sonema
votre futur, notre engagement

LIVRE BLANC **Sécurité**

*WHITE PAPER **Security***

« Si vous pensez que la technologie peut résoudre vos problèmes de sécurité, alors vous n'avez rien compris aux problèmes de sécurité ni à la technologie. »

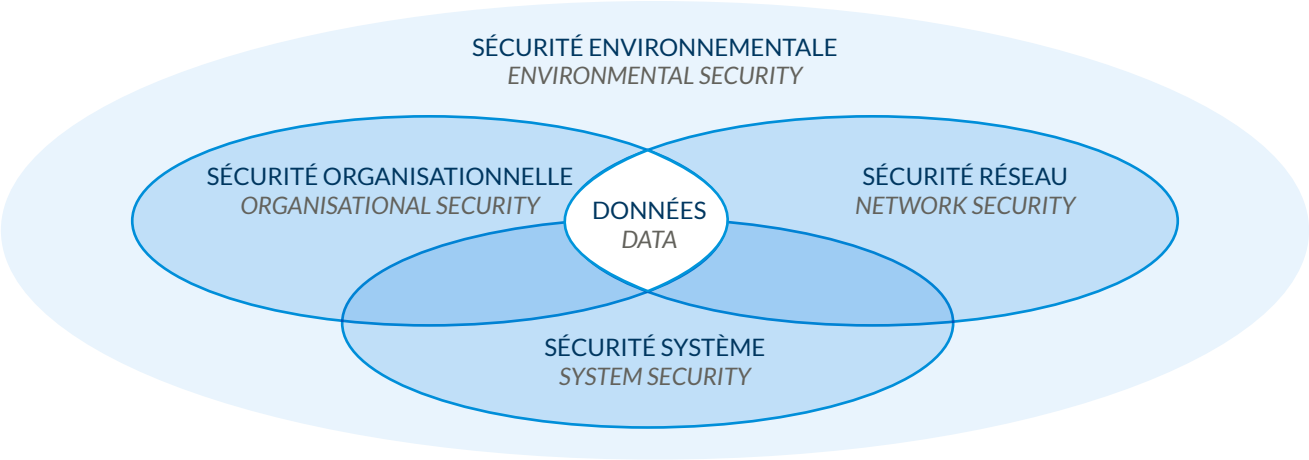
«If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.»

Bruce Schneier
Resilient Systems, Inc
Security technologist & Chief Technology Officer

LA SÉCURITÉ DE VOS SYSTÈMES D'INFORMATION EST-ELLE OPTIMALE ?

IS YOUR INFORMATION SYSTEM AS SECURE AS POSSIBLE ?

Pensez-vous être correctement **protégés des attaques** sur votre Système d'Information ?
Pensez-vous qu'installer des **firewalls et antivirus** soit suffisant ?
Avez-vous une idée des **impacts** des menaces et attaques virales et malveillantes ?
Quelles mesures pensez-vous mettre en place pour limiter les risques ?
Imaginez-vous que les **risques** puissent venir de « l'intérieur » de l'entreprise ?
Comment encadrez-vous la **gestion de données sensibles** par les collaborateurs ?
Comment anticipez-vous l'**incident informatique** causé par négligence ?



*Do you believe that your IT system is **fully protected against attacks?***
*Do you think that installing **firewalls and antivirus software** is enough?*
*Do you have an understanding of the **impacts** of viral and malicious threats and attacks ?*
***What steps** are you taking to reduce the risks? Have you considered that the risk could come from inside your business?*
*How do you regulate **handling of sensitive data** by your staff?*
*Are you prepared for an **IT incident** caused by negligence?*

SOMMAIRE
SUMMARY

INTRODUCTION / *INTRODUCTION*

Aujourd'hui, les Systèmes d'Information sont au cœur de tous les processus des entreprises. Omniprésents, ils évoluent sans cesse, assimilant et traitant chaque jour plus de données sensibles. Désormais socles du développement stratégique d'une entreprise, ils sont particulièrement exposés aux risques d'attaques.

Ces attaques sont de plus en plus sophistiquées et ne sont plus seulement le fait de groupes organisés et disposant de moyens importants. De nombreux outils accessibles librement et facilement sur Internet permettent de déployer des attaques informatiques sophistiquées sans connaissances avancées.

Les attaques de type « ingénierie sociale » se multiplient également, en exploitant les informations détenues et partagées par les utilisateurs sur les réseaux sociaux.

Enfin, au-delà des attaques malveillantes, on constate des problématiques de sécurité liées aux menaces environnementales (risques naturels, incendie, inondation, énergie), ou comportementales (mauvaises manipulations, absence de règlementations, négligence…).

These days, IT systems are at the heart of all business procedures. Omnipresent and ever evolving, they absorb and treat increasingly sensitive information every day. As cornerstones of strategic development for businesses, they are particularly vulnerable to the threat of an attack.

These attacks are increasingly advanced, and are no longer carried out uniquely by organised groups with significant resources. Tools which are freely and easily available on the Internet, enable users to carry out sophisticated IT attacks without any prior in-depth knowledge.

«Social engineering» attacks are also becoming more frequent, exploiting information held and shared by users of social networks.

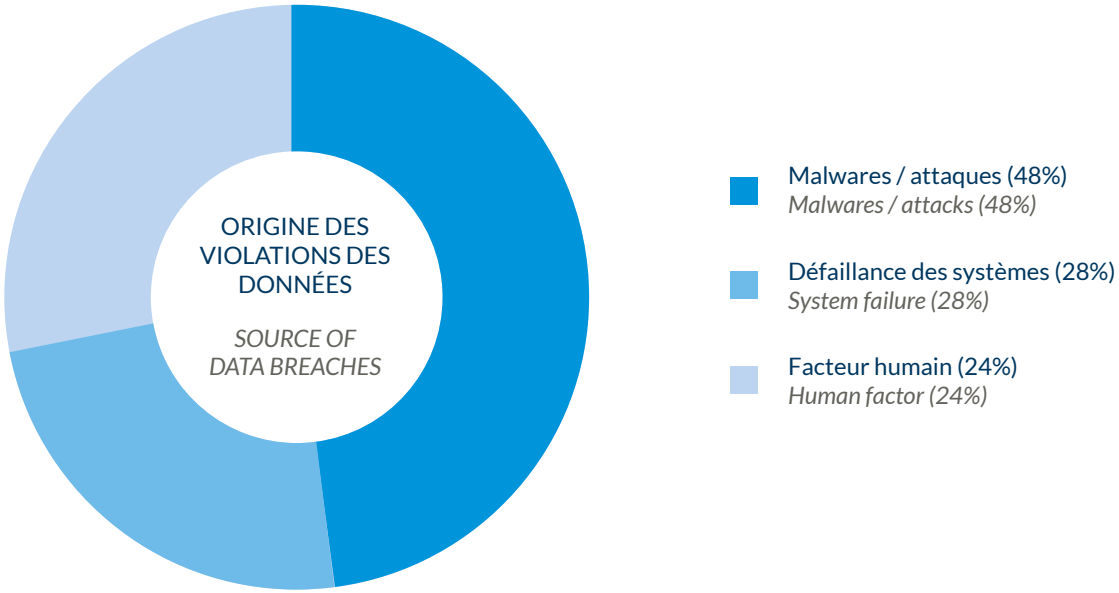
Finally, above and beyond malicious attacks, there are also security problems relating to environmental threats (natural risks, fire, floods, power) or behavioural threats (incorrect handling, lack of regulations, negligence…)

C'est dans ce contexte que le rôle des DSI et RSSI évolue et devient structurant pour faire face aux enjeux liés à la sécurité, et déployer les processus et outils adaptés.

Ce livre blanc définit les différentes menaces auxquelles les entreprises sont confrontées et décrit les principales solutions techniques et organisationnelles à mettre en place.

With this in mind, CISO and CIO roles are evolving and becoming more structured to address security issues using suitable procedures and tools.

This white paper describes the various threats which businesses are facing, and outlines the main technological and organisational solutions to apply.

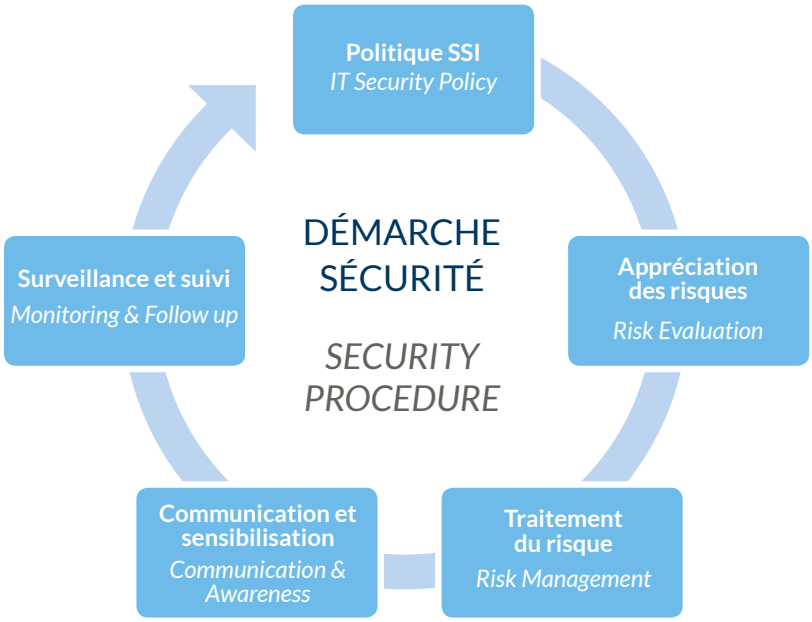


Source:
Ponemon IBM (mai 2015) avec la participation de 29 sociétés françaises
Source:
Ponemon IBM (May 2015) with participation of 29 French companies

1. QUELLE DÉMARCHE ADOPTER ? / *WHICH APPROACH TO ADOPT?*

Il est nécessaire d'adopter une approche globale pour identifier toutes les vulnérabilités possibles.

It is vital to adopt a global approach to identify all potential weak spots.



1. Définir une politique de sécurité de l'entreprise (PSSI), par la formalisation de règles responsabilisant l'ensemble des collaborateurs. L'implication et l'engagement de la Direction sont des prérequis nécessaires.

1. Establish a security policy for the company, *formalizing the regulations for staff accountability. Management involvement and commitment are required pre-requisites for this.*

2. Analyser au préalable l'ensemble des « biens et actifs »* ainsi que des risques associés avant même d'investir dans des solutions techniques pour assurer l'adéquation entre les investissements et le réel besoin de l'entreprise.

3. Mettre en place des mesures organisationnelles et techniques afin de déterminer la bonne posture face à chaque risque : l'accepter, l'éviter, le transférer (ex sous-traitance) ou le réduire (ex nouvelles mesures mises en place).

4. Sensibiliser les collaborateurs sur les mesures mises en place mais aussi sur les menaces identifiées et les risques résiduels.

5. Déterminer un modèle continu et récurrent : tout au long de la vie de l'entreprise pour être efficace ; les risques et les attaques criminelles sont dynamiques et évolutives.

* Matériel, physique, humain, services, expertise, base de données, documents internes, codes sources, infrastructure etc.

2. First analyse the total assests* *plus associated risks before investing in technological solutions, to ensure that any investment is compatible with the company's requirements.*

3. Put in place organisational and technical measures *in order to determine the appropriate position to take with regards to each risk: accept it, avoid it, transfer it (eg subcontracting) or reduce it (e.g. putting new measures in place).*

4. Educate the staff *about the measures which have been introduced and any threats which have been identified plus their residual risks.*

5. Establish an ongoing and recurring long-term model for the company: *risks and criminal attacks are aggressive and ever-evolving.*

** Physical material, staff, services, expertise, data base, internal documents source codes, infrastructure etc.*

2. ATTAQUES INFORMATIQUES ET SYSTÈMES / *INFORMATION SYSTEM ATTACKS*

Nous distinguons 3 types de menaces principales en terme d'attaques de système d'information :
We can identify 3 main types of threat in terms of information system attacks :

MENACES CONVENTIONNELLES

Les technologies de l'information et de la communication peuvent être utilisées pour soustraire des informations à des utilisateurs en abusant de leur crédulité. Elles permettent ainsi une transposition des délits classiques sur les réseaux numériques.

TRADITIONAL THREATS

Information and communications technology can be used to obtain information from users by abusing their trust. IT allows criminals to transfer traditional crime to digital networks.

Ces informations confidentielles sont ensuite utilisées illégalement :

- Extorsion de fonds, escroqueries diverses,
- Menace de type «vengeance» ou atteinte à l'image d'une entreprise,
- Fraude commerciale (vol de données bancaires),
- Abus de confiance et usurpation d'identité.

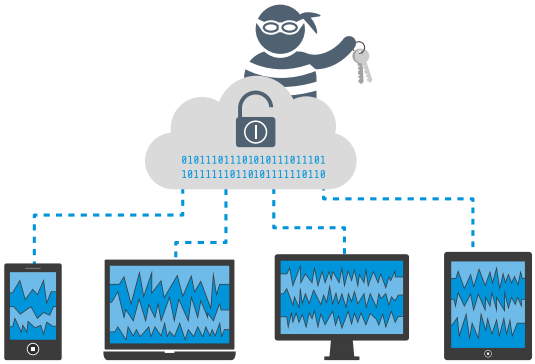
Confidential information is then illegally used for:

- *Extortion & various types of fraud*
- *Revenge type threats, or damaging a company's reputation,*
- *Commercial fraud (bank data theft),*
- *Breach of trust and identity theft.*

MENACES TECHNOLOGIQUES

Ces menaces ciblent principalement les failles des systèmes d'information. Elles cherchent à corrompre l'intégrité de ces systèmes par diverses manipulations :

- Installation de programmes espions ou de programmes pirates, intrusions,
- Déni de service surchargeant les réseaux et serveurs d'entreprise,
- Relais à partir de sites informatiques victimes.



TECHNOLOGICAL THREATS

These threats primarily target weak spots in the Information systems. They seek to corrupt the system's integrity by various means :

- *Installing spyware or high jacking software, intrusions*
- *DoS attacks overloading the company's networks and servers*
- *Relay from victim information sites*

L'ensemble de ces menaces obéit à différentes motivations :

- Dérober des données sensibles dans un objectif stratégique concurrentiel,
- Diffuser des idées ou des pensées illicites,
- Servir des actions terroristes,
- Rechercher une reconnaissance auprès d'une communauté de hackers,
- Nuire à l'entreprise ciblée.

There are different motives for all these threats :

- *Stealing sensitive data with a competitive strategic goal,*
- *Transmitting illegal thoughts or ideas,*
- *Terrorist actions,*
- *Looking for recognition within the hacker community,*
- *Targeting a business to harm their reputation.*

MENACES LIÉES À L'ERREUR OU L'ACCIDENT

THREATS FROM MISTAKES AND ACCIDENTS

Elles font partie des menaces les plus répandues et récurrentes. Elles sont particulièrement rencontrées quand les collaborateurs de l'entreprise (employés, fournisseurs, stagiaires, etc.) ne sont pas suffisamment sensibilisés sur les risques liés à leur métier.

These are among the most widespread and recurrent threats. They often occur when company employees (staff, suppliers, trainees etc.) are not made properly aware of the risks relating to their profession.

Elles engendrent différents types de vulnérabilités :

- **Conception** : mise en place d'une architecture technique ou logicielle sans connaissance des risques associés.
- **Réalisation** : absence de contrôles suite à la mise en place d'une nouvelle solution ou architecture. Ex: mots de passe configurés par défaut utilisés sur les systèmes.
- **Utilisation** : Mauvaise utilisation d'un applicatif. Ex: un utilisateur sature le serveur de messagerie suite à l'envoi d'une pièce jointe trop volumineuse.
- **Comportementale** : un collaborateur transmet des données professionnelles et confidentielles via sa messagerie privée personnelle.

This then leads to various weaknesses :

- ***Conception:*** *Installation of technical architecture or software without prior knowledge of the risks involved.*
- ***Development:*** *Lack of monitoring following the installation of a new solution or architecture. For example: default passwords used on the system.*
- ***Use:*** *Improper use of an application. E.g. A user overloads the message server by sending an attachment which is too large.*
- ***Behavioural:*** *A staff member sends confidential company data via his private or personal email.*

3. MESURES DE SÉCURITÉ / *SECURITY MEASURES*

Afin de lutter efficacement contre les menaces, il est important de mettre en place des mesures de sécurité. Qu'elles soient techniques (réseaux et systèmes), organisationnelles (liées à l'humain), ou environnementales (catastrophes naturelles), les mesures à appliquer s'appuient sur des techniques et technologies actuelles. Nous pouvons distinguer les principales mesures en termes de criminalité sur les systèmes d'information.

In order to deal with these threats efficiently, it's important to set up security measures. Whether they are technical (network and systems) organisational (the human factor) or environmental (natural disasters) the measures to be applied rely on up to date skills and technologies. In terms of criminality we can identify the main measures on the information systems.

3.1. MESURES DE SÉCURITÉ TECHNIQUES / *TECHNICAL SECURITY MEASURES*

DÉPLOYER DES ANTIVIRUS ÉVOLUTIFS

Les antivirus évoluent avec le **développement permanent de nouveaux virus et attaques**. Les antivirus les plus répandus aujourd'hui s'appuient sur la détection de signatures (fichiers ou données préalablement définis et connus par le développeur du produit comme étant infectés) et sont peu à peu dépassés. **Les antivirus de nouvelle génération, utilisent en**

USING DYNAMIC ANTIVIRUS PROGRAMS

*Antivirus programs are evolving with the **continuous development of new viruses and attacks**. Today the most widespread antivirus programs use signature detection (previously defined files or data, known to be infected by the product developer) but this is increasingly outdated. **The new generation of antivirus programs use behavioural-based detection of information** which*

plus l'analyse comportementale des informations, ce qui permet, lorsqu'un fichier ou une donnée sont non connus des bases d'information antivirus, de les bloquer avant même qu'ils ne puissent être exécutés ou pendant leur exécution par le poste de travail ou le serveur. Cette nouvelle technique d'analyse permet de lutter plus efficacement contre les **nouvelles attaques informatiques « zero day »**, qui sont développées chaque jour par milliers (généralement « sur mesure » particulièrement dans le domaine bancaire) et en ce sens, non reconnues dans les bases de données antivirales.

*allows a file to be blocked during execution or before it can be executed by the PC or server when the files or data are unknown to the antivirus database. This new analysis technique fights more efficiently against the **new "zero-day" type of attacks** which are being developed in their thousands every day ('tailor-made' particularly in the banking sector) and which to this extent, are not recognised in the antivirus database.*

VÉRIFIER L'ÉTAT DE LA SÉCURITÉ DES POSTES DE TRAVAIL ET AUTRES TERMINAUX

CHECK THE SECURITY STATUS OF WORKSTATIONS AND OTHER DEVICES

La **vérification des postes de travail** constitue la base en matière de cyber sécurité. Il faut en priorité qu'il y ait une **maîtrise des droits d'accès** aux postes de travail et serveurs. Il faut également vérifier qu'ils soient sécurisés par **des anti-virus mis à jour** régulièrement au même titre que les applications installées. Une vérification de l'ensemble du parc des machines est recommandée, par l'utilisation d'outils de supervision, pour des raisons d'efficacité et de simplicité.

***Verifying workstations** is the basis of cyber security. First and foremost, the **access controls of workstations and servers must be managed**. Also, the workstations plus any applications which have been installed must be checked to make sure they are protected by **regularly updated anti-virus programs**. An audit of the entire pool of machines is recommended, using supervisory tools for ease and efficiency.*

MAÎTRISER L'UTILISATION DES OUTILS NOMADES PROFESSIONNELS ET PERSONNELS

L'augmentation de l'utilisation de données professionnelles en dehors des postes de travail, notamment en utilisation extérieure (terminaux mobiles, PC portable, tablettes, smartphone, et BYOD (Bring Your Own Device)) est à surveiller. Ce sont des terminaux qui sont davantage exposés aux risques de vol et de casse. On y stocke de plus en plus de données qui peuvent être sensibles, et ils ont souvent un accès à distance à des données sensibles. Il est alors recommandé d'utiliser un outil de gestion centralisée permettant un contrôle optimal sur l'ensemble de ces terminaux nomades.

HANDLING THE USE OF PROFESSIONAL AND PERSONAL ROAMING DEVICES

The increased use of professional data away from the workstation *is something to monitor, in particular exterior use by mobile terminals, laptops, tablets, smartphones and BYOD (Bring Your Own Device).*

This type of terminal is more prone to the risk of theft or damage. We keep increasingly large amounts of sensitive data on these terminals, and they often have remote access to sensitive data as well.

Using a centralised management tool for greater supervision of these mobile terminals is therefore recommended.

CONTRÔLER OU BLOQUER LES SUPPORTS DE DONNÉES AMOVIBLES (DE TYPE CLÉS USB, CD ROM, DISQUES DUR EXTERNES,...)

Fortement utilisés dans l'environnement professionnel pour les échanges de documents, **les supports de données amovibles comme les clés USB ou disques durs externes font partie des systèmes idéaux pour le transport de codes malveillants** (virus, logiciels espions, etc.).

CONTROL OR BLOCK REMOVABLE STORAGE DEVICES (SUCH AS USB KEYS, CD ROMS, EXTERNAL HARD DRIVES,...)

Widely used in professional environments to exchange documents, ***removable storage devices such as USB keys or external hard drives are an ideal method of transporting malicious codes*** *(viruses, spyware, etc.).*

Tout comme les outils mobiles personnels, il est très aisé pour un employé d'utiliser une clé USB pour le transport de données entre son PC de bureau et son PC personnel entrainant un risque très important d'infection des postes. Il est donc nécessaire de les contrôler, et d'en limiter l'utilisation (limitation de l'usage des ports sur les machines) en fonction de la politique de sécurité en place.

As with other personal roaming devices, it's easy for an employee to use a USB key to transfer data from his work computer to his home computer. But this comes with a substantial risk of infection between the 2 computers. Therefore, it is necessary to monitor and restrict the use of USB keys (by restricting the use of USB ports on the computer) according to the existing security policy.

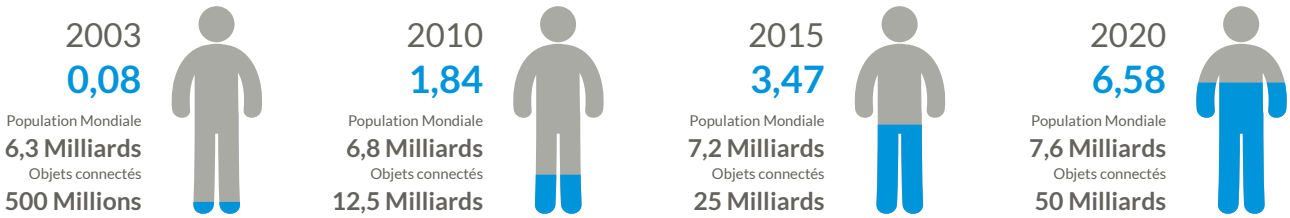
CONTRÔLER LES OBJETS CONNECTÉS

De la montre, aux bracelets d'activité sportive, en passant par les cafetières intelligentes, véhicules de sociétés, tableaux blancs ou lampes de bureaux, les objets connectés passent désormais la porte des bureaux des entreprises pour faciliter la vie de leurs employés. Cette évolution d'utilisation de simples objets de la vie courante et professionnelle entre dans l'ère de la transformation digitale.

MONITOR SMART DEVICES

From watches to fitness trackers, coffee machines, company cars, whiteboards to office lamps, smart devices are omnipresent in the workplace to make employees lives easier. With the development of the use of these simple products in everyday and work life, we have entered into the age of digital transformation.

OBJETS CONNECTÉS PAR PERSONNE (Prévisions Cisco)



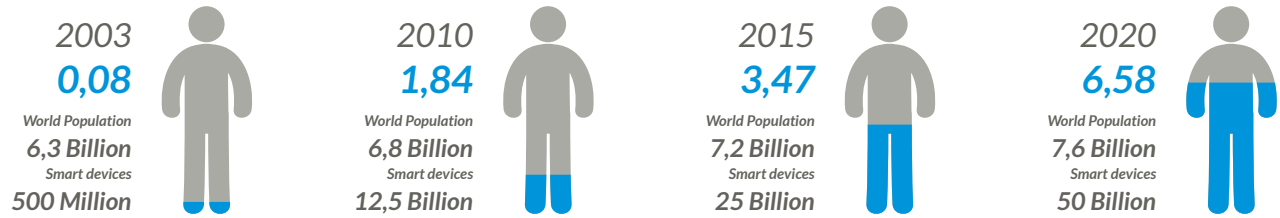
On en oublie alors que **ces objets sont connectés à internet et représentent un risque en matière de sécurité**; ils peuvent être porteurs de virus capables de se propager sur les supports bureautiques en place (PC, smartphone, base de données,..). Ils collectent généralement une multitude de données de l'entreprise qui peuvent être utilisées à des fins malveillantes si un attaquant réussit à les extraire ou à les fausser.

La démultiplication de ce type de technologie, alourdissant le système d'information de l'entreprise, implique une vigilance accrue sur l'intégration de ces objets connectés dans les réseaux d'entreprise.

*We forget that **these items are connected to the internet and therefore pose a security threat**: they can carry viruses which are capable of spreading to office equipment (computers, smartphones, data bases etc.). They usually compile a multitude of company data which could be used for malicious purposes if a cyber attacker was able to extract or falsify it.*

The increase in this type of technology overburdening business information systems requires constant vigilance when it comes to the integration of smart devices in business networks.

SMART DEVICES PER PERSON (Cisco Forecast))



CHIFFRER

Il est important de garder à l'esprit **qu'une faille de sécurité sur les données clients peut engendrer de graves conséquences sur une entreprise** (financière, sociale, juridique, image).

Le chiffrement est donc la première mesure de sécurité pour la protection des données.

Le chiffrement permet de conserver la confidentialité des données, à la fois en transit et celles stockées, le plus longtemps possible, car toute technique de chiffrement n'est pas infaillible dans le temps.

La mise en place d'une **stratégie de chiffrement**, nécessite de maîtriser les fondamentaux de la cryptographie et donc d'avoir des ressources qualifiées ; un système mal configuré pouvant ainsi faciliter l'action des attaquants (ex clé de chiffrement non confidentielle). Pour être sécurisées, les données des clients, qu'elles soient sur le web, stockées ou en transit, doivent être chiffrées en fonction de leur niveau de confidentialité.

ENCRYPT

*It's important to bear in mind that **a client data security breach could lead to severe consequences for a business** (financial, social, legal, reputation).*

Encryption is the most important security measure for data protection.

Encryption allows us to keep data confidential for as long as possible while it's in transit or stored for, but no encryption technique is fail-proof over time.

*Establishing an **encryption policy** requires knowledge of the basics of encryption and qualified staff members. An incorrectly configured system could allow hackers to attack more easily (e.g. a non-confidential encryption key) In order to be secure, client data whether it be on the web, stored or in transit, must be encrypted according to its level of confidentiality.*

- **LES DONNÉES WEB**

De nombreuses entreprises possèdent des serveurs web, accessibles depuis Internet, par exemple, dans le cas de sites marchands, bancaires ou de santé, échangeant des données sensibles. Se pose alors **la question du chiffrement des données diffusées depuis le web.**

Pour un client dont les données échangées sont confidentielles et peuvent impacter la stratégie de l'entreprise : si elles tombent dans de mauvaises mains ou si elles sont piratées, ce point est crucial et nécessite une mise en place d'un chiffrement. Le protocole https permet de garantir le chiffrement des connexions, surtout pour protéger les transactions monétiques.

Aujourd'hui, avec l'évolution des applications métiers en mode « cloud public », et l'accessibilité au monde entier, il est important de ne pas négliger le chiffrement des données.

- *WEB DATA*

Many companies have web servers accessible via the Internet, which in the case of commercial, banking or health websites, exchange sensitive data. ***The question of encrypting data posted on the web therefore arises****.*

In the case of a client who exchanges confidential data which can have an impact on their business strategy (if it falls into the wrong hands or is pirated) this point is vital and requires encryption. The https protocol allows us to guarantee encrypted connections, particularly for financial transactions.

With the development of business applications in 'public cloud' mode and global accessibility, these days it is crucial not to overlook data encryption.

- **LES LIAISONS**

Dans le cas d'interconnexions de multiples sites distants entre eux, il est important, pour la confidentialité des données, de les chiffrer lors du transport.

Comment ? Le chiffrement des liaisons peut s'effectuer via un réseau VPN (Virtual Private Network) qui établit une communication privée entre deux ou plusieurs sites.

Cette communication est sécurisée grâce à l'utilisation d'algorithmes de chiffrement permettant d'assurer l'échange de données privées de manière sécurisée au travers de réseaux dit « publics » comme Internet par exemple.

- *LINKS*

***When it comes to the interconnection of multiple remote sites**, it is important to encrypt data in transit to maintain data confidentiality. How? Link encryption can be carried out via a VPN network (Virtual Private Network) which establishes a private connection between two or more sites.*

This communication is secure thanks to the use of data encryption algorithms which allow the exchange of private data in a secure fashion through public networks like the Internet.

- **LES DONNÉES STOCKÉES**

Nommées **« données au repos », les données stockées constituent bien souvent le dernier point de défense en matière de sécurité;** or, leur chiffrement est tout aussi important. Tout comme les données en transit, les données stockées ayant un niveau de confidentialité élevé doivent être chiffrées. Il existe alors des solutions qui permettent de chiffrer ces données, qu'elles soient structurées ou non, indépendamment de leur emplacement.

- *STORED DATA*

*Called **data « at rest », stored data often represents the last point of defence when it comes to security**; yet its encryption is just as important. As with data in transit, stored data with a high level of confidentiality must be encrypted. There are solutions which allow us to encrypt this structured or unstructured data, regardless of its location.*

3.2. MESURES DE SÉCURITÉ ORGANISATIONNELLES
ORGANISATIONAL SECURITY MEASURES

CONTRÔLER LES ACCÈS ET UTILISATEURS

MONITOR ACCESS AND USERS

Un utilisateur, si ses droits d'accès ne sont pas maîtrisés, peut nuire sans le vouloir, aux systèmes d'information. C'est pourquoi il est préférable d'établir des règles de droit d'accès aux collaborateurs (employés, prestataires, fournisseurs) afin de contrôler leurs comportements. Les administrateurs maintiendront à jour ces droits d'accès sur les systèmes. Cela permet de limiter l'erreur ou l'acte de malveillance pouvant avoir de lourdes conséquences sur l'entreprise (financière, sociale, image) et sur **la Direction juridique, responsable légalement de son organisation.**

If a user's right of access is not managed, they could unintentionally harm the information system. *Which is why it's better to set right-of-access rules for staff (employees, service providers, suppliers) in order to monitor their behaviour*

The administrators keep these rights of access up to date on the system. This allows us to reduce error or malicious acts which could have severe consequences for the business (reputation, financial, social) and ***the legal department who are lawfully responsible for the company.***

SENSIBILISER LES UTILISATEURS AUX ATTAQUES PAR PHISHING OU INGÉNIERIE SOCIALE EN LES FORMANT

TRAIN USERS TO MAKE THEM AWARE OF PHISHING SCAMS AND SOCIAL ENGINEERING ATTACKS

Le phishing (hameçonnage) ou ingénierie sociale, sont des pratiques dans lesquelles les cybers criminels font l'acquisition de

Phishing scams and social engineering *are practices whereby cyber criminals acquire data and information illegally. Techniques are*

données et d'informations de manière déloyale. Leurs techniques évoluent, obligeant les experts en cyber criminalité, mais aussi l'ensemble des collaborateurs de l'entreprise, à se former en permanence à combattre ce genre d'attaque. Tous les supports de communication (messagerie électronique, sms, pages web, appels téléphoniques,...) sont la cible de ce type d'attaques.

evolving which forces experts in cybercrime plus the entire company workforce to keep up to date with this type of attack. All communication devices (emails, texts, web pages, phone calls etc.) are targeted by this type of attack.

SENSIBILISER LES UTILISATEURS AUX BONNES PRATIQUES

Pour une bonne prise en compte de la protection des données au sein d'une organisation, **des séances de sensibilisation des collaborateurs doivent être organisées régulièrement.** Cette sensibilisation permettra d'informer les collaborateurs sur les moyens organisationnels permettant de garantir :

1. **La disponibilité des informations :** l'information est accessible en continu dans des conditions de performance et de qualité satisfaisantes
2. **L'intégrité des informations :** l'information ne peut faire l'objet d'aucune altération non autorisée; l'exactitude et l'exhaustivité doivent être assurées.
3. **La confidentialité des informations:** l'information doit être destinée et exploitable aux seules personnes autorisées.

TRAIN USERS TO FOLLOW BEST PRACTICE TECHNIQUES

*To take data protection into proper account within a company, **staff training sessions must be organised regularly**.*

These training sessions keep staff updated about the organisational means which will ensure:

1. ***Information availability**: Satisfactory information is always available in performance conditions.*
2. ***Information integrity**: Information cannot be altered without prior authorisation; accuracy and thoroughness are therefore ensured.*
3. ***Information confidentiality**: Information intended for staff must only be used by authorised personnel.*
4. ***Information traceability:** Any event in relation to the previous factors must be identified and saved for*

4. **La traçabilité des informations :** tout évènement en rapport avec les critères précédents doit être identifié et conservé à des fins d'analyses ; en vue d'établir la non-répudiation d'une action; pour des besoins juridiques (preuve).

analysis, with a view to establishing the non-repudiation of an action for legal purposes (proof).

3.3. MESURES DE SÉCURITÉ ENVIRONNEMENTALES
ENVIRONMENTAL SECURITY MEASURES

PRÉVENIR DES RISQUES NATURELS

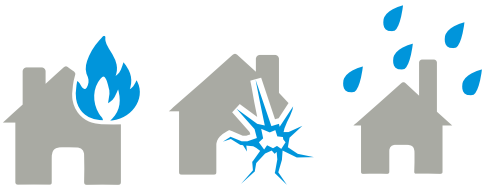
En fonction de la localisation de l'entreprise et de ses systèmes d'information, il est nécessaire de se poser les bonnes questions sur **les risques environnementaux (catastrophes naturelles) et menaces extérieures (origines humaines)** tels que:

- Incendies
- Tremblements de terre
- Inondations
- Risques géopolitiques
- Troubles civils
- Explosions
- …

PREVENTING NATURAL RISKS

*Depending on the location of the business and its information systems, we must ask appropriate questions about **environmental risks (natural catastrophes) and outside threats (from man-made sources)** such as :*

- *Fires*
- *Earthquakes*
- *Floods*
- *Geopolitical risks*
- *Civil unrest*
- *Explosions*
- …



Pour cela, il sera recommandé de faire appel aux conseils de spécialistes des différents domaines. Certaines mesures peuvent être mises en place comme :

In order to do so, it is advisable to ask for expert advice from specialists in various fields. Certain measures can be put in place as follows :

- Détecteurs de fumées
- Sondes thermiques couplées à un système de supervision
- Drainage des eaux limitant les risques d'inondations
- Limitation de l'emplacement de systèmes sensibles sur des zones à haut risques sismiques

- Smoke detectors
- Temperature sensors linked to a monitoring system.
- Water drainage system to reduce the risk of flooding.
- Restrictions on placing delicate systems in high-seismic risk zones.

SÉCURISER LE PÉRIMÈTRE

SECURING THE PERIMETER

Les accès aux locaux de l'entreprise doivent être protégés et pour cela il est recommandé de définir différents types de **zones de sécurité**. La définition de zones physiques de sécurité permettra de **conserver une cohérence entre les biens à protéger et les mesures de sécurité à mettre en place**.

Dans une entreprise nous pouvons avoir par exemple des zones dites publiques (accueil, parties communes, etc.), des zones restreintes (bureaux, etc.) et zones privées/confidentielles (salles blanches, machineries, etc.). Plus la zone est critique, et plus les mesures à mettre en place seront élaborées.

There must be a secure access to the company premises *and defining different types of* ***security zone*** *is recommended. Defining physical security zones* ***maintains consistency between the assets which need protecting and the security measures to put in place****.*

In a business environment, there can be so-called public areas (reception, common areas etc.) areas with limited access (offices etc.) and private/confidential areas (clean room, machinery zones etc.). The more important the area, the more significant the safety measures to put in place.

Il est également important de considérer dans le périmètre la sécurisation des supports de communications, qu'ils soient filaire ou radio, sans lesquels les données ne pourraient transiter.

It is equally important to consider securing the all-important communication tools for data transfer within the perimeter whether they are cable or wireless. .

4. AUTRES MESURES DE SÉCURITÉ / *OTHER SECURITY MEASURES*

PLAN DE REPRISE ET DE CONTINUITÉ D'ACTIVITÉ

Le plan de reprise d'activité (PRA) et le plan de continuité d'activité (PCA) sont des démarches complètes impliquant une organisation fonctionnelle et technique. Elles permettent de **sécuriser et maintenir le(s) système(s) d'information de l'entreprise** en cas de sinistre plus ou moins important, pouvant parfois entraîner des pertes de données ou affecter l'activité. Une activité suspendue ou la perte de données peuvent avoir de lourdes conséquences financières, juridiques et économiques sur l'entreprise. La mise en place d'un PRA/PCA est longue et coûteuse, et nécessite des compétences permettant de limiter ces risques. C'est pourquoi l'implication de la Direction est primordiale; l'entreprise entre alors dans une analyse des risques engageant la responsabilité de sa Direction.

DISASTER RECOVERY AND BUSINESS CONTINUITY PLANS

The disaster recovery plan (DRP) and the business continuity plan (BCP) are comprehensive procedures involving functional and technical organisation. They enable us to ***secure and safeguard the business information system(s)*** *in the event of a minor or major incident, which could lead to data loss or impact business operations.*

If business is interrupted or data is lost, there can be heavy financial or legal consequences for the company. Putting in place a DRP/BCP is long and costly and requires skills to minimise risk which is why management involvement is crucial. Management will be responsible for carrying-out a company-wide risk management assessment.

SAUVEGARDE EXTERNALISÉE

La sauvegarde externalisée est une autre mesure permettant de sécuriser les données critiques de l'entreprise et de les restaurer en cas de catastrophes ou d'attaques.

OUTSOURCING BACKUP

Outsourcing backup is another measure which enables us to secure a business's critical data and restore it in case of an attack or disaster.

CONCLUSION / *CONCLUSION*

Aujourd'hui de nombreuses technologies permettent de se protéger contre la cybercriminalité et autres défauts de systèmes pouvant impacter les données: antivirus, firewall, antispam, protection physique des installations, etc. Cependant la technologie ne protège pas l'entreprise de toutes les menaces.

Si en amont, les utilisateurs ne sont pas sensibilisés, les équipements n'ont aucun sens et ne permettent que de rattraper certains aspects de la négligence voire la malveillance d'un utilisateur du système. Pour cela, la sensibilisation sur la sécurité au sein de nos entreprises doit être la priorité, et de préférence encadrée par des experts métiers afin de formaliser

These days, multiple technologies provide protection against cybercrime and other system flaws which can impact data: antivirus, firewalls, antispam, the physical protection of facilities etc. However, technology cannot protect businesses against all types of threat.

If users have not been made aware beforehand, the technology devices won't make sense and will only be able to make up for certain aspects of a system user's carelessness or malevolence. To this end, raising awareness about security within the business must be a priority, and preferably supervised by professionals in order to formalise the process internally and provide the best security practices for the IT systems.

les processus en interne et fournir les bonnes pratiques de sécurité sur les systèmes d'information.

Qu'elle soit technique, organisationnelle ou environnementale, aucune démarche de sécurisation n'est à négliger, et nos entreprises doivent en prendre conscience. Les différentes démarches représentent un travail continu sur la technologie qui ne cesse d'évoluer, mais aussi sur l'étude des menaces qui se complexifient de jour en jour.

Au-delà de la technologie qu'il développe et qu'il utilise, l'homme reste au cœur de la problématique de sécurité du monde numérique. Il est donc le vecteur essentiel à placer au centre des politiques de sécurité et de protection des données.

Whether it be technical, organisational or environmental, no security procedure must be overlooked, and businesses must be aware of this. The different procedures represent an ongoing effort to study ever-evolving technology, and threats which become more complex every day.

Above and beyond the technology which he develops and uses, man is still at the heart of security problems in the digital world. He is therefore the key element which must be at the core of security policies and data protection.

Après lecture... vos systèmes d'information sont-ils vraiment protégés des attaques et menaces malveillantes ?

Having read this paper... are your information systems truly protected against malicious attacks and threats?

VOTRE SÉCURITÉ RÉSEAU PAR SONEMA

AUDIT RÉSEAU

Audit réseau, système et organisationnel

Qu'il soit technique ou organisationnel, SONEMA établit un diagnostic précis et détaillé de l'état actuel de vos infrastructures, pour vous proposer des recommandations d'amélioration. Selon les moyens à mettre en place, SONEMA propose de vous accompagner dans la réalisation des travaux d'optimisation projetés.

NETWORK AUDIT

Network, system and organisational audit

Whether it be technical or organisational, SONEMA will provide a detailed and accurate diagnosis of the current state of your infrastructure in order to offer recommendations for improvement. Depending on the resources to set up, SONEMA will assist you to implement the planned optimisation work.

MAIL PROTECTION

Filtrage et analyse des mails

Solution entièrement managée, et sans investissement*, permettant de filtrer vos flux mails transitant par l'infrastructure SONEMA grâce à des serveurs relais mails filtrant les mails à destination de vos serveurs.

**«as-a-service» en option*

MAIL PROTECTION

Mail filter and scans

An entirely managed solution which requires no investment and allows us to filter your mail traffic which will pass through the SONEMA infrastructure, thanks to mail server relays which filter emails sent to your servers.

**optional «as-a-service»*

NETWORK PROTECTION

Analyse et infogérance réseau et serveurs web

Solution entièrement managée, et sans investissement*, permettant de sécuriser vos flux internet transitant par l'infrastructure SONEMA grâce à des firewalls next generation UTM (Unified Threat MGT), ainsi qu'une sécurisation de vos serveurs mails (WAF Web Application Firewall).

*«as-a-service» en option

NETWORK PROTECTION

Network and web server analysis and outsourcing

An entirely managed solution which requires no investment and allows us to secure your Internet traffic which will pass through the SONEMA infrastructure thanks to next generation UTM firewalls plus the safeguarding of your mail servers (WAF Web Application Firewall).

*optional «as-a-service»

L' ACCOMPAGNEMENT SONEMA / *SONEMA ALWAYS WITH YOU*

Une équipe d'experts à votre service / *A team of experts at your service*

INSTALLATION

FORMATION / TRAINING

SUPPORT & ASSISTANCE

sonema
votre futur, notre engagement

A propos de Sonema

Partenaire proactif de nos clients, nous développons des solutions télécom sur mesure et évolutives pour les accompagner au quotidien dans leurs projets.

Notre engagement fondé sur une forte compréhension de leurs enjeux, leur permet de se concentrer sur leur cœur de métier et leurs innovations business.

About Sonema

By operating and managing scalable, bespoke telecommunication solutions, Sonema accompanies its customers with their projects on a daily basis.

Bearing in mind commitment, and with a strong understanding of what is at stake, we aim to be a proactive partner to our customers by allowing them to focus on their core business.

Contact: securite@sonema.com
Information : www.sonema.com