Recent high-profile cases of financial institutions being targeted by cyber criminals, such as the attack on the Bangladesh Central Bank in February 2016 that resulted in a loss of $81 million, illustrate the dangers posed by cybercrime to the international financial system.

In early 2015, the US Director of National Intelligence, James R Clapper, ranked cybercrime above terrorism and espionage as the greatest threat to national security. GCHQ has also categorised the issue as a Tier 1 threat, indicating that cybercrime is now a high priority on the agenda of governments worldwide.

Governmental and international statistics indicate that the use of information and communication technologies (ICT) to facilitate criminal activity is increasing. In the UK, both Action Fraud and the National Crime Agency (NCA) have recorded an increase in cybercrime. Both large-scale organised crime groups and low-level, non-organised criminals have moved their operations online, creating new avenues for profit and diversifying their activities. In the UK, while there has been an increase in the use of cybercrime by ‘traditional’ organised crime networks, a law enforcement official interviewed for this article said that there has also been an increase in the cyber ‘marketplace’ type of crime, where anyone may purchase tools to carry out fraudulent operations, data theft, ransom and blackmail.

The great advantage of ICT for criminals has been the democratisation of access to tools and thus the ability to carry out relatively small-effort crimes for large profits. Perpetrators range from state-sponsored to members of organised criminal groups, internet hackers, terrorists and small-time offenders. In the UK, law enforcement has identified marketplace criminals as the most prevalent actors in cybercrime, for whom – in contrast to the larger-scale organised crime groups – political and ideological reasons, rather than economic gain, are the motivating factors.

Cybercrime is now the most-reported type of crime by financial institutions

Undoubtedly, the banking sector’s embrace of the digital world has left it more vulnerable to cybercrime. Financial institutions, particularly those operating across different jurisdictions, are particularly at risk as online banking, frequent international transactions, new payment systems (such as PayPal and Apple Wallet, among others) and the significant databases held by banks provide easy targets and high profits. Financier Worldwide magazine suggests that more than half of the world’s top 50 banking websites have been accessed illegally in the last decade, leading to a loss of more than $1 billion. According to Kaspersky Lab, financial institutions must address a variety of different cyber threats, including malware (harmful software), phishing (the use of electronic communication to lure individuals to divulge sensitive information) and denial of service (DoS) attacks (where a machine or network resource is made unavailable to its intended users).

Threats to financial institutions include two types of cybercrime. ‘Cyber-dependent’ crimes, such as hacking and DoS attacks, are not possible without the use of the internet. Cyber-enabled (or ‘cyber-assisted’) crimes, by contrast, are ‘traditional’ crimes – such as fraud, robbery and extortion – which are facilitated and made easier by technology, but would still take place if the technology were not available. Financial institutions need to have strategies in place that allow them to respond to and understand both types of threat.

While economic cybercrime is not exclusively directed at financial institutions, recent reports suggest the threat towards them is increasing. For example, the ThreatMetrix Cybercrime Report for Q4 2015 noted that there had been a 40% increase in cybercriminal activity against banks over the preceding 12 months, including more than 100 million attempts at fraud.

Cybercrime is now the most-reported type of crime by financial institutions, and as providers of national infrastructure through their financial services, the ways in which these businesses respond to and understand threats is of particular importance to a nation’s security and resilience.
A study by the Ponemon Institute, a US-based research centre specialising in data protection and security policy, suggests that it can take over eight months (on average 256 days) before a financial institution detects a malicious attack. By that time it is likely that high volumes of sensitive corporate information will already have been siphoned off to outside criminal masters. Typically malware spends some time surveying a network, looking for weaknesses and compromising user accounts with high access privileges. This ‘attack timeline’ constitutes a double-edged sword for organisations. On the upside, the delay provides an opportunity for technologies such as data analytics to identify the breach before significant data loss has taken place. On the downside, the fact that such breaches have often lain undiscovered for months illustrates the vulnerabilities of organisations that are unprepared for this type of threat.

There are a number of steps that financial institutions can take to improve the robustness of their defences to cybercrime: better understanding of the problem through partnerships; investing in technology such as analytics platforms; and sharing information that may be relevant to others.

First, there is growing agreement among financial institutions that co-operation should be encouraged between the public and private sectors, and many such initiatives have already been put in place in the UK and abroad. The establishment of initiatives, such as the UK National Computer Emergency Response Team (CERT UK) and the Cyber-security Information Sharing Partnership (CiSP), as well as the UK’s Cyber Defence Alliance (run in co-operation with the NCA), demonstrates an increased realisation that cyber-security threats cannot be addressed in isolation and that co-operation between stakeholders is key. CiSP, for example, seeks to address the issues leading to under-reporting of cybercrime, although little data are available to demonstrate whether this initiative has been successful. The World Economic Forum has similarly highlighted the importance of co-operation through its ‘Recommendations for Public-Private Partnership against Cybercrime’ and emphasis on information-sharing.

The recent UK Talk Talk breach, where the perpetrator was a teenager with no criminal affiliation, and the HSBC DoS attack, where no culprit or motive has been identified thus far, demonstrate how co-operation with law enforcement before and after attacks is crucial to the management of the problem as well as for future learning and behaviour modification. While acknowledging that economic cybercrime will never be fully controlled, these instances of co-operation strongly indicate that stakeholders are moving towards a more effective and up-to-date strategy to tackle the risk.

Second, supporting investment in technological advances is also crucial for improving the robustness of defences to cybercrime. In an article in the International Business Times published in February 2015, ‘The Billion Dollar Bank Job: How Hackers Stole $1bn from 100 Banks in 30 Countries’, David Gilbert writes that, in 2013, a series of co-ordinated attacks saw criminals steal approximately $1 billion from more than 100 banks through spear-phishing emails sent to the banks’ employees. Although appearing legitimate, the emails contained malware that opened remote access to bank computers and allowed criminals to infiltrate the system. In response to these kinds of risks financial institutions are beginning to recruit staff with strong security backgrounds to improve employees’ awareness of threats and reduce reliance on technology to stop breaches.

It can take over eight months before a financial institution detects a malicious attack

In recent years the UK financial sector has made significant investment in the fight against cybercrime, with numbers reaching an annual peak of £700 million, according to a 2013 report by the Department for Business, Innovation and Skills. The majority of efforts are being channelled into updating ICT security with innovative software and analytics as well as
forensic skills and the means to trace potential attackers. However, a number of experts from the sector recently emphasised that this investment must be better guided and informed by people who understand the specific needs of each business and can therefore identify which technology is most appropriate for it. The type of technology adopted should, in addition, be capable of processing and identifying human factors and their impact on the wider system.

**If financial institutions are perceived to be vulnerable to cybercrime they risk grave reputational damage**

While basic firewall systems are essential for the provision of some level of protection against known security attacks, hackers continue to slip unnoticed into corporate networks and spend days, weeks or months exploring the resources available online. Malware may quietly collect sensitive information as it traverses the network, harvest users’ internet sessions looking for passwords, send corporate documents or databases to cyber criminals outside the target, or simply sit waiting for an external trigger to take particular actions, such as deleting critical business information.

Advanced analytics technology provides some defence against this kind of infiltration. As Mike Burgess, the chief information security officer at Telstra, explains:

*Analytics gives you the opportunity to strike back in the early days, with greater understanding of what’s happening within your organisation. It lets you understand what never before seen threats are happening on the network, why this behaviour is taking place, and what it is doing.*

In these situations, analytics technology appears to offer the best hope for organisations needing to identify threats and to manage them at different levels.

However, many institutions are not up to date with the latest tools and crucially lack the ability to: implement strong cyber-security systems without expert, technological support; profile and investigate attacks so as to develop best practices; and fully co-operate with other financial institutions in order to improve knowledge. As a result, a high proportion of large organisations continue to suffer some form of breach.

If financial institutions are perceived to be vulnerable to cybercrime they risk grave reputational damage, as well as the impact on share prices and the stability of the wider financial market. According to a report published by the British Bankers Association and PwC, this is of considerable concern to most banks and has led to under-reporting of attacks or threats. So, as the NCA has stressed, a key factor in the failure to control some of these breaches appears to be the institutions themselves and their reluctance to communicate.

**Financial institutions need to do more to communicate, or share information, with both law enforcement and cyber-security experts**

This culture needs to change. Indeed, the third step that financial institutions need to take if they are to improve the robustness of their defences to cybercrime is to do more to communicate, or share information, with both law enforcement and cyber-security experts. This would improve their response capability and allow them to better understand criminal trends and emerging threats. As economic cybercrime has an ever-evolving nature, there is a corresponding need for ongoing co-operation to identify and share risks and new ways to reduce them.

At the EU level there are plans to expand legislation on cyber-security that will require operators of essential services in the energy, transport, banking and healthcare sectors, and providers of key digital services such as search engines and cloud computing, to take appropriate security measures and report incidents to the national authorities. The hope is that this will in turn lead to the creation of platforms for co-operation not only at a forensic but also at a preventative level. As the problem of cybercrime expands and is increasingly being discussed in open forums, financial institutions and other businesses should work towards putting in place robust strategies that address technological difficulties whilst simultaneously understanding the human factors behind the risks and the need to constantly share (quality) information with others, and particularly with law enforcement.

Dr Inês Sofia de Oliveira  
Research Fellow, Centre for Financial Crime and Security Studies, RUSI.

Alexandra Stickings  
Research Support Officer, National Security and Resilience Studies, and Centre for Financial Crime and Security Studies, RUSI.

This article and the research that informs it was kindly supported by the Wynyard Group.