WAVESTONE

CYBER-RESILIENCE
BEND WITHOUT BREAKING

Successive cyberattacks, Wannacry and NotPetya, highlighted the limits of the current resilience and business continuity plans and the capacity of cyberthreat to cripple the Information System. Affected organizations paid the high price. What can we learn? What actions can we take to prepare for major cyberattacks?

When confronted with a major cyber attack, whether destructive or leading to a loss of trust in vital systems, the first reaction of a majority of companies is to activate their business continuity plan (BCP). The latter is a strategic element to the resiliency of organisations, in order to ensure their survival against disasters whose magnitude causes computing resources, communication infrastructures, buildings and possibly even users to be unavailable.

Yet major cyber attacks, be they destructive as Wannacry or NotPetya or leading to a loss of trust in infrastructure components (network, access control, inventory...) as targeted attacks have not been taken into account when developing most BCPs. Focused on an availability agenda, they failed to address the issue arising from the simultaneous destruction or the loss of confidence in Information System (IS) caused by cyberattacks.

Moreover, these IS continuity plans, frequently intimately linked to the resources they protect, are equally affected by these attacks. Indeed, for over a decade continuity processes (user fallback or IT recovery) have adopted principles of infrastructure pooling and “hot” recovery to cope with both rapid business recovery and the need for better operability.

In effect, this « proximity » between the regular IS and its recovery counterpart makes continuity plans vulnerable to cyberattacks.

As an example, various dedicated and connected recovery stations of fallback sites were contaminated by NotPetya and were useless for the remediation.

AUTHORS

GÉRÔME BILLOIS
gerome.billois@wavestone.com

FRÉDÉRIC CHOLLET
frederic.chollet@wavestone.com

Legacy « cold » recovery/emergency plans (often consisting in activating recovery system in case of incident) concern less and less applications, and the ones left are often secondary.

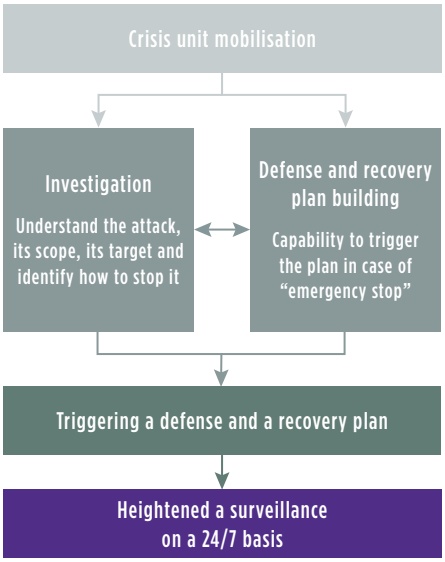
Unfortunately, when dealing with an in-depth compromission, backups embark de facto malevolent elements, due to the anteriority of the intrusion (detection often happens hundreds of days following the initial infection), such as malwares, base camps or modifications meticulously operated by attackers beforehand. Not to mention that the continuity of the backup systems themselves are often neglected. During the NotPetya crisis management, the very backup management servers were destroyed. Restoring them took several days given their complexity and their nested nature within the information system (an ActiveDirectory was necessary to launch the restorations while the ActiveDirectory backup was a prerequisite to rebuild it...).

The same findings hold for industrial IS. Industrial digital systems are resilient against technical breakdowns or anticipated mechanical incidents. However, they were rarely designed with the potential for human malice being considered and as a result often lack advanced security systems. To compound this, industrial IS has long lifecycles (several decades) that expose them to old vulnerabilities. Finally, the independence of control channels (SIS see side note below) with regards to digital systems they oversee is not always applied.

STRENGHTHENING CRISIS MANAGEMENT

Cybercrisis are specific: they are often long (several weeks) and sometimes difficult to grasp (what has the attacker been able to do? For how long? What is the impact?). It also implies that often, external parties themselves are poorly prepared on that topic (lawyers, authorities, suppliers, sometimes even clients). It is thus necessary to adjust existing plans that have not been designed to cater for the cyber aspect.

Cybercrisis management method



TWO ILLUSTRATED MAJOR ATTACK SCENARII

LOGICAL DESTRUCTION OR THE UNAVAILABILITY OF A LARGE CHUNK OF AN INFORMATION SYSTEM: made real by attacks from true-false ransomware, Wannacry and NotPetya. This type of attack causes mass unavailability of services due to the encryption of data files and/or the operating system. The companies affected by this attack (Merck, Maersk, Saint Gobain, Fedex... as well as Sony Pictures and Saudi Amramco) lost up to 95% of their information systems (tens of thousands of computers and servers) in a timeframe that often lasts less than an hour. At the start of such a crisis, the situation is highly difficult since there is no longer any means of communication or exchange mechanism within the affected company, including the ISD. Victims have outlined losses of several hundred million euros following these attacks.

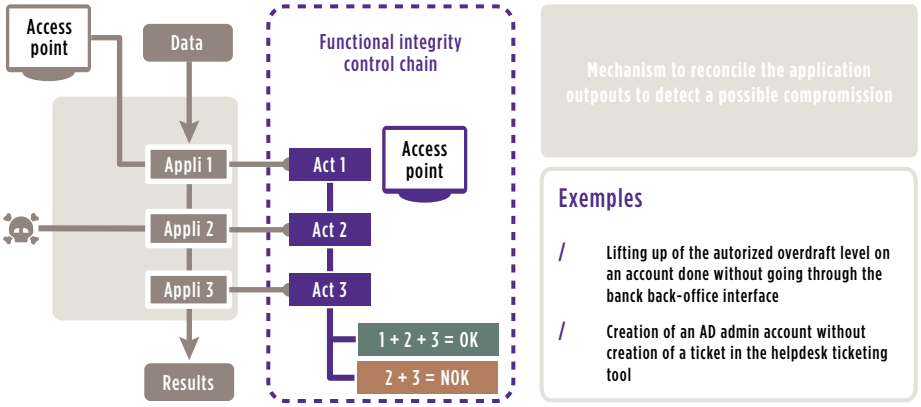
A COMPROMIZE AND LOSS OF CONFIDENCE IN INFORMATION SYSTEMS: it concerns a targeted attack which does not challenge the proper functioning of the system. Rather, it aims to give attackers access to all of the company's information systems (email and messaging, files, business applications etc.) allowing them to steal the identity of any employee and carry out actions in their name. The attackers may then extract any type of data or carry out business actions which require several successive validations. These attacks affected a large number of companies across all sectors incurring massive fraud as a result, including the bank of Bangladesh. These attacks also affected financial and payment data theft as was the case for several distribution groups in the United States including Target and even Home Depot. The situation at the start of the crisis is complex since there is no more confidence in the information system and there is considerable uncertainty about what the attacker could do and their motives. It involves quietly investigating until being able to remove the attacker and rebuild a secure system. Victims affected by these attacks have also reported financial impacts worth several hundred million euros.

Even if (s)he is an operational player in the cybercrisis management, the CIO should not be over-utilised on the investigation and the defence, if it is detrimental to production and recovery. This aspect constitutes an important anticipation point not to be neglected. It is necessary to clearly identify the teams that need to be mobilised for the crisis and organise the parallel interventions on the investigation and the defence plan construction.

Beyond the organisational point of view, the CIO will have to ensure that (s)he also has the investigation tools (mapping, search for attack signature, independent crisis management IS, capability to analyse unknown malware, etc.), remediation tools (capabilities to rapidly deploy technical corrections, fragmentation of the IS to save what could be saved, IS surveillance toolkit) and reconstruction tools (access to backup, access to minimal documentation, capabilities to deploy worksation) required to understand the position the attacker took in the IS, to repel it and to ensure it doesn't return.

Writing a crisis management guide that defines the essential steps, the macro-level responsibilities and the key decision points will be a bonus. It is essential to practice ahead of a real crisis to ensure readiness when it really happens, hence conducting a crisis exercise will be a valuable indicator of the real situation.

Functionnal integrity control chain



RETHINKING CONTINUITY PLANS

Continuity plans have to evolve to adapt to cyberthreats, and sometimes may have to be completely rebuilt.

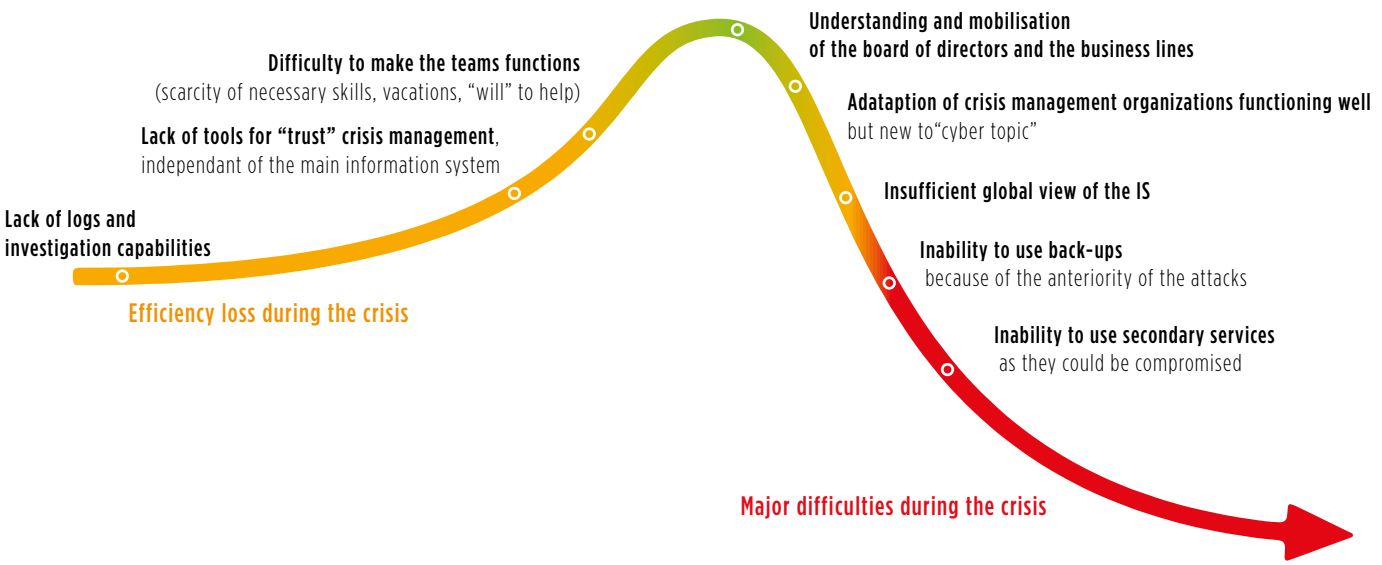
There are many possible solutions and they can cover all types of continuity plans.

The user recovery plan can evolve to integrate, for example, the availability of USB keys containing an alternative system. Employees could use it in case of logical destruction of their workstation. Some organisations have decided to provision a specific quantity of workstations directly with their suppliers to be able to deliver them quickly in case of physical destruction.

The IT continuity plan can include new solutions to be efficient in the event of a cyberattack. The most publicised one aims to build "non similar facilities". It is about duplicating an application without using the same software, operating system and production teams. It is an extreme solution, very costly and difficult to maintain, but that is considered for some specific critical applications in the financial industry (notably payment system infrastructure).

Other less complex solutions are envisioned, for example adding functional integrity control in the business process. The concept relies on the implementation of regular controls, at different levels and different places in the application chain ("multi-level controls"). This enables quick detection of attacks. For example, an interaction with

Main issues experienced during cybercrisis managemenent



technical layers (modification of a value directly inside a database) without passing through regular business workflows (via graphical interfaces). These mechanisms can also apply to infrastructure systems, for example, by reconciling admin account creation request tickets with the number of accounts really in the system.

At an intermediate level of complexity, it is possible to envision a "floodgate", as a system and network isolation zone.

This floodgate can be activated in the event of an attack and could isolate the most sensitive systems from the rest of the IS. To that end, the industrial IS could be one of these isolation zones separated from the rest of the IS.

These often major evolutions must be part of an existing recovery strategy review, so that one can assess their vulnerability and the interest of deploying new cyber-resilience solutions, in particular on the most critical systems. The evolution of Business Impact Analysis (BIA) to include this dimension crtainly is a key first step.

WITHOUT CYBERSECURITY, CYBER-RESILIENCE IS NOTHING

Implementing these new cyber-resilience measures requires significant efforts. These efforts will be in vain if these recovery solutions and the regular systems are not already secured correctly and under detailed surveillance. The CISO is the key player to make these, often started but rarely finalised, initiatives happen. Help from the Risk Manager (RM), or the Business Continuity Manager (BCM) if in place, will be valuable. It is widely acknowledged today that it is impossible to secure a system at a 100% level, which means one has to accept the probability of an attack occurring, and at that moment the RM or the BCM will make full use of their role.

Protect, detect, respond, remediate and rebuild. Here are the pillars of a strong cyber-resilience. And it will only be attained if the BCM and the CISO work hard hand-in-hand!

Example of actions to be taken in a cyber-resilience strategy

ANTICIPATE FOR NOT BREAKING

Spreading diversity and flexibility
(workstations, infratrustructures, applications, third parties...)

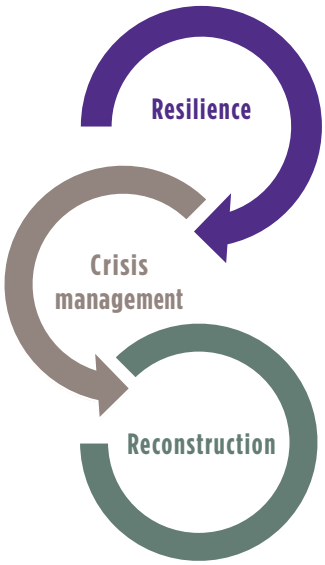
Limit amplification effect
(harden, partition...)

Reshape alerts and continuity plans
(prioritize, practice...)

REBUILD FAST AND SAFELY

Test the strength
(Realize penetration tests...)

Industrialize the reconstruction
(Restart unaffected services quickly, parallelize, rely on users...)



ACT RAPIDLY AND EFFECTIVELY

Organize
(Structure crisis units, communicate with authorities, mobilize expertise, have sufficient fallback telecommunication means...)

Identify and prioritize what can be saved
(Ensure audit trail, investigate, immunize...)

WAVESTONE

www.wavestone.com

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European Business (excluding retails and consumer goods outside of France). The firm is counted amongst the lead players in European independent consulting.

Wavestone's mission is to enlighten and guide their clients in their most critical decisions, drawing on functional, sectoral and technological expertise.