UK FINANCE

INCIDENT MANAGEMENT

Cyber Incident Response – Is Your Firm Ready?

June 2020

UK Finance is the collective voice for the banking and finance industry. Representing more than 250 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation. We work for and on behalf of our members to promote a safe, transparent and innovative banking and finance industry. We offer research, policy expertise, thought leadership and advocacy in support of our work. We provide a single voice for a diverse and competitive industry. Our operational activity enhances members' own services in situations where collective industry action adds value.

Contents

Foreword - UK Finance

Hannah Gurga

Managing Director, Digital Technology & Cyber and Chief of Staff, UK Finance

Cyber Security has been identified as a Tier 1 threat, alongside Terrorism, War and Natural Disasters. Defending against the cyber threat is therefore a priority for businesses across all sectors, but as important is the ability of firms to stand up an effective cyber incident management response in the event of an attack.

The UK financial services sector is one of the most targeted globally, so it is vital that firms assess their cyber incident response processes and determine whether these are fit for purpose. Understanding where strengths and weaknesses lie ahead of a crisis can save time and improve a firm's ability to respond when a successful breach occurs.

This paper is intended to help firms as they reflect on their incident response plans by providing insight on some of the regulatory and operational considerations, including a number of issues that are specific to the financial sector, such as how to contact customers during a cyber crisis when systems might be compromised; how regulatory reporting is to be managed; or what access to cash provisions need to be made.

In addition, and with thanks to the expertise provided by colleagues from the crisis management team at Deloitte, the paper explores how a business can best plan, exercise and prepare for an incident. This also includes the importance of ensuring lessons can be learned, with staff from across the organisation given the opportunity to feedback findings into the incident management team.

If a financial institution is hit by an attack that it cannot respond to, loses customer information or in extreme cases ceases operations then it could lose its licence to operate. Cyber is integral to the operation of all business functions, yet too often the cyber security team may operate, or be perceived as operating, at arm's length from the rest of the business. This whitepaper seeks to address this gap.

As ever, we appreciate readers' time and interest in our whitepapers and would encourage anyone with comments or observations to get in touch with our Digital, Technology and Cyber team who lead work in this space at UK Finance. I hope you enjoy the report.

Foreword - Deloitte

Rick Cudworth

Partner, Deloitte

The cyber threat landscape is ever evolving and cyber criminals continually change their attack methods and targets to maximise their chances of success. This poses a significant challenge for organisations to keep themselves safe and protected at all times with the attack vectors being so varied.

Therefore, there is a need to be well prepared for when an attacker does breach an organisation's defences. Having an experienced and highly capable incident response team is crucial for managing any type of cyber incident, but they also need mature response plans and principles to ensure the organisation is responding coherently across what could be a complex incident.

In addition, the organisation as a whole, from operational teams to executives and board members, must have a consistent view of what services are most important to the organisation's customers and the broader market as a whole.

The best courses of action can then be coordinated to protect the systems and assets that would most impact on customer service. Working through these actions pre-incident will allow plans to be developed, and "pre-considered options" to be worked through, in case they are needed.

Achieving this alignment will require a good relationship between incident response teams and business leaders, both in the preparation for an incident, and during the response too.

Incident Management

Cyber-attacks are increasingly a feature of the business landscape and for many firms, it will be a case of if not when. Organisations can invest heavily in staff and technology, but it is impossible to totally secure the perimeter of a digital estate. This is why it is so important that organisations have a clearly defined cyber incident management process that is known and followed by staff.

While breaches of data and systems are a reality for all organisations, they cannot just be left to run their course. It can take months or even years to detect a security breach – firms take 197 days to identify and 69 to contain such breaches on average – giving criminals considerable time to exploit the accessed information. Such 'dwell time' can be costly for the breached organisation, especially when the breach is detected by an external party, which happens around 40 per cent of the time, meaning that dwell time can significantly increase.

However, having the right processes and a well-rehearsed plan in place can help mitigate any potential impacts to an organisation by:

- ensuring unauthorised access to data is identified and addressed or stopped
- improving the general cyber posture of the firm by identifying vulnerabilities in the digital estate, missing controls or training requirements for staff
- helping to quarantine malware infections, work through the remediation process to remove the actor from the network and gather any relevant learning to harden security
- improving an organisation's understanding of the threat landscape, those seeking to attack them and their tactics, techniques and procedures (TTPs)
- understanding the likelihood of any breached data being released and where and what the impacts to your organisation might be
- knowing the operational impacts to an organisation, the costs associated with this and the work needed ahead of time to understand how long financially you can be without key services and/or systems.

The need for a well-rehearsed incident management process can have exponential benefits for an organisation under attack and the quicker a firm can respond, the better the outcome.

THE REGULATORY REQUIREMENTS

Before getting into the internal steps firms must take to manage the risk, it is important to understand the regulatory picture.

In addition to a threat to operations, it is important firms are aware and have factored in any necessary regulatory reporting. In the UK especially, it is important firms note and understand their responsibilities when it comes to reporting to the regulators in the event of a cyber incident.

The regulatory picture demonstrates the potentially wide-ranging impacts of a cyber-attack – it is not just a case of affecting operations or customers but also about the wider market stability. The regulators' statutory objectives are therefore linked to ensuring that firms maintain operational capability during an incident and central to this is a strong incident management plan. In this regard, cyber serves as a key focus in the operational resilience landscape, which is discussed later in this report.

There are several areas of focus for the FCA including:

- Principle 3 of the Principles for Businesses – a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

- Principle 11 of the Principles for Businesses – a firm must deal with its regulators in an open and cooperative way, and must disclose to the appropriate regulator appropriately anything relating to the firm of which that regulator would reasonably expect notice.

- SYSC 3.1.1 – a firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business.

- SYSC 3.2.6 – a firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime.

- SUP 15.3.1 – a firm must notify the FCA immediately it becomes aware, or has information which reasonably suggests, that any of the following has occurred, may have occurred or may occur in the foreseeable future: (i) the firm is failing to satisfy one or more of the threshold conditions; (ii) any matter which could have a significant adverse impact on the firm's reputation; (iii) any matter which could affect the firm's ability to continue to provide adequate services to its customers and which could result in serious detriment to a customer of the firm; or (iv) any matter in respect of the firm which could result in serious financial consequences to the UK financial system or to other firms.

The PRA provides similar guidance for firms:

- Fundamental Rule 2: a firm must conduct its business with due skill, care and diligence.

- Fundamental Rule 5: a firm must have effective risk strategies and risk management systems.

- Fundamental Rule 6: a firm must organise and control its affairs responsibly.

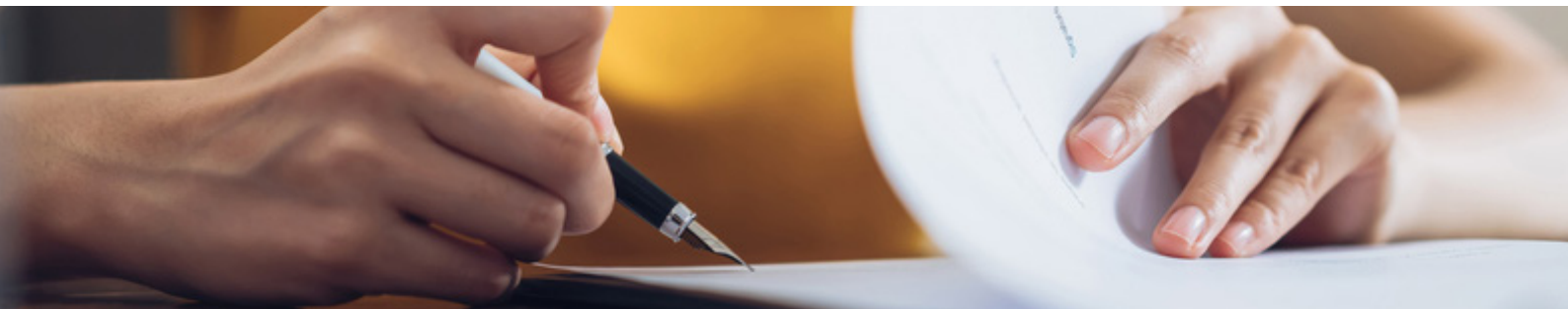
- Fundamental Rule 7: a firm must deal with its regulators in an open and cooperative way and must disclose to the PRA appropriately anything relating to the firm of which the PRA would reasonably expect notice.

- Firms must establish, implement and maintain adequate risk management policies and procedures, including effective procedures for risk assessment, which identify the risks relating to the firm's activities, processes and systems, and where appropriate, set the level of risk tolerated by the firm.

- Firms must adopt effective arrangements, processes and mechanisms to manage the risk relating to the firm's activities, processes and systems, in light of that level of risk tolerance.

- Have adequate, sound and appropriate risk management processes and internal control mechanisms for the purpose of assessing and managing its own exposure to group risk, including sound administrative and accounting procedures.

- Ensure that its group has adequate, sound and appropriate risk management processes and internal control mechanisms at the level of the group, including sound administrative and accounting procedures.



Cyber and operational resilience remains high on the UK regulatory agenda and firms must be aware of the requirements and have the right preparations and controls in place. Those that do not will face heavier regulatory repercussions.

In addition, firms need to think about any other regulatory responsibilities that they may be required to adhere to depending on the environment they work in or the jurisdiction in which they operate. The EU's General Data Protection Regulation (GDPR) and NIS Directive are two such regulations that organisations operating in Europe will need to understand and abide by. Specifically, organisations are required to implement an effective incident response plan to manage data breaches and prevent any further damage from taking place.

In such instances, firms will need to have an incident response process in place that has capability to contain incidents and minimise subsequent risks. Firms must look to what could happen following a data breach and the risks to customers – for example, what protections are in place to ensure customers affected by a data breach do not become victims of a subsequent fraud attack?

This is not an exhaustive list of regulations in place and there is rarely, if ever, a one size fits all solution so firms will have to interpret and apply in a way that is specific and appropriate to them.

WORKING IN PARTNERSHIP, NOT ISOLATION

An incident management function is only as good as the information that informs it. In order to ensure it is able to respond quickly when necessary, it needs to have a strong threat intelligence and situational awareness capability – as well as existing relationships that stretch across the business. These are essential to prevent damaging delays in a time of crisis.

It is crucial that threat intelligence informs the incident management team and there are seamless links between the two. The difference between a good and bad incident response can be down to the level of information those managing the incident receive. This encompasses both a strategic understanding of the threat and a tactical one.

Organisations that are able to combine an understanding of the threat landscape – of who the threat actors are, where they originate, why they might be targeting your firm and geo-political influences – and tactical analysis – how actors carry out the threat, are likely to be best placed when responding to incidents. Firms with the resource and appetite can go in-depth and reverse engineer malware, build threat-hunting teams and use automation and artificial intelligence to further their capabilities. Financial institutions can also outsource this capability if they don't have capacity or the will to do this internally. For firms without the resources to do either cross-sector and public sector support is available, such as the Financial Sector Cyber Collaboration Centre (FSCCC), a public private partnership between the UK financial services sector and the National Cyber Security Centre, National Crime Agency and the regulatory authorities – FS-ISAC, the Cyber Defence Alliance and cross-sector groups run by the Financial Conduct Authority and the PRA.

Firms can also look to frameworks that are available to inform capabilities within their organisations such as TIBER-EU[1], CREST[2] and ISO27001[3]. TIBER-EU mimics the tactics, techniques and procedures of real attackers, based on threat intelligence designed to reveal the strengths and weaknesses of a firm's response. CREST's approach draws on ISO 27001 advocating firms to put appropriate measures in place, thus mitigating the risks that can be mitigated, whilst also adhering to ISO 27035's guidance to ensure an organisation is ready for any incident and can respond to them accordingly.

1. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html
2. https://www.crest-approved.org/
3. https://www.iso.org/isoiec-27001-information-security.html

ENSURING THE RIGHT EXPERTISE

Organisations will need to make a risk-based decision on what the cyber incident management team needs to consist of, taking into considerations such as:

- what internal technical expertise is required?
- do we need experts in specific areas – e.g. ATM malware, DDoS etc?
- is it more cost effective to have in-house or to outsource?
- does the firm need 24/7 coverage?

Once a firm has made these decisions it will need to consider the information that the team produces and at what cadence:

- Collecting incident information – for breaches or just 'events' which may have been successfully managed
- Producing incident reports and reviews tailored for business units
- Attack data on the infrastructure to understand what normal looks like
- Producing reports on a quarterly, biannual or annual basis to identify changes in threat landscape and to reflect what threats to the firm have been addressed.

Equally, if a firm decides that it is going to outsource this capability it is important it is clear in articulating what information it requires and how regularly.

In addition to a set cyber incident management function, it is important the institution has experts from each relevant business unit that are involved in the response process. Firms will each need to decide what is appropriate for them but it is advised that there are experts that are on point for each business area including legal, communications, HR, infrastructure, facilities, operations, as well as a business leader who is responsible for the business decisions associated with the incident. For firms that provide one or a number of services it is important to have representatives from these areas so that they can provide the required expertise and knowledge – e.g. credit, relationship management, insurance, payments etc.

Likewise, organisations might span multiple locations nationally, across continents or worldwide and it is important that the right connections and relationships are in place to ensure that incidents that cross borders can be managed appropriately.

IDENTIFYING YOUR ASSETS AND WHERE THE RISKS LIE

To best inform an incident management function an organisation needs to have identified its key assets, important business services and the vulnerabilities and risks to those operations. It should also consider how the incident management function must work with other areas of the business to inform the response process. Understanding what systems, suppliers and information are core to business operations informs what to prioritise during the initial stages of an incident that might be affecting more than one system – such as ransomware – and can ensure systems and services are brought back online in line with business requirements.

Organisations must also reflect on the potential impact to their customers of a cyber or operational incident that takes services offline. Recent regulatory focus has sharpened in this area and considering what is crucial to the wellbeing of customers and ensuring the continuation of services means there may be additional assets that need to be protected. Institutions must identify what is important to the customer – either what will cause harm or from a systemic perspective – then consider what assets must be protected to ensure delivery of the services.

Once an organisation has identified its core systems and information it is important to map the threats to those systems, and how attackers might seek to access them. Awareness of who is trying to access systems, how they are doing it and what vulnerabilities might be exploited ensures that the response is quicker and more efficient.

Having this information will better inform the wider business response. By letting business leaders and other teams with less of a cyber focus know what is at risk and what this means for them, it will help provide clarity to the business and assist leaders in their own priorities during such an event. The incident management team is unlikely to know business processes that sit around these key systems and information, so being able to harness leaders' expertise and experience can immeasurably improve the speed and efficiency of the response.

Assessing the risks and vulnerabilities that exist in the estate means that firms can identify them ahead of time and put the right controls and mitigations in place. It is important to remember in this regard that the incident management process can bring preventative benefits as well as benefits created through a firm's response.

Most organisations will already have controls in place that manage these risks; these will vary from basic antivirus and firewalls right up to scheduled patch management, threat hunting and well developed and exercised red, blue and even purple team exercises. It is important that an institution assesses the risks and sets impact tolerances and puts the relevant controls and processes in place to manage these risks. The recent BoE Operational Resilience consultation papers have set the direction for firms to follow; important business services based on an assessment of harm caused, financial stability risk and risk to the organisations' viability is key. Operating within an acceptable tolerance (i.e. within a tolerable level of impact) will be the focus for firms – whether that is through effective recovery, substitution of service, alternative procedures or a combination of all three.

AGREE INCIDENT DEFINITIONS AND A COMMON UNDERSTANDING OF CYBER INCIDENT RESPONSE (CIR)

Ensuring that all of your team have an awareness of when and how to use CIR, and what is meant by an incident is an important early step to building a successful response capability.

To activate the appropriate level of response during an incident your organisation should have a clear definition of what an incident is, supported by criteria to distinguish between the severities of particular incidents.

In reality, incidents never fit into neat categories or types. Therefore, you should use your incident criteria as a guide, rather than precise triggers points, to activate the right level of response. This is particularly relevant for cyber incidents, where the initial scope and scale of the problem may be unclear, however the potential impact could be severe.

Incident responders will deal with incidents daily, and typically have the skills, knowledge and capability to respond to most of these effectively and mitigate any risks. However, they need to be clear about when they should escalate those incidents, which are – or have the potential to be – more severe, and may require support from outside of the CIR teams, severely affect your organisation's business operations, customers and other parties or cause a potential systemic risk to the sector.

DESIGN CONSIDERATIONS FOR EFFECTIVE INCIDENT RESPONSE

An incident response team requires the right protocols to operate effectively during an incident. These protocols can be organised to align with the different phases of an incident (as defined in the NIST cyber security framework) to provide a repeatable and simple structure for responders to follow.

Specifically, your organisation should establish protocols for CIR activation and communication.

The protocols for activation should directly link to the incident definitions your organisation has set, and the alerts received through monitoring tools. On receiving a specific alert, you should be able to activate a suitable team, made up of the right skills, and initiate a planned incident response to that threat type.

For example, a DDoS monitoring tool could indicate an influx of traffic to a particular port/location on your network. The team monitoring the network should be able to follow a predefined process to activate the CIR team, open a bridge call and immediately contact any relevant third parties, following an initial investigation. All these processes should be pre-defined and practiced.

Communication is vital during an incident and is the key to a coordinated response. You should give a considerable amount of time and energy to defining how incident communications will work in practice. There are four factors to consider when designing effective incident communications:

- the tools or methods (how you will communicate)
- the people responsible (who communicates)
- the nature and content of messaging (what is communicated)
- the frequency (how often).

Having a pre-agreed set of principles for communications alongside your CIR plan will enable the right people to be promptly involved and, importantly, allow those responsible for activating specific contingencies or mitigation options to do so early on in the incident, with the intention of limiting potential contagion effects or irreparable damage.

PLAN AND PREPARE FOR WHAT MIGHT CONFRONT YOUR ORGANISATION

A key part of managing incidents lies in the preparation and ensuring the process is slick and exercised when response is required. Planning ahead to assess the risks to critical business services, information and systems will ensure that worst case scenarios are known, understood and can be managed at speed, ensuring minimal service disruption.

It is important that such scenario planning includes both the incident management function's roles and responsibilities as well as wider business considerations. These should include how and what messages will be communicated to specific staff and when; how regulatory reporting is managed; and more operational aspects such as up to date checklists and current contacts.

The level of detail an organisation goes into on these scenarios will depend on the resources available but for the more mature end of the spectrum, risk assessments and penetration testing will indicate areas of highest concern. Firms with less time and money to spend on identifying threats to the business can focus on those that are key to remaining operational or those that key services depend on. Each organisation should be able to identify the biggest threats it faces and apply a cyber-security perspective to this. For example, if a firm's existence hinges on online services and sales, it should assess the risk to these systems and what could force them offline or how malicious actors seek to capture payment details.

Many financial institutions in the contemporary market will be relying on online products and services; a number of which will be supported by third-party providers. It is important organisations are aware of the risks that face both them and any core suppliers they use, and this is also an area of regulatory focus. By analysing these scenarios ahead of time, a firm will be able to make alternative arrangements or put into place contingency plans to prevent either delays or a fall in service standards to customers.

DEVELOPING PRE-CANNED DECISIONS – IMPACTS AND BENEFITS OF A DECISION BEING MADE

The Bank of England, PRA and FCA have recently emphasised the need for organisations to plan for 'severe but plausible disruption scenarios' in the Operational Resilience discipline. This is highlighted in their discussion paper (DP01/18) and associated consultation paper[4].

These events could affect large parts of an organisation for a prolonged period. Preparing for these scenarios is challenging, however there is value in considering what a severe but plausible disruption scenario could look like from a cyber-risk perspective.

For example, a ransomware attack could affect a significant proportion of your organisation's endpoints and servers, with no decryption key available, resulting in the need for a mass rebuild of devices. This type of scenario may require difficult decisions: if the malware is already on the network, and security tools have been unable to limit the spread, what other options are there? A manual network switch-off could limit the contagion effect, however this could also cause self-inflicted downtime.

4. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=DAD20B3E08876E418863D37A242214BB1F32FE0A

These types of decisions are characterised as last resorts in the most severe scenarios. However, exploring these types of decisions as part of incident response planning can help your organisation to understand the options open to it in a severe but plausible disruption; your current capabilities and opportunities to improve your defences.

Scenarios can be written and held in a location for staff to access but unless they are tested, they are as good as useless. Organisations will have individual testing cycles which are set to their own risk appetites, but it is crucial they are tested regularly enough for staff to be comfortable with the process and feel well-versed should a real incident occur. Testing with sufficient regularity will also ensure that the scenarios and processes are kept up to date and that gaps and weaknesses are identified and acted on in a steady state as opposed to in times of response.

Training staff is clearly paramount as they will likely provide the route in for attackers and when carrying out the response they will be tasked with understanding the threat and making the right decisions, be it leaving a service offline, quarantining a breach or choosing to watch and learn. Firms must also tailor this training to individual teams based on their role in defending the firm.

All staff should be able to identify a phishing email, know escalation and reporting routes and understand the basic cyber hygiene levels that the business expects. This can be woven into mandatory training or carried out on arrival or at regular agreed intervals. Employees with cyber incident response roles from across the business will need additional training on specific scenarios and processes specific to the firm and perhaps broader training in topics such as crisis management, colleague and public messaging and any technical skills relevant to their areas of work.

Specific technical responders will clearly require the most regular testing to ensure that there are no technical gaps in the firm's incident response (whether these are addressed in house or through outsourcing) as well as ensuring they are aware of the decision-making process. At the higher end of maturity, firms can look to train staff in penetration testing, forensic analysis and reverse engineering and will have to make a risk decision on the investment in this resource from specialised training providers.

Yet while staff may be well versed and well exercised, there is no replacement for experience in real-life situations where processes are walked through in heightened conditions. It is important therefore that staff have the opportunity to feed findings back into the incident management function so that lessons learned can be identified and acted on, ensuring gaps are addressed. Simple findings such as a lack of understanding as well as technical gaps can be equally as beneficial to spot, so staff must have the opportunity to provide their feedback and perspectives.

INTEROPERABILITY WITH THIRD PARTIES

Response plans also need to consider an organisation's reliance on, and use of, third parties during a cyber-incident. You should identify those third parties who may be relevant to your organisation in several scenarios.

There are various roles for third parties during an incident response: they may actively support the response by mitigating the cyber risks or implementing technical fixes or they may be affected by your system downtimes and will need you to communicate the progress of the incident, and to activate relevant contingencies.

Incident response plans should document what third parties can do for you, what you can do for them, and how you will communicate during an incident.

These relationships form an integral part of an effective response, and you should practice how you will work with third parties as part of your CIR tests/exercises.

CONSTANT TESTING, CONSTANT LEARNING

Attackers are relentless in their efforts to access the systems that they target. Whether through developing their own skills and capabilities or through sheer brute force and effort, they have time and resources in their favour. To counter this, it is important firms continue to improve their internal security processes and harden their defences, to make them a less attractive target. Staying abreast of the threats to your sector or on the systems and software you utilise can ensure that you prevent an incident or are able to respond efficiently should one occur.

A cyber-mature organisation will look to build this into a regular process that is reviewed and updated on a set basis. This will build in lessons learned in exercises or intelligence gathered from previous incidents, utilising the experience and information produced by peers or experts to ensure that your defence management is up to date and not stagnant. It is important that business considerations are managed and involved in the decision-making process. For example, if a piece of software is going end of life, is it better to move to a new operating system – which can be lengthy and expensive in the short term – or maintain a strict and/or tailored management process which might be less secure and more expensive in the long term.

Firms also need to consider what financial planning they put in place to ensure they have access to cash if a significant incident takes place.

ACCESS TO LIQUIDITY

In times of crisis it is crucial that firms can make payments quickly and two ways to apply the plaster are through access to liquidity and cyber insurance. Both are designed to allow a firm access to emergency funds to alleviate the immediate problem or to help bring in expertise required to resolve the threat or, in extreme instances, to rebuild software and hardware.

Having access to liquidity, and the means to make that payment, allows a firm to be more agile in responding to a cyber incident and plan what is required. During cyber-incidents organisations may need access to services or new technology as a matter of urgency, and that means access to cash. If a firm is unable to make payments or access funds, then this can significantly undermine their ability to manage the cyber incident and minimise the damage. In order to ensure this is not the case, there are several steps an organisation can take beforehand so that the incident response process includes sufficient financial planning.

Firms should scope potential costs to the business should a significant, destructive attack take place. Questions such as "how much would this critical system cost to be rebuilt?" and "how much is a cyber incident response company likely to cost?" should be considered to try and quantify how much might need to be spent quickly from a technical perspective.

But the cyber incident response function can also leverage business expertise and begin to cost how much it might lose if key systems and services are offline for certain periods of time. A more mature organisation will ask itself how long it can survive without these services in operation, identifying how much money it will be losing and at what rate.

CYBER INSURANCE

The cyber insurance market is one of the fastest growing insurance markets providing a number of beneficial services to firms experiencing a crisis:

- Forensic investigations
- Legal advice/assistance
- Notification (drafting /printing/call centre/advertising)
- Card replacement
- Monitoring services (credit and intrusion)
- Public relations
- Response to a data breach as a result of actions by an employee, contractor or external party such as a hacker - includes physical theft of data on paper or digital media
- Time used in remedial actions directly related to the breach
- Costs incurred through dealing with third parties i.e. hosting companies
- Assessments and fines levied by card brands and through acquiring banks and/or payment processors
- Subsequent fraud resolution costs
    - » Credit rating analysis/resolution
    - » Close monitor on trending
    - » Identity theft insurance for breach victims

Each business will need to make a risk-based decision as to whether it deems a cyber insurance policy necessary. However, where possible firms should look to apply the benefits to their scenarios. For example, if a firm's key risk is a destructive ransomware attack and it is considering cyber insurance as a means to access cash to rebuild systems, how long will it take to access that insurance payment?

As with any insurance policy, it is important organisations select the cyber insurance policy that is appropriate for them and their situation. Timeframes, levels of engagement with the provider, a strong relationship with the provider and checking whether the policy is clear on specifics, such as what constitutes human error (such as a staff member clicking a link) should all be important considerations when deciding on the most appropriate cyber insurance policy.

ESTABLISHED RELATIONSHIP BETWEEN BANKING PROVIDER AND CUSTOMER

Banks want to protect your money and prevent fraudulent attacks. If they see requests for large sums of one-off payments coming from a digital infrastructure then it is appropriate for them to query that payment before authorising. This is exactly the situation that can occur in a ransomware attack.

If a firm does not have access to its systems, as was the case during the NotPetya attack for large and small organisations alike, then it can be difficult to contact a provider to authorise a payment. Without access to phones, emails or online via a corporate system it can be difficult to verify payments. It is therefore imperative that an organisation has a good relationship with their relationship manager and that this is not a single point of failure on both sides.

Commercial customers and financial institutions alike must think about how they can contact and verify themselves to their financial providers without access to normal systems. A bank engaging with a customer it knows or suspects is experiencing a cyber incident will naturally be more cautious. It is therefore crucial the firm and customer have both taken steps to make sure the bank has the assurances they need to grant access to accounts and the client is able to authenticate themselves, thus speeding up their access to cash in times of crisis.

It is crucial therefore to make alternative arrangements in the event that your systems are compromised. For example:

- are contact details for banking providers stored off the main corporate network?
- are log in details known off the corporate network, and in a secure location?
- should you be unable to verify payments through email authentication can you contact the provider over the phone?
- does the provider accept phone calls as authentication alone or is there a second factor which relies on a corporate network?
- are phones connected to the corporate network?

Firms can support their customers and clients by informing them of what they will require in such instances to aid authentication and should have steps in place to plan for this. If a bank is rigid in its requirements for customers in the midst of a crisis, it could directly impact their ability to maintain operations.

FUNDING KNOWN CRIMINAL ACTIVITY

Ransomware has in recent years been flavour of the month for attack groups due to the lucrative profits that can be made. The advice from law enforcement and government is unequivocal: do not pay ransoms.

- There is no guarantee that you will get access to your systems back and you could end up being complicit in criminal activity by funding it.
- Attackers can simply be threatening to conduct an attack without the actual means to do so.
- If you were relying on paying a ransom in incident response plans, there is no guarantee that your banking provider will carry out the payment as it could be in their policy to not make payments to known criminals.

CUSTOMER CARE

Central to many financial institutions' strategies is to be there for their clients through thick and thin, in times of profitability and in times of crisis; cyber risk should also be considered in these terms.

Firms will of course have to take appropriate steps to protect their corporate network and in some cases may deem it appropriate to stop email traffic between organisations or disconnect and direct connections. However, to ensure that they are doing what they can to support customers they will need to think about what they, as a financial services provider, can do to ensure that the adverse effects of a cyber-attack are not too severely felt.

Organisations at both ends of the cyber-maturity spectrum will have some sort of internal response plans in place, but the response of firms when clients are hit by a cyber-attack could be the difference between staff being paid and going without wages for the duration of an attack.

Some firms are thinking about what an incident response process looks like when one, or a number of customers are hit by attacks and how this varies between corporate and retail clients. For example, what would be appropriate for a fraud attack on one retail client will be considerably different to a firm's response to hundreds of commercial clients knocked offline by a ransomware attack.

Organisations could consider:

- whether internal teams consisting of cyber experts and relationship managers need to be convened to support the client
- fraud controls put in place on accounts known to be affected by a cyber-attack
- fast mechanisms for customer authentication and authorising payments
- regular touchpoints and engagements to maintain a clear picture of the incident and customers' requirements from their financial providers
- options for intelligence sharing and incident management recommendations (through process, as a service or through recommended paid for providers).

Financial firms will make individual decisions on whether such a comprehensive level of customer care is required but in such technological and competitive times, organisations with a customer focus at the heart of their strategies can develop relationships and support customers when cyber-attacks occur.

Contributors

Ian Burgess - Director, Cyber and Third Party Risk, UK Finance
Ian leads UK Finance's operational and policy work on cybersecurity and third party risk management. In this role he engages with key industry stakeholders to determine the applicability of collective action on behalf of the financial sector. Through this engagement he is currently creating a single standard to assess the resilience of critical suppliers, having previously operationalised the Financial Sector Cyber Collaboration Centre (FSCCC), an industry utility designed to promote cyber intelligence sharing amongst financial institutions.

Before joining UK Finance Ian worked for BNY Mellon, where amongst other things he led the development and deployment of a global system to map technology risk regulatory controls to global cyber, technology and data privacy regulations. Prior to this he served as a British Army Officer for eight years.

Ben Payne – Principal, Cyber-Security, UK Finance
Ben joined UK Finance in March 2019 and is responsible for cyber-security with a specific focus on developing the Financial Sector Cyber Collaboration Centre (FSCCC), providing expert advice and guidance and lobbying and responding to policy developments on behalf of members. Through the FSCCC Ben is focusing on professionalising intelligence sharing and incident management across industry, as well as with government and law enforcement partners.

Prior to UK Finance Ben was responsible for cyber-security at Lloyds Commercial Bank, with the role split between ensuring the organisation was resilient from attacks as well as supporting the Bank's customers with their cyber defences. Before Lloyds Ben held a number of operational cyber roles in government, with a focus on incident management and threat intelligence.

Rick Cudworth, Partner, Deloitte
Rick is a Partner in Deloitte's Reputation, Crisis and Resilience practice in London. He has over 25 years' industry-leading experience in High Impact Events, Resilience by Design, incident response and Crisis Management. He has been interim Group Head of Resilience & Crisis Management at two global banks and has supported and facilitated executive leadership teams in responding to crisis events and major incidents. He has undertaken several high profile Independent Post-Event Reviews examining the root causes and effectiveness of response to crisis events, including the independent review at the Bank of England into an unprecedented outage of a critical UK intra-bank settlement and payments system, reporting to the Parliamentary Treasury Select Committee.

He is Chair of the British Standards Institution Technical Committee for Continuity and Resilience and was a contributor and review panel member for BS 11200: Crisis Management and BS 65000: Organisational Resilience.

Charles Barlow, Senior Manager, Deloitte
Charles is a Senior Manager in Deloitte's Reputation, Crisis and Resilience practice in London. He has worked with multiple retail banks, wholesale banks, insurers and asset managers to help them plan and prepare for high impact events and incidents.

Charles has developed end-to-end contingency plans for major cyber-attacks covering the overall organisational response for a major UK retail bank and has led similar projects to design incident response plans for a multitude of cyber threat ranging from ransomware to data loss and major fraud.

Charles is a specialist in incident response simulations, and has designed and delivered around 20 simulations with major financial institutions testing response procedures for incident response teams, right the way through to executive and board decisions.