WAVESTONE

RISKINSIGHT

LETTER FROM THE WAVESTONE CYBERSECURITY
AND DIGITAL TRUST CONSULTANTS

CYBERSECURITY AND THE NIS DIRECTIVE

A CHALLENGE OF CONSISTENCY FOR THE EUROPEAN UNION

EDITO

Cybersecurity in Europe, an opportunity to seize today!

The NIS Directive was adopted in August 2016. This directive lays the foundations for a European cybersecurity framework. It emphasises the need for countries to secure their own infrastructures and to function consistently across the continent. In order to achieve such consistency, each country should harmonise their security approaches and practices. This will prevent large pan-European companies from operating in a fragmented regulatory environment, which would otherwise render their compliance efforts useless.

The regulations on personal data protection highlight that the directive is a prerequisite for meeting subsequent European regulation, which will be more significant. In order to make the NIS directive successful, it is necessary to ensure consistency among security principles at a European level. More detailed information on this topic can be found in our paper. Our Risk Insight letter concludes with thoughts about a new security model to comprehensively tackle 2020, our view on incident detection, Hong Kong regulatory developments and a proposition for the security of self-driving cars.

Gérôme BILLOIS
Senior manager Cybersecurity & Digital Trust

OVERVIEW

DOSSIER

FOCUS

CYBERSECURITY AND THE NIS DIRECTIVE: THE EUROPEAN UNION FACED WITH A NEW DUTY OF CONSISTENCY

The European NIS directive (The Directive on the Security of Network and Information Systems) sets out measures designed to ensure a "heightened level of security for networks and information systems within the Union." To achieve this, it puts in place a formal framework for cooperation on cybersecurity and requires member states to strengthen their national capabilities by identifying their critical stakeholders, in order to implement security rules and monitor their application.

As its name suggests, the NIS directive is neither a law nor a regulation. It provides an objective to work towards, but leaves the choice of how to get there open. As with any directive, it must be transposed into law by each member country, who will establish the means of reaching the objective. The French Military Planning Law (LPM) or the German IT Security Act are examples of where this has taken place. In order to prevent a variety of interpretations from inhibiting effective implementation for Pan-European companies, consistency is the challenge that member states and the European Union will need to grapple with between now and 2018.

DECODING THE NIS DIRECTIVE

Unlike texts such as the GDPR (General Data Protection Regulation), the NIS directive provides for a minimum level of harmonization. Member states can add provisions or retain ones in their national legislation, in order to achieve a higher level of security than that provided for in the NIS directive.

Establishing a framework for cooperation between EU member states

At a European level, the directive establishes an **NIS Cooperation group** that is responsible for supporting and facilitating strategic cooperation between member states, especially through the exchange of information and good practice. This group will bring together the European Commission, ENISA - the European Network and Information Security Agency - and the representatives of the member states.

Moreover, the cooperation results in the implementation of a **network of CSIRTs** (Computer Security Incident Response Teams), bringing together the **CERT-EU** and each member state's **CSIRT**, whose existence in the first place is required by the directive. It is responsible for **promoting operational cooperation between member states**. ENISA will provide the administration of this network, and the European Commission has observer status.

Strengthening national cybersecurity capabilities

Each member state will adopt a **national strategy** by setting objectives and appropriate legislation in order to achieve a high level of national security.

For that, each country must, as a minimum, set up a **competent authority** responsible for transposing the directive into law. This authority can be separate, as is the case in France with ANSSI (National Agency for Information System Security). These authorities are advised to approach ENISA for assistance. A **national CSIRT** must be appointed. With responsibility to manage national incidents, its mission is to make people aware, to share information about risks and incidents, and to report incident notifications to the appropriate bodies.

This **European cybersecurity governance**, firmly centered on cooperation between the European institutions and member states, and played out through the NIS directive, is an unprecedented approach, to say the least.

Providing security through each state ensuring the cybersecurity of its "operators of essential services"

The entities identified by countries as being essential in terms of carrying out critical activities must implement measures to understand the risks and their impacts. These operators are also **required to notify** the appropriate authority immediately of any incident that could significantly impact the continuity, availability, and integrity of the service. The view of the impact, which the entity can assess freely, depends on the number of users impacted, the duration of the incident, and its geographic scope.

The establishment of common European cybersecurity laws for digital service providers

The directive also affects new players (excluding very small businesses) who are rarely affected by these schemes: the "digital service providers." Included in this are companies that play a significant role in the digital sector, namely search engines (Yahoo, Google, etc.), cloud computing (Dropbox, Google Documents, etc.), e-commerce sites (Amazon, eBay, etc.), and also online marketplaces. Their obligations are slightly less onerous (specific rules at member state level and less demanding notification obligations) as their activities do not directly impact people's lives, but affect the economy. It is, however, a major change for these stakeholders, who are now considered essential for the proper functioning of countries and their economies.

What are the timescales?

Between the date that the directive comes into force and its transposition into national law, a period of two years will be required.

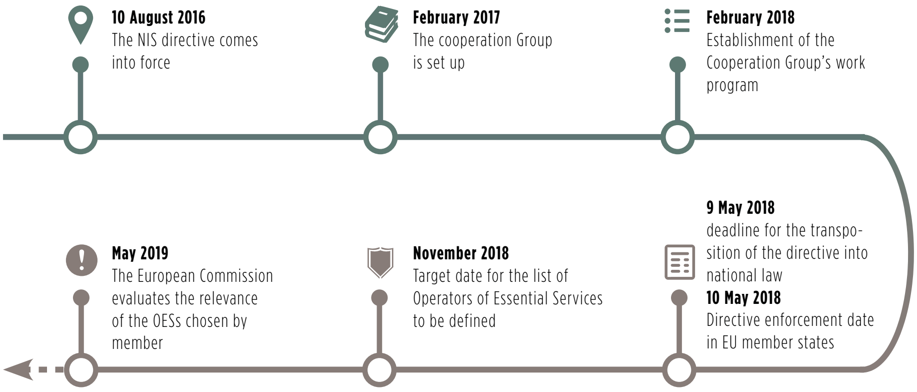
However, while the transposition into national law is an important deadline, it's not an end in itself. Aside from transposition, is the whole issue of effective implementation by the parties concerned. This varies not only according to the current legislation in the country but also as a function of the approach it takes to determine security measures. A country may opt for a collaborative approach with stakeholders which will, therefore, be more time-consuming than simply applying best practice from the top down.

WHAT ARE THE CONSEQUENCES FOR BUSINESSES?

Freedom of implementation by country

The directive applies to public and private operators. The companies that are affected by its security obligations are those with an important role in society and the economy: operators that provide Operators of Essential Services (OESs) The affected sectors are: energy, transport, banking, financial markets, health, the supply and distribution of water and digital infrastructure.

Transposition of the NIS directive



10 August 2016
The NIS directive comes into force

February 2017
The cooperation Group is set up

February 2018
Establishment of the Cooperation Group's work program

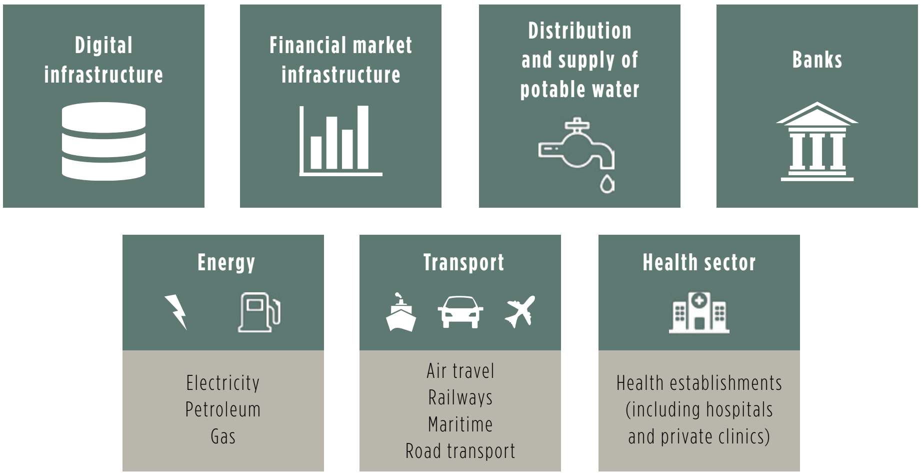
9 May 2018
deadline for the transposition of the directive into national law

10 May 2018
Directive enforcement date in EU member states

November 2018
Target date for the list of Operators of Essential Services to be defined

May 2019
The European Commission evaluates the relevance of the OESs chosen by member

Sectors affected by the NIS directive



Digital infrastructure

Financial market infrastructure

Distribution and supply of potable water

Banks

Energy
Electricity
Petroleum
Gas

Transport
Air travel
Railways
Maritime
Road transport

Health sector
Health establishments (including hospitals and private clinics)

Currently, however, each country has its **own list**. For example, France has 12, including its "military activities"; the UK has 13, some of which are very specific, like "Coastguards"; Poland has 9, including "systems that relate to the production, use or storage of radioactive substances and pipelines". A rationalization process will be required, and potentially one of identifying new players too, in particular, the "digital services providers."

Overarching principles and obligations but no precise measures

There are numerous obligations on Operators of Essential Services as a result of the cybersecurity directive.

The operators concerned must take appropriate measures to prevent **incidents resulting in compromise** in their networks and information systems. In this regard, to ensure compliance, the appropriate authorities can order audits by independent bodies and issue binding instructions. It is also incumbent upon operators to take appropriate technical and organizational measures to **manage security risks**.

Finally, the directive sets out an **obligation to notify** the appropriate authorities in the event of hacking and an incursion into the information systems of the OES. This is a major change for many countries and stakeholders in the field of cybersecurity.

The directive imposes similar duties on **digital service providers**. Their obligations are slightly less onerous (specific laws at member-state level and fewer notification obligations). Furthermore, they only affect digital service providers that are within the purview of a given member state. This is deemed to be the state where the provider has its head office. If the latter is in a state that is not a member of the EU, but it provides services that are covered by the scope of the directive, then it is deemed to be «represented in the EU.” The company will, therefore, come under the jurisdiction of the member state(s) in which it operates.

The final highlight of the directive is the provisions on the criminal liability relating to players. Member states should therefore plan for effective, proportionate and dissuasive measures.

In short, the directive lays down principles and obligations, but does not go as far as imposing security measures themselves. This will fall to the member states.

FRANCE, A CYBERSECURITY PIONEER, DELIVERS THE FIRST EXPERIENCE-BASED FEEDBACK

A gradual deployment over three years

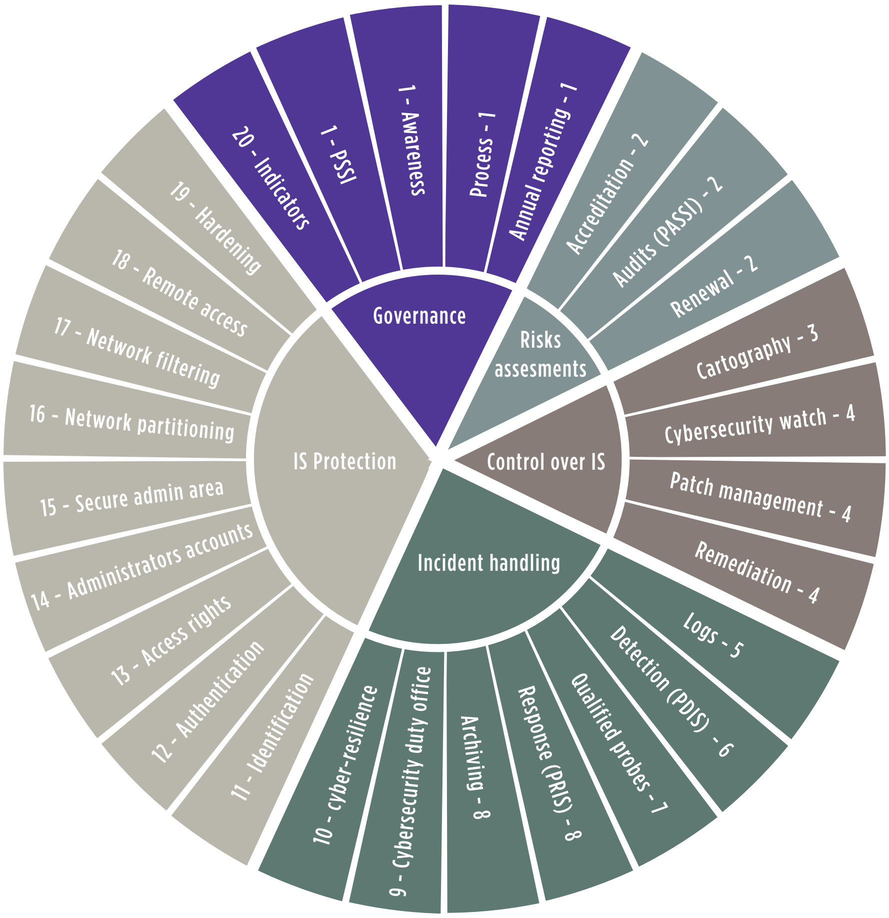
A pioneer in the implementation of cybersecurity policy for its operators of vital importance, the equivalent of operators of essential services in the NIS directive, France incorporated these requirements in its Military Planning Law following the direction set by a 2013 white paper on defense and national security. The law sets out measures for the **strengthening of protection, and for the defense of, information systems** against cyberattacks, espionage, destabilization, and sabotage. It is the legislative tool that allows **Operators of Vital Importance** (OIV) to the country, whether they are public or private, to better protect themselves, and for the ANSSI to better support them in the event of a cyberattack.

Announced on 18 December 2013, the implementing decrees relating to digital-trust service providers and the OIVs’ IS security were not published until 27 March 2015. The latest sector decrees were published and implemented at the beginning of December 2016. Moreover, it is important to note that the Military Planning Law requires the use of providers and products that are not yet all available. The French experience thus demonstrates that looking beyond promulgation of information, the **timescales for implementation** may be fairly lengthy. It should be noted, however, that France has chosen to take a **collaborative approach** with its OIVs, which partly explains the period needed for implementation.

Specific rules tailored to sectors

Several requirements are imposed: the need to adhere to **specific security rules**, to have access to **appropriate equipment and competent providers**, detect security

L’exemple français : 20 règles pour promouvoir les bonnes pratiques



events, mandatory notification of security incidents, regular security checks sponsored by the National Security Agency for Information Systems (ANSSI). The **sanctions** applicable to OIV companies that do not meet their obligations amount to €150,000 for the OIV's senior officer, and €750,000 for it as a corporate entity.

It is important to note that the requirements only cover VIIS (Vital Importance Information Systems), not the OIV 's entire IS. On the other hand, feedback on identifying VIISs shows that views of what is "vitally important" differ between the company (whose aim is to ensure its own survival) and that of the state (whose aim is to ensure the security of its citizens.) In practical terms, this means that commercial systems for sales and billing are often not registered on the VIIS list.

In terms of organization, OIV **compliance** with the LPM begins with a **gap analysis** between existing provisions and what is required. The next step is to identify the critical systems and their boundaries. Finally, the OIV must supply the **budget** required for compliance. On-the-ground-feedback shows that budgets for large companies lie **between 5 and 20 million Euros depending on the complexity and number of** VIISs.

Senior management gets involved It is now clear that the LPM has engaged management at the highest levels in companies. It has gone well beyond the traditional scope of cybersecurity and is becoming a real opportunity for Heads of Information Systems Security to bring security challenges to the attention of senior managers who have now properly grasped the issue. This development must be replicated at the European level.

THE NIS DIRECTIVE, AN INHERENTLY CONSISTENT OBLIGATION

Challenge for major European players

The NIS directive **sets a cap** on the formulation of principles and obligations. However, it is the member states that will have the task of identifying their critical sectors, their OESs, the digital service providers under their jurisdiction as well as the security measures that result. **Minimal harmonization** leaves them free to go beyond the list of sectors provided and define security requirements. On the other hand, as a consequence, **cybersecurity obligations could, therefore, vary from one country to another**... for the same company with subsidiaries in various European countries. A company may also be identified as an OES in one country, but not in another.

It is, therefore, essential that players, whether they be European institutions, or public or private sector companies, grasp this subject fully, straightaway, in order to ensure consistency. Without this, the security of networks and information systems in Europe could become a real **headache** that would r**un counter to the spirit of the directive**: harmonization at European level.

The key roles of ENISA and of the organization it will become

ENISA's mission is to ensure a high level of network and information security. It operates as an expert body on network security and information to national authorities and European institutions, and **promotes the exchange of good practice** as well as **facilitating contacts between institutions** (both national and European) and businesses. As a result of its role as a facilitator, this European Agency **has the capacity to bring consistency** to a range of national strategies.

This is also a route that has been used for several other initiatives. Notable among these are the closer ties between the French and German agencies, ANSSI and the BSI, developed during a joint-working session, in 2016, on building Europe-wide cybersecurity. Also worthy of note is the Polish Government's invitation to ANSSI at the CyberGov forum in May 2016 to share the feedback from the French experience. These initiatives reflect an encouraging level of awareness among some players. The challenge remains the question of their roll-out at European level and their capacity to deliver a unified and harmonized set of regimes, across the EU, by May 2018.

Gérôme BILLOIS
gerome.billois@wavestone.com

Étienne CAPGRAS
etienne.capgras@wavestone.com

Thibault JOUBERT
thibault.joubert@wavestone.com

Esther LYONNET
esther.lyonnet@wavestone.com

TIME FOR SOCS TO TAKE STOCK

The early 2000s saw the creation of the first teams, as initiatives to address the first large attacks of viruses. Ten years later, operational teams in a SOC (Security Operation Center) must meet challenges of a different order of magnitude with the multiplication of targeted attacks: ever more efficient and rapid detection are required to be able to respond effectively.

What are the difficulties that these teams face on a daily basis? How can they remain effective as attacks by cyber criminals become increasingly sophisticated?

SIEM: A CORE TOOL FOR THE SOC... AS LONG AS IT'S WELL IMPLEMENTED!

The emergence, some ten years ago, of tools like **SIEM** (Security Information and Event Management), has enabled operational security teams to automate surveillance activity, simplifying the analysis of security events from multiple sources (antivirus console, proxy, Web Application Firewall, etc.). This tool has also made it possible to correlate multiple events from hardware or a diversity of applications, **allowing advanced threat scenarios to be detected**.

However, putting in place robust SIEM requires taking an approach where **investment levels** are proportional to the complexity of the information system being monitored. In fact, the value of SIEM relies both on:

- **The presence of contextualized controls** in the information system, in particular with respect to the sensitivity of the assets being monitored;
- **The analysis and implementation of threat scenarios** developed and adapted to address the challenges of the company's business.

Looking at the scope of surveillance, the first type of equipment to be integrated is typically **security equipment** because this is configured - by design - to produce data that can be used by operational teams. Having said that, the integration of this kind of equipment is often limited to **simple retranscription** of existing controls, something that does not make use of the benefits of event correlation that SIEM offers.

However, the integration of business applications is more difficult, mainly as a result of the different needs of business and security teams. The main concern for business functions is usually the unavailability of an application (or some of its features), while security teams need to address a **more comprehensive range of risks**. These might be **unavailability**, **integrity of data being compromised**, or **leakage of confidential information**.

For this reason, it is essential to **educate business functions** about security issues, in order to develop realistic threat scenarios that are tailored to each area. Moreover, these applications do not traditionally have advanced functionality in terms of security. As a result, it is difficult to operate an effective monitoring system (configuring complex logs to be sent, log files with little explanatory wording, etc.).

In general terms, too simplistic an implementation of controls in SIEM renders the SOC's activities inefficient. Surveillance teams will then find themselves **drowning in "false positives"** , and security events are dealt with on a piecemeal basis instead of being **analyzed as a whole** in order to detect real threat scenarios (for example, unauthorized authentication taking place on a server, followed by antivirus measures being disabled and fraudulent transactions being executed should be treated as a single incident that needs to be investigated).

SOC TEAMS INSUFFICIENTLY INTEGRATED INTO THE SECURITY STRUCTURE

In addition to the problems related to the poor implementation of SIEM discussed above, there can also be issues in terms of **organizational structures**.

SIEM is often perceived as a "**Black Box**" by Level 1 and 2 analysts in SOC teams. This is normally due to their ignorance of the production environment (such as the identification of critical assets and interactions between different systems.) The incidents detected through SIEM may then all be treated at the same level, without any prioritization.

To maintain a sufficient level of skill within operational security teams, **internal IT and technology watch** must be carried out by Level 3 investigators, so that it can then be communicated to Level 1 and 2 analysts. Tasks such as the **presentation of new IOCs** (Indicators of Compromise) can then come in as a complement to the detection rules, allowing teams to make efficiency gains in the way they approach incidents. These types of initiatives will contribute to **continuous improvement** of the service's capability, avoiding its degradation over time.

In addition, teams **need to continually participate in a range of security initiatives** initiated at the global IT organization level, such as infrastructure or application-security projects. In addition, crisis management exercises need to be organized to test the various processes and tools in place, and to allow colleagues from business functions and security teams to discuss their respective roles in the event of a crisis.

In a world where cybercrime is constantly reinventing itself (as demonstrated by the recent attack on the systems of SWIFT, the global financial messaging system) operational teams are increasingly being required to broaden the scope of their activities. The **constant pressure** being exerted, in particular by decision makers, tends only to exacerbate issues related to the poor **implementation of controls** and ignorance about real threat scenarios. Good surveillance requires more than just the sending of logs within a SIEM system; project teams must be committed to embracing and implementing the entire process in order to integrate the new areas: identification of attack scenarios, implementation of collection mechanisms, creation of detection rules, testing and putting into production. Ignoring any one of these stages may render the collection of logs virtually useless.

WHAT DOES THE FUTURE HOLD FOR SOCS?

There are many factors on the horizon that will disturb the ecosystem for operational security providers (also named MSSP Managed Security Service Providers).

In fact, **France's LPM** (Military Programming Law) will require all Operators of Vital Importance» (usually named critical infrastructure providers), who use external cybersecurity providers to ensure that they use only "**Certified Security Incident Detection Providers**." A range of prerequisites will be required to qualify for certification, such as the **compartmentalization of customer data or the establishment of dedicated administration areas**, which are only accessible by the service provider, and through which the logs will be collected, before forwarding for SIEM analysis. These factors will entail numerous changes in the organizational structures and infrastructure in place today at most of the MSSP providers.

Furthermore, the increasing proportion of cloud-based solutions in business information systems adds a new complexity: that of **collecting logs from external providers, especially cloud based ones**. As a result, a new breed of players has appeared in the security market: **CASBs** - Cloud Access Security Brokers. What do they offer? The capacity to address cloud-related security issues. These actors position themselves between the users and a variety of cloud-related services, offering new safeguards, such as the use of APIs to directly detect threat scenarios (for instance the creation of log files when an application is accessed) and the integration of this data into SIEM analysis.

AND TOMORROW'S OBJECTIVE? TO GROW IN MATURITY

Operational security still has **many challenges** to overcome. Most companies are currently ensuring at least the **minimum levels required** for their information systems and the maturity of their teams allows them to protect against a simple range of threats (viruses, spam, etc.). However, the current approach **requires an overhaul** to meet the new challenges in cybersecurity, in order to protect against **opportunistic threats** (lone hackers) and **targeted activity** (cyber-mafia attacks, governments, etc.), which are more complicated in detection terms.

Against this backdrop, and given increasing legal obligations, SOCs have, and will continue to have, a very important role to play, requiring **in-depth technical expertise** as well as the ability to **integrate into projects the security requirements for an efficient detection**.

Hamza KHARBACHI
hamza.kharbachi@wavestone.com

Hugo MORET
hugo.moret@wavestone.com

HONG KONG LAUNCHES A MAJOR CYBERSECURITY PROGRAM FOR ITS BANKING INDUSTRY

At the end of June 2016, while SWIFT (the worldwide financial messaging system) was disclosing substantial losses due to cyber-attacks, the authorities of Hong Kong were announcing new regulations for the financial institutions.

During the 2016 edition of the Cyber Security Summit – one of the main local cybersecurity events – the Hong Kong Monetary Authority (HKMA) announced the launch of its CyberSecurity Fortification Initiative (CFI), a multi-year approach to strengthen the security of local banks.

Here are the main points to keep in mind about this initiative, which brings best-of-breed cybersecurity international practices, but also an innovative approach to cyber threat intelligence.

A THREE-FOLD INITIATIVE TO IMPROVE THE LEVEL OF SECURITY

The CFI is an initiative on which the HKMA has been working to strengthen cyber-resilience (i.e. the capacity to resist/survive cyber-attacks). It targets all the Authorized Institutions (AIs), in other words the banks of Hong Kong. It is underpinned by three pillars:

Cyber Resilience Assessment Framework

This framework will have to be deployed by each bank, thus allowing the HKMA to "get a holistic view of the preparedness of individual AIs as well as the entire banking sector".

It consists of 3 steps:

/ **Inherent risk assessment**: an evaluation of an institution's riskiness. It includes technological and business factors that will require a good understanding of both areas. The risk level will be rated as High, Medium or Low.

/ **Maturity assessment**: an evaluation of the institution's actual level of maturity in terms of cybersecurity

/ **Intelligence-led Cyber Attack Simulation Testing (iCAST), only for banks with High or Medium risk level.** The goal is to simulate cyber-attacks not only from a technical perspective, but also taking into account the "people" and "process" elements.

While all the details are not yet public, the first two steps are similar to the United States FFIEC Cybersecurity Assessment Tool, which has been deployed by many major banks since 2015. A matching has to be done between the risk level and the actual maturity level. In case of gaps, the bank will have to provide a roadmap to fill them.

iCAST is more innovative as a regulatory requirement, in the way that it does not only rely on penetration testing, but will also replicate real-life attacks, based on specific and up-to-date threat intelligence. This type of testing is referred to as "red team". As of today, it is the most realistic way to test the actual security level of an organization.

Professional Development Programme

This programme aims at improving the overall skillset of security professionals, by implementing a certification scheme and trainings that will offer three levels of competence: "foundation", "practitioner" and "expert". The British CREST will be part of this professional development, and suitable arrangements will also be introduced to "ensure that relevant or equivalent experience and expertise in the cybersecurity field will be appropriately recognized".

Cyber Intelligence Sharing Platform

In cyber-warfare, as in conventional warfare, threat intelligence has become key. Each company can develop its own skills and methods, but the very success of intelligence goes through sharing the information. Therefore, the HKMA is going to launch a Cyber Intelligence Sharing Platform, with access open to all the licensed banks in Hong Kong. Its goal will be to offer a secure and comfortable system to share relevant data, without compromising proprietary information.

What are the next steps for banks?

For banks in Hong Kong, few milestones were defined:

- **Starting from end of May 2016, a three-month consultation** has been launched by HKMA with the banking industry, in order to have feedbacks and comments on a draft version of the risk-based Cyber Resilience Assessment Framework.
- It is important to note that HKMA demands an **involvement of the AIs' Boards or senior management**. The assessment will have to be conducted by "qualified professionals who possess the necessary knowledge and expertise".
- HKMA has worked with the professional and public organizations to **roll-out the first training courses and set-up the Cyber Intelligence Sharing Platform** by the end of 2016.

EVOLVING STANDARDS IN HONG KONG

This move by the HKMA falls within a rapidly evolving regulatory context in Hong Kong. Several game-changing approaches will indeed shape the future of information security in the coming years. Among others, we can list the recent circular on cybersecurity that targets organizations regulated by the Securities and Futures Commission (SFC), and the upcoming review of the data privacy laws.

With around 200 banks, Hong Kong clearly takes the full measure of the cybersecurity challenge in order to keep its position as a leading financial hub in Asia.

An Authorized Institution in Hong Kong is an institution authorized under the Banking Ordinance to carry on the business of taking deposits. Hong Kong maintains a Three-tier Banking System, which comprises banks, restricted license banks and deposit-taking companies. Authorized Institutions are supervised by the HKMA.

Chadi HANTOUCHE
chadi.hantouche@wavestone.com

AIRLINES: TOMORROW'S SECURITY MODEL?

To illustrate its different approaches, the world of cybersecurity looked first to the image of the castle, and then to the airport. For the next phase of development, it might be that of the airline.

For years, the cybersecurity industry has been trying to explain the complex concepts it grapples with every day. It is a major challenge to persuade business functions and leaders, or simply to explain to users what the cybersecurity teams are doing. Today, information systems are undergoing major changes, involving a rethink in the way that security is configured. But then, what's the right model to turn to to persuade decision makers?

WE'VE GONE FROM THE CASTLE TO THE AIRPORT... BUT WHAT'S NEXT?

In 2008, we set out our initial view of developments in security models. The historical model, one based on perimeter security, was, at that time, illustrated by the image of a castle. A fort-like castle with impenetrable high walls (the perimeter), a drawbridge (the firewall), but also a central area accessible to all (the non-partitioned, internal networks).

And then, as time went by, opening up the IS became a key element in successful digital transformation to allow more innovative uses (such as client direct access to application, data exahcnge with partners, cloud-based working, BYOD, etc.). The castle was, thus, transformed into an airport.

An airport open by default, with a hall providing information, or simply to do some shopping. But an airport with secure areas, like the tarmac and aircraft, where the most critical areas are protected. This model aims at opening up the IS while protecting the most critical assets. This is the model that most of the companies are currenlty deploying.

TOMORROW: THE INCREASINGLY DECENTRALIZED IS

Analyzing current developments, it is clear that the IS is going to change fundamentally. "Internal" ISs will reduce in scale and cover only historical, or highly critical, areas. External suppliers and clouds will proliferate, and come to hold a prominent position in the IS. They will exchange data directly between themselves, and interact in groups on complex business processes. The terminals consuming this information will diversify, incorporating client terminals, connected objects, or employees' own devices. Data, then, will flow in all directions, within systems and environments over which there is no direct control.

How to ensure cyber security in this new model will almost certainly rely on the creation of a central function: an overarching security control center. This will allow the various external providers (clouds, partners, etc.) and terminals to access the data according to their identity (person, role), but also their level of compliance (update version, encryption, location, etc.).

A MODEL INSPIRED BY THE AIRLINES

To explain this development, a simple image can be used. That of airlines! Today, an airline's most critical assets is aircraft. They are the equivalent of data in our information system. These aircraft are highly critical for these companies, they transport their clients and the airline's employee teams.

But airlines depend on a complex ecosystem to ensure that planes arrive safely. The airports who handle aircraft and passengers - like cloud providers can host data and process it. Airports are able to deal with aircraft from a range of airlines, assuring their safety and privacy, just as a cloud provider handles data from multiple clients.

Air traffic control ensures the overall functioning of the sector and the security of different flights.

When an airline decides to open a new route, it assesses security in the country and the airport, before taking a final decision: a process equally necessary before subscribing to a cloud-based service. And, depending on the level of security in the country and at the airport, the company may decide to add additional security measures, and even, at times, temporarily close the route in response to sudden developments.

Above all, an airline uses an operational control center, which tracks and monitors all flights and all its aircraft, and assures security levels at airports based on the information being fed back to it, or intelligence it receives from the security services (threat intelligence). In the case of an incident or crisis, it is the operations center that will take control and manage it, imposing new security measures if necessary.

A DIFFICULT MODEL TO IMPLEMENT

It is clearly this model, one of "dynamic confidence", with an assessment of access rights according to the security of those who access it (devices, servers, people, etc.), the ability to comprehensively monitor data wherever it resides, and to develop new security policies in a dynamic way; something that will be at the heart of cyber security in the coming years. This model will be required to fully embrace future innovations.

The model is still a challenge, although there are numerous moves in this direction. Of particular note are the "software defined perimeter" standard of the Cloud Security Alliance and Google's "Beyond Corp" initiative. So, this is the direction of travel for the coming years... and a good image to keep in mind if you want to explain it in simple terms!

Gérôme BILLOIS
gerome.billois@wavestone.com

CYBER CRASH TESTS: THE SECURITY SOLUTION FOR AUTONOMOUS CARS?

Autonomous cars represent the future of the automotive sector, and promise a major break with today's driving habits.

But recent events have shown that these vehicles are not immune from cyberattack. How to integrate efficiently cybersecurity concerns?

SOME VERY REAL RISKS: THE EXAMPLES OF CHRYSLER AND TESLA

Un autonomous car is, by definition, a connected car: GPS, sensors, and the internet - via 3G/4G. All these elements represent gateways into the car, which is, in this respect, nothing other than a network of dozens of specialized computers. These components manage the various parts of the vehicle. The steering wheel, the brakes, and the accelerator—each must be computerized in order for the "brain" of the autonomous car to direct them.

The combination of these external connections, and the computerization of the functions that drive the car, poses real risks today.

Considered a hypothetical scenario for a long time, autonomous cars' vulnerability to attack has been demonstrated in two symbolic cases. The first was the attack against the Chrysler Jeep, in the summer of 2015. After several years of research, Charlie Miller and Chris Valasek showed how they could remotely take control of a production vehicle. In August 2016, they demonstrated that they could go further still in their ability to control the driving functions. The second hit Tesla in September 2016. In the same vein, a Chinese research team at Tencent managed to penetrate a Tesla car and completely take control of it.

The consequences proved serious, a heavy toll on the manufacturers' reputations, and, above all, a costly rectification program for the Chrysler Jeep, sent via a USB key to the millions of affected customers. Tesla, a player more familiar with cyber environments, has the means to update its vehicles remotely, managing to correct the fault in the space of ten days. It should be noted that this was an exceptionally short time, compared with the current norms for connected objects.

A GROWING SENSE OF AWARENESS

These two demonstrations of vulnerability have raised awareness among the public and vehicle manufacturers about the challenges of cybersecurity. Many manufacturers are making investments and strengthening their capabilities in this respect. Volkswagen, for example, has invested in the creation of the Cymotive company. Tesla has previously instigated its "bug bounty" program, where security researchers are paid according to the number and criticity of faults they find on vehicles, something that also helps prevent knowledge of these vulnerabilities being sold on the cybercrime black market.

THE CYBER CRASH TEST: OR HOW TO CHOOSE THE RIGHT AUTONOMOUS CAR

Not all manufacturers are at the same level when it comes to cyberattack awareness and investments. How then can customers choose a car that will be "cyber secure"? Today, beyond reading a handful of research papers, there is no simple way to answer this question. It's high time then for organizations, such as EuroNcap, which specializes in crash tests, to grasp the nettle, and identify and define the what constitutes the cybersecurity indicators for a vehicle! A number of simple characteristics could be used to help assess the level of security on offer: the degree of protection fitted to the driving functions, a reliable and non-blocking update capability, a system that alerts both the driver and manufacturer in the event of an attack, etc. This could be developed into a star-based system to rate vehicles on cybersecurity: a simple method that would be understood by all. Customers could then make an informed choice. And, in the same way as traditional crash tests, such a system would energize manufacturers when it comes to cybersecurity.

Gérôme BILLOIS
gerome.billois@wavestone.com

AGENDA

23.01.2017

HTCIA, What security model after 2020? (Hong Kong)

25-26.01.2017

International Cybersecurity Forum (Lille, France)

06.02.2017

CLUSIR PACA, bend without breaking (Nice)

Discover our expertise
RISK INSIGHT

@Risk_Insight

Director of the publication: Frédéric Goux

Editor-in-chief: Gérôme Billois

Contributors: Gérôme Billois, Etienne Capgras,
Chadi Hantouche, Hamza Kharbachi,
Esther Lyonnet, Hugo Moret,

Printer : Axiom Graphics

ISSN 1995-1975

www.wavestone.com

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European activities (excluding retail and consumer goods consulting outside of France)

Wavestone's mission is to enlighten and guide its clients in their most strategic decisions by relying on its functional, sectoral and technological expertise.

With 2500 employees across 4 continents, the firm is amongst the independent European leaders in consulting and is number 1 in France.