NCA
National Crime Agency

NCA Strategic Cyber Industry Group

Cyber Crime Assessment 2016

Need for a stronger law enforcement and business partnership to fight cyber crime

7 July 2016

Version 1.2

Overview

This assessment has been jointly produced by the National Crime Agency (NCA) and the Strategic Cyber Industry Group (SCIG).[1] It outlines the real and immediate threat to UK businesses from cyber crime. It argues that the speed of criminal capability development is currently outpacing our response as a community and that only by working together across law enforcement and the private sector can we successfully reduce the threat to the UK from cyber crime.

[1] The Strategic Cyber Industry Group provides an overarching forum within which the National Cyber Crime Unit (NCCU) of the NCA and private sector organisations work in partnership to: coordinate joint activity against cyber crime, identify intelligence gaps and improve intelligence sharing, understand the capabilities available in law enforcement and industry, and steer the activities of Virtual Task Forces and ad hoc working groups. We would like to thank Bill Trent of Stroz Friedberg who led the SCIG contributions to this assessment.

Executive Summary

A cyber attack that poses an existential threat to one or more major UK businesses is a realistic possibility. The long-term impact of such a cyber attack could include substantial loss of revenue and margin, of valuable data, and of other company assets. The impact of litigation costs (and, with the arrival of new regulations, potential fines), the loss of confidence from reputational damage and possible executive-level dismissals could also result in immediate and material loss of shareholder value.

The NCA estimates that the cost of cyber crime to the UK economy is billions of pounds per annum – and growing. Although estimates of the cost of cyber crime vary considerably, our view is consistent with that of other industry analyses. In any calculation we must consider that there are millions of individual victims, many thousands of corporate victims and correspondingly substantial losses.

Moreover, the accelerating pace of technology and criminal cyber capability development currently outpaces the UK's collective response to cyber crime. This 'cyber arms race' is likely to be an enduring challenge, and an effective response requires collaborative action from government, law enforcement, industry regulators and, critically, business leaders.

Government, law enforcement and other bodies have increased efforts to tackle cyber crime. However, these efforts alone cannot, and will not, fully address the challenges presented by cyber crime. UK business has also made valuable contributions to tackling cyber crime, but there is much more that needs to be done, working with the government and law enforcement, to reduce vulnerabilities and prevent crime.

Directors of businesses should challenge their business management teams to go beyond compliance with minimum cyber security standards to ensure that rapidly evolving cyber security and resilience challenges are addressed and the threat to the UK is reduced.

Directors also have an important role in addressing the under-reporting of cyber crime which continues to obscure the full understanding of, and hence responses to, cyber crime in the UK. In particular, we urge businesses to report when they are victims of cyber crime and to share more intelligence, both with law enforcement and with each other.

These and other challenges for boards to consider are set out summary in Annex A, together with links to further resources.

Action by businesses will not be enough. A collaborative approach, based on an enhanced partnership between business and law enforcement, is necessary to build a better understanding of the cyber crime threat, facilitate the investigation of cyber crime and disrupt criminal networks. Such a partnership, building on existing intelligence sharing initiatives and encouraging and enabling the reporting of cyber crime, would be a major contributor to the disruption of criminal activity, business risk mitigation and a reduction in the cyber crime threat to the UK.

Cyber crime activity in the UK in 2015 and the threat to business

The UK's internet economy is one of the strongest in the world, and an increasing proportion of our daily life is now carried out online. International and domestic cyber criminals increasingly view UK-based businesses and private individuals as attractive targets for a range of cyber crime.

This range includes both cyber-dependent[2] and cyber-enabled[3] crime. Cyber criminals see major opportunities for financial fraud, theft and monetisation of stolen data and other valuable information, and extracting value from threats of criminal damage to businesses.

Cyber criminals targeting the UK include international serious organised crime groups as well as smaller-scale, mostly domestic, criminals and hacktivists. The NCA assesses that the most advanced and serious cyber crime threat to the UK is the direct or indirect result of activity by a few hundred international cyber criminals, typically operating in organised groups, who target UK businesses to commit highly profitable malware-facilitated fraud. These cyber attacks include attacks directly targeting business systems and attacks against individuals, although those targeting individuals can also impact upon business (e.g. through customers and supply chain vulnerabilities).

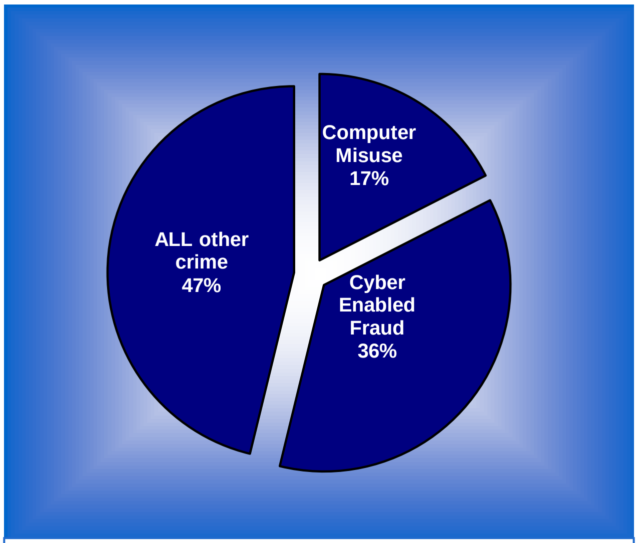
Although the most serious threat comes, directly or indirectly, from international crime groups, the majority of cyber criminals have relatively low technical capability. Their attacks are increasingly enabled by the growing online criminal marketplace, which provides easy access to sophisticated and bespoke tools and expertise, allowing these less skilled cyber criminals to exploit a wide range of vulnerabilities.

Under-reporting continues to obscure the full impact of cyber crime on the UK. However, 2015 saw the Office of National Statistics trial the inclusion of cyber crime in the annual Crime Survey for England and Wales for the first time. The ONS estimated that there were 2.46 million cyber incidents

[2] **Cyber-dependent** crimes can **only** be committed using computers, computer networks or other forms of information communication technology (ICT). They include the creation and spread of malware for financial gain, hacking to steal sensitive personal or industry data and denial of service attacks to cause reputational damage.

[3] **Cyber-enabled** crimes, such as fraud, the purchasing of illegal drugs and child sexual exploitation, can be conducted **on or offline**, but online may take place at unprecedented scale and speed.

and 2.11 million victims of cyber crime in the UK in 2015. These figures highlight the clear shortfall in established reporting, with only 16,349 cyber-dependent and approximately 700,000 cyber-enabled incidents reported to Action Fraud over the same period.



Cyber Crime as a proportion of total UK crime in 2015 (Source: ONS)

Cyber crime activity is growing fast and evolving at pace, becoming both more aggressive and technically proficient. As such it is a major and growing threat to UK businesses:

- The skills and sophistication of international crime groups make them the most competent and dangerous cyber criminals targeting UK businesses. These groups are increasingly professional and have industrialised their criminal activity so they can act at scale. Some of these groups are now so well established and business-like that they have well-defined organisational structures, access to specialist skills and functions like call centres and translators.
- These groups are believed to be responsible for, amongst other crimes, the use and sale of sophisticated financial "trojan" malware. This malware is a substantial source of financial crime in the UK, with three variants: DRIDEX, NEVERQUEST and DYRE /DYREZA, appearing frequently and responsible for many hundreds of thousands of individual crimes in 2015.
- There is also a significant number of technically competent cyber criminals active in the UK, engaging in much of the confrontational cyber crime now targeting business and other organisations and the public. The threats from Distributed Denial of Service (DDoS) and "ransomware" attacks have increased, driven by ready access to easy-to-use tools and by wider criminal understanding of its potential for profit through extortion. Ransomware attacks have also increased in frequency and complexity, and now include threats to publish victim data online, as well as the permanent encryption of valuable data.
- Data breaches are among the most common cyber crimes committed against businesses. Almost all large companies and a substantial

majority of smaller companies have experienced a data breach. Meanwhile, cyber-enabled fraud – most commonly, but not exclusively, targeting retail customers – is a rising cost for banks, retailers and other businesses.

- Technological advances, including the widespread use of anonymisation tools, and constantly improving criminal operating methods have made many corporate cyber security tools and basic procedures insufficient alone to protect corporate networks. Criminal adoption of encryption has also become a challenge for law enforcement when tackling specific threats.
- Finally, UK businesses, particularly in the financial sector, are also increasingly exploited and used as a vehicle to cash-out the proceeds of cyber crime committed in the UK and internationally.

Despite the growth in scale and complexity of cyber crime and intensifying attacks, visible damage and losses have not (yet) been large enough to impact long term on shareholder value. The UK has yet to experience a cyber attack on business as damaging and publically visible as the attack on the Target US retail chain.[4]

A RECENT CORPORATE CYBER ATTACK

A UK company website was subject to the criminal access of a customer records database, followed by a ransom demand asking for payment in exchange for the return of stolen data. Coordinated law enforcement action, working on information provided by the company, quickly identified a number of suspects who were then subsequently arrested.

The attack received widespread media attention. It is possible that stolen data from this breach have been used to aid unlawful access to other online accounts. Criminals continue to use breaches of this type to cross-market data and commit further criminality such as social engineering fraud.

This company's experience shows the importance of investment in a 'major incident response plan' that incorporates incident response,

Part of the cyber crime challenge is that, at present, aggregate corporate losses from cyber crime are not well understood. Amongst other

[4] In late 2013, Target was hit by one of the biggest data breaches in history. The impact of this was severe and included the resignation on the CEO, expensive remediation and updating of systems, and long term damage to share price and income.

problems, the tracking of fraud is inconsistent, with poor measurement of total losses from cyber-dependent or cyber-enabled fraud for financial institutions and their customers, and even weaker measurement and reporting of the costs of cyber-enabled theft of intellectual property and business interruption.

Despite significant customer education efforts by retail financial institutions, Policing and others, private individuals are typically even less aware than corporate victims of malware infections on their home computers and other devices. Private individuals who are infected can be a major source of infection and vulnerability for many businesses – for example, when their infected computers are used by cyber criminals as part of a botnet to deliver further malware to businesses and other individuals.

Although general cyber awareness is improving in the UK as a result of significant investment in education and training by government and efforts to educate customers by retail financial institutions; there remains a lack of understanding of cyber crime. Many businesses and most of the public are unsure about how best to protect against it and how to report it when it happens. In many instances, victims may not even be aware that it has taken place. This is a long-term education and training challenge that government and some businesses have recognised – and sustained efforts will be required to deliver required change.

Challenges for business in fighting cyber crime

Cyber crime is intrinsically challenging for business, as:

- Perfect security is almost impossible. Almost all organisations, no matter how much money and effort they put in, are vulnerable to determined attacks by high-end crime groups which have developed tools and techniques that can penetrate all but the very best defences.
- It is an international activity – paying no heed to borders. UK-focused efforts (by both business and law enforcement) can only be part of the solution.
- The technical challenges are evolving at a rapid rate. Solutions that may have worked last year may not necessarily work this year or next.

Nonetheless, substantial – and much greater – risk mitigation by business is possible. Cyber crime mitigation efforts within many businesses are hampered by a combination of limited board and top management engagement in addressing cyber security and cyber crime challenges, limited resourcing and cyber capabilities, and limited investigation and reporting of cyber crime.

THE OBSTACLES WITHIN BUSINESS TO IMPROVING RISK MITIGATION:
(As identified by the Strategic Cyber Industry Group)

- **Limited engagement by boards**
- **"Box-ticking" approach to cyber security**
- **Limited expertise**
- **Under-investigation**
- **Under-reporting**

Corporate cyber crime mitigation – as well as corporate cyber-risk management – is hampered by many businesses continuing to see the threat as a purely technical issue – rather than as a challenge for the board, the entire organisation and for business strategy.

A 'compliance approach' that aims to meet minimum standards does not adequately deal with intelligent and evolving adversaries, as threats are evolving faster than most defensive technologies and security practices. Additionally, there remains a skills gap across the cyber community for individuals who can help design, deliver and manage cyber security and cyber crime fighting programmes.

Law Enforcement and Government action

The UK Government made building cyber defences and funding the fight against cyber crime a Tier 1 priority in the 2015 Strategic Defence and Security Review. The Government will invest £1.9 billion over the next 5 years in the UK's cyber defences - almost double the investment over the previous 5 years - which includes funding for enhanced capability within law enforcement to respond to cyber crime. It also includes:

- a new National Cyber Security Centre to act as a single point of contact to simplify and strengthen government effort on cyber security and improve engagement with industry
- a programme of active defence, in partnership with some of the major companies who form the backbone of internet services in the UK to enable them to implement a series of measures to divert known malware and block malicious sites
- support for cyber businesses, including two new innovation centres, one in Cheltenham, to support talent and drive growth in the cyber sector
- developing and improving national offensive cyber capability.

To tackle cyber crime, UK law enforcement work in a partnership that includes the NCA's National Cyber Crime Unit (which leads the UK's response to cyber crime), the Metropolitan Police (through FALCON, its specialised Fraud And Linked Crime ONline unit), the City of London Police (who provide the Action Fraud reporting service), Regional Organised Crime Units and Police Forces across the country.

Law enforcement's strategy is to focus on responding to:

- **Cyber attacks targeted at UK victims**: increasing the reporting of cyber crime, supporting victims and increasing the take-up of protective security;
- **UK-based cyber criminals**: making the UK a high-risk country for criminals to host and perpetrate cyber crime;
- **International cyber criminals and groups**: identifying, prosecuting and disrupting the most significant cyber criminals worldwide; and
- **The enabling international cyber crime marketplace**: degrading the criminal marketplace, undermining the profitability of

the cyber criminal business model and raising the barrier to entry and operating for cyber criminals.

Amongst visible successes of these industry and international cooperation initiatives have been the multinational takedowns of the GameOver Zeus Dridex and RAMNIT criminal virus "botnets", exploited by major organised crime groups.

DRIDEX malware (October 2015)

DRIDEX malware was developed by technically skilled cyber criminals in Eastern Europe to harvest online banking details, which are subsequently used to steal money from individuals and businesses around the world. Global financial institutions and a variety of different payment systems have been targeted by criminal groups using DRIDEX, with reported UK losses of £20m.

Computers become infected with DRIDEX malware when users receive and open documents in seemingly legitimate emails and it is likely that there are many thousands of infected computers in the UK, the majority being Windows users.

The NCA and the FBI, with support from teams at Europol, the Metropolitan Police Service, GCHQ, German and Moldovan authorities; and private sector security partners developed and deployed techniques to safeguard victims and frustrate the technical networks used by the criminal groups behind DRIDEX. Importantly, law enforcement agencies were also able to make significant arrests and disrupt these criminal groups.

DRIDEX is also an important example of how criminal groups react with speed to action against them and to new business opportunities - DRIDEX has been further modified since law enforcement and industry action in late 2015, and the botnet operators who were spreading DRIDEX are now, reportedly, spreading the "Locky" ransomware alongside it.

RAMNIT botnet (February 2015)

The NCA took part in a major European operation against RAMNIT malware. RAMNIT infected over three million Windows operating system computers worldwide – with around 33,000 computers of these being in the UK. RAMNIT started life as parasitic “worm” but evolved into financial theft malware that allowed criminals to undertake covert and fraudulent transactions.

Europol had been alerted by Microsoft Corporation’s Digital Crimes Unit to the evolving RAMNIT malware threat after big data analysis found a sharp increase in infections and tactics aimed at financial theft. The NCA then worked alongside international law enforcement colleagues and private sector partners (Symantec and Microsoft) to shut down command and control servers used by RAMNIT.

This operation was a clear demonstration of the value of joint operational activity to disrupt criminal infrastructures, and ensure the UK is a safe place to interact and do business online.

UK law enforcement are active in helping to build the capability of overseas partners, developing strong operational relationships across national boundaries and increasing the ability of partner law enforcement agencies to contribute to tackling cyber crime.

The way forward for businesses, law enforcement and Government

> *Policing, especially in cyberspace, is no longer the exclusive preserve of law enforcement. The private sector, academia, and citizens themselves all need to be involved'*
>
> INTERPOL 22 January 2016

Major businesses need to see cyber crime and cyber security as an ever-present challenge, requiring continuous investment and monitoring at management and, crucially, board level.

In the context of increasing and more technically complex attacks, businesses firstly need to ensure that adequate cyber security is in place, but they also need to increase cyber resilience – in particular their ability to detect, contain and remediate breaches (whether accidental or deliberate) and other cyber incidents.

It is critical that businesses not only implement and maintain the latest good practices, but also actively test how well they are prepared for criminal attacks. This testing should encompass both their resistance to threats, and their ability to minimise and mitigate the damage caused by successful attacks.

Businesses also have an important role in educating and encouraging their customers and suppliers to improve their own cyber security, as vulnerabilities within supply chains can be exploited and targeted by criminals.

There are a number of resources that can help businesses looking to protect themselves in cyberspace, such as:

10 Steps to Cyber Security (https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary)

Cyber Essentials Scheme (https://www.gov.uk/government/publications/cyber-essentials-scheme-overview)
Cyber Security Skills, a guide for business (https://www.gov.uk/government/publications/cyber-security-skills-a-guide-for-business).
Get Safe Online (https://www.getsafeonline.org)

However, cyber crime is a threat of such magnitude, complexity and fluidity that neither businesses, nor law enforcement, will be able alone to meet the challenges now being presented. What is needed is a partnership approach to mitigating threats and identifying and disrupting criminals. Closer working between law enforcement and business to identify and arrest serious 'upstream' cyber criminals will protect businesses, stop future attacks and reduce the threat.

Cyber crime response should therefore be treated as a **strategic priority** and include a stronger public-private partnership to investigate, report and combat cyber crime.

Such a partnership would build on existing intelligence sharing initiatives, including sector based information sharing forums and the Government's Cyber-security Information Sharing Partnership (CiSP), but would go further in encouraging and enabling the reporting of cyber crime.

The **under-reporting** of cyber crime is a serious problem, hampering the disruption and prosecution of cyber crime. To illustrate this, the Information Commissioner's Office statistics reveal that fewer than 200 data breaches were reported in 2015.

Discussions with industry representatives suggest that major factors in corporate under-reporting may include:

Many businesses are unaware of breaches and other intrusions

Senior management and boards may believe that it is better just to settle customer losses and fix problems quietly.

Some IT management teams may be reluctant to inform senior management for fear of criticism

Some lawyers may advise their clients that it is not in their best legal interest to report

Under-reporting may also be accompanied by the under-investigation of cyber crime by corporate victims. This is a substantial problem that not only hampers crime fighting, but also hinders corporate risk management. It directly harms and undermines efforts to improve cyber resilience, which are needed to address the almost inevitable risk of corporate network and system penetration, by identifying, containing and remediating breaches as quickly as possible.

The improved reporting of cyber crime would directly enable better investigation of major events and would contribute to the ability of law enforcement to disrupt the activities of the serious organised crime gangs responsible, directly or indirectly, for the bulk of cyber crime.

Information sharing

Law enforcement recognise many of the practical challenges for business and, in particular, understand the confidentiality and other concerns of businesses and their legal advisers in relation to reporting.

That said, reporting of cyber crime brings clear benefits to the business community. Amongst others, reporting helps law enforcement and other agencies to disrupt criminal operations. Reporting can also bring direct benefits to the reporting business. Reporting often facilitates investigation and then improves remediation and subsequent risk management.

Cyber crime should always be reported to Action Fraud, but 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. If businesses require any further information about "intelligence basis" information sharing with the NCA, please contact NCCUIndustry@nca.x.gsi.gov.uk.

What can business do?

Board and top-level management engagement in cyber security and cyber resilience is critical to reducing cyber crime. However, even with such engagement there are no easy answers to the challenges facing UK businesses. Encouraging a robust and continuing debate in boardrooms will be critical. In this context, we set out below some of the questions we believe that boards should debate and try to find answers for.

1. Do you think you have been the victim of a material cyber-attack? Have you treated it as a crime and reported it? How have you investigated it? Have you received a detailed, yet understandable, report on the investigation?
2. How do you measure attacks on your business? Do you record penetrations and data breaches you've suffered? Do you take into account direct losses and indirect costs, including damage to customer confidence?
3. Have you asked independent testers to determinedly attempt a break-in, using realistic criminal techniques on live systems? If you have, what have they been able to extract?
4. What are you doing to reduce the risks your customers face? How do you measure how successful you have been?
5. Do you share information with competitors and law enforcement about the attacks you suffer? How do you make sure that your understanding of the threats you face is comprehensive, up to date – and meaningful to the board and top management?
6. Have you engaged the entire board in planning – and practicing – to deal with a major cyber crime attack?
7. Have your major suppliers and service providers been attacked? What damage was done and have you become a victim of crime as a result? How well are you doing in comparison with your competitors? How confident are you about your business' cyber security and cyber resilience? How does the board test its confidence?

Top-level public guidance resources for boards and top management

- 10 steps to cybersecurity (https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary)
- Cyber Essentials guidance (https://www.gov.uk/government/publications/cyber-essentials-scheme-overview)
- For major critical infrastructure businesses, the CPNI and CESG websites.