

2016 RETAIL CRIME SURVEY

FEBRUARY 2017



BRC

AT A GLANCE



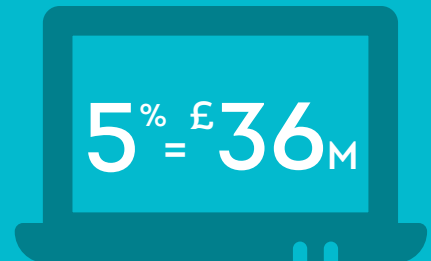
= DIRECT FINANCIAL COST
OF RETAIL CRIME



3.6_M

OFFENCES OF RETAIL CRIME

AT LEAST



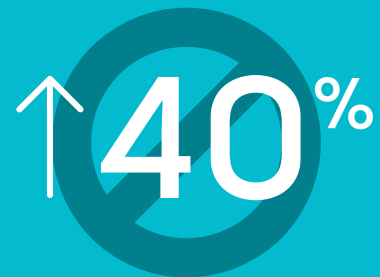
COST OF CRIME IS
CYBER CRIME



= TOTAL COST OF CUSTOMER
THEFT AFFECTING THE
INDUSTRY



ESTIMATED 53% OF
REPORTED FRAUD IN THE
RETAIL INDUSTRY IS CYBER-
ENABLED (£100M APPROX.)



VIOLENCE AND ABUSE
AGAINST STAFF IS UP BY
40% ON LAST YEAR



51 INCIDENTS OF VIOLENCE
AND ABUSE PER 1000 STAFF



= THE AVERAGE CAPITAL
SPEND ON CRIME AND
LOSS PREVENTION



OF RETAILERS BELIEVE
POLICE PERFORMANCE IS
POOR OR VERY POOR

CONTENTS

A // FOREWORD	04
B // ASSESSMENTS OF RISKS	05
RETAIL CRIME RISK ASSESSMENT	05
> STRATEGIC VIEW	05
> DETAIL	05
C // SURVEY OVERVIEW	06
INTRODUCTION	06
SURVEY COVERAGE	06
KEY FINDINGS AND HEADLINE TRENDS	06
> THEFT	06
> VIOLENCE AND ABUSE	06
> FRAUD AND CYBER SECURITY	07
> INSIDER THREATS	08
> ROBBERY, BURGLARY AND CRIMINAL DAMAGE	08
D // OTHER RESULTS	09
CYBER SECURITY	09
CRIME PREVENTION	09
UK RESPONSE	10
E // POLICY IMPLICATIONS	11
F // FUTURE STRATEGY	12
VISION	12
AIMS AND OBJECTIVES	12
PARTNERSHIPS	13
G // GLOSSARY	14
H // CRIME AND SECURITY POLICY AT THE BRC	16
I // CONTACTS FOR FURTHER INFORMATION	17

A // FOREWORD



The BRC's Annual Crime Survey collects data about the character and impact of all forms of crime on retailers and their staff. It is considered vital by our stakeholders in Government and across the policing community, and with our retail members and the wider business community. It also offers businesses an opportunity to compare their losses from criminal activity against the industry average. The UK retail industry suffers from both the reputational and financial impacts of crime levelled against it, which in financial terms cost £660m in 2015-16.

This year's survey highlights the growing problem of fraud and cyber-crime, which in light of the acute threats facing retail companies now represent major security priorities for the BRC. In consultation with our members, we report brand new data on cyber security risks and the effectiveness of the UK's response to them. For the first time, we have sought to measure the scale of the problem more accurately, and generate an initial industry view of the effectiveness of the UK's response.

As a preliminary, conservative estimate, the survey finds that crimes such as hacking and data breaches represent 5% of the total direct cost of crime to retail businesses - an approximate direct financial loss to the industry of £36 million per annum. Separately, we also asked retailers to estimate the percentage of the total cost of fraud levelled against them that was conducted online ('cyber-enabled fraud'). This was estimated at 53% - approximately 15% of the total cost of crime - representing a total direct cost of cyber-enabled fraud on the retail industry of around £100 million.

The industry faces many additional challenges, not least violence and abuse against colleagues which, regrettably, this year's survey shows is a growing problem. Overall, incidence of crime against staff in this category has increased significantly, with the biggest increases in aggressive and abusive behaviour. Abuse in any form is unacceptable and more must be done to ensure it is never accepted. In 2017, we will be looking to work closely with partners including USDAW to develop the UK's strategy to reduce the impact of violence and abuse against retail staff.

Retail crime is not limited to violence and cyber-crime and, in line with previous years, our survey provides a snapshot of industry perceptions on, and the impact of, other types of crime facing our industry including theft, insider threats, burglary, robbery and criminal damage. Customer theft remains the most common type of crime, accounting for 75% of crime by incidents and 66% of the direct cost of retail crime (£438m).

In view of the challenges outlined in the following pages, the BRC believes that retail crime must be addressed through even stronger cooperation between industry, the government, law enforcement and the private security industry; cooperation that needs to be focused on both the prevention of crime, and the response to it. Whilst this presents a major partnership opportunity, there is much to do to improve and organise forms of collaboration between the UK retail industry and its partners, and raise standards of security and policing across the country.

It is for this reason that, as a new feature, this report provides a high level overview of our strategy for tackling retail crime. We will look to build on the strong foundations we have in the cooperation under development to maximise the benefits that can be achieved through partnership working.

In 2017, we aim to work more closely with key stakeholders to reduce the impact of particularly the highest priority forms of retail crime, such as cyber-crime and violence against colleagues. We hope that all our partners will look upon this Retail Crime Survey Report as both a useful contribution to the debates already underway, and as a foundation document that can help to shape a joint approach for the future.

A handwritten signature in dark ink, reading 'Helen Dickinson'.

HELEN DICKINSON OBE
Chief Executive, BRC

B // ASSESSMENT OF RISKS

I. RETAIL CRIME RISK ASSESSMENT

STRATEGIC VIEW

The BRC adopts a risk-based, intelligence-driven approach to tackling all forms of crime facing the retail industry. In our view, a genuinely strategic approach to tackling business crime must take account of the budgetary pressures that exist in both the public and private sectors, and adopt a hard-headed approach towards prioritising those forms of crime which have the greatest impact on the industry, and society more generally.

In this context, the BRC conducted an exercise with the Retail Security community on 21 September 2016 with the aim of identifying, on a cross-industry basis, perceptions of the highest priority current crime risks facing the retail industry. Three groups were invited to rank the top risks facing the industry from among the following categories:

- i. Terrorism
- ii. Organised Crime
- iii. Fraud
- iv. Cyber Crime
- v. Violence and abuse against staff
- vi. Customer Theft
- vii. Insider Threats
- viii. Burglary
- ix. Robbery
- x. Criminal Damage

Having considered all the issues in terms of likelihood and impact, the three groups reported back and their results were aggregated. The exercise identified four tiers of priority risks as follows:

.....

RETAIL CRIME ASSESSMENT (2016)

TIER 1	VIOLENCE + ABUSE			
TIER 2	CYBER CRIME	ORGANISED CRIME	FRAUD	
TIER 3	THEFT	TERRORISM	INSIDER	ROBBERY
TIER 4	BURGLARY		CRIMINAL DAMAGE	

.....

It is important to stress that the prioritisation of issues into four tiers arises from 16 senior retail security practitioners' perceptions of the likelihood and impact of specific crime issues at a specific moment in time (21 September 2016); it should therefore be seen as a 'snapshot' of the BRC's retail security community.

It is also important to note that all of the highlighted risks are important; those on the 'lower' tiers were simply judged at a particular point in time to be either less impactful and/or less likely than those appearing as higher tier priorities.

Nevertheless, the exercise usefully identified that violence and abuse against staff is almost unanimously regarded as the highest priority crime risk facing the retail industry. Whilst some overlap and difficulties in definition existed, cyber-crime, fraud and organised criminality are also clearly seen by the retail security community as other common 'top tier' risks to the industry.

DETAIL

To generate an even better, more nuanced understanding of how crime risk is viewed within the retail industry, this year we again asked retailers which crime they considered will represent the most significant threats to their business over the next few years.

.....

WHAT CRIME DO YOU CONSIDER WILL REPRESENT THE TWO MOST SIGNIFICANT THREATS TO YOUR BUSINESS OVER THE NEXT TWO YEARS?



% OF RESPONDENTS WHO INDICATED THE CRIME WAS A SIGNIFICANT THREAT

.....

Some striking variances can be observed since last year, with cyber-attacks and violence rising as highest priority issues; 50% of respondents cited cyber-attacks as one of the most significant future threats (in contrast to 14% last year). In short, the data supports the well-versed mantra that the UK's business crime landscape is evolving rapidly.

C // SURVEY OVERVIEW

I. INTRODUCTION

Overseen by the BRC's Heads of Security Member Group, the BRC's annual Retail Crime Survey has a long tradition and represents our main statistical output on the character and impact of all forms of crime facing the UK retail industry. We measure this annually because retail crime has wide-reaching consequences for businesses, their employees and customers. Offending in retail stores creates negative perceptions of the local community and criminals who target businesses also commit other types of criminal activity.

Violence and abuse is on the rise and crimes committed in cyber space are also increasingly having an impact on businesses of all kinds. Overall, business crime is a blight on both the economy and society and, in view of our commitment to evidence-based policymaking, it is important to generate a detailed picture of the landscape.

II. SURVEY COVERAGE

This year the BRC Retail Crime Survey sample covered 37% per cent of the retail industry by turnover and 35% by staff, accounting for 1.1 million employees.

As in previous years, a significant range of BRC member companies participated in the survey, particularly large multiples, including pure online retailers. The sample included regular participants and new respondents, providing a representative cross-section of UK retailing. The BRC is grateful to all of its members that participated in this year's survey.

Readers familiar with historical editions of the BRC Crime Survey should note that changes have been made to the aggregation methodology for this year's edition. In particular, to gain the most accurate picture of the actual, known cost of crime in the retail industry, we did not ask retailers this year about undetected crimes, and so have estimated the past five years' data accordingly, and made a small number of other related adjustments.

III. KEY FINDINGS AND HEADLINE TRENDS

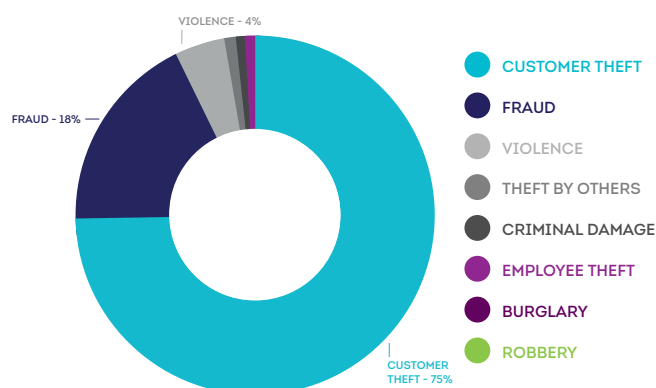
Incidence of retail crime has risen again this year, and our survey finds that the direct financial cost of crime suffered by our industry was £660m in 2015-16. A breakdown of this figure is as follows:

DIRECT COST	
CUSTOMER THEFT	438M
EMPLOYEE THEFT	13M
THEFT BY OTHERS	7M
ROBBERY	5M
BURGLARY	11M
CRIMINAL DAMAGE	3M
FRAUD	183M
TOTAL	660M

THEFT

Customer theft remains the most common type of crime, accounting for 75% of crime by incidents and 66% of the direct cost of retail crime (£438m).

INCIDENTS BY CRIME TYPE

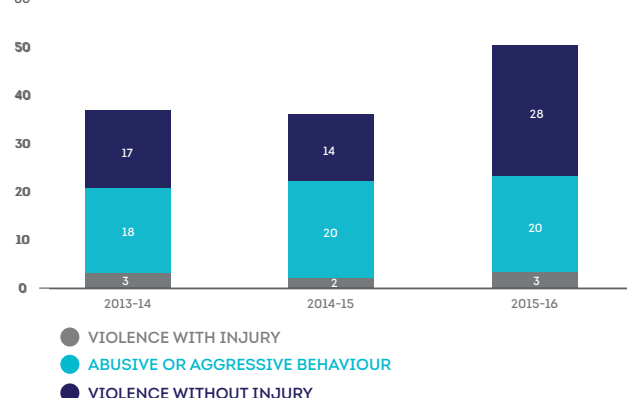


The continuing onward upward trend in theft is thought to relate to both the capacity of the UK police service to respond to this crime and the impact of international organised crime groups operating inside and outside the UK. In a separate exercise we conducted in 2016, retail security practitioners indicated that this is a multi-million pounds per year problem, and one which is growing. The types of activity that such groups are conducting include bulk theft (Alcohol/DVDs), ATM fraud, fraudulent payments, and trolley push outs. As section F outlines, the BRC's strategy for 2017 will place a strong emphasis on working closely with law enforcement bodies to tackle the blight of this criminal activity.

VIOLENCE AND ABUSE

Retail staff continue to suffer unacceptable levels of violence and abuse, which rose by 40% since last year. Incidence of violence against staff has therefore increased significantly, with the biggest increase in aggressive and abusive behaviour. In 2015-16, there were 51 incidents of violence and abuse per 1000 staff (up from 41 last year).

INCIDENCE OF VIOLENT CRIME PER 1000 STAFF



Whilst the pattern is not uniform - some retailers have seen incidence of violence fall - the overall picture is concerning. Several factors are seen to account for this unfortunate situation; amongst them, an inconsistent police response to even this form of retail crime means that deterrence is seen to be failing, as there is a growing sense that offenders are able to act with impunity.

The connection between violence and abuse against colleagues and the rising level of shoplifting should also not be underestimated; a large proportion of aggressive incidents are thought to be linked to the act of shoplifting, and abuse is particularly likely to occur when a confrontation takes place around an attempted theft. The perception of a lack of punishment for shoplifting is an aggravating factor for the violence and abuse that retailers are experiencing.

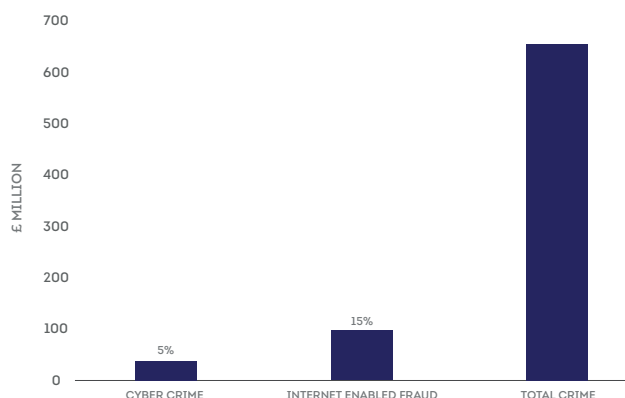
This sort of crime is never acceptable and the BRC will place a strong emphasis in 2017 on the development of a partnership, multi-agency approach to this problem.

FRAUD AND CYBER SECURITY

Measuring the exact cost of cyber-crime and internet-enabled fraud presents several methodological challenges, and the overall impact of these forms of criminality are not easy to determine, nor limited to financial harm. However, our survey shows that cyber-crime such as hacking and data breaches represents 5% of the total direct cost of crime to retail businesses. This preliminary, conservative estimate amounts to an approximate direct financial loss to the industry of £36 million per annum.

Separately, this year we also asked retailers to estimate the percentage of the total cost of fraud levelled against them that was conducted online ('cyber-enabled fraud'). This was estimated at 53% - approximately 15% of the total cost of crime - representing a total direct cost of cyber-enabled fraud on the retail industry of around £100 million.

DIRECT COST OF CRIME, CYBER CRIME & INTERNET ENABLED FRAUD



We plan to conduct work in 2017 to refine further the distinctions that must be drawn between cyber-enabled fraud and cyber-crime, in close collaboration with retailers, to ensure that we generate the most accurate picture possible of the cost of crime occurring online. It is clear in the meantime, however, that alongside the considerable amount of financial and societal harm being inflicted, there is little sign of the threat is abating. 91% of respondents reported that the overall number of cyber breaches is increasing (36%) or remaining the same (55%).

OVERALL, WOULD YOU SAY THAT THE OVERALL NUMBER OF CYBER SECURITY BREACHES SUFFERED BY YOUR BUSINESS IS:



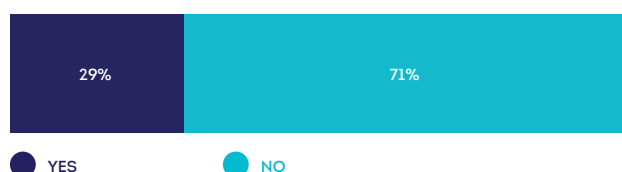
A significant aspect of the cyber security challenge for retailers is the attractiveness of customer data from the point of view of criminals, many of whom operate outside UK borders but can nevertheless gain relatively easy access to UK digital networks. As well as protecting companies better, we believe that industries including retail also now require extra support from the public authorities.

To help combat this high priority threat, the BRC will publish a brand new Cyber Security Toolkit for Retailers in March 2017. Developed under the auspices of our Fraud and Cyber Security Member Group in 2016, this new product is designed for the whole industry, and aims to be a practical, step-by-step, user-friendly guide that will have widespread application.

INSIDER THREATS

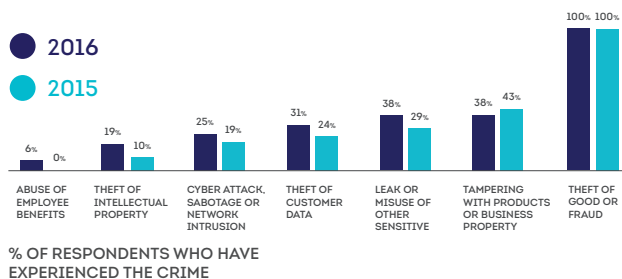
29% of retailers reported that their business had seen an increase in malicious insider incidents in the past two years, highlighting the ongoing severity of the problem.

WOULD YOU SAY YOUR BUSINESS HAS SEEN AN INCREASE IN MALICIOUS INSIDER INCIDENTS OVER THE PAST TWO YEARS?



More specifically, all respondents suffered theft by employees in 2015-16 and there have been notable rises since last year in cyber-related criminality at the hands of employees, suppliers, contractors or others with inside access.

IN TERMS OF MALICIOUS INSIDER ACTIVITY, HAS YOUR BUSINESS SUFFERED ANY OF THE FOLLOWING FROM 1 APRIL 2015 TO 31 MARCH 2016?



In 2015, the BRC published guidelines to help retail businesses minimise their vulnerability to insider threats. These remain highly relevant and, as we reported last year, they set out simple, practical steps that companies can put in place, and implement across their businesses.

ROBBERY, BURGLARY AND CRIMINAL DAMAGE

By and large, the cost per incident of these forms of retail crime has fallen since last year.

	2014-15	2015-16
ROBBERY	£921	£729
BURGLARY	£1,545	£1,506
CRIMINAL DAMAGE	£86	£67

Several factors might account for the decreases, including the emergence of opportunities for criminals to focus their effort on cyber-related crime, but this is also likely to be driven by the fact that better reporting means more marginal or 'smaller' crimes are being captured more effectively.

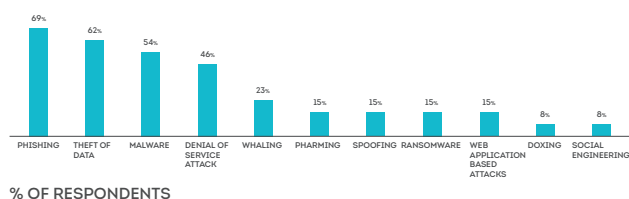
The financial costs of these crime types are not insignificant (Robbery £5m; Burglary £11m; and Criminal Damage £3m), and need to continue to be addressed and monitored carefully. Reflecting our retail crime risk assessment, however, the data suggests that they may be unlikely to represent the highest priorities for the industry in 2017.

D // OTHER RESULTS

CYBER SECURITY

In view of the growing problem for our industry of cyber-crime and internet-enabled fraud, this year's survey asked retailers a set of brand new, more detailed questions on the character of cyber security risks facing the industry, and the effectiveness of the UK's response to them. The survey reveals that, contrary to some perceptions, retail businesses face a wide variety of threats, and that amongst them phishing and data theft are considered to be the highest priority risks.

WHAT DO YOU CONSIDER TO BE THE HIGHEST PRIORITY CYBER SECURITY RISK FACING YOUR BUSINESS?



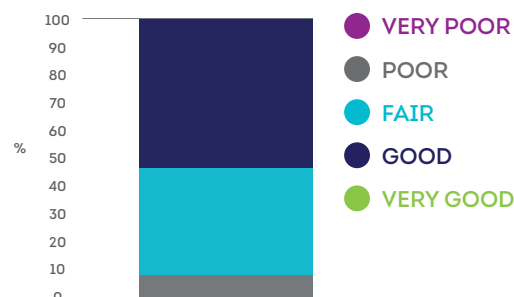
In terms of the character of actual attacks levelled against the industry, participants indicated that the biggest increases in cyber-related incidents against retailers are in the categories of phishing and denial of service attacks (DOS).

PLEASE INDICATE WHETHER INSTANCES OF THE FOLLOWING AGAINST YOUR BUSINESS INCREASED, DECREASED OR REMAINED THE SAME FROM 1 APRIL 2015 TO 31 MARCH 2016



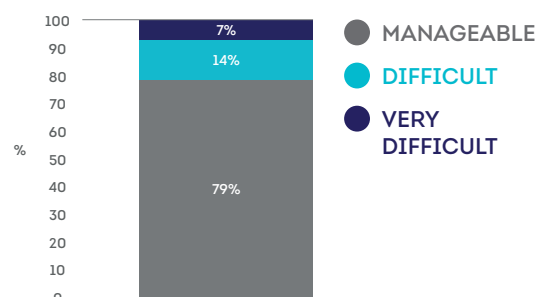
The data also shows that, whilst there is obviously room for improvement in the level of preparedness across the industry, most retail businesses feel comfortable that they are prepared to deal with cyber security incidents. Adoption of the guidance contained within the BRC's Cyber Security Toolkit and better information sharing through the Cyber-security Information Sharing Partnership (CISP) will help to ensure that all retailers can strengthen their digital resilience.

HOW DO YOU ASSESS THE CAPABILITY OF YOUR BUSINESS TO PREVENT AND RESPOND TO CYBER-CRIME INCIDENTS?



Finally, it appears that the UK's cyber security skills shortage may not yet be affecting retailers as intensely as many people may perceive - 79% of retail businesses felt that their ability to recruit staff with cyber security expertise is manageable. With 21% of retailers finding it difficult or very difficult to recruit suitably-qualified staff, however, efforts will need to be made to ensure that retail is seen to be an attractive place to work for information security professionals.

HOW EASY DO YOU FIND IT TO RECRUIT STAFF WITH CYBER-SECURITY EXPERTISE?



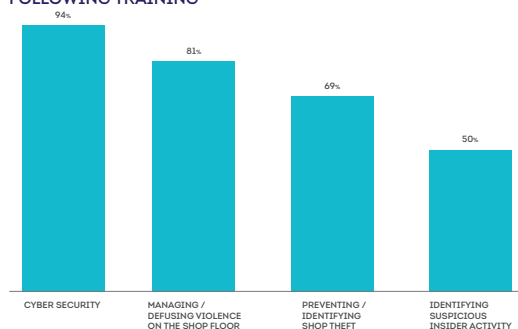
CRIME PREVENTION

Retailers take their security responsibilities seriously and continue to invest heavily in loss prevention. In 2015-16, the average capital spend on crime and loss prevention was £6.7m per retailer; a slight decrease which might be explained by the more competitive and heavily constrained market, and the finding that some retailers made particularly substantial investments last year.

Investment in training also clearly continues to be an important way that retailers build up their crime prevention capability. For example, 94% of respondents indicated that they provide training in cyber security, with 81% providing training in the mitigation of violence in store.

.....

% OF RESPONDENTS WHO PROVIDE THE FOLLOWING TRAINING

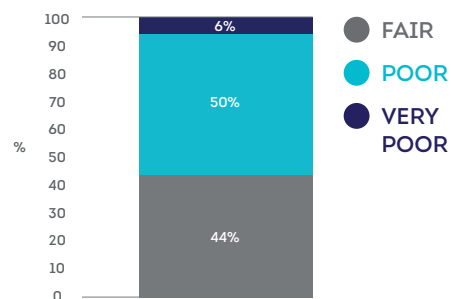


% OF RESPONDENTS ANSWERING YES

UK RESPONSE

Most retailers (56%) now feel that the police perform either poorly or very poorly in tackling the crime that they experience – this is a significant deterioration since last year, when the figure was 43%.

HOW GOOD A JOB DO YOU THINK THE POLICE DO TO TACKLE RETAIL CRIME?



.....

It is clear that retailers' experiences in this area are varied. From our own engagement, we know that some police forces view tackling business crime as a high priority.

At the same time, it is unavoidably the case that the picture is mixed. Several factors contribute to this picture. Reductions in resources available to UK policing have undoubtedly presented challenges, and more broadly the lack of consistency around the way retail crime is responded to across the country - even for the most serious crimes such as violent assaults - is judged to be a major problem.

The BRC and its members look forward to working closely with the National Police Chiefs' Council (NPCC) and other partners to ensure that the newly-created National Business Crime Reduction Hub can begin to turn the tide on deteriorating performance levels.

Regarding the effectiveness of the UK's approach to cyber security, industry views were mixed on the quality of the response arising from specific organisations and initiatives.

.....

WOULD YOU SAY THE UK GOVERNMENT'S APPROACH TO CYBER SECURITY IS:



OVERALL, HOW WOULD YOU RATE THE POLICE SERVICE'S RESPONSE TO CYBER-ATTACKS/BREACHES?



HOW VALUABLE DO YOU CONSIDER THE CYBER-SECURITY INFORMATION SHARING PARTNERSHIP (CCISP) TO BE?



HOW VALUABLE DO YOU CONSIDER THE ACTION FRAUD REPORTING MECHANISM TO BE?



0 20 40 60 80 100 %

● VERY POOR ● FAIR ● VERY GOOD
● POOR ● GOOD

.....

Unfortunately, the improvements that last year's BRC crime survey encouraged in respect of the system around the Action Fraud reporting mechanism have not yet been realised. In contrast to retailers' perceptions of central Government's performance on wider cyber security, which includes the welcome establishment of the new National Cyber Security Centre, over half of respondents to this year's crime survey indicated that the service is 'poor' or 'very poor'.

E // POLICY IMPLICATIONS

The concerning increases in retail crime levels highlighted in this report mean that renewed, focused attention is needed to stem the flow of illegal activity. A core implication arising from the data is that the UK policing community in particular must review how it works with retailers on especially the highest priority risks identified in this report.

We do not criticise the bravery and commitment of UK law enforcement. National and local police forces work tirelessly and often thanklessly as they discharge their duties, putting themselves in harms way on a daily basis to help protect, amongst others, the retail industry and the customers it serves. We would also point out that many individual forces and agencies, such as the Metropolitan Police Service and the National Crime Agency, are allocating dedicated resources to the priority of tackling business crime and improving cooperation with industries across the economy, which is extremely welcome.

Improvements can be made, however. To assist with this task constructively, the BRC has developed a new policing engagement strategy which recognises that, from an industry perspective, the UK's crime and policing landscape is characterised by unhelpful levels of fragmentation. Notwithstanding the welcome emergence of new structures that are designed to strengthen coordination of the police response at the national level - such as the NPCC, the College of Policing, and the new National Business Crime Reduction Hub - these structures remain generally underdeveloped, especially in so far as they consider industry engagement.

Police resourcing decisions made in recent years have also placed major constraints on many local forces. Whilst the appropriateness of existing police spending levels across the country should continue to be debated, it seems that, currently, the most pragmatic way forward will be for all partners to work together more closely in order to improve capabilities, particularly through such activities as training and the development of consistent approaches to business crime across police boundaries.

There is enormous scope for improvement around how the police work with retailers, and vice-versa, to tackle cyber-crime. Of ongoing concern is that the UK's fraud reporting system known as Action Fraud is not operating effectively – in contrast to the UK Government's performance on cyber security, over half of respondents to this year's crime survey indicated that it is 'poor' or 'very poor'. A policy debate is now urgently needed, perhaps within the context of the wider debate on the state of digital policing in the Twenty-First Century, around whether the structure and operation of Action Fraud is, or ever could be, 'fit for purpose'.

We also believe that, as urgent tasks for 2017, the relevant parties must now work together even more closely to re-energise a shared strategy for the UK on tackling violence and abuse in the workplace; develop a new, cross-border focus on addressing impact of Organised Crime in the retail industry; and implement an effective cyber security strategy for the retail industry, which will include the promotion of the guidance contained within the BRC's new Cyber Security Toolkit, and renewed effort to energise cyber threat information sharing through CiSP.

**“...WHERE GOVERNMENT,
LAW ENFORCEMENT, BUSINESSES
AND THE PUBLIC WORK TOGETHER
ON PREVENTION WE CAN DELIVER
SIGNIFICANT AND SUSTAINED
CUTS IN CERTAIN CRIMES”**

**HOME OFFICE, MODERN CRIME
PREVENTION STRATEGY, MARCH 2016**

F // FUTURE STRATEGY

I. VISION

Our vision is for effective cooperation and engagement between retailers, government, the police, and the private security industry at all levels, to help protect the industry and the customers it serves. The 'ideal type' of partnership we are striving would be characterised by at least the following traits:

- i. **COOPERATION**; there should be effective strategic and operational partnerships between the police, the retail industry, government, and the private security industry at all levels. 'Best practice' mechanisms, standards and examples of partnership-working, such as London's business crime strategy and associated machinery, will begin to be replicated across the country;
- ii. **AGILITY**; the government, the police, the retail industry and their partners will share and maintain an agile, razor-like focus on the evolution of retail crime, paying particular attention to updating mechanisms and strategies to tackle evolving threats. Collectively, we will begin to turn the tide of the impact of evolving threats such as violence and abuse, and industrial-scale fraud, cyber and organised crime facing industry;
- iii. **COORDINATION**; We strive for a transformation towards effective coordination across the UK policing landscape, particular in respect of engagement with the retail industry. At the national level, marked improvements will be made in coordinating the work of police forces in response to the highest priority forms of retail crime, particularly through the new National Business Crime Reduction Hub;
- iv. **UNDERSTANDING**; There should be a strong understanding amongst stakeholders and the public around the impact of all types of retail crime on victims and the economy, and the need for effective standards, training and appropriate investment by all partners. Politicians including Ministers, MPs and Police and Crime Commissioners, together with senior officers, will all understand, and be able to help to respond to, key industry issues.

II. AIMS AND OBJECTIVES

The main aim of the BRC's policing engagement and wider security strategy in this context is:

"TO RAISE PUBLIC AND POLITICAL AWARENESS OF, AND WORK WITH PARTNERS TO REDUCE SIGNIFICANTLY, THE IMPACT OF THE HIGHEST PRIORITY CRIME TYPES FACING THE UK RETAIL INDUSTRY AND ITS CUSTOMERS."

To achieve this aim, we will focus on forging effective crime prevention and response, and will pursue five more specific, deliverable objectives in 2017:

- i. Engage stakeholders across the UK's Policing and Security Policy landscape constructively
- ii. Re-energise the focus of the National Retail Crime Steering Group to drive action on the top tier risks
- iii. Promote awareness amongst partners of the evolution and real impact of retail crime
- iv. Develop new structures to reduce cyber-enabled fraud and cyber-crime in the retail industry
- v. Deliver a strategy to reduce the impact of violence and abuse against retail staff

In 2017, the BRC will work closely with its members to deliver a set of activities that have been designed to meet these objectives; progress will be overseen by the Heads of Security Member Group.

III. PARTNERSHIPS

The BRC believes that cooperation between retailers and its partners in government, policing and the private security industry will be needed to tackle retail crime. In 2017, we will seek to contribute actively to, and/or build upon those partnerships' which we believe offer maximum potential to reduce the impact of business crime in the UK.

- NATIONAL RETAIL CRIME STEERING GROUP

The NRCSG seeks to facilitate effective partnership working between government, retailers and the police. Co-chaired by the BRC, the group is made up of representatives from across the industry who come together to generate innovative solutions to prevent retail crime. Through the NRCSG, we will work to help deliver effective action on retail fraud and around the analysis of retail crime trends.

- CYBER-SECURITY INFORMATION SHARING PARTNERSHIP

CiSP, part of the National Cyber Security Centre, is a joint industry-government initiative that allows the sharing of cyber threat information to improve overall situational awareness of the cyber threat facing UK business. The BRC is working to improve cooperation within the dedicated retail group on the platform.

- NATIONAL BUSINESS CRIME REDUCTION HUB

In line with BRC priorities, the Home Secretary announced the funding of a new National Business Crime Reduction Hub in late 2016. Over £1 million has been committed across three years to address business crime in a more consistent way across the country.

Other partnerships which have also provided (or offer significant potential to provide) effective cooperation on retail crime include, but are not limited to:

- LONDON BUSINESS CRIME STRATEGY

MOPAC's Business Crime Strategy 2014-16, endorsed by the Metropolitan Police Service, the National Crime Agency, and the City of London Police, outlined how each provider would build their capability to tackle fraud and economic crimes. A first of its kind, retailers believe that dedicated business crime strategies like this should be continued and replicated across the country.

- MODERN CRIME PREVENTION FORUM

Established in 2016 as part of the Government's Modern Crime Prevention Strategy, the BRC is proud to have been invited to participate in this new Ministerial-chaired forum. The forum convenes partners from various industries involved in preventing crime to share good practice and identify emerging problems.

- BUSINESS CRIME ACTION PLAN OF NORTHERN IRELAND











Launched in 2016, the Business Crime Plan Action Plan is the first of its kind in Northern Ireland. It has been developed in partnership with the Department of Justice, the Policing Board, the PSNI and the business community. The Action Plan seeks to make streets and towns in Northern Ireland not only safer, but a better place to invest and do business through partnership working and providing business with the tools to protect themselves and their customers.

"WE WILL LOOK TO BUILD ON THE STRONG FOUNDATIONS WE HAVE IN THE COOPERATION UNDER DEVELOPMENT TO MAXIMISE THE BENEFITS THAT CAN BE ACHIEVED THROUGH PARTNERSHIP WORKING."











**HELEN DICKINSON OBE,
BRITISH RETAIL CONSORTIUM**

G // GLOSSARY

I. CRIME THREATS / TERMINOLOGY

 <p>ABUSE Incidents of non-physical aggressive, intimidating or abusive behaviour</p>	 <p>BURGLARY Entry into a premises without permission with the intent to steal</p>	 <p>CRIMINAL DAMAGE Deliberate damage or destruction of property, including arson</p>	 <p>CYBER-CRIME Crime that committed through use of ICT (e.g. hacking, malware)</p>
 <p>CYBER-ENABLED CRIME Traditional crime increased in scale by the use of computers, networks</p>	 <p>FRAUD Wrongful or criminal deception intended to result in illegal gain</p>	 <p>ICT Information and Communications Technology</p>	 <p>ROBBERY Force / threat of force used either during / before a theft, or attempt at one</p>
 <p>THEFT Where money, goods, property or services are stolen from the business</p>	 <p>VIOLENCE Assaults and robberies where physical injury may have been sustained</p>		

II. CYBER SECURITY TERMINOLOGY

 <p>DENIAL OF SERVICE ATTACK (DOS) A method of taking a website out of action by overloading of 'flooding' the server.</p>	 <p>DOXING Discovering and publishing the identity of an internet user, obtained by tracing their digital footprint.</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>PHARMING A method of deceiving an individual into ending up at a fake website, even though the correct URL has been entered.</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>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>SPOOFING Masquerading as another individual or entity by falsifying data, thereby gaining an illegitimate advantage.</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 organization, seeking unauthorized access to confidential data.</p>		

III. ORGANISATIONS / PARTNERSHIP FORA

<p>BRC British Retail Consortium</p>	<p>CISP Cyber-security Information Sharing Partnership (part of NCSC)</p>	<p>MOPAC Mayor's Office for Policing and Crime (London)</p>
<p>NCA National Crime Agency</p>	<p>NCSC National Cyber Security Centre</p>	<p>NBCRH National Business Crime Reduction Hub</p>
<p>NPCC National Police Chiefs' Council</p>	<p>NRCSG National Retail Crime Steering Group</p>	

H // CRIME AND SECURITY POLICY AT THE BRC

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

The BRC's crime and security programme is driven by a desire to help to protect the retail industry and the customers it serves. In our view, any effective strategy to tackle retail crime must involve strong cooperation between the private sector and the public security authorities at all levels.

The BRC maintains two Member Groups in the crime and security space. These each meet four times every year and are open to all retail members:

- The Heads of Security Member Group is an established BRC forum designed to lead the industry response to all forms of crime affecting the retail industry. Activities include shaping and overseeing the BRC's crime and security policy objectives, and supporting the production of the annual BRC Retail Crime Survey. At meetings, there is a regular policy round-up and external speakers from Government and law enforcement attend to deliver talks on pertinent initiatives relating to business crime.
- Our dedicated Fraud and Cyber Security Member Group leads the BRC's work on mitigating the effects of fraud and cyber-crime affecting the retail industry. 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 enabling networking with peers in the industry on cyber security issues.

We engage regularly with the multiple security-related government departments and agencies that have been identified in UK crime and security policy space. These include, amongst many others, the Home Office, the National Crime Agency, and many other law enforcement organisations including the Metropolitan Police Service and the City of London Police.

BRC co-chairs, and helps to provide the secretariat for, the Home Office's National Retail Crime Steering Group (NRCSG). Supporting this structure, in 2016 we led work on creating a new forum - the Retail Crime Tends Information Exchange - that is designed to deliver evidence-based insight around crime affecting the retail industry. We have also been working with the Home Office's Strategic Centre for Organised Crime to develop focused work on retail fraud. As part of this strand of activity, we will convene work around understanding the retail fraud threat with key partners from the NRCSG to draw together available intelligence related to different retail frauds experienced.

On behalf of its members, the BRC responds to official consultations on crime and security issues regularly. Cyber security policy is a high priority for members, and in this context we informed the establishment of the National Cyber Security Centre, 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. We have also developed a Cyber Security Toolkit for retailers under the auspices of the Fraud and Cyber Security Member Group.

Retail members of the BRC interested in participating in our security activity are welcome to join, and other companies wishing to learn more about our crime policy 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

ANY EFFECTIVE STRATEGY TO TACKLE RETAIL CRIME MUST INVOLVE STRONG COOPERATION BETWEEN THE PRIVATE SECTOR AND THE PUBLIC SECURITY AUTHORITIES AT ALL LEVELS.

HUGO ROSEMONT,
BRITISH RETAIL CONSORTIUM

I // CONTACTS FOR FURTHER INFORMATION

STATISTICAL ENQUIRIES //

RACHEL LUND
HEAD OF RETAIL INSIGHT AND ANALYTICS
E. RACHEL.LUND@BRC.ORG.UK

ANOUSH DARABI
JUNIOR ANALYST, RETAIL INSIGHT AND ANALYTICS
E. ANOUSH.DARABI@BRC.ORG.UK

POLICY ENQUIRIES //

HUGO ROSEMONT
POLICY ADVISER ON CRIME AND SECURITY
BRITISH RETAIL CONSORTIUM
E. HUGO.ROSEMONT@BRC.ORG.UK

GENERAL ENQUIRIES //

E. INFO@BRC.ORG.UK

4TH FLOOR, 2 LONDON BRIDGE
LONDON SE1 9RA

WWW.BRC.ORG.UK



BRITISH RETAIL CONSORTIUM 2017 ©

4TH FLOOR, 2 LONDON BRIDGE
LONDON SE1 9RA

+44 (0)20 7854 8900

WWW.BRC.ORG.UK



10081AKB17