WAVESTONE

CYBER-RESILIENCE
BEND WITHOUT BREAKING

«Bend without breaking» this is often how resilience is presented. How does this concept apply to cyberthreats? What actions can we take to prepare for more frequent attacks?

Cyberattacks highlight how current resilience and business continuity plans have hit their limits.

Business continuity is often presented as one of the major elements of organisations' resilience strategy. Indeed, organisations have equipped themselves with business continuity plans (BCP) in order to ensure their survival against disasters whose magnitude causes computing resources, communication infrastructures, buildings and possibly even partners to be unavailable.

But cyberattacks in their modern form have not been taken into account when developing most BCPs. Focused on an availability agenda, they failed to address the issue arising from 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, dedicated and connected recovery stations of fallback sites today are very often exposed to the same contamination (and destruction) risks as regular workstations.

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.

AUTHORS


GÉRÔME BILLOIS
gerome.billois@wavestone.fr

FRÉDÉRIC CHOLLET
frederic.chollet@wavestone.fr

Finally, back-ups performed typically on a daily basis, constitute for most organisations the tool of last resort to rebuild the IS. But unfortunately, because the intrusion preceded the detection (often by a couple hundred days), these back-ups by default carry those elements of the compromise: malwares, base camps, but also alterations already made by attackers.

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 life-cycles (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

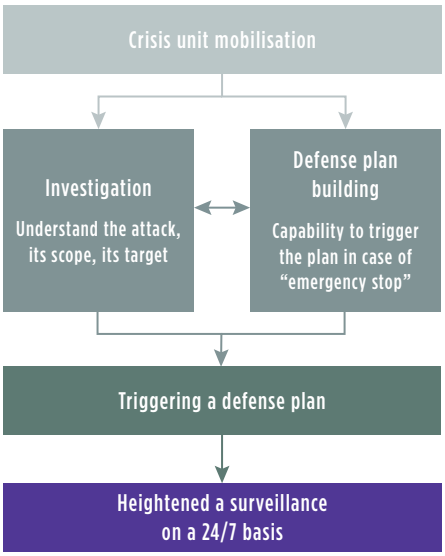
Cybercrisis are specific: they are often long (several weeks) and sometimes difficult to grasp (what has the attacker been able to do? For how long? What is the impact?). It also implies that often, external parties themselves are poorly prepared on that topic (lawyers, authorities, suppliers, sometimes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

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. In this respect the "Diamond Model: activity-attack Graph" and the "Kill Chain Model" can respectively address these needs.

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.) and remediation tools (capabilities to rapidly deploy technical corrections, IS surveillance toolkit) 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.

Cybercrisis management method



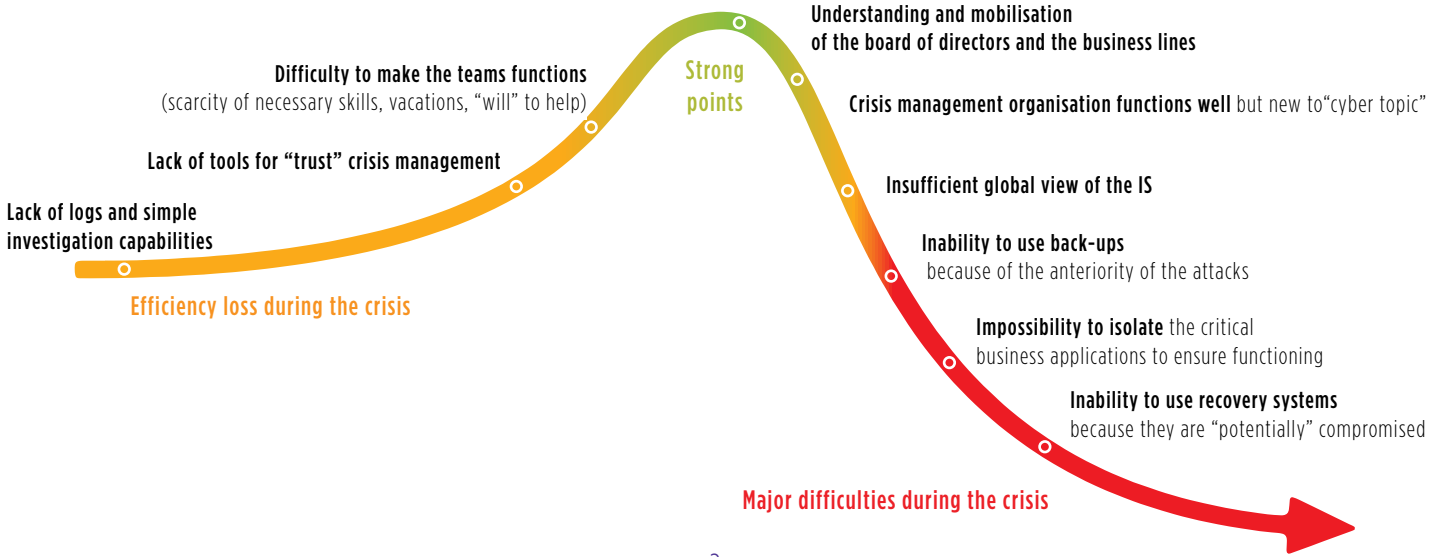
RETHINKING CONTINUITY PLANS

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

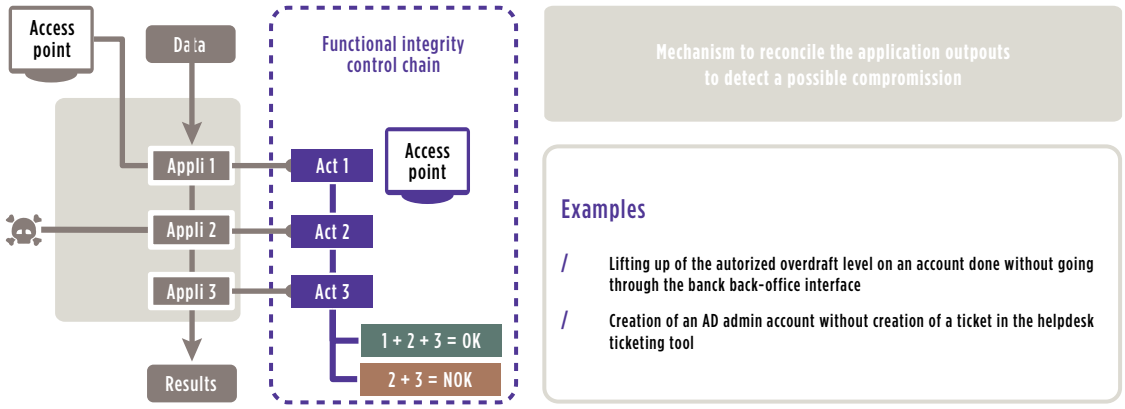
There are many possible solutions and they can cover all types of continuity plans.

The user recovery plan can evolve to integrate, for example, the availability of USB keys containing an alternative system.

Main issues experienced during cybercrisis managemenent



Functionnal integrity control chain



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 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.

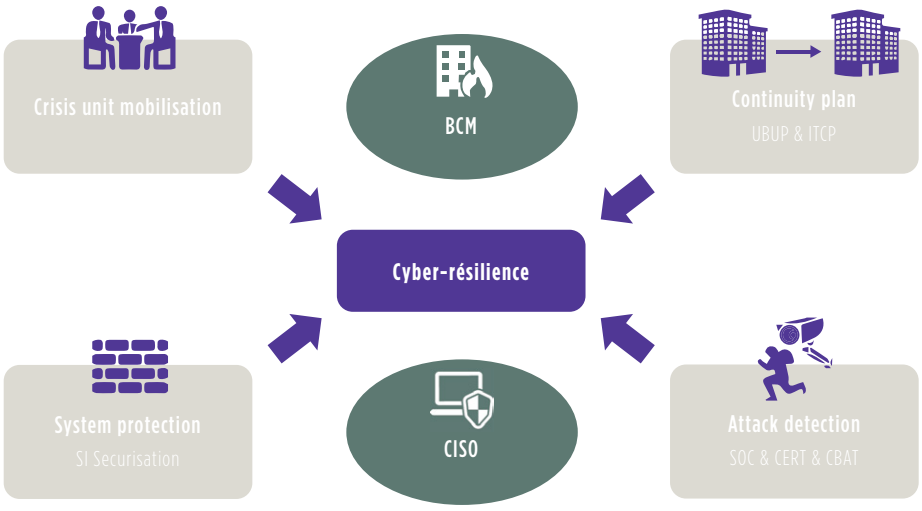
These often major evolutions must be part of an existing recovery strategy review, so that one can assess their vulnerability and the interest of deploying new cyber-resilience solutions, in particular on the most critical systems. The evolution of Business Impact Analysis (BIA) to include this dimension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

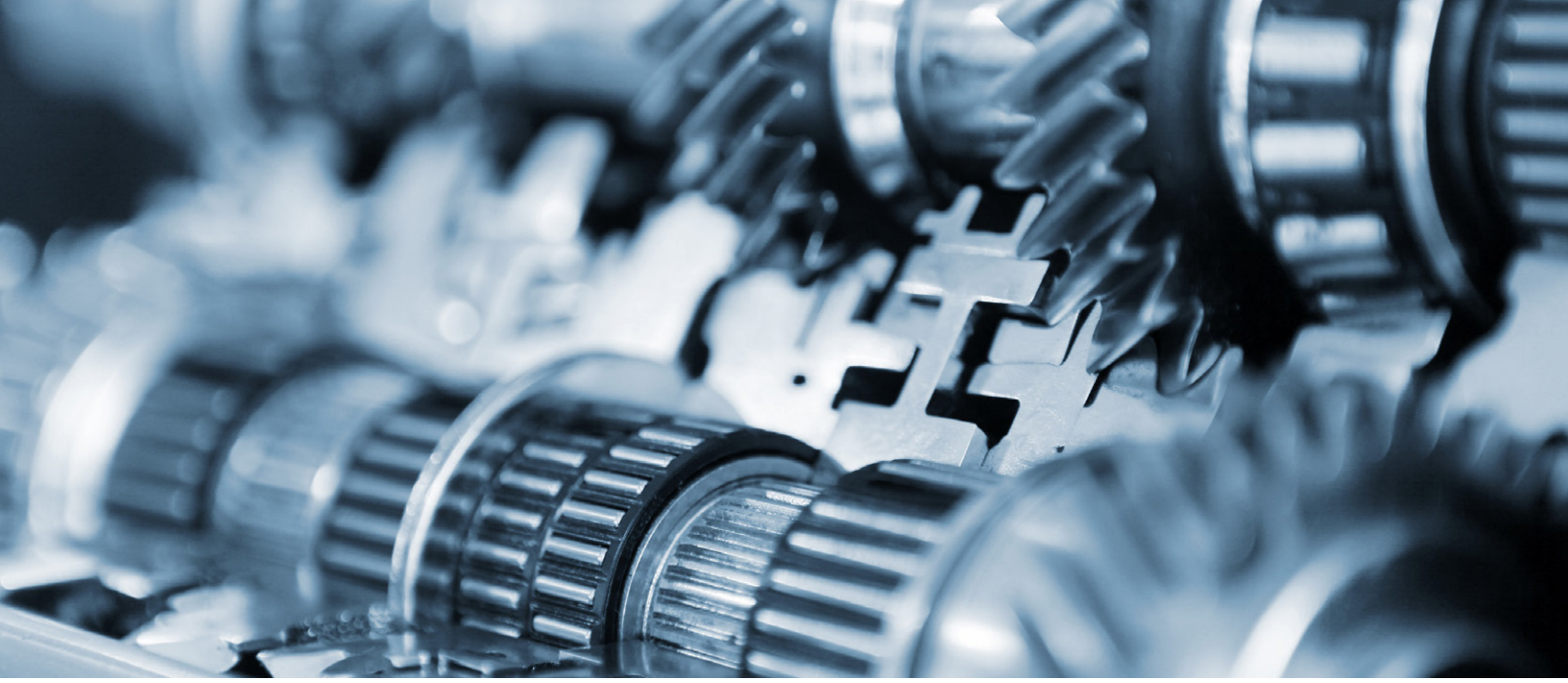
WITHOUT CYBERSECURITY, CYBER-RESILIENCE IS NOTHING

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!

Combining forces of the BCM and the CISO





INDUSTRIAL IS, SECURITY, SAFETY AND CYBER-RESILIENCE: A SQUARE PEG IN A ROUND HOLE?

The industrial world has worked for a long number of years on designing reliable systems to cope with material failures and their continuity is one of the major examples of best practice. Even if there are still few confirmed cyber-attacks, they have nonetheless put to the fore the weaknesses of industrial systems. In particular "safety" mechanisms can turn out to be inefficient too in the event of attacks.

Amongst these mechanisms, we can name the Safety Instrumented Systems (SIS). They are supposed to protect installations and limit impacts in the event of significant failure. They are designed to activate withdrawal mechanisms enabling the repositioning of an installation to a stable state (pressure, temperature, speed or other drifting) and enabling the installation to be placed back under control.

An installation's safety often relies essentially on these systems.

But this trust has been undermined by recent evolutions of these systems. Indeed, we have observed a strong trend towards pooling resources dedicated to industrial process operation with those dedicated to ensure its safety.

This pooling, more or less extended depending on the situation, can encompass sensors (verifying acceptable drifting and functioning limits drifting), SIS onboard security logic solvers (co-existing in a common SIS and process controller basket, or in some cases complete fusion of the controller and the SIS) or the network channel operation and safety flows on a common physical and logical link. This pooling is also found at the level of safety control and management applications that function on a single machine, or even on support systems like Active Directories.

For industrial security and safety managers the task is sometimes more complex than for management IS. Evolutions will have to occur as modifications are brought forward by manufacturers and suppliers. One should note that efforts have been acknowledged with regards to a regulation aiming to be more restrictive. Conducting crisis exercises with a cyber focus is a recommended first step. The cyber-resilience of industrial systems will only be achieved if security, continuity and safety spheres work together.

Anthony Di Prima

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).

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