RISKINSIGHT

WAVESTONE'S CONSULTANT RISK MANAGEMENT
AND CYBERSECURITY LETTER

CYBER-RESILIENCE

A NEW PILLAR OF CYBERSECURITY STRATEGY

SUMMARY

FOLDER

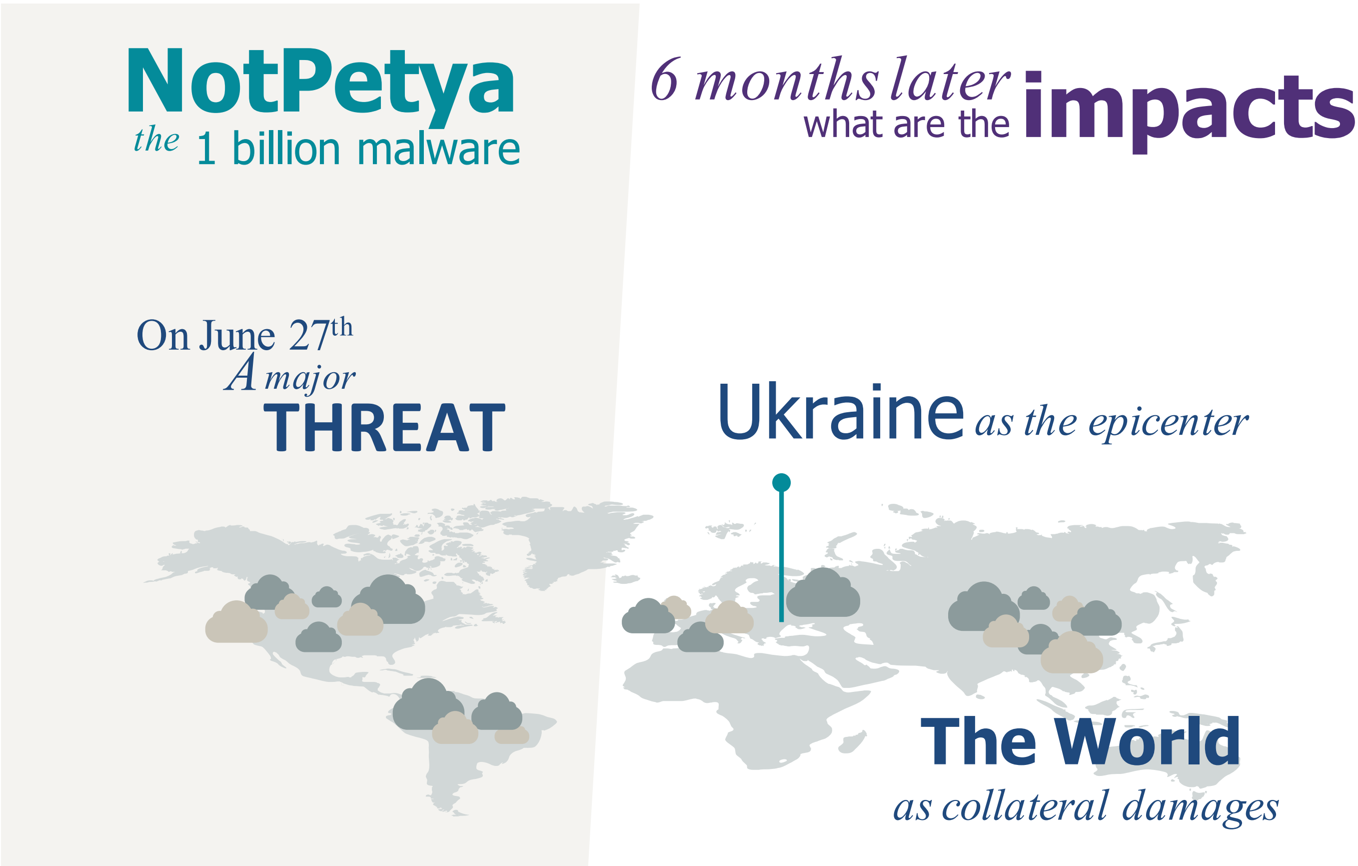
EDITORIAL

Summer 2017 has shown how global cyber attacks unfold in practice, especially with NotPetya. Although the full consequences of the "ransomworm" are still to be determined, Merck group already announced in late November 2017 that they expected the cyber attack to cost them more than 600 million dollars over the 2017 period!

Adding together the latest announcements, the 2 billion dollars threshold in lost revenues is clearly within reach. This is the first time such a high impact is measured following a cyber incident. This unprecedented escalation is rallying C-level executives who are looking for the means to limit the impacts of such attacks but also for the positions to adopt during an actual attack. We hope that the articles below will help you get a clearer view and plan the required actions.

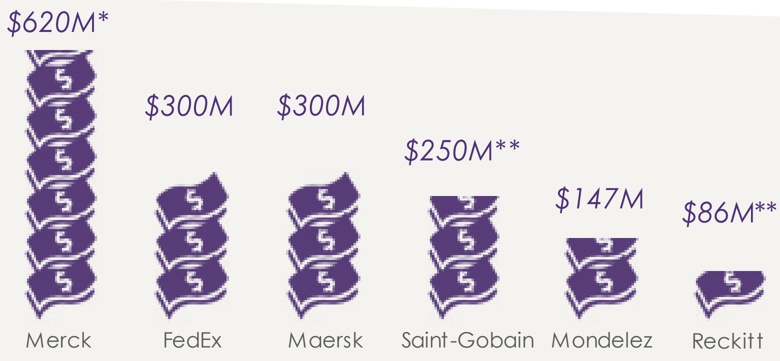
Gérôme BILLOIS
Partner Cybersecurity & Digital Trust

NOTPETYA: 6 MONTHS LATER, WHAT ARE THE IMPACTS?



Gérôme BILLOIS, Partner
gerome.billois@wavestone.com

Denis BLANDIN, Consultant
denis.blandin@wavestone.com

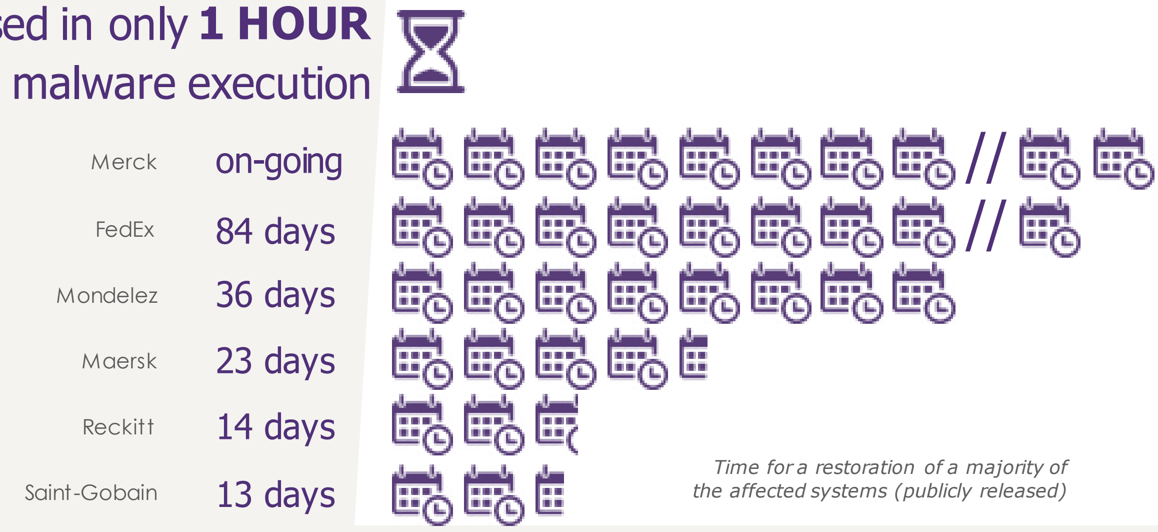


more than
1 billion $
of losses

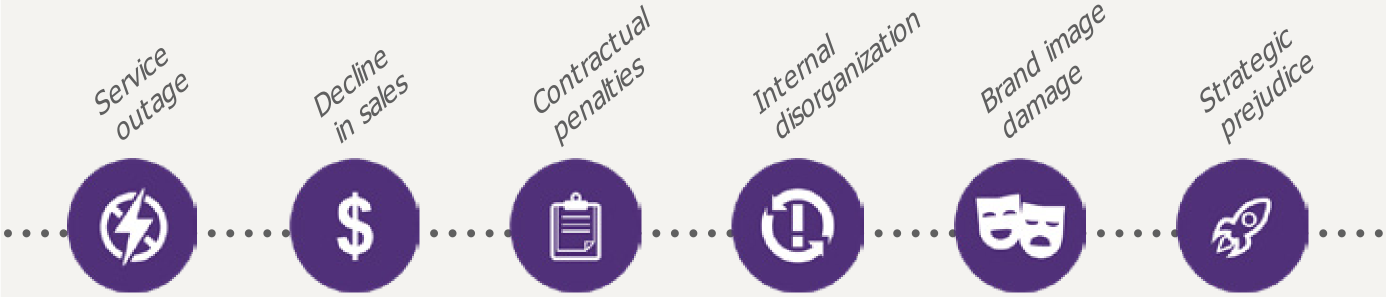
**Projection over Q4 2017 released by the company*
***Loss of revenue*

Top 6 of the financial losses due to this cyberattack (publicly released)

Weeks *of damages* caused in only **1 HOUR** of malware execution



Time for a restoration of a majority of the affected systems (publicly released)



CYBER-RESILIENCE: THE KEY ACTIONS

Successive cyber attacks, Wannacry and NotPetya, have highlighted the limits of current resilience and business continuity plans, as well as the full capacity of cyber threats to cripple Information Systems. The affected organizations paid a high price. What can we learn? What actions can we take to prepare for major cyberattacks? How can we ensure cyber-resilience?

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). This strategic element of resiliency is enacted to ensure the organization's survival against disasters whose magnitude may cause computing resources, communication infrastructures, buildings, and possibly even users to be unavailable.

Yet major cyber attacks, have not been taken into account when developing most BCPs, even though they can be as destructive in scale as either Wannacry or NotPetya, or, more often, lead to a loss of trust in the basic components of the infrastructure (network, access control, inventory, etc.). By Focusing on an availability agenda, organizations fail to address the issue arising from the simultaneous destruction or the loss of confidence in Information System (IS) caused by cyber attacks.

Moreover, these IS continuity plans are frequently intimately linked to the resources they protect and are equally affected by the attacks. For over a decade, continuity processes (either 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 improved operation.

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

WHAT VULNERABILITIES IN BUSINESS CONTINUITY SYSTEMS?

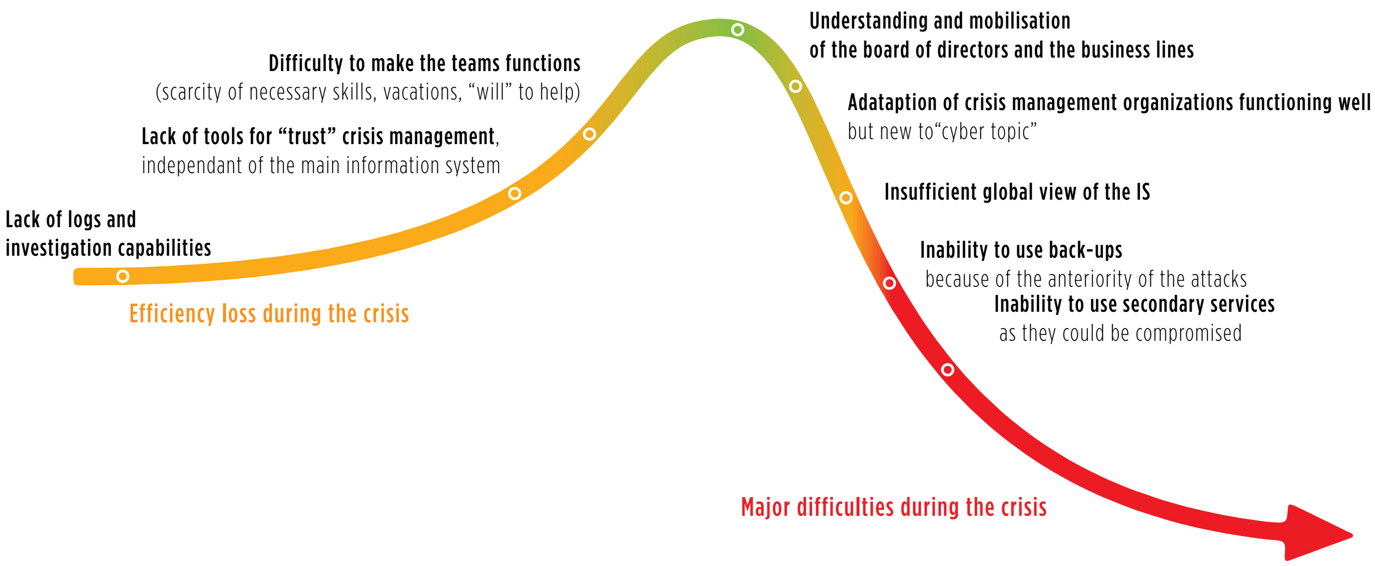
As an example, various dedicated and connected recovery stations in fallback sites were contaminated by NotPetya and were useless for the remediation.

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

Unfortunately, when systems have been deeply compromised, backups during this period may also include the malevolent elements such as malwares, base camps, or modifications meticulously operated by attackers beforehand, due to the fact that intrusions go undetected for a long period of time (detection often happens hundreds of days following the initial infection). In addition, the continuity of the backup systems themselves is often neglected. During the management of the NotPetya crisis, the backup management servers were also destroyed. Restoring them took several days, due to their complexity and 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 consideration of deliberate attack and as a result often lack advanced security systems. To compound on this, industrial IS has lifecycles of several decades which expose them to old vulnerabilities. Finally, the independence of control channels from the digital systems which they oversee is not always implemented.

Main issues experienced during cybercrisis management



TWO ILLUSTRATED MAJOR ATTACK SCENARIOS

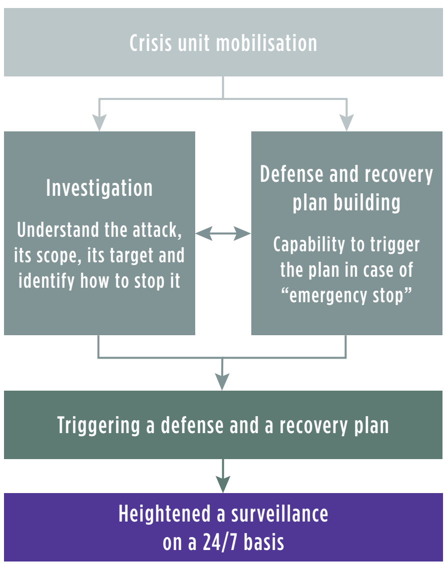
Logical destruction or the unavailability of a large chunck of an Information System

As evidenced 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 crisis, the situation is highly difficult since there is no longer any means of communication or exchange mechanism within the affected company, including ISD. Victims have outlined losses of several hundred of million euros following these attacks.

A compromise and loss of confidence in Information Systems

It concerns a targeted attack does not impact 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 Banglasdesh. These attacks also affected financial and payment data theft as was the case for several distribution groups in the United States including Target and Home Depot. The situation at the start of the crisis is complex since there is no 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.

Cybercrisis management method

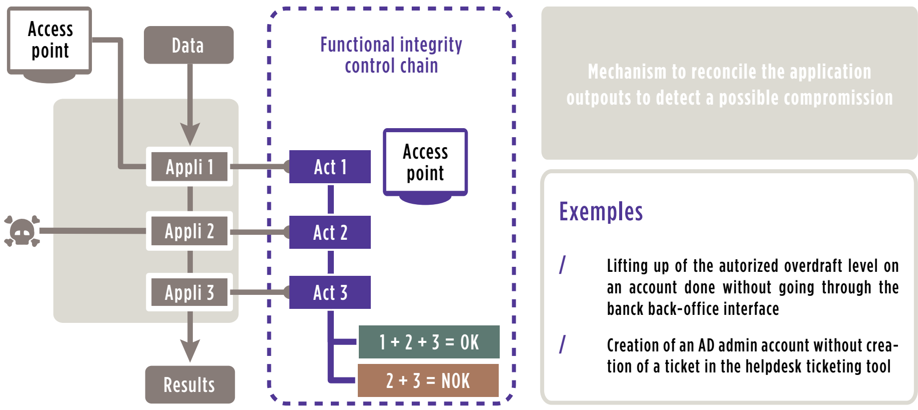


STRENGTHENING CRISIS MANAGEMENT

Cyber crisis 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?). Often, affected external parties such as lawyers, authorities, suppliers, and sometimes even clients themselves are not well-prepared on the subject matter. Thus, it is necessary to adjust existing plans that have not been designed to cater to the cyber threat aspects.

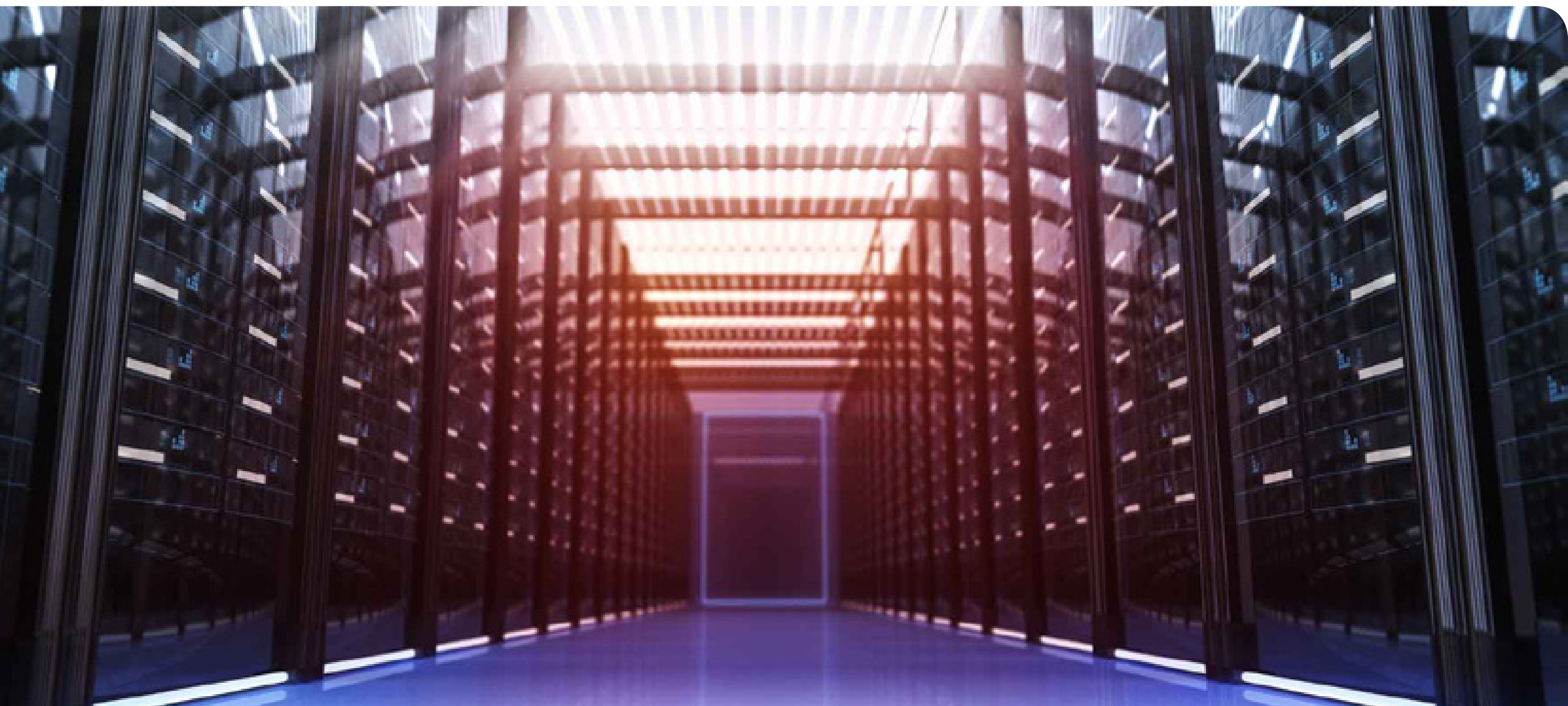
Even if they is an operational player in cyber crisis management, the CIO should not be over-utilized in either the investigation or the defense measures if it is detrimental to overall production and recovery. Anticipation of these kinds of measures is vital to the recovery effort. It is necessary to clearly identify the teams which need to be mobilized to respond to the crisis in a timely manner, and to organize the parallel activities of investigation and construction of the defense plan.

Functionnal integrity control chain



Beyond the organizational point of view, the CIO will have to ensure that they also have the investigation tools (mapping, search for attack signature, independent crisis management IS, capability to analyze 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 workstation) required to understand the activities that the attacker undertook 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 is a further recommended step. With that, it is essential to conduct crisis exercises to ensure readiness for when one actually occurs.



RETHINKING CONTINUITY PLANS

Continuity plans have to evolve to adapt to cyberthreats. Sometimes, this means they may have to be completely rebuilt.

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

The user recovery plan, for example, can evolve to integrate USB keys containing an alternative system which could be used in case of logical destruction of employee workstations. Some organizations have also decided to provision an allotted number of workstations directly with their suppliers to have them delivered quickly in case of physical destruction.

The IT continuity plan, on the other hand, can include new solutions which could be efficient in the event of a cyberattack. The most publicized one aims to build "non-similar facilities" by duplicating an application without using the same software, operating system, or production teams. It is an extreme solution, very costly and difficult to maintain, but one that is considered for specific, critical applications in the financial industry – most notably, payment system infrastructure.

Other less complex solutions such as adding functional integrity control in the business process have also been considered. The concept relies on the implementation of regular controls, at various levels and at different places within the application chain ("multi-level controls"). This enables quick detection of attacks. An alert could be raised in case of an interaction with technical layers, such as a modification of a value directly inside a database, without passing through regular business workflows (via graphical interfaces), for example. In another case, these mechanisms can also be applied to infrastructure systems by reconciling admin account creation request tickets with the number of accounts really in the system.

As a more intermediate complexity level solution, it is possible to implement a "floodgate", or as a system and network isolation zone. This floodgate – for example, the industrial IS – can be activated in the event of an attack and could isolate the most sensitive systems from the rest of the IS.

These, often major, develoments 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, particularly on the most critical systems. The development of Business Impact Analysis (BIA) to include this dimension can be a key first step.

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

ANTICIPATE FOR NOT BREAKING

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

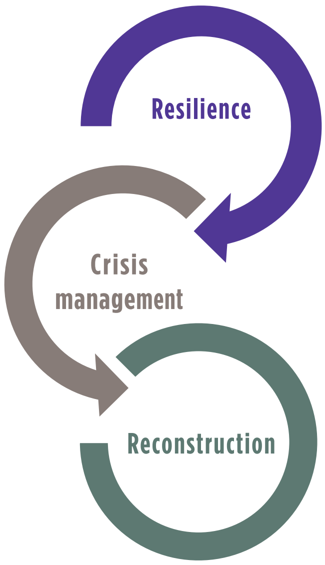
Limit amplification effect
(harden, partition...)

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...)

WITHOUT CYBERSECURITY, CYBER-RESILIENCE IS NOTHING

Implementing these new cyber-resilience measures requires significant efforts. Note that these efforts can be wasted if both these recovery solutions and the regular systems are not already appropriately secured and under detailed surveillance. The CISO is the key player to ensure that these often started but rarely finalized initiatives come to fruition. Help from the Risk Manager (RM), or the Business Continuity Manager (BCM) if such a position is in place, will be valuable. It is widely acknowledged today that it is impossible to secure a system 100%, which means that organizations have to accept the inevitability of an attack occurring, at which moment the RM or the BCM will make full use of their role.

Protect, detect, respond, remediate, and rebuild. These are the pillars of a strong cyber-resilience program which can only be attained if the BCM and the CISO roles combine their full range of capabilities and work hard, hand-in-hand!

Gérôme BILLOIS, Partner
gerome.billois@wavestone.com

Frédéric CHOLLET, Senior Manager
frederic.chollet@wavestone.com

CYBER-CRISIS, A FULLY-FLEDGED MEDIA TOPIC

Although they are based on similar objectives, methods and tools, crisis management and crisis communication necessarily appropriate the specifics of the issues they deal with to be relevant and therefore effective. In the case of a crisis of cyber origin, considering its characteristics and its exposure to often large numbers of users, requires specific anticipation and preparation. The first step is understanding the expected scale of media exposure.

ADDRESSING THE NEED TO KNOW AND THE NEED FOR REASSURANCE

Supported by the increased number of incidents and attacks on information systems, the cyber crisis has moved into the public realm. The democratization of its vocabulary is a clear indicator of the place that this subject takes up in the media. Data leakage, ransomware, hacktivist, DDoS, phishing, whistle-blower, these terms have left the server rooms and specialist blogs to make their way into national newspaper columns and most people's vocabulary. The cyber crisis is no longer a mere quality incident discreetly handled in-house but has become an event that arouses the interest of a broad audience. This interest transforms the cyber crisis into a communicational crisis. However, while this theme's new popularity is logically transposing into an increase in coverage, other elements justify a significant increase in solicitations, whether internal or external to the organization in crisis.

When the cyber crisis results in data leakage, for example, it is not only the subject of the crisis that is newsworthy, but its very object. In fact, when the data leaks or is stolen, its nature arouses curiosity, whether it is personal data, a State secret or simply a private conversation. This mechanic logically generates for many audiences both the need to know the unknown, and to make sure that they are not the victim. These two primary needs of curiosity and reassurance are the essential drivers of media coverage and more generally encourage the information consumer, the stakeholder, the client to fill that need and seek to obtain this information. The same logic assumes that the source of this information, in this case the legitimate data holder, addresses these requests and communicates on the incident.

Whether it's strategic events such as presidential elections or everyday private conversations on digital media that are compromised, the crisis' media effect is magnified by the extraordinary nature of the event. This is the result of both its supposed impossibility and the confidence that the public entrusts it. The sudden rupture of the trust placed in these «institutions» of major importance, erected in good stead in a 2.0 version of Maslow's pyramid, then generates itself the interest and the need to know, translated into an explosion of the number of requests for information to the organization in crisis.

Figure 1: Maslow Pyramid Example

COMMUNICATION WAR BETWEEN THE ATTACKER AND THE COMMUNICATOR

Cyber crisis communication is thus a specific exercise given the subject it deals with, but also by the nature of the actors present. In fact, when immeasurable sums of money are stolen without warning or institutions fall under «citizens» hacktivist attacks, opinion tends to sympathise towards the attacker perceived as a modern hero, a romantic pirate or a anonymous vigilante.

This public figure, aware of its image and the codes of the communication world, will of course be able to play this environment. Thus, the very methods of the attackers reinforce the central place of communication in the management of cyber crises. Attacks on political, ideological and militant grounds are no longer confined to the compromise of a system but send a message whose publicity must be maximised.

This obvious appropriation of the activists' specific methods is illustrated in several ways: prior warning of a DDoS, defacing a website, publication over time of proofs of a theft on social networks, dissemination of information such as exchanges of compromising private mail conversations, etc. If the attackers have learned to maximize the reputational impact of their attacks, they also use this lever to disrupt their target's crisis management and make a noise that will buy them time once their attack is discovered. While one of crisis management's key success factors of is regaining control of this rhythm and the publication of new elements, the cyber crisis inevitably leaves this power to a malicious third party.

This third party can also, if the compromise goes deeply, alter the company's means of communication. While it tries to respond to the need to express itself urgently and widely, this can severely hinder the fluidity of its communication. Without email, how to spread a message to employees? Without social networks, how to be close to the community and answer their questions?

RESTORING THE TRUST RELATIONSHIP THROUGH COMMUNICATION

Fascinated by the attackers and the magnitude of the attacks, the general public is nonetheless intransigent at a time when trust and data are the very value of a company. Intrinsically, preserving the first assumes the protection of the second. When the organization fails to achieve this goal, crisis communication is the only one able to restore this relationship of trust on which depends the future of the relation with customers and partners, who will or will not continue to entrust their data or the management of their tools, as well as their services to an organization.

This trust requirement also brings about, when it's is broken, the search for whom to point the blame. Although the reality of the facts is much more complex, the general public will easily assume that information system attacks are made possible by exploiting a vulnerability and therefore a fault.

A data leak is thus not only perceived as an attack perpetuated by a malicious third party, but also as negligence in the defenses of the company victim to the theft. The latter is automatically designated as responsible and its reputation is logically impacted. Even as the attackers have become professional, the attacks complexify and the absence of vulnerabilities is a myth, cyber-attacks are now a subject of crisis management and communication in their own right. Because of its potential impact on the general public's daily life and therefore its newsworthy nature, it forces the victim, considered to be co-responsible for its loss, to express itself.

TRY TO KEEP IT SIMPLE FOR BETTER CRISIS COMMUNICATION

Beyond defining a clear, shared and timely strategy, managing a cyber crisis with its particular rhythm and the obstacles caused by the attackers must be accompanied by a special communication which implies a final effort: keeping it simple.

Confronted by a cyber crisis, like any type of crisis, communicating implies being able to translate the events and corrective actions into clear impacts and to address them in a coherent manner. Of course, the complexity of the terms and the mechanics of a cyber crisis makes this exercise tricky and is another particularity to take into account.

In this context, through their ability to translate the technical cause into business consequences and more generally into layman's terms, the CISO and their team's role is central. During business as usual as well as in times of crisis, the CISO's mission is the responsibility for translating the facts and technical components not only into business impacts but also into understandable and convincing impacts for diverse non-expert audiences. They may also have to conceive or even bear responsibility for elements of crisis communication language in the same way that a human resources representative is exposed during a social crisis.

Without presupposing their exposure on a major TV channel's news program, information security experts' words will be expected on social networks, on professional networks, in the specialized press or in-house. In crisis communication, everyone is responsible for everything and everyone has to be prepared for it.

Thus, the subject of cyber carries a media power of its own; the immediate consequence of which is the considerable increase in expectations and requests to be informed from different divisions of an organization as well as from the public. If the impending occurrence of an information security incident involves a specific defense and continuity of operations planning, it also requires anticipation of these requests and an active preparation for this overall communication effort.

Swann LASSIVA, Consultant
swann.lassiva@wavestone.com

THE CLOUD: THE END OF IT BACKUP – OR A NEW WAY OF DOING IT?

Businesses are increasingly using cloud services (SaaS, PaaS, and IaaS) in their IT environments. They provide more flexibility on costs and can be more attractive than using conventional IT infrastructure. In 2016, in France, 48% of companies employing more than 250 people used it—an increase of 12 percentage points, compared with 2014. The greater availability of cloud infrastructure is often identified as an opportunity. However, the risk of failure of a service provider's data center is rarely addressed, even though its services rely on data centers that are decidedly physical and not in the cloud. Such data centers face the same threats as traditional data centers: natural disasters, human error, etc.

How, therefore, can backup be provided for these cloud infrastructures?

SAAS COMPUTER BACKUP: THE SERVICE PROVIDER'S RESPONSIBILITY TO PUT IN PLACE

SaaS (Software as a Service) is software that is made available on, and consumed directly from, the internet. It is managed by one or more providers. The customer does not have the wherewithal to carry out the backup activities is case of disaster (no access to raw data, source codes, applications that could duplicate the infrastructure, etc.), so it has to rely on the provider's goodwill.

Levels of disaster recovery are variable for SaaS, depending on the provider's degree of maturity

Three major trends are emerging:

/ **Providers who offer an inclusive disaster recovery plan.** As part of their standard offering, the provider offers recovery at a remote data center, usually augmented with outsourced backup. However, they rarely offer commitments on recovery times. Examples are the big SaaS players (such as: Office 365, SalesForce, and SAP), as well as some intermediate players (such as Evernote, and Xero);

/ **Suppliers who offer outsourced backup only.** In their case, there is no clearly established disaster recovery plan, as such. The customer then has to question the ability of the provider to restore backup files in the event of a disaster at the main site. Examples are intermediate suppliers (such as Zervant and Sellsy);

/ **Suppliers who don't mention the issue or do not have anything in place.** The subject of backup doesn't even get raised, so it's better to assume that nothing is being done. Small players are usually in this situation.

Getting contracts right is key

In the vast majority of cases, SaaS providers have no provisions in their contracts on how they will manage disaster recovery, even though they might stress their ability to handle that risk. In fact, contracts usually include default Act of God clauses stipulating that the supplier is not liable for a breach of contractual obligations if this is caused by an event beyond their reasonable control. The legal risks must therefore be addressed when framing the agreement, and these types of clauses should be removed to ensure an appropriate level of cover.

Just as they do when framing conventional contracts, customers must ensure that clear service level agreements are in place, in particular for disaster recovery. These need to cover:

/ **Recovery times** (Recovery Time Objective – RTO) and **data loss** (Recovery Point – RPO) in the event of a disaster;

/ The **provider's disaster recovery plan, including crisis management procedures**, as well as the obligation to carry out **conclusive tests** every year with real-world scenarios, as part of the plan, with the customer having the option to review the test report;

/ **Financial penalties** and the right to terminate the contract (in particular, with a provision to recover usable data) if commitments are breached.

IAAS/PAAS DISASTER RECOVERY: THE CUSTOMER'S RESPONSIBILITY TO PUT IN PLACE

Infrastructure as a Service (IaaS) is a standardized, automated offering of computing, storage, and network resources owned and hosted by a provider, and made available to the customer on demand. A Platform as a Service (PaaS) offering is similar to an IaaS offer, but it is different in that it only applies to software development stack (database, EDI, business process management...) according to Gartner's definition. Unlike SaaS, disaster recovery remains the customer's responsibility in both cases: IaaS/PaaS providers make services available in various data centers, and the customer is responsible for their use and configuration. Two solutions are available to customers using these services: to entrust things to a provider, or manage it themselves.

The market for cloud disaster recovery is not a mature one

Cloud disaster recovery providers are referred to by the acronym DRaaS: Disaster Recovery as a Service. Initially, DRaaS providers offered cloud-based IS disaster recovery of an "on premise" datacenter. But, today, they also offer to provide recovery for infrastructure already in the cloud, such as AWS or Azure. Levels of maturity remain very variable, depending on the provider and which cloud is used. Some DRaaS providers require that their own cloud is used for recovery, which means they cannot offer a PaaS recovery service.

As with SaaS, there are **no default contractual provisions**. Therefore, any guarantees required for data loss or recovery time will need to be negotiated. Suppliers generally promise to be able to tailor their offer to the customer's requirements! To ensure that the recovery performs correctly, the customer must plan for **disaster recovery tests** to be carried out regularly (we recommend once a year).

Operating your own disaster recovery plan, using tools offered by the supplier

For "on-premise" infrastructure, you will need to think about, and define, your DRP strategy right from the design phase. This strategy must include the option of performing tests to ensure a sufficient level of confidence in your plan.

Implementation can be simplified by the tools offered by cloud providers, and the high levels of standardization in cloud environments. The major players have set out, in white papers, the key guidelines to follow in pursuing such a project (for example, AWS and Azure).

Conceptually, these DRP strategies remain close to those used in "on-premise" data centers.

There are four main ones:

/ **backup and restore:** simple backups of data and images of machines on a remote site, which are restored if an incident occurs;

/ **pilot light:** replication of databases and the provision of machines, in the form of images, ready to be used if an incident occurs;

/ **warm standby:** full replication of the main site (data and machines); the recovery site is undersized in performance terms but ready to scale up if an incident occurs;

/ **multi-site (or active-active):** the two sites are identical and share the load from users. If an incident occurs, the remaining site can scale up to cover all users.

Hybrid solutions that are better designed to take account of recovery time requirements, and cost and complexity considerations, can also be considered.

The real contribution that the cloud can make to DRP is the numerous tools that it can offer to simplify its implementation and activation.

As a result, data replication can be simplified for asynchronous geo-replication options (where multiple copies are replicated to other regions). The RPO varies, depending on the types of data and tools involved. Aside from this option, local data redundancy is almost always included.

The high degree of standardization also makes it possible to automate the recovery: the scripts or APIs made available by providers make it possible to automate deployment of infrastructures, resize instances (according to previously defined configuration), distribute loads and traffic, carry out IP addressing, etc., in order to considerably speed up a backup site's activation time.

The monitoring and alert tools, which are also on offer, are intended to facilitate in-service support and can be used to detect an incident in the shortest possible time, or in some cases, partially automate the activation of a backup site.

Lastly, this ability to provision new resources within a few minutes enables the associated OPEX to be minimized. **By using such a strategy, it's possible to make gains of 40 to 70% on the cost of DRP infrastructure**.

Toward greater support by providers?

During 2017, Azure is planning to offer an option to provide recovery for virtual machines hosted on its platform by enhancing its "Site Recovery" service. In fact, "Site Recovery", in its current form, offers to support traditional site backup, by using the Azure cloud to host the secondary site, but Microsoft wants to extend this service to provide a Recovery as a Service option. This tool would allow the automatic deployment of the secondary site (of the active-passive type), automatic data replication, and easier testing.

This option was available as a "public preview" at the end of May 2017. There is no equivalent project in train from the other main IaaS/PaaS providers.

THE CLOUD AND PROVIDER SYSTEMIC RISK

Backup of cloud-based services is dealt with differently, depending on the type of service used. SaaS recovery must be managed through contracts and are the responsibility of the provider, while IaaS/PaaS recovery, simplified by the tools available, remains the responsibility of the customer.

There is a risk of the widespread failure of a provider's hosting region as recent incidents have shown. Even though these incidents have been short-lived, or have had minor impacts, the possibility of widespread failure cannot be ignored. The issue of cyber-resilience, then, must still be dealt with. Using a second cloud provider can cover the risk of destruction, or a major outage of a first provider's infrastructure. This solution is very complex because portability between providers is a difficult issue. For now, there are few companies that have risked it, although Snapchat is an example: it uses Google's cloud for its production, and plans to use Amazon's for its DRP within five years.

Etienne LAFORE, Manager
etienne.lafore@wavestone.com

Lesly MERINE, Senior Consultant
lesly.merine@wavestone.com

Valentin LEMENUT, Consultant
valentin.lemenut@wavestone.com

Director of the publication: Frédéric GOUX
Editor-in-chief: Gérôme BILLOIS
Contributors: Denis BLANDIN, Frédéric CHOLLET,
Swann LASSIVA, Etienne LAFORE, Lesly MERINE, Valentin LEMENUT
ISSN 1995-1975

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.