BANK OF ENGLAND

Quarterly Bulletin

2018 Q4

Topical article

Could a cyber attack cause a systemic impact in the financial sector?

ISSN 2399-4568

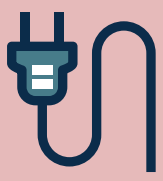
Could a cyber attack cause a systemic impact in the financial sector?

By Phil Warren (Bank of England), Kim Kaivanto (Lancaster University) and Dan Prince (Lancaster University).[1]

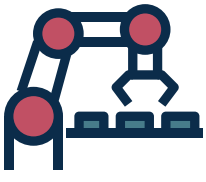
- There is not a uniform view of the link between cyber risk and systemic risk: some assume a direct link whereas others query the connection.
- Beyond nation states, the vast majority of independent cyber attackers are currently unlikely to have the capability to systemically impact the financial sector.
- The financial sector has a large number of environmental features which are conducive to a systemic cyber compromise.
- There are no current examples of systemic cyber risk crystallising and impacting the real economy but this does not prove an absence of risk.
- We conclude there is a credible case to link cyber risk to systemic risk in the financial sector.
- Recommendations for future consideration include:
  - Further development of the intelligence-led approach to cyber security.
  - Policy responses that seek to cut through sectoral, geographical and public/private boundaries.
  - Organisations should accept that compromises are likely to happen and therefore prioritise response and recovery activities.
  - Undertake further studies to better understand the relationship between data integrity and authenticity, trust in financial services and the potential for real-economy impact via a cyber attack.
  - A specific focus on risks associated with third-party dependencies.

Summary figure The context of cyber risk: securing information into the digital age

First Industrial Revolution
WATER AND STEAM
Mechanical production replaces human and animal power.



Second Industrial Revolution
ELECTRICITY
Mass production and assembly line.



Third Industrial Revolution
AUTOMATION
IT and networked production.

Fourth Industrial Revolution
CYBER PHYSICAL SYSTEMS
Intelligent, flexible and distributed production. Driverless cars, smart robotics, artificial intelligence and 3D printing.

(1) The authors would like to thank: the *Quarterly Bulletin* editors, Andrew Huddart, Dave Porter, Anne Wetherilt and Paul Williams for useful comments.

Introduction

Over four billion people are now internet users.(2) This number has nearly doubled since 2012.(3) During the same period the number of people using social media has more than doubled.(4) The fourth industrial age is being characterised by the convergence of physical, digital and biological domains. This has included radical developments in technical innovation such as the commodification of artificial intelligence (AI), mobile internet, cloud technology, nanotechnology and machine learning.

Financial services have been central to the digital revolution: demonstrated through the advent of fintech, mobile banking, digital start-ups and cryptocurrency. As well as the benefit it brings, the digital revolution has unleashed changes in the operational risk landscape.

Cyber risk is frequently cited as a top priority not just for individual institutions but for the financial system as a whole. The Bank of England's 2018 H2 *Systemic Risk Survey*(5) referenced cyber attack as the second most cited source of risk to the UK financial system.(6)

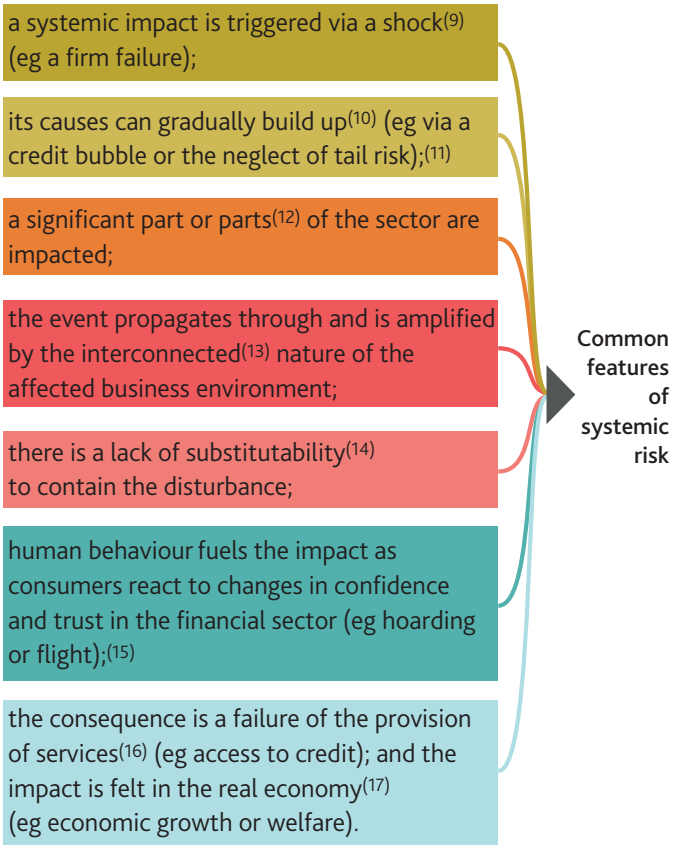
Nevertheless, a detailed understanding of systemic cyber risk within the financial sector remains embryonic. Commentaries are divided. On one side, there is a popular and alarmist discourse which assumes a direct link between cyber risk and systemic risk. Proponents cite a diverse medley of attackers and assume a successful attack would have a catastrophic impact: 'a loss ranking somewhere between those of Hurricanes Sandy and Katrina'.(7) Conversely, others claim 'there is no direct connection between the failure of computer systems, no matter how severe, and the behaviour of those economic agents which ultimately culminates in a systemic crisis'.(8)

Given the diversity of views, this paper will critically evaluate the link between cyber risk and systemic risk within the financial sector. Our approach will analyse common features of existing definitions for systemic risk and test their applicability to cyber risk.

This is the first *Quarterly Bulletin* article about cyber risk and reflects its emergence as a priority subject linked to the Bank's mission for maintaining financial stability. As cyber risk is a global, cross-cutting and topical subject, this paper will include reference to attacks which may have taken place outside of financial services but where learning points can still be surmised. Cyber attacks are frequently agnostic of sectoral boundaries; our analysis will be too.

What is systemic cyber risk?

There are a number of common features present in existing literature which help to define systemic risk. Most of these originate from analysis of financial risk which proliferated following the 2008 crisis:



(2) See 'We are Social' and 'Hootsuite' (2018).
(3) See Statista (2018).
(4) See 'We are Social' and 'Hootsuite' (2018) and Statista (2018).
(5) The *Systemic Risk Survey* is conducted on a biannual basis, to quantify and track market participants' views of risks to, and their confidence in, the stability of the UK financial system.
(6) See Bank of England (2018a).
(7) See Mee and Schuermann (2018).
(8) See Danielsson, Fouché and Macrae (2016).
(9) See Smaga (2014), Kaufman and Scott (2003).
(10) See Bloomfield and Wetherilt (2012).
(11) See Gennaioli, Shleifer and Vishny (2012), (2013).
(12) See FSB (2009), Eijffinger (2010), ECB (2009) and Kaufman and Scott (2003).
(13) See FSB (2009) and Smaga (2014).
(14) See FSB (2009).
(15) Kaufman and Scott (2003).
(16) See FSB (2009) and WEF (2016).
(17) See Eijffinger (2009), FSB (2009), Smaga (2014) and Bloomfield and Wetherilt (2012).

In other words, systemic risk is 'a risk of disruption to financial services that is (i) caused by an impairment of all or parts of the financial system and (ii) has the potential to have serious negative consequences for the real economy. Fundamental to the definition is the notion of negative externalities from a disruption or failure in a financial institution, market or instrument'.(18)

How do definitions for systemic cyber risk relate to the features of systemic financial risk? First, it is important to reflect on the boundaries of the term 'cyber' that has 'become a noun and a prefix meaning anything including or relating to computers'.(19) Of course the term cyber is not simply a reference to a desktop device but rather to the ubiquitous and connected nature of technology within the digital age: '[it] is increasingly the means by which we communicate in every sphere of our lives, locally and globally'.(20) Rather than simply focusing on the stand-alone technology, cyber risk should be analysed within this broader setting.

Related to this context, we must also consider the complex and opaque nature of data. Consequently, the forensic analysis of a cyber attack can rarely attain definitive conclusions or attribution, as it typically relies on incomplete information.

Systems are also automated and dependent on hyper-connected data sources and feeds. Hence attacks can propagate without human awareness or intervention.

In addition, compared to financial risk, there is not a well-developed historical record and accompanying empirical evidence base to support standard statistical quantification and inference.

Finally, in contrast to financial risk, cyber risk involves the presence of a malicious entity: somebody seeking to corrupt or upset normal operating equilibria. Importantly, this means that an attacker may be able to choreograph the attack so as to maximise systemic impact. For example, by timing an attack on a key institution to coincide with a period of heightened uncertainty.

For reference, we will make use of the following cyber-specific terminology:

- A 'threat agent' is a malicious actor whose intentions are to attack a socio-technical asset (eg system, network, person).
- A 'vulnerability' is a flaw in a socio-technical information asset that may be exploited (either via a person, a process or technology).
- A 'cyber attack' is the act of a malicious agent exploiting a vulnerability to compromise the socio-technical information asset.
- A 'control' is a countermeasure to identify, protect, detect, respond and recover from a cyber attack.
- An 'impact' is a result of the attack. This is typically seen as a breach of confidentiality, integrity, availability, utility, possession or authenticity of the information asset.

External shock…'know the enemy'

A common feature of systemic risk is the presence of external 'shocks' that may become a systemic event(21) such as the bank failures (eg Bear Sterns, Lehman Brothers and Northern Rock) in 2007–8. Could a cyber attack shock the financial sector in a comparable manner?

Commentaries of cyber risk frequently cite the offensive activities of cyber criminals, hacktivists, malicious insiders and hostile states to evidence the transmission channels of shock. Conversely, Danielsson, Fouché and Macrae (2016) contend that 'the only actors with sufficient resources to cause a systemic crisis are the largest sovereign states' and that they must 'be very lucky'. They suggest it 'might be just as easy to…[make] credible threats to world trade'.(22)

We agree that beyond nation states, the vast majority of independent cyber attackers are currently unlikely to have the capability to cause a shock with the magnitude to systemically impact the financial sector.

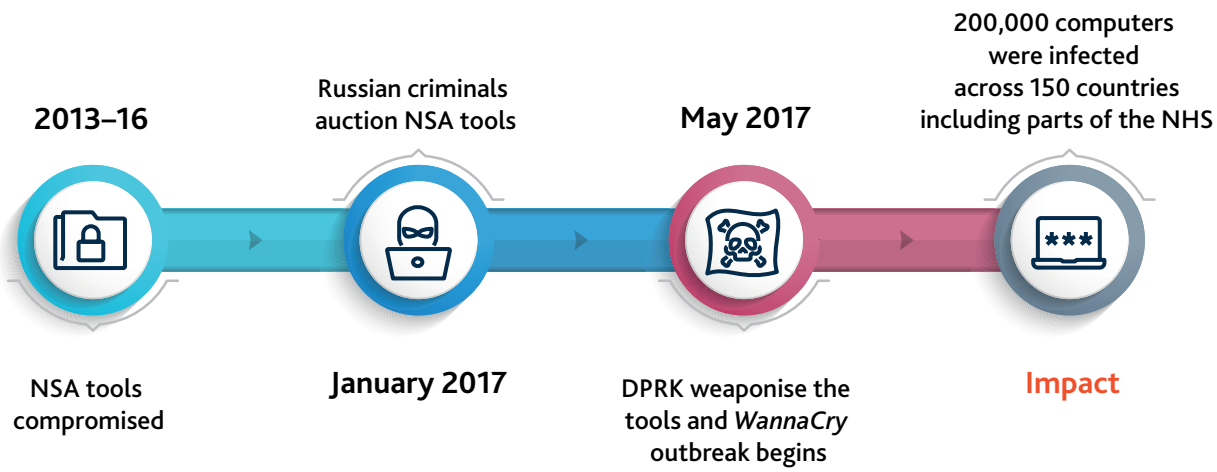
Yet we need to be careful not to pigeon-hole our analysis. A cyber attack frequently combines different groups of attackers; their activities stimulated by a black-market economy where the exchange of tools and knowledge cuts through traditionally defined boundaries. As an example, the *WannaCry* global ransomware attack which impacted legacy technology within the NHS was reportedly rooted in a compromise of US government intelligence tools, was monetised by Russian-linked criminals and weaponised by the North Korean state (DPRK) (see **Figure 1**).(23)

Our analysis must also consider that state-sponsored cyber capabilities are shrouded in secrecy and cases brought into the public view often provide only glimpses of the facts. We must assume that more offensive capability exists beyond our reach.

There are, however, some indicators of nation-state cyber capability. For example, US intelligence officials testified in January 2017 that as of late 2016, more than 30 governments were actively developing offensive cyber attack capabilities.(24)

(18) See FSB (2009).
(19) See Wright (2018).
(20) See Wright (2018).
(21) See IMF, BIS and OECD (2001).
(22) See Danielsson, Fouché and Macrae (2016).
(23) See UK Foreign Office (2017) and *The Telegraph* (2017).
(24) See Clapper (2017).

Figure 1 The anatomy of the *WannaCry* attack: spooks, criminals and the NHS



There is also evidence of their use. The Russian war in Ukraine (2014–present) has seen the deployment of traditional kinetic weapons but has also reportedly included the destructive *Sandworm*(25) cyber attacks against Ukrainian power networks. Therefore, some nation states have the offensive capability to supplant the need to rely on luck for achieving a systemic impact. Comparable outcomes could be achieved via conventional means such as trade sanctions. Yet with their relative low cost and ease of deniability compared to trade or military force, it seems logical that cyber capability is an increasingly viable choice for nation-state attackers.

How does this threat relate to financial services? Even when the capability may be present, there also needs to be an intention by attackers to use it. While nation states probably recognise the attacking opportunities, evidence suggests current offensive cyber resources are heavily deployed against traditional government targets, such as military and political establishments, rather than the financial sector.(26) State-sponsored attackers also probably understand an attack which has a systemic impact would break international law.(27) Offensive cyber capabilities, therefore, may currently be held in a state of readiness as deterrence, given their known capabilities in the event of escalation. However, we must not confuse readiness-for-deterrence with an absence of risk to financial services.

Gradual build-up…'death by a thousand cuts'

Beyond shock, causes of systemic risk can gradually build up 'such as credit and asset market bubbles that…may unravel suddenly'.(28) Discussions of cyber risk have, to date, primarily focused on the triggers of destructive or disruptive attacks, rather than focusing on their causes. Our analysis should reference these contributory factors. For example, many parts of the financial sector continue to depend on legacy technology. This is steadily increasing the likelihood of a subsequent cyber compromise as services become technically obsolete and therefore more vulnerable to an attack. Similarly, there is an emerging skills gap in the cyber security sector;(29) gradually reducing the capability among defenders and therefore increasing the chances of success for would-be attackers.

Data loss is another example of cyber risk which is building up in financial services. These cases have the potential to gradually undermine the confidence and trust in identities used to access financial services, such as credit provision. The breach of Equifax of May 2017, compromised 15.2 million personal records and according to the National Cyber Security Centre (NCSC), 'the majority of these … [contained]…the name and date of birth of certain UK consumers'.(30)

In isolation, examples like data loss are not currently systemic risks but these instances may aggregate to contribute to systemic events in the future. For example, if an attack were able to use these credentials as part of a concurrent widespread compromise of retail banks, this could compromise consumer confidence and lead to a run on services.

Financial services…'a complex system'

The Financial Stability Board (FSB) outlines three criteria to determine the susceptibility of a business environment to a systemic impact: size, substitutability and interconnectedness.(31)

How does this relate to cyber risk in the financial sector? Size reflects '*the volume of financial services provided by the*

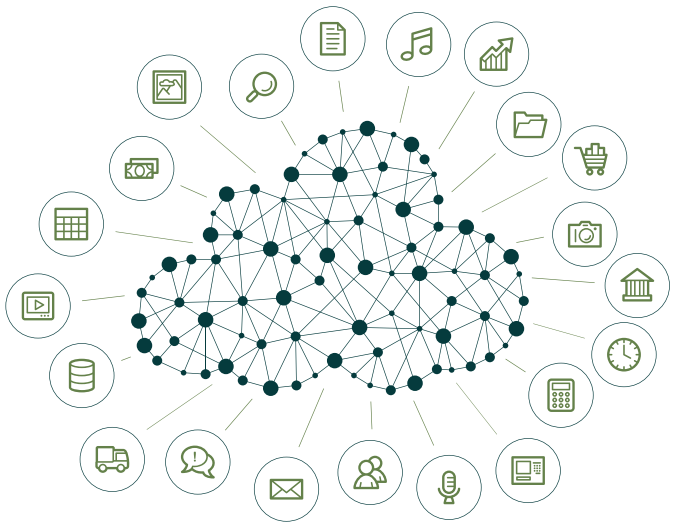
(25) The Sandworm cyber attack took place on 23 December 2015 and is considered to be the first known successful cyber attack on a power grid. For more information see Wired (2017).
(26) See NCSC (2018a).
(27) See Wright (2018).
(28) See Schwaab, Koopman and Lucas (2011).
(29) See Joint Committee on the National Security Strategy (2018).
(30) See NCSC (2017).
(31) See FSB (2009).

individual component of the financial system'.[32] In short, a single hammer blow to a key institution could resonate throughout the sector. A cyber attack could theoretically crystallise in this way, although to bypass all the controls, it would probably have to be extremely sophisticated.

A similar outcome could be achieved with greater ease via a more rudimentary attack on multiple institutions. Common sector-wide technology components have made this easier. An NCSC advisory of April 2018 detailed Russian state-sponsored cyber actors targeting network infrastructure devices. In the report, NCSC stated 'The current state of US and UK network devices — coupled with a Russian government campaign to exploit these devices — threatens the safety, security, and economic well-being of the United States and the United Kingdom'.[33] And although financial services were largely immune from the *WannaCry* attack which targeted Microsoft operating systems, it demonstrated how the exploitation of a common vulnerability can have a severe, widespread and rapid impact across multiple organisations.

Substitutability relates to the 'extent to which other components of the system can provide the same services in the event of a failure'.[34] Analysts of financial risk cite examples of key assets that cannot be replaced if lost or interrupted such as payment systems, messaging systems and clearing and settlement systems. In theory, a successful cyber attack against these types of critical assets has the potential to cause a systemic impact. However, our analysis should not be limited to these classic examples. Representing the changing shape of the sector (see **Figure 2**), we should also focus on common dependencies such as those third-party providers offering cloud computing and other utility services. A 2018 Lloyd's of London report forecasts 'a cyber incident that takes a top three cloud provider offline in the US for 3–6 days would result in ground-up loss central estimates between US$6.9 billion and US$14.7 billion'.[35] Yet the potential for concentration risk of cloud services needs to be balanced against the likely security benefits they bring 'because the scale and expertise of cloud service providers allowed them to build resilience in a way that exceeded the capability of individual firms.'[36]

Figure 2 Cloud computing — transforming the model of IT service



The importance of interconnectedness ('*linkages with other components of the system*'[37]) is well understood and well studied in financial risk literature: '*systemic risk involves spillovers of risk from one institution to many others*'.[38] Beyond the financial view, interconnectedness also needs to be viewed from a data-centric perspective. As the sector has used technology to broaden access to its services, it has introduced an incalculable number of new connections. Banks cannot just centralise their security around their cash vaults, their digital assets are now spread globally. From a cyber-risk standpoint, this has hugely increased the number of attack vectors, as each new node is a potential source of infection. And while financial services may wish to prioritise security, their services are necessarily situated within a broader technology environment where manufacturers are challenged to balance the competing priorities of convenience and connectivity with security.

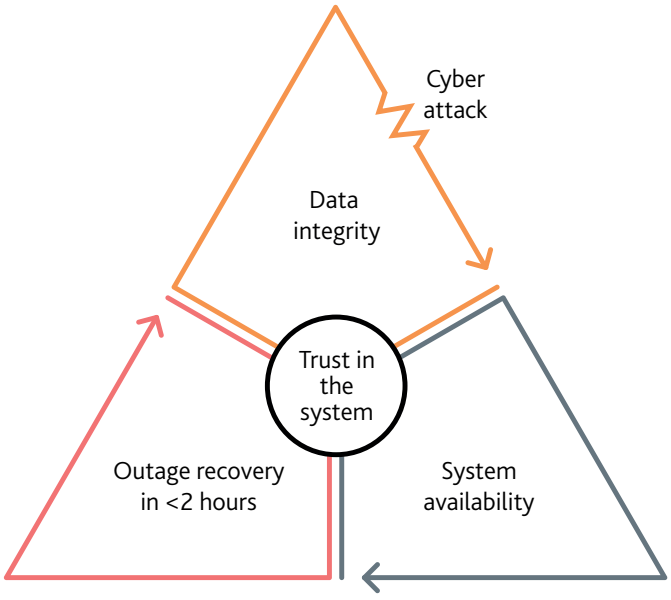
As well as the FSB's three characteristics which inform vulnerability to a systemic impact, we should also reference the related issue of technology dependency. Exposure of a business environment to cyber risks is directly correlated to a business' reliance on technology. Conversely, an environment without such technology dependency has a reduced cyber risk exposure: you cannot hack a typewriter. Nobody would challenge the assertion that financial services have become dependent on technology to fulfil their business functions. Nonetheless, the ubiquity of technology within financial services needs to be understood from the perspective of cyber risk. Cyber risk cannot be simply hived off to the IT department to fix; it is a core component of every business function. While not the victims of a cyber attack, the TSB IT failure of April 2018 demonstrates the overall point: a failure of technology can also lead to a failure of a business service.[39]

As outlined, certain data characteristics (complexity, opacity, hyper-connectivity and automation) can impact the management of cyber risk. These characteristics become force-magnifiers for attacks on data integrity. Such an attack 'can cause special problems for recovery, in particular when it

(32) See FSB (2009).
(33) See NCSC (2018b).
(34) See FSB (2009).
(35) See Lloyd's of London (2018).
(36) See Bank of England (2018b).
(37) See FSB (2009).
(38) See ECB (2009).
(39) See BBC (2018).

is not known whether and when the integrity of data has been compromised'.(40) These compromises can automatically spread corruption into the broader system. And a thorough forensic investigation of a data integrity compromise can frequently take days or weeks to fully investigate. Added to this is the CPMI-IOSCO guidance for services providing financial market infrastructure (FMI). 'An FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption…' This leaves system operators with a difficult decision: resume services which are potentially corrupted, or keep the service down and miss the target (see **Figure 3**). CPMI-IOSCO recognise this unique challenge and encourage operators to 'exercise judgement in effecting resumption so that risks to itself or its ecosystem do not thereby escalate, whilst taking into account that completion of settlement by the end of day is crucial'.(41) There have been some examples demonstrating the potency of a data integrity attack. In 2015, BNY Mellon had a technical glitch that mispriced some securities. The system failure caused panic among BNY Mellon's US fund management clients over concerns that hundreds of funds may have been traded at inaccurate prices. As it was a data integrity issue, the back-up facility corrupted preventing an automatic failover.(42)

Figure 3 The triangle of trust: integrity, availability and recoverability



Human factors…'fear, uncertainty and doubt'

The financial system relies on trust to support its function. When that trust is shattered, confidence in the financial system can falter leading to falls in market or funding liquidity. Fear that an institution may be or has become insolvent leads to capital flight and ultimately leads to the negative spillovers we associate with systemic events. The Northern Rock run of 2007 provides a stark example.

How does this relate to cyber risk? Importantly, cyber risk needs to be viewed from a social as well as a technical perspective. There is a direct link between trust in the authenticity of data and how people behave. This means that a knowledgeable attacker who understands the fragility of the socio-technical relationship is well placed to undermine the system. As an example, on 27 June 2014, Bulgaria's largest domestic bank FIB experienced a depositor run, amid heightened uncertainty due to the resolution of another bank. This followed spurious emails and social media coverage implying that FIB was experiencing a liquidity shortage. Deposit outflows on that day amounted to 10% of the bank's total deposits and the bank resorted to use a liquidity assistance scheme provided by the authorities.(43)

Consumer trust in financial services has always been linked to media coverage. However, the rapid developments of technology have broadened the trigger points for influence of consumer behaviour. This includes the compromise of media outlets by attackers. In 2013, a hacker took over the Twitter account of the Associated Press and tweeted 'Breaking: Two Explosions in the White House and Barack Obama is injured'. The Dow Jones stock market instantly fell 140 points.(44) No longer can financial institutions simply rely on defending their immediate perimeter to mitigate systemic risk; technology advances have transformed the scale, span and diversity of potential attack vectors.

Real-economy impact…'wages, welfare and wallets'

At the heart of the concept of systemic risk is real economic impact: a failure of the provision of services which can effect economic growth or welfare. Those challenging the link between cyber risk and systemic risk argue that, to date, there is little evidence to demonstrate such impacts occurring.

Nevertheless, there are clear, direct and recent instances of cyber attacks causing systemic impact outside of the financial sector. A prime example is the *Stuxnet*(45) attack which reportedly damaged one fifth of Iran's nuclear centrifuges. The absence of such examples in the financial sector may simply be because there has not yet been the correct synchronisation of attacks at the right time and place to create such an impact. Instead, proponents of systemic cyber risk analysis suggest

(40) See Kashyap and Wetherilt (2018).
(41) See BIS (2016).
(42) See Finextra (2018).
(43) See Bouveret (2018).
(44) See CNBC (2013).
(45) Stuxnet is a malicious computer worm, first uncovered in 2010. For more information, see Wired (2014).

using theoretical scenarios. For example, co-ordinated attacks across multiple or core systems, or even spoofing the Global Navigation Satellite System timing, which underpins the timing integrity of all trades and ATM transactions.(46)

We should also reference cyber crime. In aggregate form, it is an example of an issue affecting economic activity and welfare. In April 2018, a UK Finance and KPMG report claimed that cyber crime had a 'global impact exceeding $450 billion a year as crime, extortion, blackmail and fraud move online'.(47) Yet, at present, cyber crime has not currently led to an obvious failure in the provision of service. Therefore, while it is a vitally important system-wide issue, at present it is not a systemic one.

Finally, our analysis of real-economy impact should differentiate between events which may happen from those that have happened. Just because there has not been a clear example of a systemic impact in the sector yet, it does not mean it cannot or will not happen in the future.

Systemic uncertainty…'the unknown unknowns'

Beyond the outlined characteristics of cyber risk through the lens of financial systemic risk, cyber risk also has some unique characteristics which may contribute to a systemic impact in its own right.

For example, both in the financial sector and beyond, there is the growing gulf between the complexity of the technology environment we are operating and our ability to understand it. This makes the mitigation of cyber attacks increasingly challenging. Legacy infrastructure, complex technology environments and an increasingly mobile workforce are preventing defenders from effectively understanding or managing the associated risks. Traditional risk assessment requires a known outcome; characterised around structured taxonomies, risk registers, defined appetites and assessed impacts. However, the technology environment is a highly complex and opaque system. The result is that we cannot expect to discern cause and effect; cyber risk outcomes are emergent rather than resultant.

Although not fundamentally impacting the financial sector, the destructive *NotPetya* attack is illustrative. This attack was reportedly carried out by the Russian state against government targets in Ukraine. Yet as well as the intended targets, there was considerable collateral damage: 'the worm raced beyond Ukraine and out to countless machines around the world…it crippled multinational companies including Maersk, pharmaceutical giant Merck, [and] TNT Express…it even spread back to Russia, striking the state oil company Rosneft'.(48)

What was the common factor? Reportedly, the attack was delivered via an update to an accountancy programme. Victims were simply chosen because of their choice of software.

Conclusion

Necessarily, this paper has examined each of the characteristics of systemic risk in isolation. Of course, capable attackers could synchronise these elements in order to maximise their impact. Therefore, we should avoid trying to seek a binary answer for each characteristic; instead we should seek an overall assessment.

In our view, there is a credible case to link cyber risk to systemic risk in the financial sector. The connection, however, is not self-evident. This conclusion is based on context and signal rather than a glut of clear evidential examples. It is also based on an increasing risk trajectory. Many of the examples cited in this paper have taken place over very recent years. As technology dependency keeps increasing, we expect the number of cyber attacks to increase commensurately.

Nor does this mean that we have concluded that there is a cataclysmic level of risk within the sector; the current reality is more nuanced. For example, nation states are probably the only threat actors with the current capability to cause a systemic shock within the sector. However, we expect the threat to increase as capability is fuelled by the development of the black market for attack tools. As a case in point, the *Stuxnet* worm which was launched as a weapons-grade capability was freely available to download just months later. With increased access, sophisticated capabilities will reach a broader set of attackers, including groups such as terrorists who may have a stronger intent to disrupt the financial sector.

Like financial risk, cyber risk also has features which in the right circumstances could contribute to systemic outcomes. As just one example, the results of mass data loss are being used by attackers to compromise the authenticity of financial transactions in the sector. This risk is growing: data loss numbers are staggeringly large and attackers have probably only just started to exploit its potential value.(49)

Then we look at the business environment of financial services. It is a complex system with an incalculable number of compromise points for data, a total dependency on technology, a time-bound reliance on data integrity and a number of functions without substitutability. This is a landscape with a large number of features which are conducive to compromise.

(46) See Bloomberg (2018).
(47) See UK Finance (2018a).
(48) NotPetya was a global ransomware attack in June 2017. For more information see Wired (2018).
(49) See Verizon (2018).

There are also the human factors. The sector has always been immensely reliant on trust and confidence to fulfil its functions. And with technology advances, the trigger points for behavioural influence are widening. We are probably only just beginning to understand the relationship between the authenticity of information and its role within financial services. The early signs suggest a relationship which could be easily undermined by a savvy attacker; leading to typical behavioural responses seen in financial risk, such as capital flight.

Finally, we are seeing a further growing gap between the technology environment we operate and our ability to understand and secure it. As we build automated processes and artificial intelligence into its services, this will, by definition, compound the problem; making the mitigation of attacks significantly more challenging.

There are few obvious and current examples of cyber risk impacting the provision of financial services to the real economy. The absence of examples may simply be because the contributing factors to a systemic risk have not yet synchronised to cause a crisis. This may be down to luck or, more likely, that those with the capability have yet to pull the trigger.

Next steps

This paper has sought to explore the link between cyber risk and systemic risk rather than suggesting specific mitigation actions. Nevertheless, our findings should act as both a primer for future study and as a reference to inform our policy responses. For completeness, the following recommendations are suggested for consideration:

- Defenders of vital services should continue to develop their intelligence-led approach to cyber security. An improved understanding of our attackers will help to calibrate the finite resources to improve our defence of the sector.

- As reflected in the supervisory authority's Operational Resilience Discussion Paper,(50) organisations should reflect the reality of systemic uncertainty and accept that compromises are likely to happen and therefore prioritise response and recovery activities rather than just protective security.

- Reflecting the changing and global business environment, policy responses should seek to cut through sectoral, geographical and public/private boundaries. The progressive vision of UK Finance's Financial Services Cyber Co-ordination Centre exemplifies this approach.(51)

- Undertake further studies to better understand the relationship between data integrity and authenticity, trust in financial services and the potential for real-economy impact via a cyber attack.

- As per the June 2018 *Financial Stability Report*, there should be a specific focus on risks associated with third-party dependencies; specifically those '*that are outside the regulatory perimeter*'.(52)

(50) See Bank of England (2018c).
(51) See UK Finance (2018b).
(52) See Bank of England (2018d).

References

Bank for International Settlements (BIS) (2016), 'Guidance on cyber resilience for financial market infrastructures', Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions.

Bank of England (2018a), 'Systemic Risk Survey Results', 2018 H2.

Bank of England (2018b), 'Record of the Financial Policy Committee Meetings on 20 and 27 November 2018', 5 December 2018.

Bank of England (2018c), 'Building the UK financial sector's operational resilience', July 2018.

Bank of England (2018d), '*Financial Stability Report*', June 2018.

BBC (2018), 'TSB: How it all went so wrong for the bank', 28 April.

Bloomberg (2018), 'The world economy runs on GPS. It needs a backup plan', 25 July.

Bloomfield, R E and Wetherilt, A (2012), 'Computer trading and systemic risk: a nuclear perspective', *Foresight Driver Review DR26*, Government Office for Science.

Bouveret, A (2018), 'Cyber risk for the financial sector: a framework for quantitative assessment', *IMF Working Paper WP/18/143*.

Clapper, J R (2017), 'Joint Statement for the Record to the Senate Armed Services Committee — Foreign Cyber Threats to the United States', the Director of Intelligence, 5 January.

CNBC (2013), 'False rumor of explosion at White House causes stocks to briefly plunge; AP confirms Its Twitter feed was hacked', 23 April.

Danielsson, J, Fouché, M and Macrae, R (2016), 'Cyber risk as systemic risk', *CEPR Policy Portal*.

Eijffinger, S C (2010), 'Defining and measuring systematic risk', *Banking and Finance*, January(1).

European Central Bank (ECB) (2009), 'Defining and measuring systemic risk', Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policies, Economic and Monetary Affairs, 23 November.

Financial Stability Board (FSB) (2009), 'Guidance to assess the systemic importance of financial institutions, markets and instruments: initial considerations', IMF-BIS-FSB, October.

Finextra (2018), 'SunGard apologises for BNY Mellon system glitch', 28 August.

Gennaioli, N, Shleifer, A and Vishny, R W (2012), 'Neglected risks, financial innovation, and financial fragility', *Journal of Financial Economics,* Vol. 104.

Gennaioli, N, Shleifer, A and Vishny, R W (2013), 'A model of shadow banking', *Journal of Finance*, Vol. 68, No. 4.

International Monetary Fund (IMF), Bank for International Settlements (BIS) and Organisation for Economic Co-operation and Development (OECD) (2001), 'Report on Consolidation in the Financial Sector'.

Joint Committee on the National Security Strategy (2018), 'Cyber security skills and the UK's critical national infrastructure: Government response to the Committee's second report of Session 2017–19', 13 November 2018.

Kashyap, A and Wetherilt, A (2018), 'Some principles for regulating cyber risk', *Centre for Economic Policy Research Discussion Paper DP13324*.

Kaufman, G G and Scott, K E (2003), 'What is systemic risk, and do bank regulators retard or contribute to it?'.

Lloyd's of London (2018), 'Cloud Down — Impacts on the US economy'.

Mee, P and Schuermann, T (2018), 'How a cyber attack could cause the next financial crisis', *Harvard Business Review*, 14 September.

National Cyber Security Centre (NCSC) (2017), 'Latest information on the Equifax cyber incident', 10 October.

National Cyber Security Centre (NCSC) (2018a), 'Reckless campaign of cyber attacks by Russian military intelligence service exposed'.

National Cyber Security Centre (NCSC) (2018b), 'Advisory: Russian state-sponsored cyber actors targeting network infrastructure devices'.

Schwaab, B, Koopman, S and Lucas, A (2011), 'Systemic risk diagnostics — coincident indicators and early warning signals', *ECB Working Paper No. 1327*.

Smaga, P (2014), 'The concept of systemic risk', *Special Paper No. 5*, Systemic Risk Centre, London School of Economics.

Statista (2018), 'Number of internet users worldwide from 2005 to 2017 (in millions)'.

***The Telegraph* (2017)**, 'NHS cyber attack: everything you need to know about 'biggest ransomware' offensive in history', 20 May.

UK Finance (2018a), 'Staying ahead of cyber crime'.

UK Finance (2018b), 'News in brief', 18 October.

UK Foreign Office (2017), 'Foreign Office Minister condemns North Korean actor for WannaCry attacks', press release, 19 December.

Verizon (2018), 'Data Breach Investigations Report'.

We are Social and Hootsuite (2018), 'Digital Yearbook'.

Wired (2014), 'An unprecedented look at Stuxnet, the world's first digital weapon', 11 March.

Wired (2017), 'Your guide to Russia's infrastructure hacking teams', 7 December.

Wired (2018), 'The untold story of NotPetya, the most devastating cyberattack in history', 22 August.

World Economic Forum (WEF) (2016), 'Understanding systemic cyber risk'.

Wright, J (2018), 'Cyber and international law in the 21st century', 23 May.