolkit of its kind to take account of the way the retail industry works, seeking to move beyond the level of generic advice that can be found in other equivalent efforts.

In the pages that follow, the BRC Cyber Security Toolkit will provide:

- A high-level picture of the UK cyber security landscape and how it affects retailers
- An introduction to the role of government and police in UK cyber security
- Advice and best practice on how to strengthen protection against cyber security incidents
- Specific guidance for retailers on how to set about handling incidents such as cyber breaches
- Checklists of key questions for boards and communications teams
- Options for retailers on how to work with customers to improve cyber resilience
- A glossary of key cyber security organisations and types of fraud and cyber-attacks

Online fraud and cyber-attacks now represent a pervasive, potentially existential threat to UK retailers. They can cause serious damage from both commercial and security perspectives, and it is for this reason that every company now needs to devise an appropriate, proportionate response. This cyber security toolkit aims to help retailers achieve this by providing a practical, step-by-step guide for all parts of an industry that has a growing stake in implementing effective cyber security.

HOW TO USE THIS TOOLKIT

This toolkit sets out for the retail industry a practical, industry-specific set of guidelines for how to mitigate the growing risks of cyber-attacks and online fraud. Having introduced the type and scale of the threats facing the industry and the shape of the UK cyber security policy landscape (including what to expect from it), the document introduces retailers to what they can do. It is designed to help companies prevent cyber incidents before they occur, before outlining a step-by-step approach to Incident Management that should be widely adopted.

Crucially, the document stresses that cyber security is not a matter that can be addressed by the IT security department alone. Effective cyber security strategies demand a collective response, and require everyone - Boards, CEOs, Financial Directors, Communications Directors and indeed all staff more broadly - to understand, and implement, their respective roles in achieving the necessary levels of protection. This guidance breaks down where these responsibilities sit across the retail business.

The BRC recommends that in their security postures retailers adopt risk-based, intelligence-driven strategies for countering fraud and cyber security risks. As it promotes a practical set of guidelines to help them do so, the toolkit places a particular emphasis on how the different constituencies within retail companies all play important roles in the management of major incidents - whether it relates to testing and exercising, or participation in the risk assessment process. Guidelines are provided on the questions each grouping should be asking before such an incident, and the roles they arguably must be able to fulfil in the event of such an attack.

The toolkit deliberately draws on, and in some places reproduces, a wide range of existing available cyber security material promoted by various organisations in the UK. In this sense it does not seek to 'reinvent the wheel', but signpost and disseminate available advice that is recognised as emerging best practice in the field.

ATTACKERS

 STATE ATTACKS	 INDUSTRIAL ESPIONAGE
 HACTIVIST	 BLACK HAT HACKER
 INTERNATIONAL ORGANISED CRIMINALS	 ONLINE FRAUDSTERS
 SCAMMERS	

FOR AN EXPLANATION OF THESE VARIOUS TYPES OF ATTACKERS AND METHODOLOGIES, SEE THE GLOSSARY IN SECTION G, ON PAGE 38.

TYPES AND METHODOLOGIES OF CYBER-ATTACK

 DENIAL OF SERVICE ATTACK	 PHISHING
 PHARMING	 SPOOFING
 DOXING	 MALWARE
 WHALING	 RANSOMWARE
 SOCIAL ENGINEERING	 SPEAR PHISHING
 THEFT OF DATA	 PORT SCANNING
 CREDIT CARD THEFT	

THE ANATOMY OF CYBER CRIME AND DATA BREACHES: REAL WORLD PROBLEMS FOR RETAILERS

Fraudsters use a method known as 'phishing' as an industrial-scale way of accessing valuable personal details, such as usernames and passwords. What appear to be authentic communications - emails, instant messages or text messages - are in fact bogus. URL links within such messages often direct users' false websites where personal details may be requested.

Targeted, 'spear-phishing' attacks on third-party contractors have allowed criminals to gain access to a wider set of corporate systems than necessary. Attackers can penetrate, and steal company data via organisations within the supply chain - some of which may be less well protected.

The targeting of point of sale systems have enabled criminals using 'scraping malware' to access connected information systems. In-store payment systems can introduce substantial vulnerabilities if they are not properly segregated from wider systems.

Hackers have proved their ability to gain access to retailers' databases and information systems, obtaining extensive lists of credit card numbers that can be used for criminal transactions.

Unprotected, vulnerable web pages have enabled cyber criminals to gain easy access to customer information within underpinning databases.

Cyber security vulnerabilities can be introduced when weaknesses in legacy IT systems are not addressed, or perhaps not properly appreciated following a merger or acquisition.

Attackers can overload or 'flood' websites with digital traffic to make them inoperable, if only sometimes temporarily, in so-called distributed denial of service (DDoS) attacks.

Companies can be targeted by 'Ransomware'. In this type of attack, systems have become encrypted by malicious software (malware), following which the hacker demands a fee (often in an anonymised, digital currency) to restore access to the data.

Using fake email addresses, criminals have posed as company CEOs in an effort to dupe their finance teams into transferring corporate financial assets into fraudulent bank accounts. So-called CEO fraud is on the rise and serves as an example of cyber-enabled social engineering.

"JUST AS TECHNOLOGY PRESENTS HUGE OPPORTUNITIES FOR OUR ECONOMY – SO TO IT POSES A RISK. TRUST IN THE INTERNET AND THE INFRASTRUCTURE ON WHICH IT RELIES IS FUNDAMENTAL TO OUR ECONOMIC FUTURE"

- Philip Hammond, Chancellor of the Exchequer -

SECTION B

CYBER SECURITY LANDSCAPE

UNDERSTANDING THE RISKS TO RETAIL

Cyber security is here to stay for retailers; the British population is one of the world's biggest users of e-commerce. Retail industry sales in 2015 were £340bn, up £7bn on 2014. Of this, online retail sales totalled £43bn, indicating the scale of e-commerce that needs to be protected. It is also apparent that customers want to see retailers working with the authorities to manage the risk. According to the Institute of Customer Service Data, 30 per cent of consumers said they would change suppliers if the company they are using becomes a victim of a cyber-attack.

It is in this context that the BRC recommends a step-change in cyber security awareness and activity both within, and by the authorities supporting the retail industry. To achieve this, boards and senior executives are encouraged to recognise and take ownership of, the range of cyber security risks facing retail companies, and enshrine these within their overall corporate risk management regime. In short, an effective board should drive and support the embedding of an Information Risk Management Regime all the way across a retail organisation.

Individual retailers will face different cyber security risks and vulnerabilities as a result of their particular business, placing a premium on companies developing effective risk management processes (introduced in Section C). However, a number of general observations can be made about character of the industry and its potential cyber vulnerabilities. The UK retail industry is a highly competitive market offering choice and benefiting consumers, and it makes a substantial contribution to the British economy. It is the largest private sector industry in the UK with around three million employees.

Cyber-crime is now widely recognised as a major threat to the UK economy. The Office for National Statistics estimates that 5.8 million incidents of fraud and computer misuse were experienced by adults in England and Wales in the year ending 2016. It is a serious issue for the UK retail industry, with 91 per cent of those responding to the latest BRC annual crime survey stating that the overall number of cyber breaches is either increasing or remaining the same. Types of online fraud and cyber-crime affecting the industry are extremely varied and those covered in this guide include the proliferation of low-level scams, 'phishing', malware, all the way through to Denial of Service attacks.

The ability for cyber criminals to sell customer data and passwords on the 'dark web', too frequently with relative impunity, means that systems processing customer data designed to benefit the consumer can be targeted by sophisticated criminals.

The challenge that retailers face is not limited to financial harm. High profile data breaches affecting the industry, such as those experienced by the major U.S. retailers Target and Home Depot - and more generally by household names including LinkedIn, Yahoo, and TalkTalk - have shown the reputational damage that can be caused when cyber criminals are successful in their attacks upon companies' digital networks. Such trends are not unique to the retail industry, but the increasing volume of personal data that consumers are willing to share with retailers (and vice versa) is a notable characteristic that means the industry can be a target for hackers and cyber criminals.

The challenges from a cyber security perspective that arise from the industry's highly diverse, transnational supply chain, and by an industry characterised by a wide range of ownership models, such a large number of employees, and the need to protect an extremely diverse set of data (ranging from payment systems to personal customer information details) are also increasingly well understood.

A proportionate approach to cyber security is imperative for retailers, such is the requirement to balance security with customer facilitation and experience. In this context, retailers also need to adopt ever more sophisticated technological solutions to remain competitive, with innovation introduced at such a speed that presents challenges for those responsible for 'designing in' security measures. The potential implications for security of the dawn of the 'Internet of Things', for example, have arguably only just begun to be considered. The promised longer-term benefits that autonomy might bring to an improved customer experience similarly has the potential to challenge retail security practitioners in completely new ways.

Substantial cyber security investment is now being made by retailers, not least because there are two sets of victims in crime of this nature - both the customers (whose systems are compromised, whose data is hacked, or whose money is stolen), and the retailers themselves. The frequent calls that companies 'must do more' to protect their customers, whilst well-intentioned, often fail to recognise that retailers are themselves the victims of what the Director of GCHQ has referred to as 'industrial scale' criminality.

Cyber-crime is therefore now an inevitable part of working in the digital economy. It is for this reason that this toolkit seeks to provide practical guidance to retailers so that they might better protect themselves, as well as signposting the support that is available to companies from the public authorities.

ROLES OF GOVERNMENT, POLICE & OTHER PUBLIC AGENCIES

It is evident that any effective strategy to tackle cyber-crime must be nimble and also involve strong cooperation between industry and the authorities - as ministerial speeches make clear, neither government nor industry can achieve this on their own. In short, cooperation between the public authorities and the retail industry is an absolutely core component of UK cyber security.

The UK's fraud and cyber security policy and policing landscape is characterised by fragmentation and complexity, with multiple departments and agencies involved in different aspects of the response.

Many of the structures and processes that have been designed to assist industry in tackling fraud and cyber security threats are at an early stage of development, but it is now clear that the first port of call for the reporting of routine, day-to-day online fraud and cyber-criminal activity is the UK's national reporting centre known as 'Action Fraud'.

The following section outlines the key stakeholders/initiatives for retailers to be aware of, providing contact details where they are available:

KEY STAKEHOLDERS

CITY OF LONDON POLICE (COLP)

ROLE

Action Fraud is the UK's national reporting centre for fraud and cyber-crime where you should report fraud if you have been scammed, defrauded or experienced cyber-crime. The City of London Police also hosts the National Fraud Intelligence Bureau.

CONTACT / REPORTING DETAILS

The first point of call for cyber-crime is Action Fraud. We recommend calling Action Fraud in the first instance. Get advice about fraud or internet crime by calling ***0300 123 2040*** (textphone ***0300 123 2050***).

Fraud and cyber-crime can also be reported online:
http://www.actionfraud.police.uk/report_fraud

Retailers can also subscribe to fraud alerts from the National Fraud Intelligence Bureau. Contact the following to be added to the distribution list:
NFIBOutputs@cityoflondon.pnn.police.uk

Note on Reporting: Crime reports score on a viability basis. The more viable, the more likely to be investigated by a police service. Where a crime report is being created, the following lines of enquiry will assist in making a crime report viable for investigation:

- Bank account number
- Bank card number Name
- DOB
- Address Phone Numbers
- Email address
- IP Address
- Vehicle registration number
- CCTV in existence

Bulk Reporting: If you report offences on a regular basis and believe your business could significantly save time by using free tools to input multiple fraud reports at once. Please contact the National Fraud Intelligence Bureau and request contact from one of the Business Stakeholder Managers: ***NFIB-BSM-Referral1@cityoflondon.pnn.police.uk***

NATIONAL CYBER SECURITY CENTRE (NCSC)

ROLE

Significant incidents should be reported to the NCSC. Launched in October 2016, the NCSC is the bridge between industry and government, providing a unified source of advice and support on cyber security, including the management of cyber security incidents.
The NCSC's remit is therefore much wider than Incident Response; it is a place where companies can go to receive guidance and further details on government schemes.
The NCSC also hosts the Cyber-security Information Sharing Partnership (CiSP)

CONTACT / REPORTING DETAILS

NCSC Website: ***https://www.ncsc.gov.uk***/

If you feel you are the victim of a significant cyber security incident, you can report this to the NCSC. A significant incident for the NCSC is the following:

1. Impact on UK's national security or economic wellbeing.
2. The potential to cause major impact to the continued operation of an organisation.

In order for the NCSC Incident Management team to understand the potential scale, severity and impact of the incident, please provide them with answers to the following points:

1. Who are you?
2. What organisation are you reporting an incident for?
3. What is your role in this organisation?
4. What are your contact details?
5. A summary of your understanding of the incident, including any impact to services and/or users
6. What investigations and/or mitigations have you or a third party performed or plan to perform.
7. Please provide the output of any technical analysis.
8. Who else has been informed about this incident?
9. What are your planned next steps?

Answers to the above questions should be sent to the NCSC Incident Management Team at the following email address: ***webreportedincidents@ncsc.gov.uk***

(You should indicate in your response if you are requesting any secret sauce information.)

NATIONAL CRIME AGENCY (NCA)

ROLE

The National Cyber Crime Unit (NCCU) at the NCA leads the UK's response to cyber-crime. Businesses can share information with the NCA though the 'Information Gateway' provisions provided in Section 7 of the Crime & Courts Act 2013. This allows the NCA to receive information on an intelligence only basis, "relevant to the exercise of our statutory purpose", namely the investigation and disruption of serious crime. Any information received through this route will be subject to "restricted" handling to facilitate the protection of business confidentiality.

CONTACT / REPORTING DETAILS

Businesses requiring further details about the intelligence basis of information sharing with the NCA can contact:
NCCUIndustry@nca.x.gsi.gov.uk

ICO

ROLE

Although there is currently no legal obligation on data controllers operating in the retail industry to report breaches of security under the Data Protection Act (DPA), this is anticipated to change in 2018 with the introduction of the General Data Protection Regulation (GDPR). In any event, it is recommended that serious breaches are reported.

CONTACT / REPORTING DETAILS

Report it online:
https://ico.org.uk/for-organisations/report-a-breach/

Full details of what companies need to include in the report are outlined in the ICO's 'Data protection breach notification form', available at the above website.

Helpline on completing report: ***0303 123 1113*** or ***01625 545745***
(operates 9am to 5pm Monday to Friday)

CITIZENS ADVICE

ROLE

If appropriate, Citizens Advice may refer the case on to Trading Standards and action may be taken against a rogue trader.

CONTACT / REPORTING DETAILS

To report a scam, a consumer can call the Citizens Advice Consumer Helpline on ***08454 04 05 06*** or they can use the ***online enquiry form***.

Further details of the roles and responsibilities of the different government departments and agencies involved in cyber security are included in the BRC's Fraud and Cyber Security Policy Landscape Map, available to members of the Fraud and Cyber Security Member Group (see Section H for more details.)

SECTION C

TACKLING CYBER SECURITY

RISK MANAGEMENT

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. Cyber security in the retail industry can however be improved by implementing effective risk management processes. Understanding the nature of the cyber risks to your 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 your digital assets.

In completing a cyber security risk assessment, retailers are encouraged to consider the various types of online risks facing their companies, and the potential scale of them. The risk assessment should ultimately be owned by someone on the board, but it will need to draw on the expertise of functional areas across the business, and address questions including (but not necessarily limited to):

- What would be the impact of a cyber security incident to your business?
- What are your sensitive and / or businesses' critical digital assets? (e.g. customer data / payment systems)
- Where do your sensitive and/or businesses' 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 security skills?
- Are any proposed new cyber security measures proportionate?
- How regularly does your business review its cyber security preparedness through exercises such as 'red teaming' (i.e. testing plans and processes in a structured, robust and independent manner)?
- 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 Government's 10 Steps to Cyber Security guidance: ***https://www.ncsc.gov.uk/guidance/10-steps-cyber-security***

CYBER RESILIENCE LIFECYCLE

Having assessed the cyber security risks facing your 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:
Seeking to avoid cyber security breaches by introducing stronger security protections

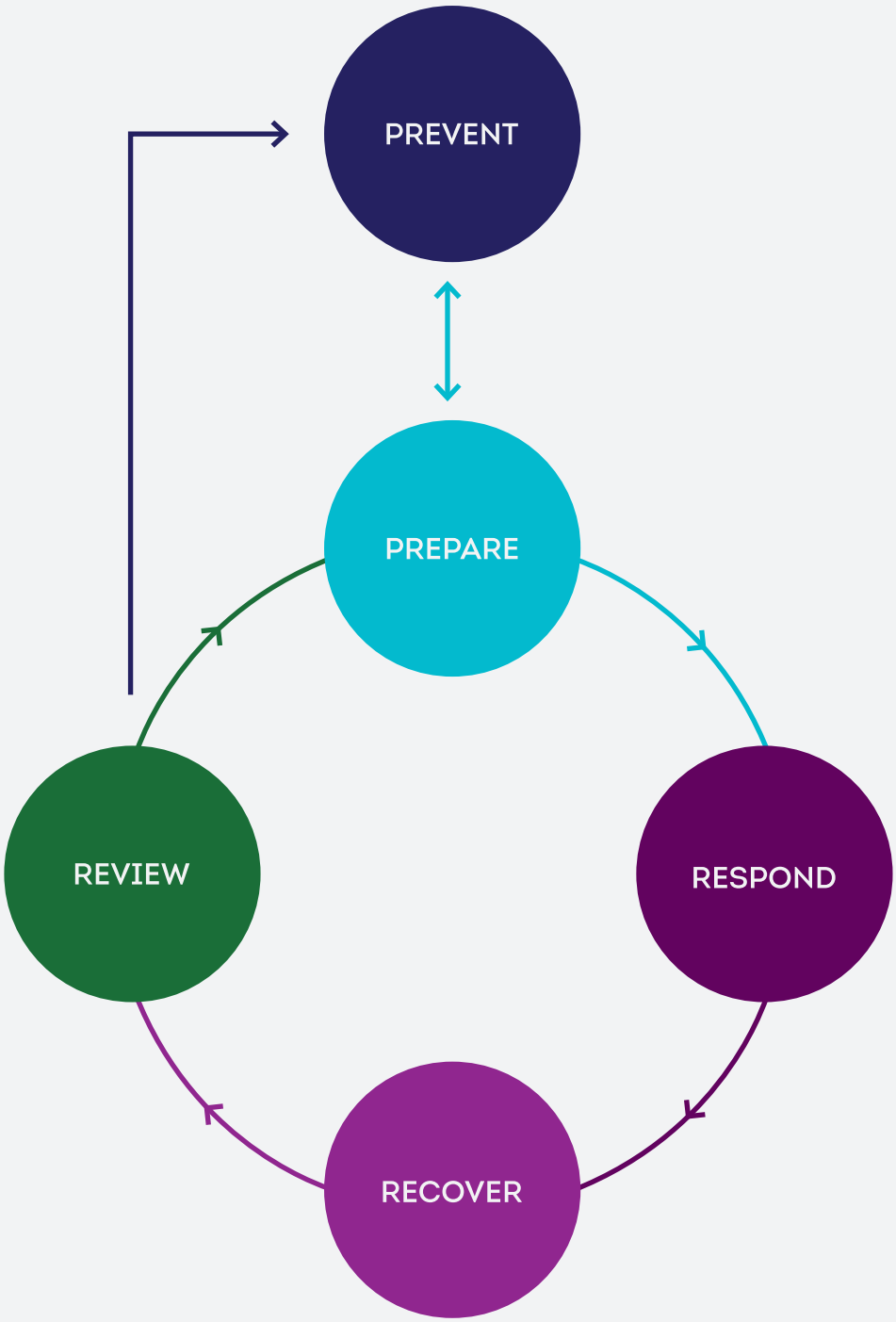
PREPARE:
Developing structures and plans to mitigate the impact of a potential cyber security breach

RESPOND:
Convening all relevant parts of the business to implement the incident management plan

RECOVER:
Reducing any residual cyber vulnerability and managing any resulting reputational damage

REVIEW:
Taking stock of lessons learnt from any incident and incorporating these into the strategy

This **CYBER RESILIENCE LIFECYCLE** for retailers can be summarised as follows:



PREVENT

A retail company should consider placing 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 basic 'cyber hygiene' amongst employees, contractors, and consumers. Often small changes in behaviour can lead to tangible benefits for corporate cyber resilience.

Levels of protection can be achieved by participating in and/or adopting the guidance and advice offered within a number of existing initiatives:

FOR BASIC PROTECTION:

CYBER AWARE

DETAILS

Cyber Aware (formerly Cyber Streetwise) is a cross-government awareness and behaviour change campaign delivered by the Home Office in conjunction with Department of Culture, Media & Sport alongside the National Cyber Security Centre, and funded by the National Cyber Security Programme in the Cabinet Office.

VALUE

Campaign aims to drive behaviour change amongst small businesses and individuals.
Its output is based on expert advice from the National Cyber Security Centre, a part of GCHQ.

Cyber Aware promotes the two prioritised protective things people and businesses can do to improve cyber security:

- Use strong passwords made up of three random words
- Always download the latest software updates as soon as they appear

More information:
http://www.cyberaware.gov.uk

GET SAFE ONLINE

DETAILS

The Get Safe Online website is a resource providing practical advice on how to protect yourself, your computers and mobiles device and your business against fraud, identity theft, viruses and many other problems encountered online.

VALUE

Leading source of unbiased, factual and easy-to-understand information on online safety.
Will be particularly valuable to acquaint staff with the website.

More information:
https://www.getsafeonline.org/

ISO 27001

DETAILS
The ISO 27000 family of standards helps organizations keep information assets secure. Using this standard will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

VALUE
ISO/IEC 27001 is a well-known, basic standard providing requirements for an information security management system.

More information:
http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

SECURITY TRAINING

DETAILS
Basic, free introductory courses that help retailers understand information security.

VALUE
Access free online training for you and your staff:

Cyber security training for business:
https://www.gov.uk/government/collections/cyber-security-training-for-business

Introduction to Cyber Security course offers a comprehensive introduction to cyber security and how to protect your digital life online:
https://www.futurelearn.com/courses/introduction-to-cyber-security

CYBER ESSENTIALS

DETAILS
A Government-backed, industry supported scheme to guide businesses in protecting themselves against cyber threats.
Requires completion of a self-assessment questionnaire, with responses independently reviewed by a certifying body.

VALUE
The Cyber Essentials Badge allows your company to advertise the fact that it has received an accreditation that adheres to government-endorsed standards.

Details of the scheme:
www.cyberaware.gov.uk/cyberessentials

For **GREATER CONFIDENCE:**

10 STEPS TO CYBER SECURITY (INCIDENT MANAGEMENT)

DETAILS
Bespoke guidance explaining how effective incident management policies and processes will help to improve resilience, support business continuity and reduce any financial impact resulting from an information security incident.

VALUE
Though not retail-specific, HMG offers free guidance on the right steps to take, and questions to ask:

Guidance available at:
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

DMARC

DETAILS
A group of organisations came together in Spring 2011 to find a way to combating fraudulent email at Internet-scale.

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

Details of the resource:
https://dmarc.globalcyberalliance.org/about-dmarc.html

ADDITIONAL OPTIONS:

10 STEPS TO CYBER SECURITY (FULL IMPLEMENTATION)

DETAILS
Government guidance for businesses looking to protect themselves in cyberspace.
The 10 Cyber Security Steps - originally published in 2012 and now used by around two thirds of the FTSE350 - are effective means in protecting your organisation from cyber-attacks.

VALUE
Defining and communicating your Board's Information Risk Management Regime is central to any organisation's overall cyber strategy.
This regime and the steps that surround it are provided by GCHQ.

Guidance available at:
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

CYBER ESSENTIALS PLUS

DETAILS
A Government-backed, industry supported scheme to guide businesses in protecting themselves against cyber threats.

For Cyber Essentials PLUS, tests of systems are carried out by an external certifying body, using a range of tools and techniques.

VALUE
The Cyber Essentials Badge allows your company to advertise the fact that it has received an accreditation that adheres to government-endorsed standards.

Cyber Essentials PLUS is the same as Cyber Essentials in terms of the requirements, but tested more rigorously to make sure the protections are in place.

Details of the scheme: ***www.cyberaware.gov.uk/cyberessentials***

CREST CYBER SECURITY INCIDENT RESPONSE GUIDE

DETAILS
Guide 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
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.

Guidance available at:
https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

CYBER-SECURITY INFORMATION SHARING PARTNERSHIP

DETAILS
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. The NCSC and the BRC are working to improve the level of participation in the dedicated retail group on the platform.

VALUE
Retail participants of CiSP benefit from access to the retail group on the platform, which is populated each month with additional material, content and discussion points. Working together in this way, businesses are helping to protect each other on an industry wide basis. To register for the platform, please apply via the relevant page of the NCSC website:
https://www.ncsc.gov.uk/cisp

If you are a member of BRC and do not know of another commercial organisation already registered on the platform, please contact Hugo Rosemont to discuss a BRC-supported application sponsorship. Email: ***hugo.rosemont@brc.org.uk***

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.

Recommended Roles and Responsibilities on **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 RETAIL COMPANY SHOULD CONSIDER PLACING A STRONG EMPHASIS ON INSTALLING AND EMBEDDING A PREVENTATIVE CYBER SECURITY CULTURE ALL THE WAY ACROSS THE BUSINESS"

PREPARE

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 Government's '10 Steps to Cyber Security'.

WHAT TO DO?

- Establish cyber security as a board level issue
- Establish a cross-functional Cyber Steering Committee, comprising all constituent groups
- Encrypt and back up business critical data and systems
- Mitigate the 'insider threat' by applying guidance outlined in BRC guidance (see page 36)
- Participate in retail-specific information-sharing through CiSP (see page 25)
- Establish (and invest in) a cyber security training & exercising programme (e.g. red teaming)
- Integrate cyber security into the corporate business continuity plan
- Conduct review of cyber security capability (people and technology)
- Assess need to appoint external, CESG-approved consultant / supplier to enhance capability (focus should be on assessing core needs around identification, patching, and monitoring).
- Consider working with customers to improve awareness of cyber security

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 the specialist training that underpins the response
- An outline of the roles and responsibilities across the organisation, including lines of internal communication
- Details on the company's data recovery capability
- Overview of company's strategy for monitoring all ICT systems
- A schedule on regular testing of the incident management plans
- An overview of what information will be shared, when, and with whom
- Guidance on the collection and analysis post-incident evidence
- A commitment to conduct a lessons learned review (see 'Review' below)
- A plan for educating users and maintaining their awareness
- A stated commitment to report criminal incidents to Law Enforcement (see 'Respond' below)

WHO DOES WHAT?

Recommended Roles and Responsibilities on **PREPARE**:

NOMINATED BOARD MEMBER	Ensure creation of Incident Management Plan by the Leadership Team Ensure cyber training / exercising takes place across the business
FINANCE DIRECTOR	Allocate funding to cyber security skills, training and exercising in business
COMMUNICATIONS	Integrate cyber security awareness in customer engagement strategy Lead work on what information will be shared and when during an incident
CISO	Advise Board on internal capability / need to appoint external support Allocate staff to contribute to CiSP Encrypt and back up business critical data
DATA CONTROLLERS	Ensure Board are aware of responsibilities arising from DPA/GDPR

RESPOND

WHAT TO DO?

- Convene the Cyber Steering Committee
- Implement Cyber Security Incident Response Plan
- Understand which system and where in the network an incident has occurred
- Establish clear lines of internal communications
- Take action to stop the breach as soon as possible (e.g. patches, software solutions)
- If necessary, engage technical experts and specialist suppliers for support
- Establish the facts, communicating with customers as appropriate
- Log all facts and developments in a through, systemic manner (i.e. for investigation)
- Consider appointing an accredited forensic investigator who is familiar with NPCC (ACPO) principles of digital evidence
- Initiate cyber security aspects business continuity arrangements
- Report incident as quickly as possible through the appropriate channels, in the following order:
  - Action Fraud (i.e. if breach is criminal activity)
  - NCSC (if a significant incident)
  - ICO (within 72 hrs)
  - CiSP
- When reporting, highlight if you have received any linked extortion threats
- Initiate clean up actions. NCSC offers information on Cyber Incident Response schemes to give organisations confidence about the quality of this external assistance: https://www.ncsc.gov.uk/scheme/cyber-incidents
- If the attack involves cardholder data, consider appointing a PCI Forensic Investigator who can help determine the occurrence of a compromise and when/how it occurred: https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators
- Communicate with staff on type and impact of breach

WHO DOES WHAT?

Recommended Roles and Responsibilities on **RESPOND**:

NOMINATED BOARD MEMBER	Convene Steering Committee Oversight of implementation of Incident Management Plan Appoint additional support as required (working with CISO)
FINANCE DIRECTOR	Make additional cyber security funding available as may be necessary
COMMUNICATIONS	Inform customers of facts in line with strategy agreed in the Incident Management Plan Communicate with staff on type and impact of breach
CISO	Take technical measures to stop breach Source external support as necessary (the NCSC's 'Marketplace' is a useful source of certified advice and products: https://www.ncsc.gov.uk/marketplace) 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	Submit report of breach to the ICO

If in doubt, do not hesitate to ask for help. Seek advice from the organisations that are listed from pages 16 to 18.

RECOVER

WHAT TO DO?

- Complete implementation of business continuity plan
- Deliver public communications strategy
- Ensure customers are informed of, and where necessary compensated for, impact of breach
- Conduct further penetration testing and other measures as necessary
- Share learning of incident on CiSP

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"

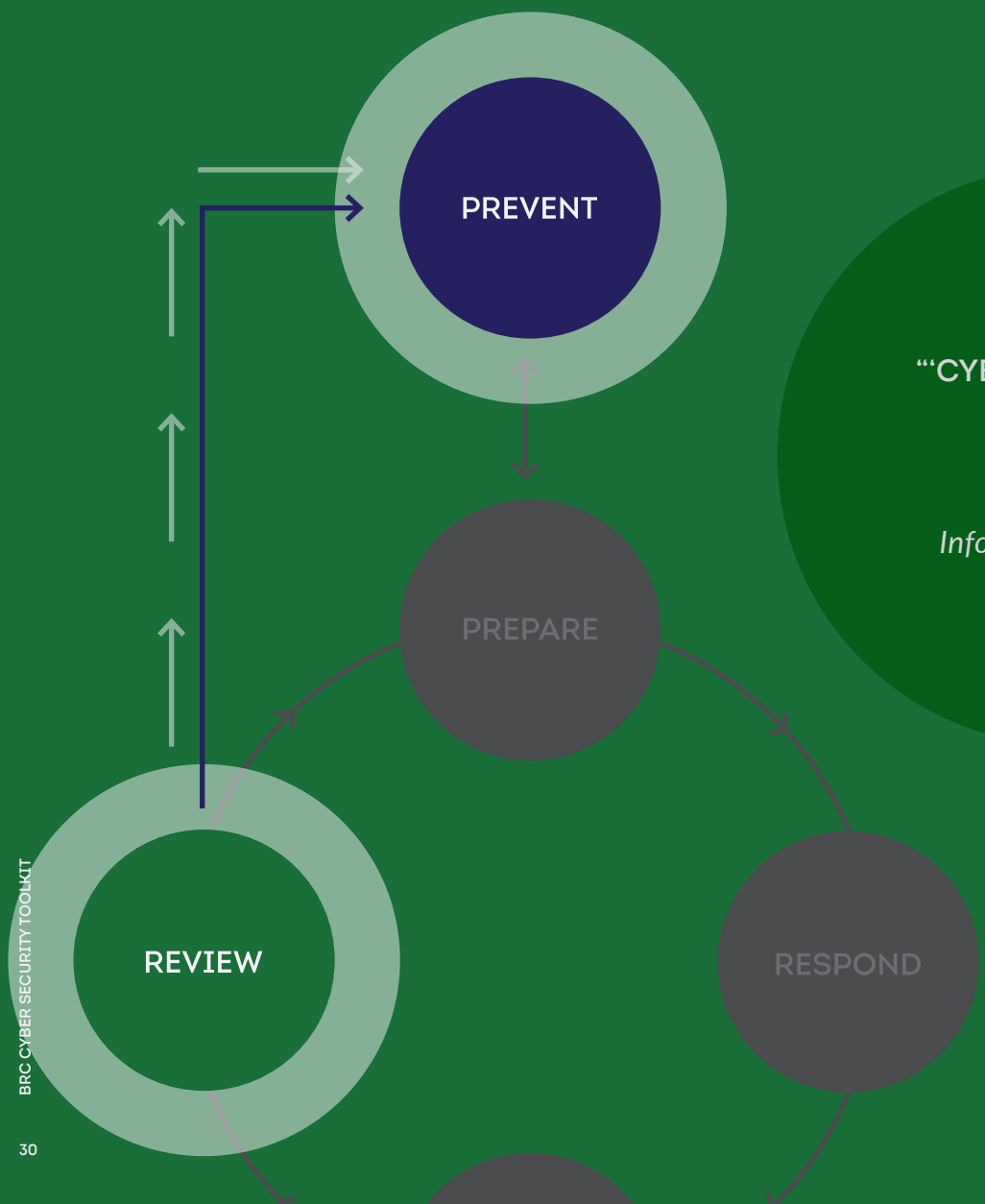
- HM Government, 10 Steps to Cyber Security -

REVIEW

WHAT TO DO?

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

- Conduct a 'Lessons Learnt' review
- Ensure 'Lessons Learnt' are integrated in all stages of the cyber resilience lifecycle for retailers
- Brief board on type and impact of incident, actions taken, and any ongoing vulnerabilities
- Publish details of incident and response in annual report



"'CYBER SECURITY IS NOT AN I.T. ISSUE, IT IS A BOARDROOM ISSUE"

- Elizabeth Denham, Information Commissioner -

SECTION D

CYBER SECURITY CHECKLISTS

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 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 any response.

The following checklists highlight the crucial roles and responsibilities that the BRC recommends should sit with someone on the board (the operational aspects of which should be led by a nominated board member) and the Communications Team of a retail company.

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 what details we will publicise in the event of a data breach, when will we do this, and whom will we communicate with?
Do we have an Incident Management Plan in place and is it regularly reviewed? Is this plan integrated into our wider Business Continuity plans? Have we invested sufficiently in Cyber Protection? • Do we have sufficiently qualified staff? • Have we invested in the appropriate technology? (Pen Testing etc.) • Do we have appropriate cyber security training and exercising regime across the business?	Have we arranged cyber security-related media training for a nominated Board Member and/or the CEO? Have we developed a strategy to maintain ongoing communications with customers? (Good cyber citizenship)
Is our company engaged in relevant external initiatives (e.g. CiSP, BRC Fraud and Cyber Security Member Group)?	Have we implemented an internal communications plan to promote cyber security amongst staff?
Have we reported the incident to the appropriate authorities, and conducted a post-incident review?	Have we liaised with communications teams across supply chain to mitigate vulnerabilities?

GUIDANCE FOR SMALL AND MEDIUM SIZED ENTERPRISES (SMES)

The Department for Business, Energy & Industrial Strategy (BEIS) has produced a cyber security guide for small businesses. Small companies operating in the retail industry are advised to become familiar with this document, paying particular attention to the following five areas of advice:

- Using strong passwords
- Updating software
- Providing simple staff awareness and training
- Managing risk
- Using the Cyber Essentials scheme to protect against common online threats

The guidance document is available to download: ***https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know***

SECTION E

OPTIONS FOR WORKING WITH STAFF AND CUSTOMERS

In addition to developing their own cyber resilience, individual retailers may wish to play a role in promoting awareness of the need for stronger basic 'cyber hygiene' across British society, including amongst the three million employees in the industry. There is no set 'template' for how companies may wish to communicate with their staff and customers in this area, but options they might consider could include:

- Promoting existing cyber security advice, such as the need to use strong (and varied) passwords consisting of three random words and having different strong passwords for key accounts such as email, and always downloading software updates as soon as they appear.
- Providing basic protective cyber security advice at the points where staff and customers enter their personal details (for example, at the online check out), and advising customers to log out following completion of a transaction.
- Demonstrating commitment to cyber security by making use of the 'Take 5' toolkit, the 'My Digital Footprint' campaign, and by supporting the Government's Cyber Aware campaign to build staff and consumers' resilience against the cyber threat such as by using its toolkit of assets.
- Providing a clear and accessible link to the Action Fraud reporting system on your website, offering your customers direction on where to report fraud and cyber-crime.

"'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 -

SECTION F

USEFUL RESOURCES

GOVERNMENT AND POLICING DOCUMENTS/RESOURCES:

 **BEIS** 'Cyber security – what small businesses need to know'	 **CPNI** 'My Digital Footprint asset library'	 **HMG** '10 Steps to Cyber Security'	 **HMG** 'Cyber Essentials'	 **HMG** 'Cyber Security Breaches Survey 2016'
 **HMG** 'National Cyber Security Strategy 2016 to 2021'	 **NCSC** 'Certified Cyber Security Consultancies'	 **NATIONAL CRIME AGENCY** 'National Cyber Crime Assessment 2016'	 **ACTION FRAUD** 'A-Z of Fraud'	 **METROPOLITAN POLICE** 'Little Book of Big Scams'

OTHER RESOURCES:

 **BRITISH RETAIL CONSORTIUM** 'Tackling the Insider Threat: Best Practice Guidelines for Retailers'	 **CREST** 'Crest Incident Management Guide'	 **FEDERATION OF SMALL BUSINESSES** Report, 'Cyber security and fraud: The impact on small businesses'	 **CITY UK** Report, 'Cyber and the City'	 **DELOITTE** 'Seven hidden costs of a cyberattack'
 **INSTITUTE OF DIRECTORS** Report, 'Underpinning the Digital Economy'	 **PWC** 'Global Economic Crime Survey 2016'	 **PWC** 'Global State of Information Security 2016'	 **SANS INSTITUTE** 'Reading Room'	 **SOPHOS** 'Threatsaurus: The A-Z of computer and data security threats'
 **TAKE 5** 'Campaign Materials'	 **THE BREWERY JOURNAL** 'Cyber-crime'	 **VERIZON** 'Data Breach Investigations Report'	 **CYBER AWARE** 'Toolkit of Assets'	**Go to page 37 for a full list of websites.**

GOVERNMENT AND POLICING DOCUMENTS/RESOURCES:

- **ACTION FRAUD**, 'A-Z of Fraud': http://www.actionfraud.police.uk/a-z_of_fraud
- **BEIS**, 'Cyber security – what small businesses need to know': https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know
- **CPNI**, 'My Digital Footprint asset library': http://www.cpni.gov.uk/advice/Personnel-security1/Employee-Digital-Footprint-Campaign/My-Digital-Footprint-asset-library/
- **HMG**, '10 Steps to Cyber Security': https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary
- **HMG**, 'Cyber Essentials': https://www.ncsc.gov.uk/scheme/cyber-essentials
- **HMG**, 'Cyber Security Breaches Survey 2016': https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016
- **HMG**, 'National Cyber Security Strategy 2016 to 2021': https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
- **METROPOLITAN POLICE**, 'Little Book of Big Scams': http://www.met.police.uk/docs/little_book_scam.pdf
- **NATIONAL CRIME AGENCY**, 'National Cyber Crime Assessment 2016': http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
- **NCSC**, 'Certified Cyber Security Consultancies': https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy

OTHER RESOURCES:

- **BRITISH RETAIL CONSORTIUM**, 'Tackling the Insider Threat: Best Practice Guidelines for Retailers': http://www.brc.org.uk/brc_show_document.asp?id=4518&moid=8446
- **CITY UK REPORT**, 'Cyber and the City': https://www.thecityuk.com/research/cyber-and-the-city/
- **CREST**, 'Crest Incident Management Guide': https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf
- **DELOITTE**, 'Seven hidden costs of a cyberattack': https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-cfo-insights-seven-hidden-costs-cyberattacks-final.pdf
- **FEDERATION OF SMALL BUSINESSES REPORT**, 'Cyber security and fraud: The impact on small businesses': http://www.fsb.org.uk/docs/default-source/fsb-org-uk/policy/assets/publications/fsb_cyber_security_and_fraud_paper_final.pdf?sfvrsn=0
- **INSTITUTE OF DIRECTORS REPORT**, 'Underpinning the Digital Economy': https://www.iod.com/Portals/0/Badges/PDF's/News%20and%20Campaigns/Infrastructure/Cyber%20security%20underpinning%20the%20digital%20economy.pdf?ver=2016-04-14-101230-913
- **INTERNET SECURITY FORUM**, 'Tools and Methodologies' https://www.securityforum.org/tools/
- **PCI DSS**, 'Payment Card Industry Data Security Standard' https://www.pcisecuritystandards.org/document_library
- **PWC**, 'Global Economic Crime Survey 2016': http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html
- **PWC**, 'Global State of Information Security 2016': https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
- **SANS INSTITUTE**, 'Reading Room': https://www.sans.org/reading-room/categories#R
- **SOPHOS**, 'Threatsaurus: The A-Z of computer and data security threats': https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=en.pdf
- **TAKE 5**, 'Campaign Materials': https://takefive-stopfraud.org.uk/resources/campaign-materials/
- **THE BREWERY JOURNAL**, 'Cyber-crime': https://issuu.com/freuds8/docs/brewery_final_single_pages
- **VERIZON**, 'Data Breach Investigations Report': http://www.verizonenterprise.com/verizon-insights-lab/dbir/

SECTION G

GLOSSARY

COMMON THREATS AND TERMINOLOGY[1]

BLACK HAT HACKER

A computer hacker who breaks into an information system or digital network with the purpose of inflicting malicious intent.

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".

DENIAL OF SERVICE ATTACK (DOS)

A method of taking a website out of action by overloading or 'flooding' the server.

DOXING

Discovering and publishing the identity of an internet user, obtained by tracing their digital footprint.

HACTIVIST

A combination of 'hacker' and 'activist', someone who uses computers and computer networks to promote a political agenda.

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.

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.

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.

PORT SCANNING

A technique employed to identify open ports and services on a network, potentially with a view to exploiting weaknesses illegally.

PHARMING

A method of deceiving an individual into ending up at a fake website, even though the correct URL has been entered.

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.

1 Sources: Definitions included in this glossary draw upon / develop open source material published by Get Safe Online, Action Fraud, Trend Micro, Sophos, Ocean, TechTarget Networks, The Brewery Journal, Wikipedia, the Information Commissioner's Office, and the National Cyber Security Centre. Refer to Section F for hyperlinks to a selection of useful resources.

SOCIAL ENGINEERING
In a cyber security context, the general art of manipulating people online so they give up confidential information.

SPEAR PHISHING
As per phishing, except that it is a directed attack against a specific target.

SPOOFING
Masquerading as another individual or entity by falsifying data, thereby gaining an illegitimate advantage.

SQLI
SQL injection attacks are a common way of trying to penetrate websites, through which attackers steal large volumes of information from underpinning databases.

THEFT OF DATA
Stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information.

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 organization, seeking unauthorized access to confidential data.

KEY ORGANISATIONS

NCSC

Established in October 2016, the National Cyber Security Centre (NCSC) aims to be the authoritative voice on information security in the UK.

CISP

The Cyber-security Information Sharing Partnership is a joint industry/government initiative designed to facilitate the sharing cyber threat and vulnerability information to reduce the impact on UK business.

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.

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.

SECTION H

CYBER SECURITY AT THE BRC

WORKING WITH PARTNERS TO HELP PROTECT THE RETAIL INDUSTRY AND ITS CUSTOMERS

The BRC's cyber security programme is driven by a desire to help to protect the retail industry and the customers it serves. Any effective strategy to tackle online or cyber-enabled criminality must involve strong cooperation between the private sector and the public security authorities.

The BRC maintains a dedicated Fraud and Cyber Security Member Group which leads the BRC's work on mitigating the effects of fraud and cyber-attacks affecting the retail industry. Chaired by John MacBrayne (Tesco), its activities include working closely with the UK's law enforcement and the wider security communities to improve public-private cooperation in a fast-evolving field. The group offers members a valuable forum for shaping the BRC's policy direction, and for enabling networking with peers in the industry on cyber security issues.

We engage regularly with the multiple cyber security-related government departments and agencies that have been identified in the BRC's Fraud and Cyber Security Policy Landscape Map; a resource that is available to all BRC members. These include, amongst many others, the NCSC (including CiSP), DCMS, the NCCU, the Home Office, and the City of London Police.

On behalf of its members, the BRC responds to official consultations on cyber security regularly. We informed the establishment of the NCSC, launched in October 2016, urging the new organisation to include within its scope regular engagement with, and new levels of support for, the UK-based retail industry in the event of serious incidents. BRC also provided feedback to the government during its Cyber Security Regulation and Incentives Project, finalised in late 2016, which took account of retailers' views that an effective cyber security approach is based on effective risk management, rather than compliance.

This cyber security toolkit for retailers was developed under the auspices of the BRC's Fraud and Cyber Security Member Group. Retail members of the BRC interested in participating in the group are welcome to join, and other companies wishing to learn more about our cyber security programme and/or join the BRC are encouraged to contact us.

HUGO ROSEMONT
Policy Adviser on Crime and Security
British Retail Consortium
E. hugo.rosemont@brc.org.uk

"THE BRC AND ITS MEMBERS ARE PLACING A PRIORITY ON STRENGTHENING THE PUBLIC-PRIVATE COOPERATION THAT IS NEEDED TO IMPROVE THE UK'S CYBER RESILIENCE."

- Helen Dickinson OBE, BRC -

"'IF WE'RE GOING TO RETAIN CONFIDENCE IN OUR INCREASINGLY DIGITIZED ECONOMY, WE HAVE TO MAKE SURE THAT EVERYONE – OUR PRIVATE CITIZENS, OUR SMALL BUSINESSES, OUR NOT-FOR-PROFITS, AS WELL AS OUR LARGEST AND MOST PIVOTAL PUBLIC AND PRIVATE INSTITUTIONS – CAN DO BUSINESS IN A DIGITAL ENVIRONMENT THAT IS FUNDAMENTALLY SAFER THAN IT IS NOW."

- Ciaran Martin, Chief Executive, National Cyber Security Centre -

BRITISH RETAIL CONSORTIUM

2 London Bridge, London SE1 9RA
+44 (0)20 7854 8900 | info@brc.org.uk | brc.org.uk