WAVESTONE

CYBER-RESILIENCE LESSONS LEARNED

THE LATEST UK DEVELOPMENTS

AUTHORS



FLORIAN POUCHET
florian.pouchet@wavestone.com

MAXIME ROCHE
maxime.roche@wavestone.com

GEOFFROY AUDOUSSET
geoffroy.audousset@wavestone.com

Recent major cyberattacks, especially global destructive ones such as WannaCry and NotPetya in 2017, but also targeted ones, have shown how significantly business activities can be disrupted for affected organisations, resulting in huge financial losses.

Consequently, organisations are looking for ways to become cyber-resilient and thus limit the impacts of such attacks. Besides this, more regulations related to cyber-resilience are emerging and pushing organisations to take appropriate action; particularly when incentivised by the threat of exposure to possible sanctions and fines for non-compliance.

How is the UK regulatory framework developing on this topic? What have we learned from recent major cyberattacks? How should organisations prepare to react promptly and effectively in case of such attacks?

CYBER-RESILIENCE IN THE UK – AN INCREASINGLY RESTRICTIVE REGULATORY FRAMEWORK

NIS Regulations, the first implementation of cyber-resilience principles in UK law

Following the European Union directive on the security of Networks and Information Systems (NIS directive) and despite Brexit, the NIS Regulations[1] came into force in the UK on 10th May 2018. This regulation has marked a clear shift of the regulators' role from a helpful supportive party to a more restrictive one.

As per this regulation, Operators of Essential Services (OES) and Digital Service providers (DSP) must consider cyber-security measures to manage the security of their systems and facilities, their existing processes and procedures to handle security breaches and maintain business continuity.

OES, who had to register to their Competent Authority (CA - i.e. regulator identified for sector) by the 20th August 2018, are considered as more critical than the DSPs in the event of an attack; and hence why they face much stricter requirements. Therefore, OES are subject to audits conducted by their CA's. These controls will assess organisations against the 14 security principles outlined in the Cyber-assessment framework published by the UK National Cyber Security Centre (NCSC).

If there is non-compliance with the NIS Regulations, organisations are now exposed to sanctions that can go from notices for further information to monetary penalties (up to a maximum of £17 million).

DSP's will not be audited, they will only face enquiries in case of incident. They have also been given more time to register to their CA with a deadline of the 1st November 2018. For organisations falling into the OES / DSP scope, not registering is considered as a blatant violation of the NIS Regulations, and could lead to severe disciplinary action.

Cyber-resilience regulation for the UK financial sector

Financial services have always been considered as 'one-step-ahead' when it comes to Cyber-resilience. Therefore, this market is a good indicator of the future trends related to this topic.

Surprisingly, the Banking and Financial Market infrastructure sectors are not listed as OES by the NIS Regulations – as opposed to the NIS Directive (the EU text) that includes these two sectors.

However, on 5th July 2018, the Bank of England (BoE), the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) quickly reacted by publishing a Discussion Paper on the UK financial sector's operational resilience[2].

This initiative gave Financial Services organisations until 5th October to report on their exposure to risks and how they respond to outages.

One of the key aspects highlighted in this paper is the notion of cyber-tests. The structure of the paper clearly sets out the cyber-resilience aspects that will be tested by the regulators across the full incident lifecycle management: Preparation, Recovery, Governance and Communication.

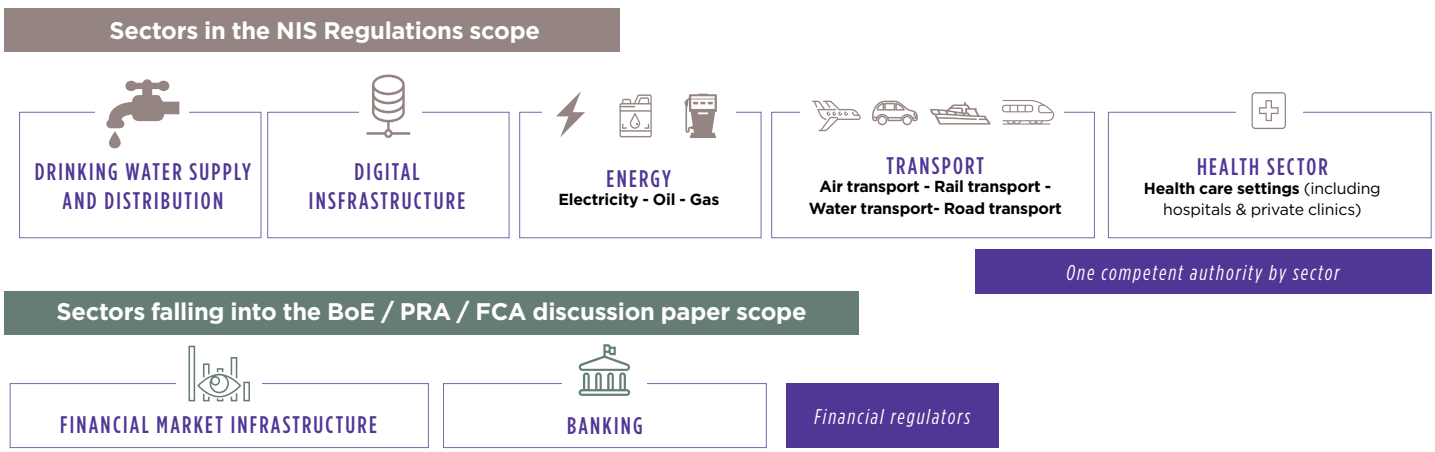
Future of cyber-testing: the use of Red-Teaming by the regulators?

The notion of cyber-resilience testing has also been put forward in the new testing framework published by the European Central Bank (ECB) in May 2018: the Threat Intelligence-based Ethical Red Teaming (TIBER) EU Framework[3]. The objective of this framework is to facilitate an approach towards intelligence-led tests which mimic the tactics, techniques and procedures of real hackers posing a genuine threat.

Even if the UK regulators are not obliged to implement this framework, it could give them some ideas to use these types of tests across all industries (like they did for the NIS Directive).

We expect that failing these tests will expose financial services organisations to sanctions in a similar vein as the Financial stress tests conducted in the last couple of years.

UK cyber-resilience regulatory landscape



1. https://www.legislation.gov.uk/uksi/2018/506/made
2. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf
3. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

CYBER-RESILIENCE – WAVESTONE'S LESSONS LEARNED

Organisations affected by major cyberattacks cannot continue to use their IT as normal and must fully or partly stop them to clean or rebuild them. Indeed, in some cases, attackers destroy critical parts of the IT infrastructure whilst in other cases, they penetrate and propagate the IT system for weeks to steal data or corrupt internal systems (Advanced Persistent Threat), thus causing a loss of confidence in the IT system.

For an organisation, to be cyber-resilient means being able to maintain vital activities in a downgraded mode in the event of a major cyberattack, while taking actions to quickly regain confidence in the IT system to be able to operate it as usual.

At Wavestone, we have developed strong expertise in supporting major cyber-crisis and cyber-resilience programmes. You will find below what we have learned on the topic, and in particular the 3 key aspects we recommend working on to become cyber-resilient.

Business Continuity Plans and Disaster Recovery Plans need to be reworked to face cyberthreats

Today's Business Continuity Plans and Disaster Recovery Plans aim to respond to scenarios like a pandemic or a datacentre physical destruction, but many have been built without taking into account major cyberattack scenarios and the possible loss of confidence in the organisation's IT that could result from such cyberattacks.

Within an organisation, 'everyday' IT and 'backup/recovery' IT systems are close in many ways, especially to facilitate their operability. As a result, in the event of a major cyberattack, the recovery systems will most likely be compromised at the same time as the 'everyday' IT systems, for 3 main reasons:

- Replication systems could copy the malware between the main IT estate and the recovery systems; or
- Attackers could exploit the administration infrastructure, common across both normal and recovery systems, to propagate within both; or
- Finally, even if the recovery systems are fully isolated, attackers could still exploit vulnerabilities present within both. Then, triggering your recovery systems would open the door for the malware to spread.

1 Prepare to contain the attack when it occurs

Cyber-crises are specific: they last a long time (several weeks), they are difficult to understand (what have the attackers been able to do? For how long? What are the impacts? etc.), and they involve third-parties who are often unprepared on the topic (lawyers, authorities, suppliers, clients, etc.).

Therefore, current crisis management processes must be supplemented to cater for the various cyber threat aspects. In particular, it is necessary to carry out the organisational and technical actions below to contain the attack when it occurs.

Organisational actions

- Identify the necessary people to call upon during a crisis (management, forensic experts, IT department, business continuity staff, HR, communication team, etc.) and specify their roles and responsibilities, as well as what needs to be done to allow them to be rapidly mobilised when necessary
  - For instance, during the crisis, the IT department will have to prioritise its actions between the investigation, the definition and implementation of the defence plan, and business-as-usual (BAU) operations
- Define processes that allow quick decisions from operational teams for threat containment (systems shutdown, floodgate activation, etc.), without waiting for a decision from the Crisis Management Team (CMT)
- Define appropriate processes to enable investigation activities and defence-plan-related activities in parallel, and to ensure 24/7 operations over a long time via rotations (logistics, HR, etc.)

Technical actions

- Identify backup communication tools outside of normal IT to safely manage the crisis (alternative mail, website to oversee the decisions, directory, etc.), as the usual communication tools may be unavailable or no longer trusted
- Make sure you have adequate investigation means to analyse and understand the attack (sufficient, safe and searchable logs, capability to analyse unknown malware, technical and functional cartography, detection processes based on business processes knowledge, etc.)
- Define floodgates in your network to be able to limit the attack propagation by isolating the most sensitive systems from those already compromised
- Make sure you have the right tools to protect the parts of the IT estate which are still safe once the threat has been isolated (quick patch deployment, etc.)

That being so, it is essential to regularly test the cyber-crisis management process via crisis exercises using ambitious and realistic scenarios.

2 Prepare to work without your IT

Business teams need to learn how to work in a downgraded mode without IT to simulate it being unavailable or untrustworthy for a few days or weeks. This may seem a bit extreme, but is what impacted organisations had to overcome in 2017, so better being prepared than sorry.

At least, business teams should ask themselves the following key questions to define processes and tools accordingly:

- **Can we work with manual workarounds?** (paper, cash, etc.)
  - If not, how can we interrupt our business activities in a controlled manner?
- **What data do we need?** (client contracts, contractors or suppliers lists, business data, etc.)

/ **What alternative tools do we need?** (phones, applications like WhatsApp, applications like Gmail, etc.)

As for the cyber-crisis management process, these alternative ways of working must be tested to ensure the continuity of essential activities in the event of a major cyberattack.

3 Prepare to rebuild your IT

If the cyberattack is a destructive one or important parts of the IT estate cannot be cleaned of a malware infection, there may be a need to rebuild some workstations, applications or infrastructure to maintain vital business activities. This must be anticipated, and processes and tools must be defined and implemented accordingly.

Regarding workstations, a user-friendly package (USB key and documentation) can be created to allow end-users to rebuild their workstations themselves. Besides, mobile backup servers can be used to restore users' data (drop-shipping), in case the network bandwidth is not sufficient to remotely restore it for example.

Regarding applications and infrastructure, the key to success relies on two points:

/ Rebuilding must be prioritised according to business needs, which must be defined beforehand; and

/ Architectures must be standardised as much as possible to help automate and simplify their deployment in case they need to be rebuilt.

Do not forget standard cybersecurity measures, without which cyber-resilience cannot be fully complete

Implementing measures to address the 3 aforementioned cyber-resilience aspects will help you improve your cyber-resilience, but it is not sufficient. Efforts to do so must go hand-in-hand with efforts to ensure the appropriate protection and monitoring of your IT systems. Hopefully, this will help you avoid having to trigger these plans in the first place. So, keep up the hard work!

3 key take-aways for cyber-resilience preparation

1 PREPARE TO CONTAIN THE ATTACK

/ **Organisational actions**

Define and implement processes allowing quick decisions from operational teams, processes allowing 24/7 operations over a few days or weeks, etc.

/ **Technical actions**

Define and implement network floodgates, backup communication tools outside the organisation's IT infrastructure, investigation data and tools, etc.

/ **Cyber-crisis exercises**

Test cyber-crisis management processes and tools using ambitious and realistic scenarios

2 PREPARE TO WORK WITHOUT YOUR IT

/ **Can you work with manual workarounds?**

If not, how can you interrupt your business activities in a controlled manner?

/ **What data do you need?**

Client contracts, contractors or suppliers lists, business data, etc.

/ **What alternative tools do you need?**

Applications like WhatsApp, applications like Gmail, etc.

3 PREPARE TO REBUILD YOUR IT

/ **Workstations**

E.g. Create a user-friendly package (USB key and documentation) to enable end-users to self-rebuild their workstations

/ **Infrastructure and applications**

- Standardise architectures as much as possible to help automate and simplify their deployment in case they need to be rebuilt.
- Clearly define business needs to be able to prioritise rebuilding accordingly when needed.