

Virology

Malwares and Benevolent viruses

Michel Dubois

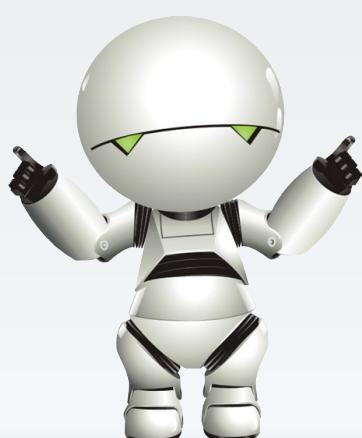
michel.dubois@esiea.fr

Dernière mise à jour: 20 mars 2017



Partie 1

Pourquoi la SSI ?



Pourquoi la SSI ?

Section 1

Généralités

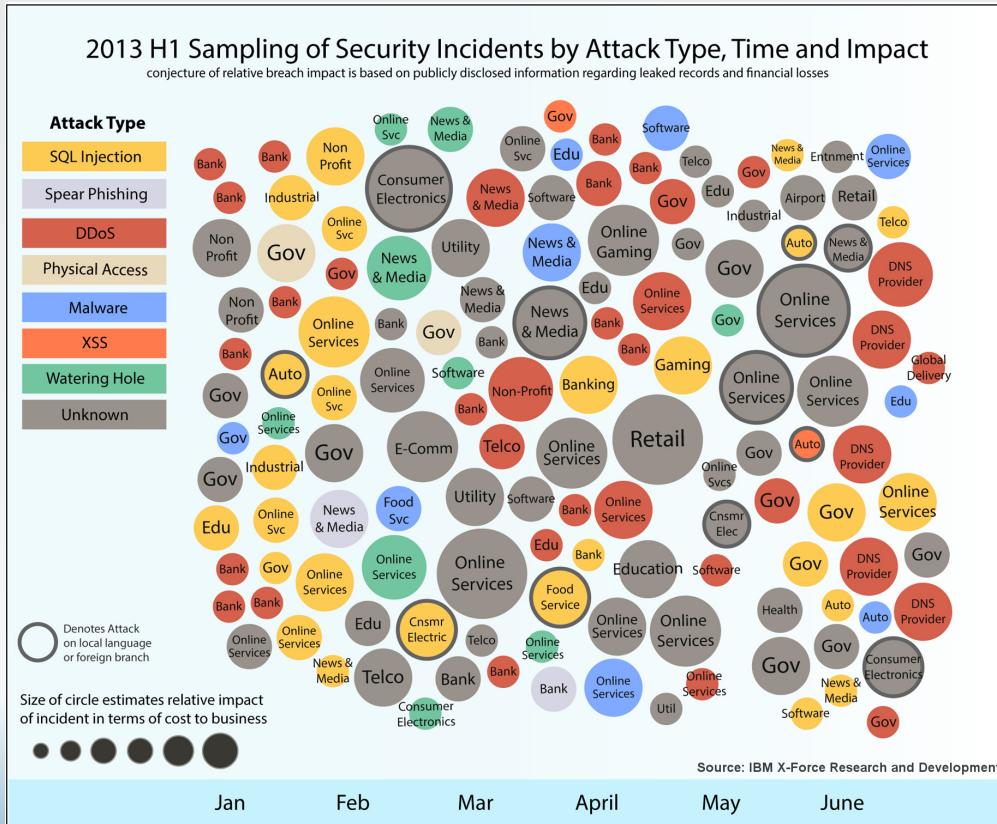


Généralités

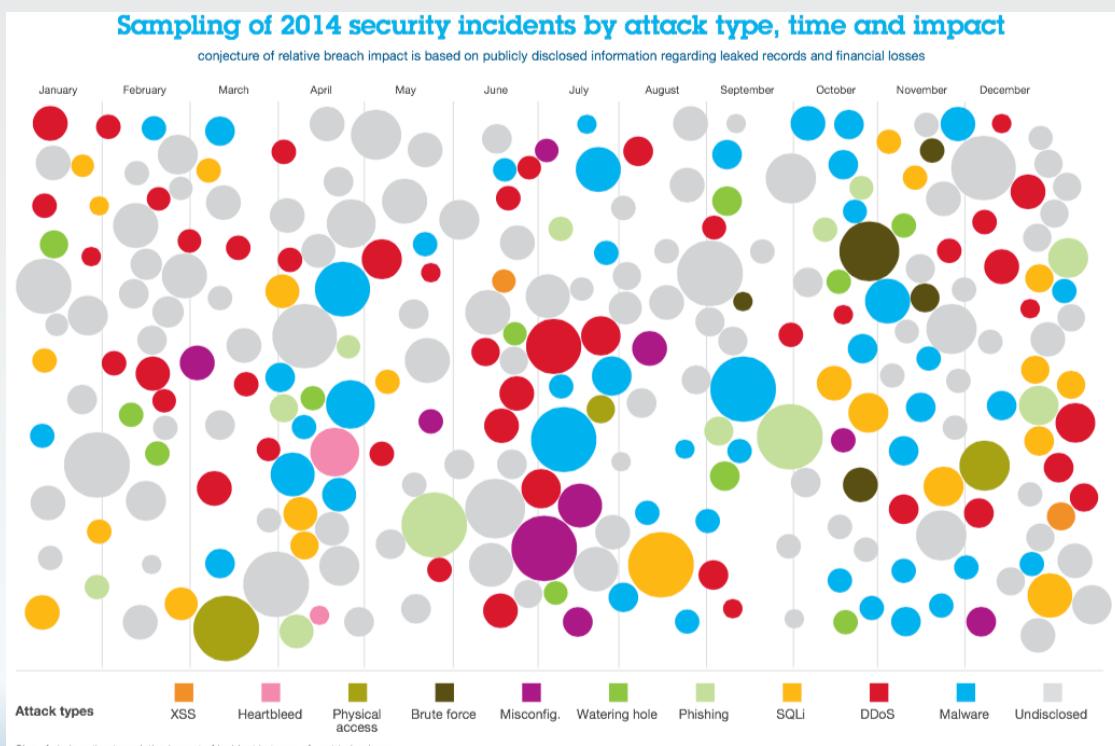
Évolution du contexte



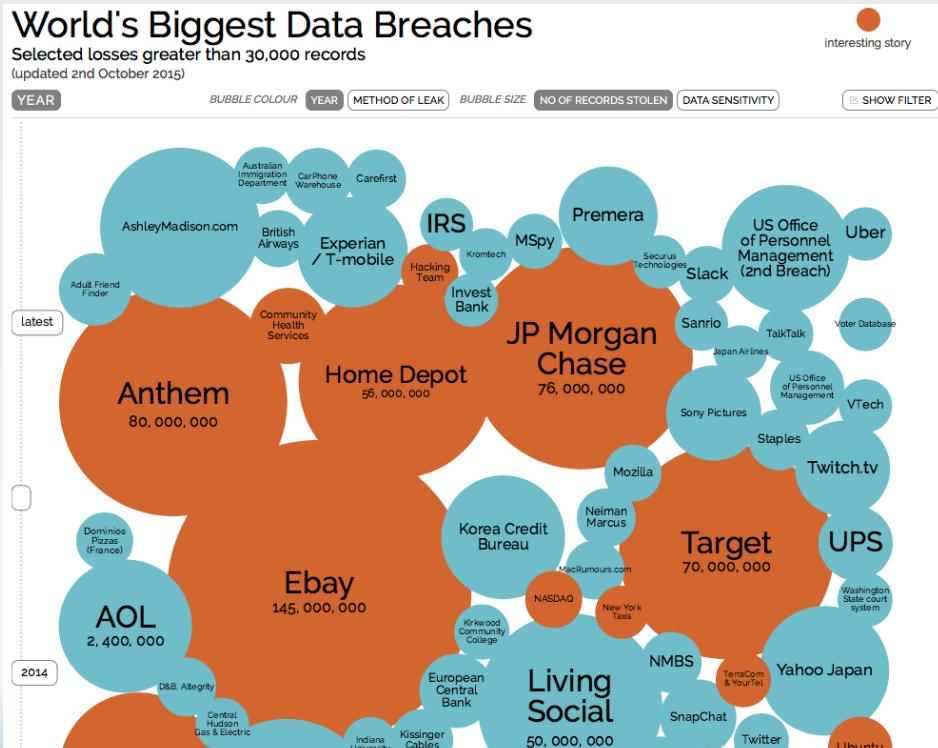
Généralités



Généralités



Généralités



Source : <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

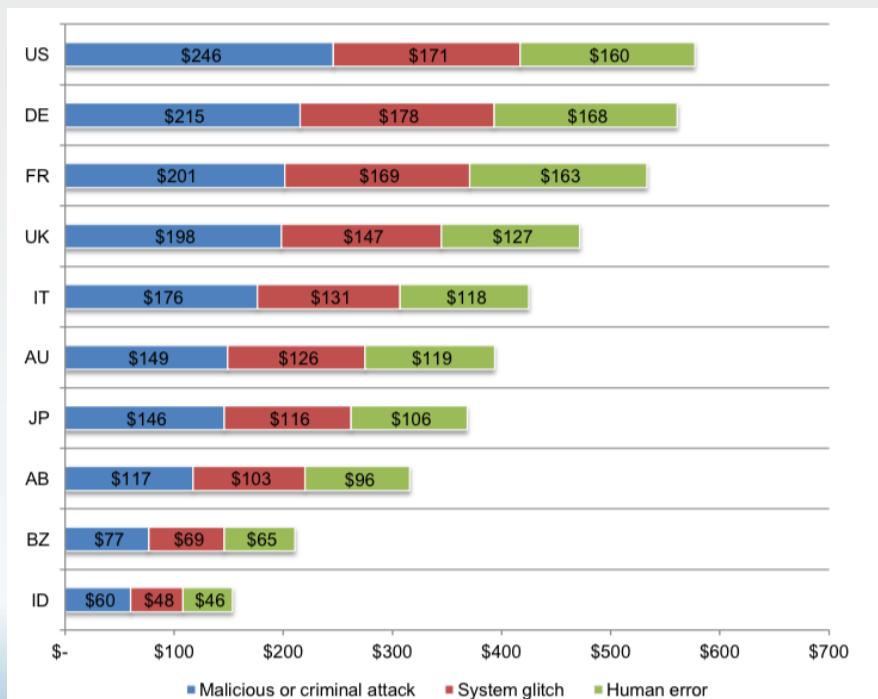
Virology

Michel Dubois © 2016

7/136

Généralités

Coût des attaques informatiques



Source : <http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/>
Michel Dubois © 2016

Virology

8/136

Pourquoi la SSI ?

Section 2

Actualités 2015



Actualités 2015

Sabotage – mardi 10 mars 2015

Un pays entier coupé du monde à cause d'un sabotage Internet



Par Challenges.fr
Voir tous ses articles

Publié le 10-03-2015 à 12h25

A+ A-

L'accès à Internet au Gabon et les communications téléphoniques à l'international ont été gravement perturbés durant 24 heures en raison d'un acte de "sabotage".



La Gabon a été coupé du monde pendant 24 heures à cause d'une panne Internet AFP

L'accès à Internet au Gabon et les communications téléphoniques à l'international ont été gravement perturbés durant 24 heures en raison d'un acte de "sabotage", a annoncé mardi 10 mars Gabon Telecom, le principal opérateur du pays, déjà paralysé il y a deux semaines par une grève.

Le sabotage a visé, selon le fournisseur d'accès internet, un câble de fibre optique dans un quartier de Libreville.

"Vers quatre heures du matin, des individus sont venus saboter le câble sous-marin Sat 3 en faisant en sorte que le trafic international, c'est-à-dire la voix, l'internet et les autres transmissions de données soit perturbés", a affirmé le directeur réseau de Gabon Telecom, Firmin Ngoye, cité par le quotidien national l'Union.

Selon l'opérateur, le rétablissement total du réseau devrait prendre deux à trois jours.

Actualités 2015

Piratage et demande de rançon - mars 2015

Labio.fr piraté : demande de rançon et publication de résultats médicaux

Allo docteur, j'ai mal à ma sécurité 123



SECURITÉ

Crédits : GuidoVrola/Stock/ThinkStock

Le laboratoire de biologie médicale Labio est la cible d'un groupe de pirates. Ce dernier revendique avoir dérobé pas moins de 40 000 identifiants (nom, prénom, login et mot de passe), ainsi que « des centaines » de bilans médicaux. Une rançon de 20 000 euros est demandée et les fuites d'informations confidentielles ont déjà commencé.

Les demandes de rançons sont de plus en plus courantes dans le cas des piratages de données informatiques. Récemment, on a par exemple le cas de **SynoLocker** sur les **NAS Synology**, de **Feedly**, puis de **Domino's Pizza**. Dans ce dernier cas, la société nous avait indiqué qu'elle se refusait à céder aux demandes de son maître chanteur, le groupe de pirates **Rex Mundi**, et qu'aucune transaction financière n'aurait lieu. Des données avaient finalement été mises en ligne quelques mois plus tard.

Rex Mundi demande une rançon de 20 000 euros ou des résultats d'analyse seront publiés

Source : <http://www.nextinpact.com/news/93499-labio-fr-pirate-demande-rancon-et-publication-resultats-medicaux.htm>

Virology

Michel Dubois © 2016

11/136

Actualités 2015

Piratage du compte Twitter de l'US central command par le cybercaliphate - lundi 12 janvier 2015

Profile summary

CyberCaliphate

We love you isis

TWEETS 3,674 FOLLOWING 1,268 FOLLOWERS 109K

Follow

U.S. Central Command @CENTCOM

Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.

MacDill AFB, Tampa, FL · [centcom.mil](#)

Followed by [Anthony De Rosa](#), [WikiLeaks](#), [Department of State](#) and 4 others.

U.S. Central Command @CENTCOM - 57s
We won't stop! We know everything about you, your wives and children.
[pic.twitter.com/lxz82ICDES](#)

U.S. Central Command @CENTCOM - 2m
ISIS is already here, we are in your PCs, in each military base.
[pic.twitter.com/xaTqTMvN5](#)

U.S. Central Command @CENTCOM - 8m
[pic.twitter.com/SdiaoKO6Zkr](#)

Go to full profile

19:14

U.S. Central Command @CENTCOM

In the name of Allah, the Most Gracious, the Most Merciful,
the CyberCaliphate continues its CyberJihad.

18:44 - 12 janv. 15

Reponde à U.S. Central Command

Actualités 2015

Piratage de TV5monde – mercredi 8 avril 2015



Virology

Source : <https://reflets.info/piratage-de-tv5monde-loperation-cyber-pieds-nickeles/>
Michel Dubois © 2016
13/136

Actualités 2015

Piratage de TV5monde – mercredi 8 avril 2015

Sécurité défaillante – Mdp : lemotdepassedeyoutube



Virology

Michel Dubois © 2016

14/136

Actualités 2015

Piratage de TV5monde - **mercredi 8 avril 2015**

Démenti du Ministère de la défense

Mise à jour : 10/04/2015 15:22

Attaque contre TV5Monde : le ministère de la Défense dément la publication de documents confidentiels le concernant

Dans la soirée du mercredi 8 avril, la chaîne de télévision TV5Monde a subi une attaque informatique. Les attaquants ont perturbé ses moyens de diffusion et ont pris le contrôle de son site Internet et de ses comptes Facebook et Twitter. Des messages de propagande ont alors été diffusés. Parmi ceux-ci figuraient des menaces proférées contre les militaires français et leur famille. Des documents prétendument confidentiels ont été mis en ligne.

Après un examen minutieux de l'ensemble de ces documents par la chaîne de cyberdéfense des armées, les services du ministère de la Défense et ceux du ministère de l'Intérieur, il s'avère qu'aucun de ces documents ne mentionne l'identité de militaires français ni de leur famille. Le ministère de la Défense dément ainsi catégoriquement que les individus s'en étant pris aux moyens de diffusion de TV5Monde aient publié des documents confidentiels le concernant.

S'agissant des activités sur les réseaux sociaux et plus généralement sur Internet, le ministère réitère ses appels à la vigilance à l'ensemble de la communauté de Défense. La menace exercée par les groupes terroristes à l'encontre de notre pays et de nos ressortissants demeure en effet à un niveau élevé.

Virology

Michel Dubois © 2016

Source : <http://www.defense.gouv.fr>

Actualités 2015

Piratage de la Hacking Team's - **dimanche 5 juillet 2015**

The screenshot shows the Twitter profile of the Hacked Team (@hackingteam). The profile picture is a stylized logo consisting of the letters 'HT' enclosed in brackets. The bio reads: "Developing ineffective, easy-to-pwn offensive technology to compromise the operations of the worldwide law enforcement and intelligence communities." It includes location information ("Milan, Italy") and a link to their website ("hackingteam.com"). A tweet from July 5, 2015, states: "Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1lhChT!rbB... infotomb.com/eyyxo.torrent". Another tweet from July 5, 2015, says: "Of course not, it's a chance to upsell! They need to pay us for training so they learn".

Hacking Team is a Milan-based information technology company that sells offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations. Its **Remote Control Systems** enable governments and corporations to monitor the communications of internet users, decipher their encrypted files and emails, record Skype and other Voice over IP communications, and remotely activate microphones and camera on target computers.

Virology

Source : <http://thehackernews.com/2015/07/Italian-hacking-team-software.html>
Michel Dubois © 2016

16/136

Actualités 2015

Piratage de la Hacking Team's - dimanche 5 juillet 2015

The screenshot shows Christian Pozzi's Twitter profile. He has 39 tweets, 30 following, and 186 followers. His first tweet reads: "We are closing down. Bye Saudi Arabia. You paid us well. Allahuhakbah." His second tweet says: "Uh Oh - my twitter account was also hacked." His third tweet states: "We are currently working closely with the police at the moment. I can't comment about the recent breach."

500 gigabytes of internal data leaked over the Internet. The leaked data revealed a zero-day cross-platform Flash exploit (CVE-2015-5119). Also revealed in leaked data was Hacking Team employees use of weak passwords, including P4ssword, wolverine, and universo.

Virology

Source : https://en.wikipedia.org/wiki/Hacking_Team

Michel Dubois © 2016

17/136

Actualités 2015

Piratage de la Hacking Team's - dimanche 5 juillet 2015

The screenshot shows a Microsoft Outlook search results window titled 'Posta inviata - d.vincenzetti@hackingteam.com - Microsoft Outlook (Product Activation Failed)'. The search term is 'Posta inviata'. The results list several emails from David Vincenzetti to Alessandra Tatissi on August 18, 2014, at 8:17 PM. The emails discuss a meeting in Prague and corporate responsibility. The interface includes a ribbon bar with Home, Send/Receive, Folder, View, and Search tabs.

The leaked data indicates that the spyware company did sell powerful spyware tools to oppressive regimes in Sudan, Bahrain, Ethiopia and Saudi Arabia.

Virology

Source : https://en.wikipedia.org/wiki/Hacking_Team

Michel Dubois © 2016

18/136

Actualités 2015

Piratage de Ashley Madison – mercredi
15 juillet 2015 – the Impact Team



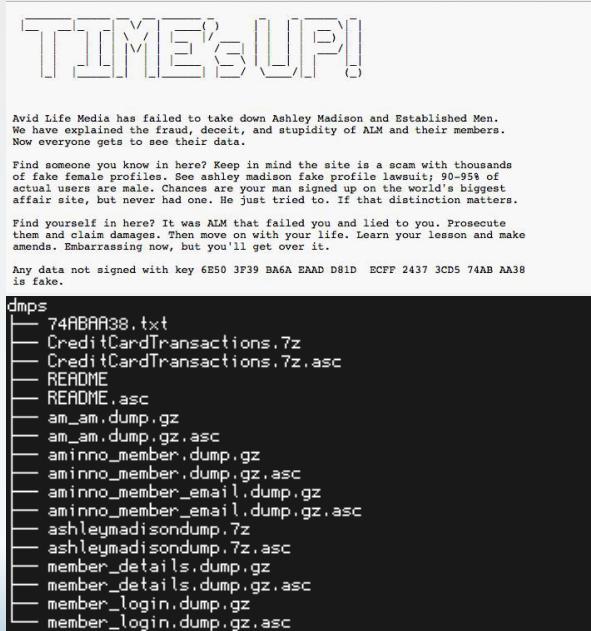
Aucun site Web ne peut garantir la protection de vos données privées : identité, carte de crédit, photos personnelles, . . . AshleyMadison.com, an American most prominent dating website, that helps married people cheat on their spouses has been hacked, potentially putting very private details of Millions of its users at risk of being exposed.

Virology

Source : <http://thehackernews.com/2015/08/ashley-madison-hack.html>
Michel Dubois © 2016 19/136

Actualités 2015

Piratage de Ashley Madison – mercredi
15 juillet 2015 – the Impact Team



Vol et diffusion de 10 Go de données client et 20Go de données internes à l'entreprise

- ▶ 33 millions de comptes divulgués
- ▶ non effacement des données utilisateurs
- ▶ utilisation majoritaire de bots féminins
- ▶ pas de protection des mots de passe
- ▶ 260000 adresses emails françaises
- ▶ utilisation de mails professionnels
- ▶ plusieurs suicides

Source : https://en.wikipedia.org/wiki/Ashley_Madison_data_breach
<http://geekbeat.tv/everything-we-know-about-the-ashley-madison-hack-plus-find-out-if-youre-on-the-list>
Michel Dubois © 2016 20/136

Virology

Actualités 2015

Internet des objets - 29 septembre 2015

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS

Security

Thousands of 'directly hackable' hospital devices exposed online

Hackers make 55,416 logins to MRIs, defibrillator honeypots



More like this

Security

Most read

- The future of Firefox is ... Chrome
- Windows 10 debuts Blue QR Code of Death – and why malware will love it
- Bundling ZFS and Linux is impossible says Richard Stallman
- How to not get pwned on Windows: Don't run any virtual machines open

http://www.theregister.co.uk/2015/09/29/thousands_of_directly_hackable_hospital_devices_found_exposed/ 21/136

Actualités 2015

Internet des objets - 29 septembre 2015

SHODAN healthcare

Exploits Maps Share Search Download Results Create Report

TOP COUNTRIES

Country	Count
United States	312
United Kingdom	21
Germany	12
India	10
Japan	8

74.213.39.17

Total results: 432

Added on 2016-04-11 18:55:36 GMT

United States, Houston

Details

52.16.203.234

ec2-52-16-203-234.eu-west-1.compute.amazonaws.com

Amazon.com

Added on 2016-04-11 18:02:00 GMT

Ireland, Dublin

Details

SSL Certificate

Issued By: EJT-DV-SV-02-CA

Issued To: staging.app.enovatehealthcare.co.uk

Organization: Enovate Healthcare Ltd

HTTP/1.1 401 Unauthorized

Server: Microsoft-IIS/8.5

WWW-Authenticate: Basic realm="Enova

X-FRAME-OPTIONS: SAMEORIGIN

Date: Mon, 11 Apr 2016 18:01:26 GMT

Content-Length: 27

Supported SSL Versions

SSLv3, TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters

Fingerprint: RFC2409/Oakley Group 2

TOP SERVICES

Service	Count
Telnet	111
HTTP	69
FTP	69
2000	64
HTTPS	41

TOP ORGANIZATIONS

Actualités 2015

PCA - US Navy - 15 octobre 2015

The US Navy is reinstating the ancient art of celestial navigation to fight a very modern threat



Sometimes old school is best. In today's US Navy, navigating a warship by the stars instead of GPS is making a comeback.

The Naval Academy stopped teaching celestial navigation in the late 1990s, deeming the hard-to-learn skill irrelevant in an era when satellites can relay a ship's location with remarkable ease and precision.

But satellites and GPS are [vulnerable to cyber attack](#) (paywall). The tools of yesteryear—sextants, nautical almanacs, volumes of tables—are not. With that in mind, the academy is [reinstating celestial navigation](#) into its curriculum. Wooden boxes with decades-old instruments will be dusted off and opened, and students will once again learn to chart a course by measuring the angles of stars.

Old school navigation pales in comparison to today's high-tech systems. It's both painfully difficult and far less precise. But it can get you where you need to go within about 1.5 miles (2.4 kilometers). That could be a matter of life and death in a scenario where [modern technology has been compromised](#).

<http://qz.com/524795/the-us-navy-is-reinstating-the-ancient-art-of-celestial-navigation-to-fight-a-very-modern-threat>

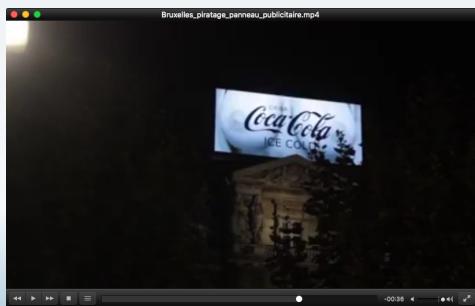
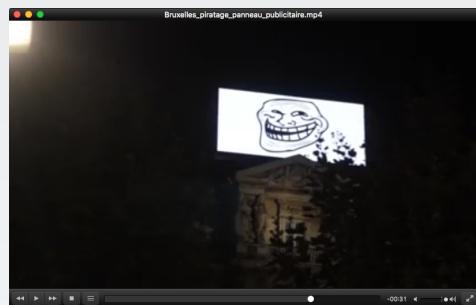
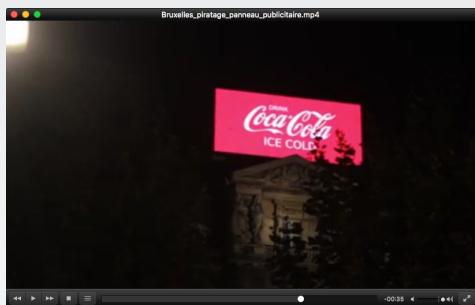
Virology

Michel Dubois © 2016

23/136

Actualités 2015

Piratage d'un écran publicitaire –
Bruxelles – lundi 28 décembre 2015



Source : <http://bigbrowser.blog.lemonde.fr/2015/12/28/piratage-dun-ecran-publicitaire-geant-a-bruxelles>

Virology

Michel Dubois © 2016

24/136

Actualités 2015

Attaque de centrales électriques –
mercredi 23 décembre 2015 – Ukraine



Une variante du malware BlackEnergy a paralysé plusieurs centrales électriques Ukrainiennes, causant une coupure électrique dans une partie du pays

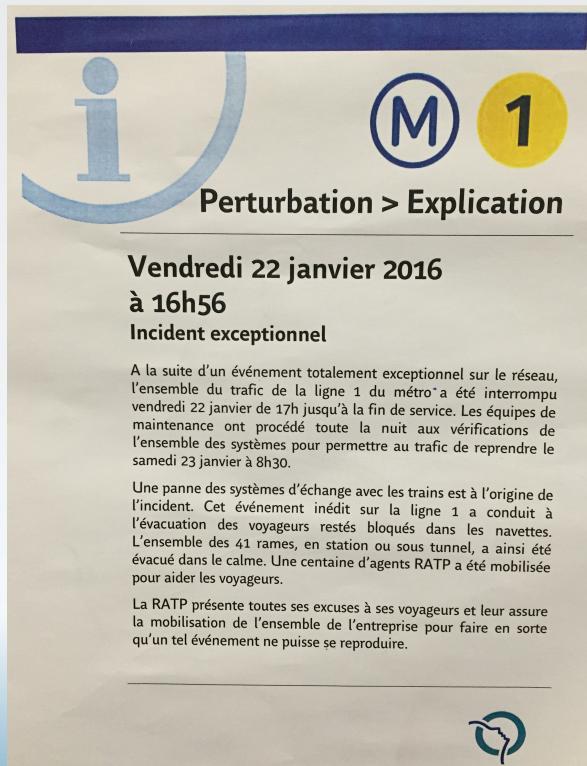
Source : http://motherboard.vice.com/en_uk/read/malware-found-inside-downed-ukrainian-power-plant-points-to-cyberattack
Virology Michel Dubois © 2016 25/136

Pourquoi la SSI ?
Section 3
Actualités 2016



Actualités 2016

Panne d'éléments actifs réseaux – vendredi 22 janvier 2016



Virology

Michel Dubois © 2016

27/136

Actualités 2016

Ransomware – mardi 16 février 2016 –
Hollywood Presbyterian Medical Center

Un hôpital américain paralysé par des pirates informatiques

TECH & WEB | Mis à jour le 16/02/2016 à 15:21

Crédits photo : PHILIPPE HUGUEN/AFP

EN BREF

- Le réseau informatique de cet établissement californien est paralysé depuis une semaine.
- On lui réclame une rançon de plus de 3,4 millions de dollars.
- Les «ransomwares» sont un type d'attaques informatiques qui visent les entreprises.

Peut-on soigner des malades sans Internet?
Depuis plus d'une semaine, un hôpital situé à



Un hôpital américain paye une rançon à des pirates informatiques

Le 18 février 2016 à 10h11

Le centre médical presbytérien d'Hollywood, en Californie, était infecté par un logiciel de racket, un programme utilisé par les pirates pour demander des rançons.

À près plus d'une semaine de paralysie, le centre médical presbytérien d'Hollywood a repris mercredi une activité normale. L'établissement victime d'un logiciel de racket a payé une rançon de 17 000 dollars en bitcoins, une

- 1 semaine de travail en mode dégradé
- transfert des patients sensibles

3,4 millions de dollars (9000 bitcoins) de rançon – 17000 dollars versés

Virology

Michel Dubois © 2016

28/136

Actualités 2016

Trop de sécurité ? Analyse des risques ? - février 2016

ÉTATS-UNIS - Un antivirus bloque la supervision de pose d'un cathéter cardiaque au beau milieu d'une opération chirurgicale

Un équipement médical considéré comme critique, Merge Hemo, s'est subitement éteint lors d'une opération cardiaque en février 2016. En cause, le balayage d'un antivirus sur l'ordinateur relié à Merge Hemo, qui s'est déclenché automatiquement et qui a bloqué les communications, entraînant une interruption brutale du service. Le personnel a eu exactement cinq minutes pour redémarrer et configurer à nouveau l'ordinateur et l'application Merge Hemo, sans mettre en danger la vie du patient opéré et endormi. L'entreprise Merge a précisé que des instructions précises recommandaient de placer Merge Hemo dans la liste blanche des antivirus. L'incident avait été immédiatement rapporté à la Food and Drug administration américaine.

MERGE HEALTHCARE MERGE HEMO PROGRAMMABLE DIAGNOSTIC COMPUTER		Back to Search Results
Model Number	MERGE HEMO V9.40.1	
Device Problems	Use of incorrect Control Settings; Use of Device Issue	
Event Date	02/08/2016	
Event Type	Malfunction	
Event Description	<p>Merge hemo monitors, measures, and records physiological data from a human patient undergoing a cardiac catheterization procedure. The system comprises the patient data module and the hemo monitor pc. The two units are connected via a serial interface. All vital parameters and evaluations are registered and calculated in the patient data module. This data is then transmitted to the hemo monitor pc via the serial interface. All data can be shown and monitored on the hemo monitor pc. On (b)(6) 2016, a customer reported to merge healthcare that, in the middle of a heart catheterization procedure, the hemo monitor pc lost communication with the hemo client and the hemo monitor went black. Information obtained from the customer indicated that there was a delay of about 5 minutes while the patient was sedated so that the application could be rebooted. It was found that anti-malware software was performing hourly scans. With merge hemo not presenting physiological data during treatment, there is a potential for a delay in care that results in harm to the patient. However, it was reported that the procedure was completed successfully once the application was rebooted.</p>	
Manufacturer Narrative	<p>Based upon the available information, the cause for the reported event was due to the customer not following instructions concerning the installation of anti-virus software; therefore, there is no indication that the reported event was related to product malfunction or defect. The product security recommendations, (b)(4), explicitly state, "the intent of these guidelines is to configure the anti-virus software so that it does not affect clinical performance and uptime while still being effective. To accomplish this, the anti-virus software needs to be configured to scan only the potentially vulnerable files on the system, while skipping the medical images and patient data files. Our experience has shown that improper configuration of anti-virus software can have adverse affects including downtime and clinically unusable performance. "</p>	
Search Alerts/Recalls		

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/detail.cfm?mdrfoi_id=5487204

Virology

Michel Dubois © 2016

29/136

Actualités 2016

Hacktivisme - lundi 22 février 2016 - www.cimd.interarmees.defense.gouv.fr

The screenshot shows the 'Administration des utilisateurs' section of the CIMD web portal. It lists various applications and their status:

- Administration des utilisateurs: En cours de développement
- Paramètres de données: En cours de développement
- Projet: En cours de développement
- Lancement et arrêt des TOMCAT: En cours de développement
- Paramètres application AUTHENTICATION
- Paramètres application PORTAL
- Paramètres application SOFREHO
- Niveau de bout Q3an
- Transfert de fichiers
- Formulaires d'enquêtes
- Gestion des codes entreprises françaises (ICAEG)
- Gestion des codes entreprises françaises (ICAEG) - Version portail
- Editor
- Gestion des évaluations des référentiels OTAN
- Gestion des formations (programmes - inscriptions)
- Gestion des formations (programmes - inscriptions) version portail

► Motivations : State of Emergency, Arm Trade,

OpNATO, OpAfrica

► Vol et diffusion de données nominatives



Afin de répondre à vos questions concernant le Système OTAN de codification ou nos outils et services, la hotline du CIMD est ouverte du lundi au vendredi de 8h00 à 16h00.
Contact téléphone: + 33 290 226 100

Our web portal will be temporarily unavailable due to maintenance actions.
February 22, 2016 - Our web portal will be temporarily unavailable due to maintenance actions, for up to 24 hours. Thank you for your understanding and looking forward to seeing you on our website.

To answer your questions about the NATO Codification System or our tools and services, you can contact our hotline from Monday to Friday, 08:00 to 16:00.

Phone Number: +33 290 226 100



<https://www.cyberguerrilla.org/blog/anonymous-hacks-subsites-of-french-defense-ministry/>

Virology

Michel Dubois © 2016

30/136

Hacking industrial vehicles from the internet

MARCH 6TH, 2016

It is possible to monitor and control float trucks, public bus or delivery vans from the internet, obtaining their speed, position, and a lot other parameters. You can even control some parameters of the vehicle or hack into the canbus of the vehicle remotely.

Those vehicles have a Telematics Gateway Unit (TGU) device and a 3g/4g/gprs/lte/edge /HSDPA modem to connect to the internet, with a public IP address.

There are thousands of TGU connected to the internet, with no authentication at all and with administrative interfaces through a web panel or a telnet session.

Finding publicly exposed TGUs in the internets

There are tons of open TGU and similar vehicle appliances on the internet. One very interesting and easy to find is the **c4max**.

The c4max smartbox is a TGU with powerful capabilities, a simple console on port 23, and is easy to identify while scanning the internet.

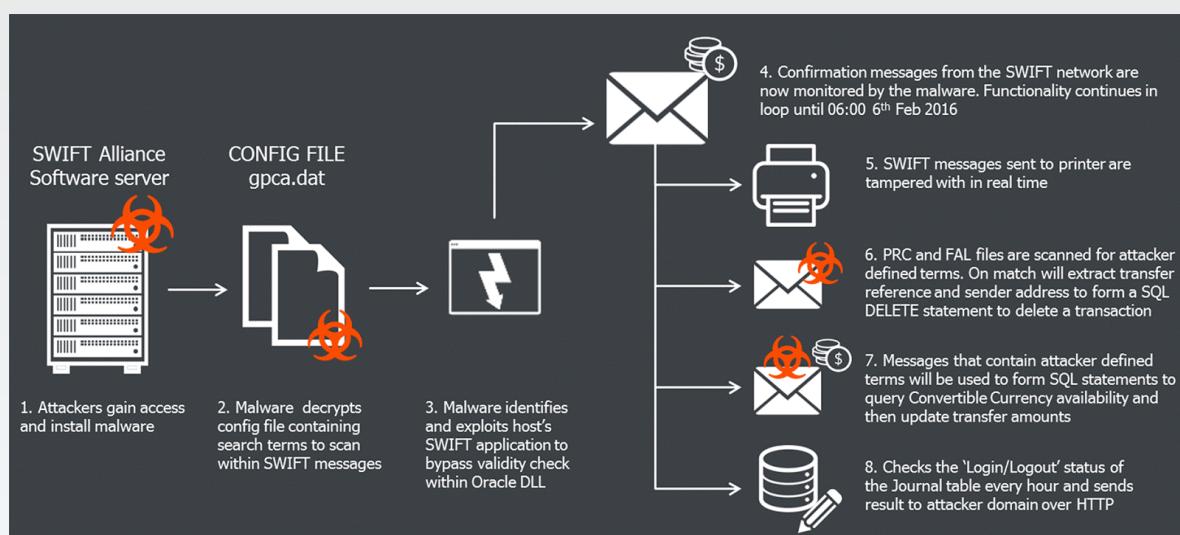


<http://plggjcarlosnorte.com/security/2016/03/06/hacking-machineries-from-the-internets.html>

31/136

Actualités 2016

81M\$ volés de comptes de la Bangladesh central bank - mars 2016



- ▶ the Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a cooperative owned by 3000 financial institutions
- ▶ the Swift banking system is used to transfer billions internationally every day
- ▶ the attackers obtained valid credentials for operators authorised to create and approve Swift messages, then submitted fraudulent messages by impersonating those people

Actualités 2016

Bug logiciel - mars 2016

◀ Back to Twitter 21:09 janes.com 52 %

IHS Jane's 360

Defence

CONTENT PREVIEW

C4ISR: Air

F-35 mission software stability poses greatest risk to USAF IOC

Marina Malenic, Washington, DC - IHS Jane's Defence Weekly 06 March 2016



A software stability problem that interferes with the F-35 radar's ability to remain on while in flight poses the greatest threat to achieving USAF IOC in 2016. Source: Lockheed Martin

Key Points

- A software glitch that interferes with the F-35 radar's ability to remain working in flight poses the greatest threat to meeting the USAF's IOC schedule
- Training on a new increment of ALIS and a fuel pressure modification are the other two unresolved issues

◀ Back to Twitter 21:10 arstechnica.com 52 %

ars

F-35 radar system has bug that requires hard reboot in flight

Virtual BSOD for radar software could delay USAF's full deployment of fighter.

by Sean Gallagher · Mar 10, 2016 5:15pm CET

Login to bookmark 157



"Hello, tech support?"
Dan Stjepich @ Flickr

In an episode of CBS' techno-procedural series *CSI: Cyber* that aired in January, pilots were forced to power off and power back on an airliner's flight computer to regain control from a hacker. As preposterous as that cold-boot of avionics sounds, it's something that test pilots have had to do with the F-35A "Lightning II" Joint Strike Fighter's radar system—not because of a hack but because of a software problem that causes the radar to degrade or stop working

●●●○ Orange F 3G 19:35 gizmodo.com 94 %

The Pentagon's New List of F-35 Bugs Is Predictably Awful

Michael Nunez 55.8K Filed to: PENTAGON



The F-35 Joint Strike Fighter program is the most expensive military program in the world, so it should be no surprise that the F-35 aircraft is loaded with powerful weapons controlled by powerful computers.

f Share t Tweet

Virology

Michel Dubois © 2016

33/136

Actualités 2016

Vague de ransomwares - janvier/avril 2016



Virology

Michel Dubois © 2016

34/136

Actualités 2016

Vague de ransomwares - janvier/avril 2016 - Locky

Enable macro if the data encoding is incorrect

3XVFC..нлв№...-6yD-©ХИЕКУь?тм
ЛейгР, Г\$|f<%оъ к†д%у} ЙльR7iK9-йN+‘®Ші<Х!Сп\$O>”-
іб[шZSfA‘\$□□4iНяы} °ВЖBSLzo
Іљ\Х3x°0¤'c"]!ЖДсLgIг□B9Й1©frfуk»Х†If6YINkë€ВО-
u□ЙАСБИ‡е©“±μ1V□±s□\$Lj%пы[шГ‘л-
;с©Вч+ь4ияДSp[;.пifзХї'ў«їмъ<гFбркуї/”ГдЛЬ>”
Ч©и”оRЬ"ЯrCg•ка†ібфСВА8МСК4...к•&тиБїэLCJХСМ”Rљ□*АДШуГВк’...їЗиїЫ§O-
¢јIN□sSS3|□Ю5Щн?ЛҮР}TM ...Р в'АтІшн~hФ6ъBr€>A5'3
мїзЭ&&JF"‡5@|пjM¶ГВ†'ЖкzИ <Be©hјB€·DjTБ...Ж;иgW-
3¶кhГїЎшжO<EPB□@™5□Hu,,8IИ्मВхм&в□Нег=nЦ|™©<V™,Ю\,ьОгmg|•НЕрш[\\A
nШгГМ±3льЛ[Юj]P24:3-----@ШN4
ою,3К],ГJхи,4-ъ»L0Чг'ЖТйСkNPЧУRГeb

Actualités 2016

Vague de ransomwares - janvier/avril 2016 - Locky

!!! IMPORTANT INFORMATION !!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

1. <http://3ezlvkoi7fwyood.tor2web.org/78634AFEA4011440>
2. <http://3ezlvkoi7fwyood.onion.to/78634AFEA4011440>
3. <http://3ezlvkoi7fwyood.onion.cab/78634AFEA4011440>

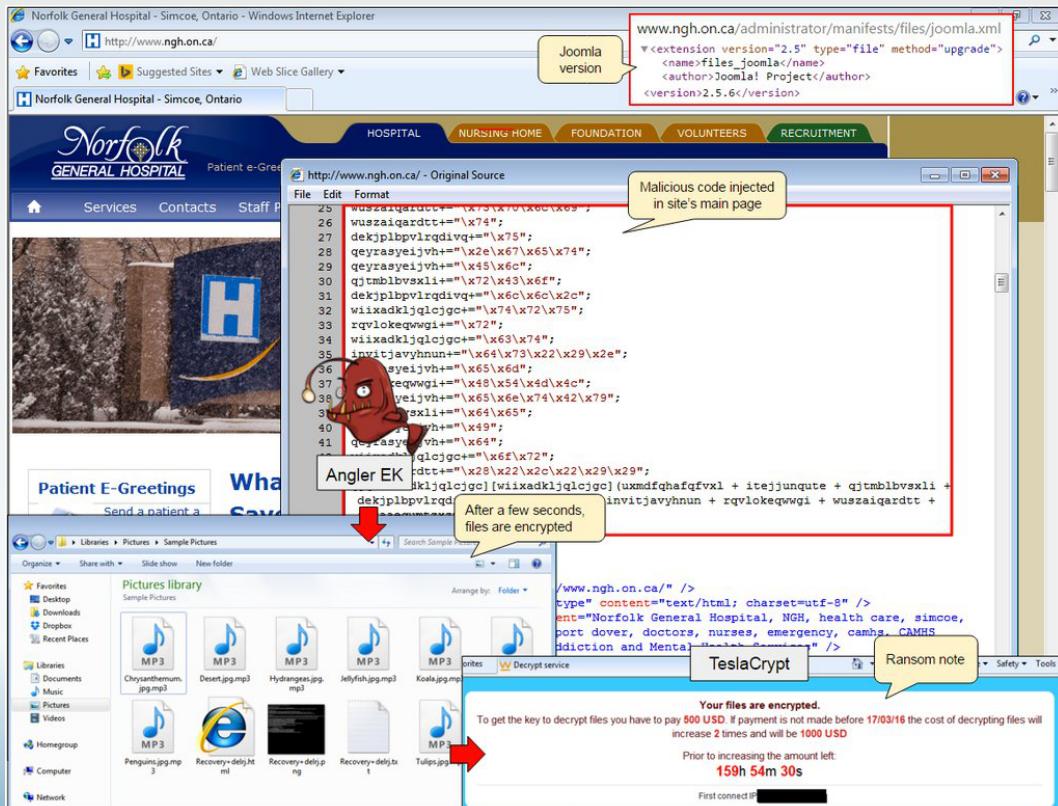
If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: i3ezlvkoi7fwyood.onion/78634AFEA4011440
4. Follow the instructions on the site.

!!! Your personal identification ID: 78634AFEA4011440 !!!□34

Actualités 2016

Vague de ransomwares - janvier/avril 2016 - Teslacrypt



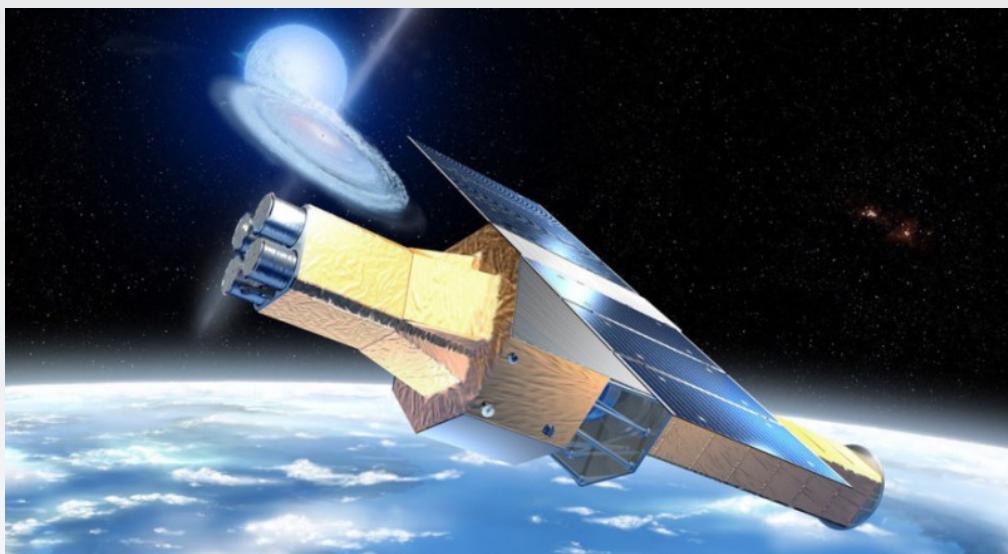
Virology

Michel Dubois © 2016

37/136

Actualités 2016

Le satellite Hitomi détruit à cause d'une mise à jour - mai 2016



The Japanese X-ray telescope **Hitomi** has been declared lost after it disintegrated in orbit, torn apart when spinning out of control. The cause is still under investigation but early analysis points to **bad data in a software package** pushed shortly after an instrument probe was extended from the rear of the satellite. JAXA, the Japanese space agency, lost **\$286 million**, three years of planned observations, and a possible additional 10 years of science research.

<http://hackaday.com/2016/05/02/software-update-destroys-286-million-japanese-satellite/>

Virology

Michel Dubois © 2016

38/136

Actualités 2016

La clé USB, contenant le dossier d'enquête sur les attentats de Charlie Hebdo, se perd dans le courrier - août 2016

Le Parisien | VAL-D'OISE | La clé USB aux infos sensibles retrouvée... à Gonesse

0 RÉACTION 2.3K PARTAGE

Gonesse. La clé USB contenait l'intégralité de l'enquête sur les attentats de janvier 2015 à Paris. (LP/B.A.)

Imprimer A A

Des policiers ont investi il y a quelques jours le centre de tri de Gonesse. Au bout de 8 heures de recherche, ils ont finalement trouvé ce qu'ils cherchaient : une clé USB qui contenait tout le dossier d'enquête des attentats de janvier 2015. Celle-ci avait été envoyée par des avocats de Bobigny (Seine-Saint-Denis) défendant des victimes à des confrères de Reims. La clé USB placée dans une enveloppe normale avait été déchirée en passant dans une machine du centre de tri. Le pli était donc arrivé vide. Étant donné le caractère extrêmement sensible des informations que contenait la clé USB, la police judiciaire de Reims a diligenté une enquête qui s'est finalement achevée à Gonesse.

Val-d'Oise
Gonesse Reims
USB Attentats
leparisien.fr

La clé USB contenant l'intégralité de l'enquête sur les attentats de Charlie Hebdo et de l'Hyper Cacher envoyée par des avocats de Bobigny à leurs confrères de Reims est perdue pendant le transport. Les avocats de Bobigny, chargés défendre des victimes, s'étaient contentés d'envoyer ce document ultra-sensible dans une enveloppe banale, timbrée au tarif minimum. Une quantité vertigineuse de procès-verbaux de garde à vue, de notes des services des renseignements ou d'identités de témoins se baladent alors dans la nature, à la portée de tous.

<http://www.leparisien.fr/val-d-oise-95/la-cle-usb-aux-infos-sensibles-retrouvee-a-gonesse-28-08-2016-6075287.php>
Virology Michel Dubois © 2016 39/136

Actualités 2016

Un faux communiqué de presse provoque une chute de 18% du cours de bourse du groupe Vinci - novembre 2016



"L'histoire commence avec un faux communiqué de presse publié à 16h05 et envoyé à différentes rédactions. Le texte explique que Vinci a découvert d'énormes irrégularités comptables, pour 3,5 milliards d'euros, et que le groupe de BTP révise ses comptes 2015 et 2016 à la baisse. Au passage, le communiqué indique que le directeur financier, Christian Labeyrie, a été licencié par la compagnie."

<http://bfmbusiness.bfmtv.com/bourse/affaire-vinci-que-s-est-il-passe-mardi-1062541.html>

Actualités 2016

Un faux communiqué de presse provoque une chute de 18% du cours de bourse du groupe Vinci - novembre 2016

mar. 22/11/2016 16:04
contact.abonnement@vinci.group
VINCI lance une révision de ses comptes consolidés pour l'année 2015 et le 1er semestre 2016

À [REDACTED]
Nous avons supprimé les sauts de ligne en surnombre dans ce message.

Nouveau communiqué de presse VINCI
Rueil Malmaison, 22 Novembre 2016
VINCI lance une révision de ses comptes consolidés pour l'année 2015 et le 1er semestre 2016

Vinci a annoncé aujourd'hui son intention de réviser ses comptes consolidés pour l'exercice 2015 ainsi que pour le premier semestre 2016. Les résultats d'un audit interne mené par le groupe Vinci ont en effet révélé que certains transferts irréguliers avaient été effectués des dépenses d'exploitation vers le bilan, en dehors de tous principes comptables reconnus. Le montant de ces transferts s'éleverait à 2.490 millions d'euros pour l'exercice comptable 2015 et 1.065 millions d'euros pour le premier semestre 2016. Selon l'audit interne les résultats opérationnels réels seraient de 1.225 millions pour 2015 et de 641 millions pour le premier semestre 2016. Le groupe reporterait donc une perte nette pour 2015 ainsi que pour le premier semestre 2016.

Vinci a rapidement informé ses auditeurs externes (KPMG Audit et Deloitte & Associés) de la découverte de ces transferts. Le 21 Novembre, KPMG a informé Vinci qu'au vu de ces irrégularités, son audit des comptes consolidés de l'année 2015 et du premier semestre 2016 ne sauraient être valides.

Vinci publiera des comptes non audités pour l'exercice 2015 ainsi que pour le premier semestre 2016 dès que possible. Une fois que le nouvel audit sera achevé, Vinci publiera de nouveaux comptes audités pour les deux périodes. Le groupe a par ailleurs lancé une révision complète des règles internes au sein de sa direction financière.

La compagnie a licencié Christian Labeyrie, directeur général adjoint et directeur financier de Vinci.

Vinci a informé l'Autorité des Marchés Financiers (AMF) de ces événements.

La révision des résultats opérationnels pour 2015 et 2016 devrait rester sans conséquence sur la trésorerie du groupe et n'affectera ni les clients ni les prestations du groupe Vinci.

« Notre équipe de direction est très choquée par ces découvertes », a dit Xavier Huillard, Président-Directeur Général de Vinci. « Nous nous engageons à ce que Vinci respecte les plus hauts standards éthiques dans la conduite des affaires du groupe ».

« Nos clients ainsi que nos employés doivent garder confiance en la viabilité du groupe Vinci et en son engagement sur le long terme. Nos services ne sont en aucun cas affectés par ces événements et notre engagement à satisfaire les besoins de nos clients reste une priorité. Les rumeurs qui circulent sur une procédure d'insolvabilité sont totalement fausses » a ajouté le Président Directeur Général de Vinci.

« Nous nous engageons à mettre en place les changements nécessaires au sein du Groupe ».

Le groupe Vinci tiendra une conférence de presse demain.

Contact médias
Paul-Alexis Bouquet
Tél. : +33 (0)7 51 93 47 48
<http://www.vinci.group/vinci.nsf/fr/communiques/pages/20161122-1557.htm>

Virology

Michel Dubois © 2016

41/136

Actualités 2016

Un étudiant de l'ESTACA de Laval a grillé 88 ordinateurs de son école d'ingénieur - novembre 2016

france bleu

INFOSSPORTSÉMISSIONSMUSIQUE

Afficher la page d'accueil de France Bleu Mayenne

FAITS DIVERS – JUSTICE

Laval : un "jeu" qui coûte très cher à l'ESTACA

Par Stéphanie Denevault, France Bleu Mayenne
Mardi 22 novembre 2016 à 22:12

<https://www.francebleu.fr/infos/faits-divers-justice/laval-un-jeu-qui-coute-tres-cher-l-estaca-1479848930>

Virology

Michel Dubois © 2016

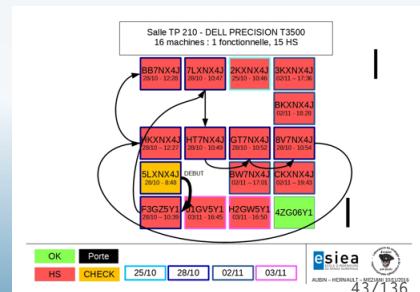
42/136

Actualités 2016

Un étudiant de l'ESTACA de Laval a grillé 88 ordinateurs de son école d'ingénieur - novembre 2016

- ▶ travail d'investigation réalisé par le laboratoire ($C + V$)^O de l'ESIEA suite à une demande d'aide de l'ESTACA
- ▶ l'ESTACA constatait des pannes informatiques se traduisant par l'impossibilité de démarrer plusieurs PC
- ▶ en investiguant sur la carte mère, constat que le microcontrôleur USB intégré présente un court circuit sur les ports de données qu'il contrôle
- ▶ le même diagnostic est fait sur tous les autres PC
- ▶ en dessoudant le microcontrôleur USB incriminé, le PC redémarre
- ▶ les disques durs étant épargnés, analyse des sauvegardes de mémoires vives (hyperfil.sys)
- ▶ à partir des dernières dates enregistrées dans le système, reconstitution des schémas horaires d'extinction des ordinateurs
- ▶ à l'aide de ces schémas les autorités ont pu les corrélérer avec les emplois du temps des étudiants

- ▶ cette analyse a permis de disculper 630 étudiants sur les 650 présents
- ▶ l'enquête de police a ensuite permis l'arrestation d'un étudiant, qui a avoué les faits
- ▶ ce dernier a fourni aux enquêteurs une clef USB appelée "USB Killer"
- ▶ cette clef décharge une tension de plus de 200V sur les fils "data" du port USB. Michel Dubois © 2016

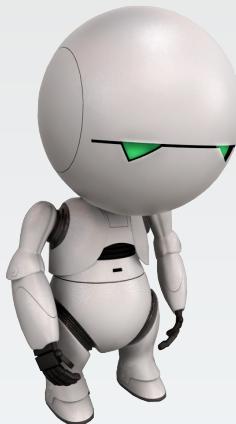


Pourquoi la SSI ?

Section 4

Les livres blancs de la défense





4. Les livres blancs de la défense

4.1. Les premiers rapports

Les livres blancs de la défense

Les premiers rapports

Rapport Lasbordes - 2006

La Sécurité des systèmes d'information - Un enjeu majeur pour la France



« La France accuse un retard préoccupant face aux impératifs de SSI, tant au niveau de l'État qu'au niveau des entreprises, quelques grands groupes mis à part. »

Rapport Romani - 2008

Cyberdéfense : un nouvel enjeu de sécurité nationale



« La France n'est ni bien préparée, ni bien organisée face à la menace d'attaques informatiques. »

Rapport Bockel - 2012

La cyberdéfense : un enjeu mondial, une priorité nationale

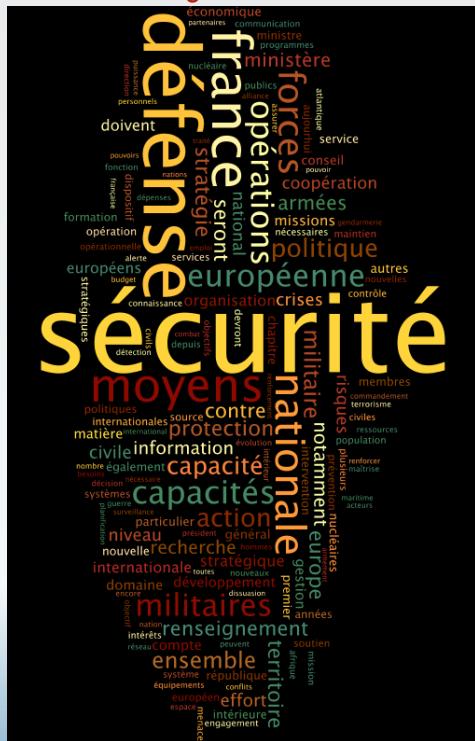


« Le renforcement de la protection et de la défense des systèmes d'information devrait faire l'objet d'une priorité nationale, portée au plus haut niveau de l'État, et d'une véritable stratégie de l'Union européenne. »

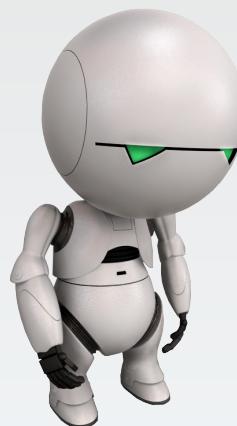
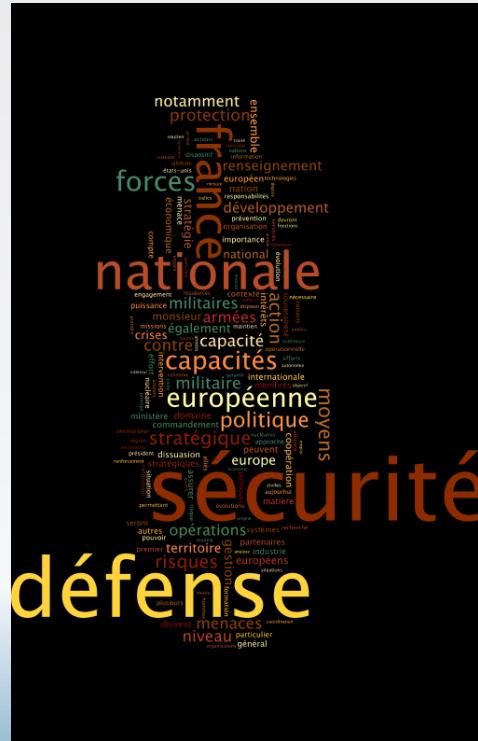
Les livres blancs de la défense

Les premiers rapports

17 juin 2008



29 avril 2013



4. Les livres blancs de la défense

4.2. Le livre blanc de 2008

Les livres blancs de la défense

Le livre blanc de 2008

2008 - De nouvelles vulnérabilités pour le territoire et les citoyens européens

Le terrorisme

« La France et l'Europe sont directement visées par le djihadisme et ceux qui s'en réclament. »



Les livres blancs de la défense

Le livre blanc de 2008

2008 - De nouvelles vulnérabilités pour le territoire et les citoyens européens

La prolifération du nucléaire

« D'ici 2025, la France et plusieurs pays européens se trouveront à portée de nouvelles capacités balistiques. »



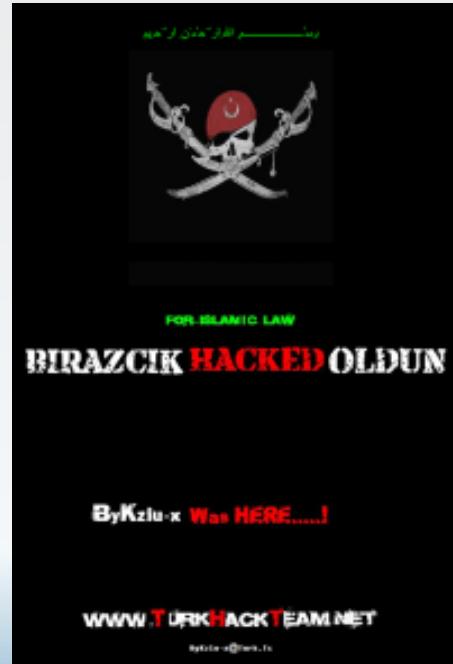
Les livres blancs de la défense

Le livre blanc de 2008

2008 - De nouvelles vulnérabilités pour le territoire et les citoyens européens

Les attaques majeures contre les systèmes d'information.

« Le niveau quotidien actuel des agressions contre les systèmes d'information, qu'elles soient d'origine étatique ou non, laisse présager un potentiel très élevé de déstabilisation de la vie courante, de paralysie de réseaux critiques pour la vie de la nation, ou de déni de fonctionnement de certaines capacités militaires. »



Les livres blancs de la défense

Le livre blanc de 2008

2008 - De nouvelles vulnérabilités pour le territoire et les citoyens européens

L'espionnage et les stratégies d'influence

« La poursuite des échanges mondialisés et le développement de nouveaux pôles de puissance sont propices à des activités de renseignement offensif visant la France et l'Europe, comme au développement de stratégies d'influences destinées à amoindrir notre rôle dans le monde et sur le marché international. »

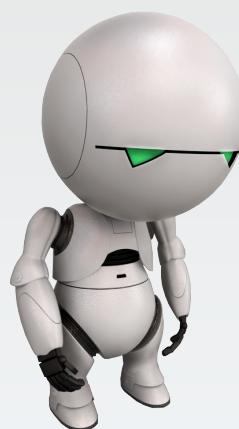
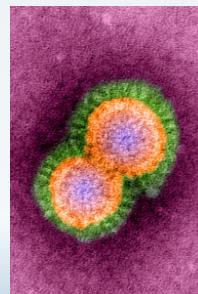


Les livres blancs de la défense

Le livre blanc de 2008

2008 - Hiérarchisation des menaces

1. Attentats terroristes
2. Attaques informatiques
3. Prolifération du nucléaire
4. Pandémie
5. Catastrophes naturelles ou industrielles
6. Criminalité organisée.



4. Les livres blancs de la défense

4.3. Le livre blanc de 2013

Les livres blancs de la défense

Le livre blanc de 2013

2013 - le cyberspace nouvel espace de bataille

« Les menaces et les risques induits par l'expansion généralisée du cyberespace ont été confirmés. »

« Le cyberespace est désormais un champ de confrontation à part entière. »



Virology

Michel Dubois © 2016

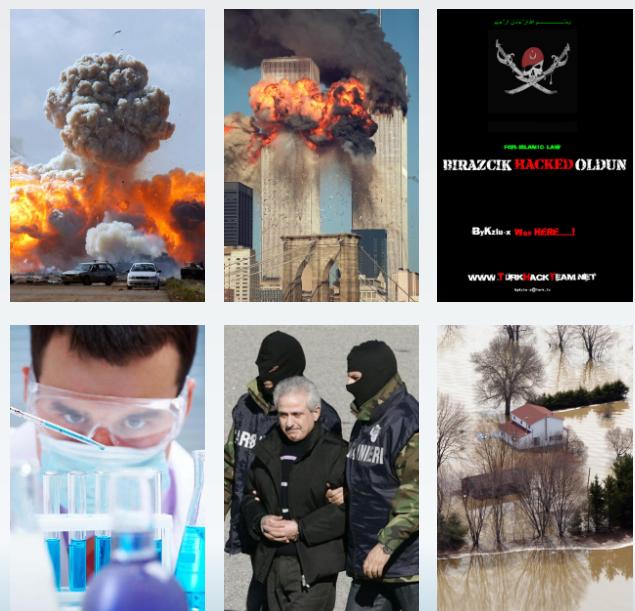
55/136

Les livres blancs de la défense

Le livre blanc de 2013

2013 - Hiérarchisation des menaces

1. les agressions par un autre état contre le territoire national
2. les attaques terroristes
3. les cyberattaques
4. les atteintes au potentiel scientifique et technique
5. la criminalité organisée dans ses formes les plus graves
6. les crises majeures résultant de risques naturels, sanitaires, technologiques, industriels, ou accidentels
7. les attaques contre nos ressortissants à l'étranger



Virology

Michel Dubois © 2016

56/136

Les livres blancs de la défense

Le livre blanc de 2013

2013 - le livre blanc prévoit une posture stratégique visant à :

- ▶ déterminer l'origine des attaques
- ▶ organiser la résilience de la Nation
- ▶ répondre, y compris par la LIO



Discours du ministre de la Défense

Ouverture du colloque
international de cyberdéfense

24 septembre 2015

La cyber n'est cependant plus seulement un enjeu défensif, et je voudrais aujourd'hui m'engager avec vous sur un terrain dont la sensibilité n'a d'égal que l'importance qu'il revêt : je parle ici, employons le terme, de **lutte informatique offensive**.

Pour nos forces armées, le premier enjeu est désormais d'**intégrer le combat numérique**, de le combiner avec les autres formes de combat. Ce nouveau milieu est devenu un domaine militaire à part entière, dans lequel il faut positionner ses forces, défendre sa puissance et y exploiter toutes les opportunités pour vaincre l'adversaire.

L'arme informatique doit apporter un appui maîtrisé aux forces conventionnelles. C'est une nouvelle forme de frappe dans la profondeur, aux effets qui peuvent être considérables. Chacun connaît ici le virus STUXNET qui a frappé le cœur d'un dispositif très fortifié, en l'occurrence une centrale nucléaire iranienne. C'est aussi une forme d'appui tactique aux combattants, par exemple pour perturber les défenses anti-aériennes en leurrant ou en neutralisant des systèmes radars. Certains l'ont déjà fait.

Les livres blancs de la défense

Le livre blanc de 2013

2013 - les moyens pour y parvenir :

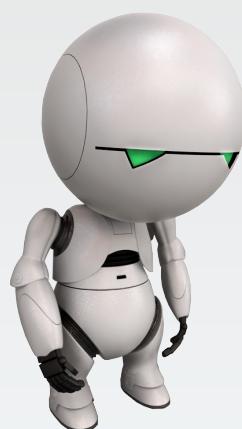
- ▶ autonomie dans la production de systèmes de sécurité
- ▶ renforcement des RH consacrées à la cyberdéfense
- ▶ amélioration de la fiabilité des SI de l'État et des OIV
- ▶ MINDEF - création d'une chaîne de commandement unifiée
- ▶ création des réserves opérationnelle et citoyenne pour la cyberdéfense



Pourquoi la SSI ?

Section 5

La SSI parce que. . .



5. La SSI parce que. . .

5.1. La Cyberguerre

La SSI parce que. . .

La Cyberguerre

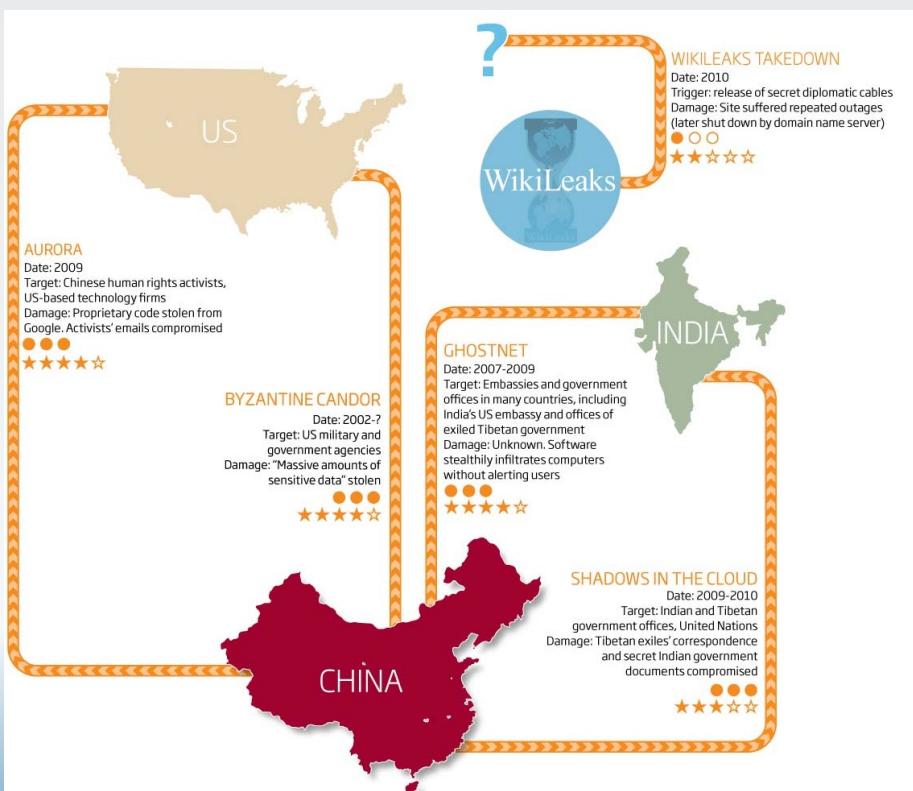


<http://cyberwar.kaspersky.com/>

La SSI parce que. . .

La Cyberguerre

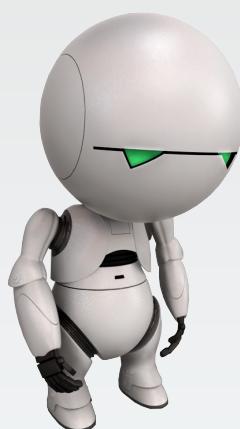
Petit résumé de cyberguerre (1/2)



La SSI parce que. . .

La Cyberguerre

Petit résumé de **cyberguerre** (2/2)

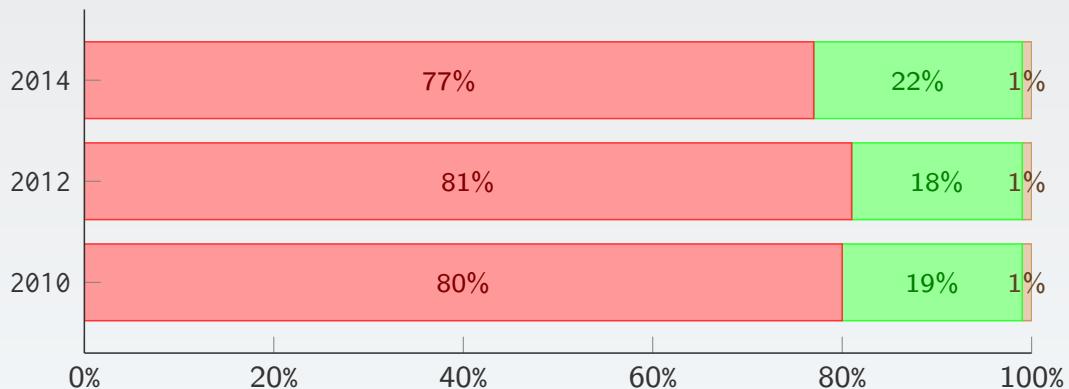


5. La SSI parce que. . . 5.2. Prise en compte du risque insuffisante

La SSI parce que. . .

Prise en compte du risque insuffisante

Dépendance des entreprises à l'informatique



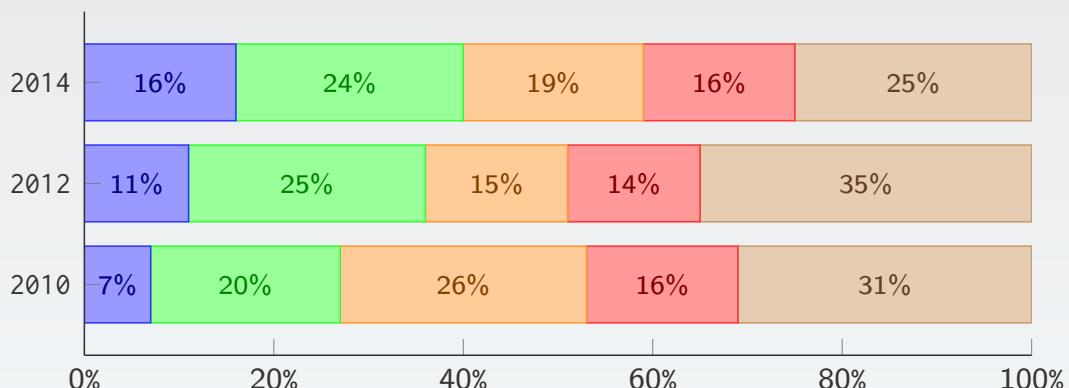
■ Forte: une indisponibilité de moins de 24h a des conséquences graves
■ Modérée: une indisponibilité jusqu'à 48h est tolérable
■ Faible: une indisponibilité même de longue durée n'a pas de conséquence grave

Source : <https://www.clusif.asso.fr/fr/production/sinistralite/>

La SSI parce que. . .

Prise en compte du risque insuffisante

Pourcentage du budget SSI par rapport au budget informatique



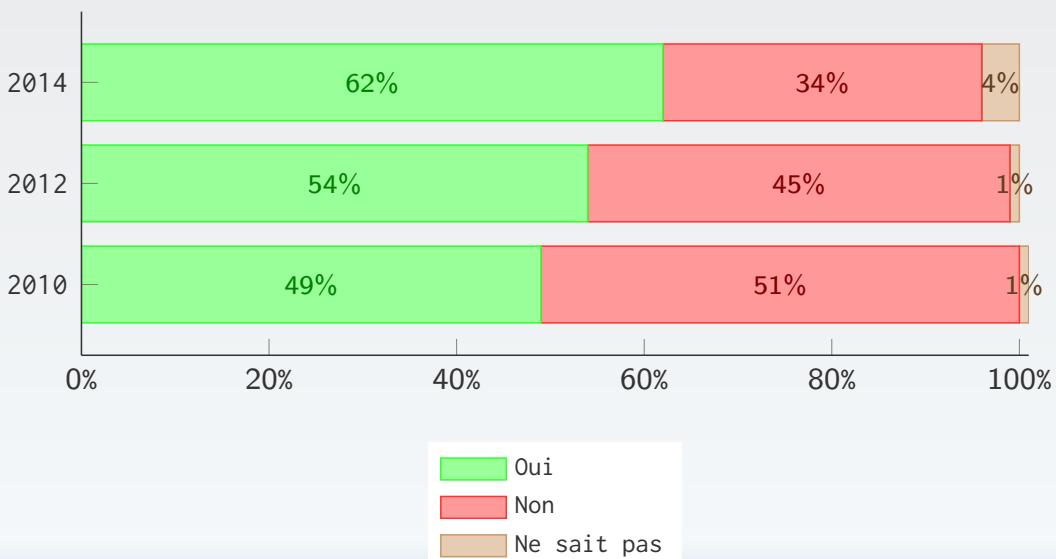
■ Moins de 1%
■ de 1 à 3%
■ de 3 à 6%
■ Plus de 6%
■ Ne sait pas

Source : <https://www.clusif.asso.fr/fr/production/sinistralite/>

La SSI parce que. . .

Prise en compte du risque insuffisante

Fonction de RSSI clairement identifiée et attribuée

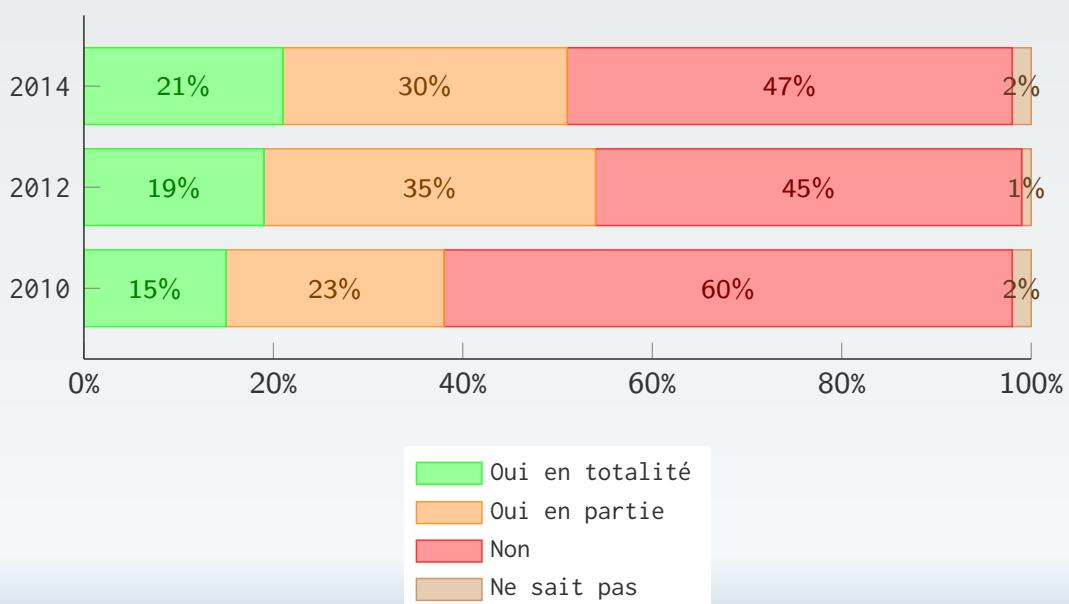


Source : <https://www.clusif.asso.fr/fr/production/sinistralite/>

La SSI parce que. . .

Prise en compte du risque insuffisante

Analyse des risques liés à la sécurité de l'information

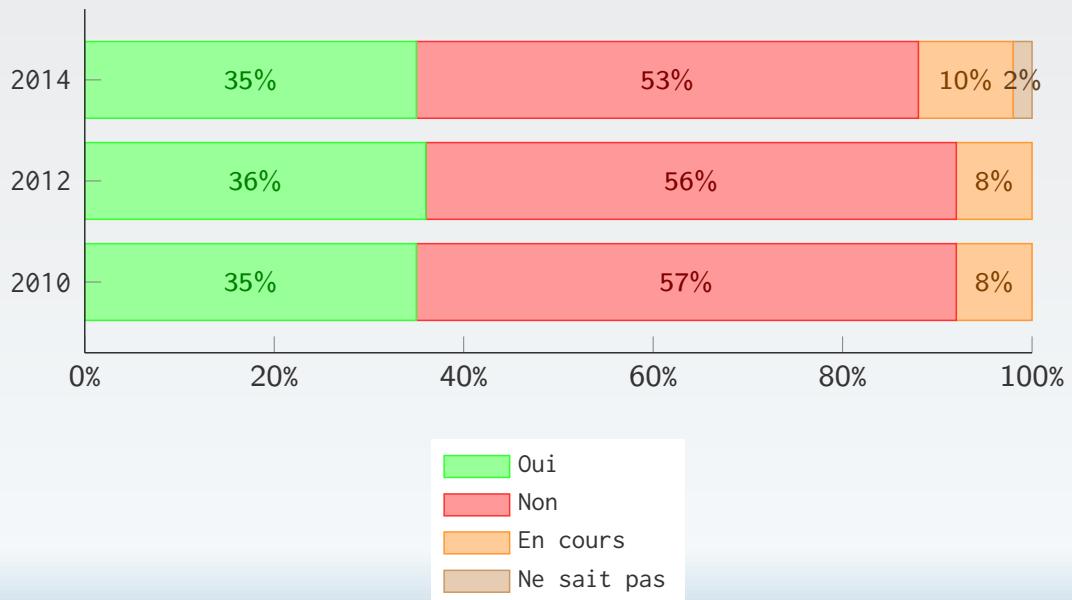


Source : <https://www.clusif.asso.fr/fr/production/sinistralite/>

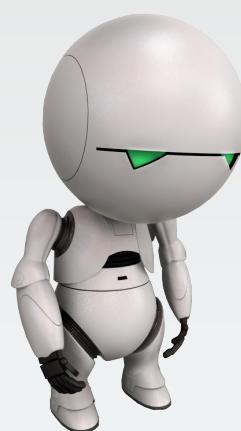
La SSI parce que. . .

Prise en compte du risque insuffisante

Existence d'un programme de sensibilisation à la SSI



Source : <https://www.clusif.asso.fr/fr/production/sinistralite/>



5. La SSI parce que. . .

5.3. Au final

La SSI parce que. . .

Au final

La Sécurité des Systèmes d'Information **parce que** :

Finalité d'ordre opérationnel

Parce que les systèmes et réseaux informatiques sont devenus des **outils de travail indispensables** pour les tâches critiques de la vie professionnelle.

Finalité d'ordre juridique

Parce que la loi l'impose (Article 34 de la loi 78-17 du 6 janvier 1978)
« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

La SSI parce que. . .

Au final

La Sécurité des Systèmes d'Information **parce que** :

Finalité d'ordre stratégique

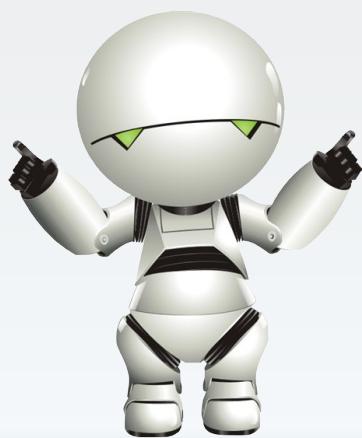
Pour pouvoir attester de son niveau de sécurité vis-à-vis de partenaires et établir des **relations de confiance** lors de l'interconnexion de systèmes d'information et de communication.

Finalité de gestion du risque

Pour être en mesure de gérer et de maîtriser de manière active, préventive et continue, les **risques liés aux systèmes d'information, plutôt que de subir leur concrétisation**.

Partie 2

Définitions



Définitions

Section 6

Information



Information

Taille de l'information

Référence : 1 page A4 enregistrée au format PDF de Adobe

- ▶ 1 page = 184 562 octets
- ▶ 1Mo = 5,68 pages
- ▶ 1Go = 5 817,78 pages
 - ▶ = 11,6 rames soit 29,028 kg
- ▶ 4Go = 23 271,13 pages
 - ▶ = 1 clef USB
 - ▶ = 46,5 rames soit 116,11 kg
- ▶ 1To = 5 957 410,66 pages
 - ▶ = 11 914,8 rames soit 29,72 T



Information

Taille de l'information

Si un grain de sable représente 1 bit... .

1 Mega octet
1 million de bits
1 poignée de sable



1 Giga octet
1 milliard de bits
1 tas de sable de 30cm de côté



1 Tera octet
1000 milliard de bits
1 bac à sable de 50m² et de 30cm de profondeur



Information

Le stockage et le monde réel

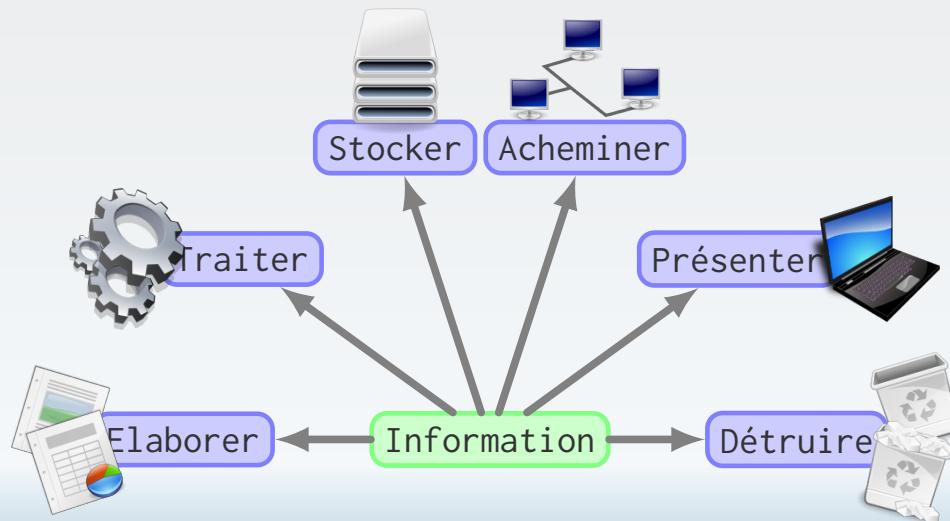
1 kilo octet (Ko)	2^{10} octets	Un petit message
1 mega octet (Mo)	2^{20} octets	Un petit roman
1 giga octet (Go)	2^{30} octets	Une symphonie de Beethoven en son haute-fidélité
1 téra octet (To)	2^{40} octets	10 To = la bibliothèque du congrès américain
1 péta octet (Po)	2^{50} octets	la moitié du contenu de toutes les bibliothèques universitaires des États-Unis
1 exa octet (Eo)	2^{60} octets	5 Eo = tous les mots prononcés par tous les habitants de la terre depuis l'origine
1 zetta octet (Zo)	2^{70} octets	Autant d'information qu'il y a de grains de sable sur toutes les plages du monde
1 yotta octet (Yo)	2^{80} octets	Autant d'information qu'il y a d'atomes dans 7 000 êtres humains

Définitions Section 7 Système d'information



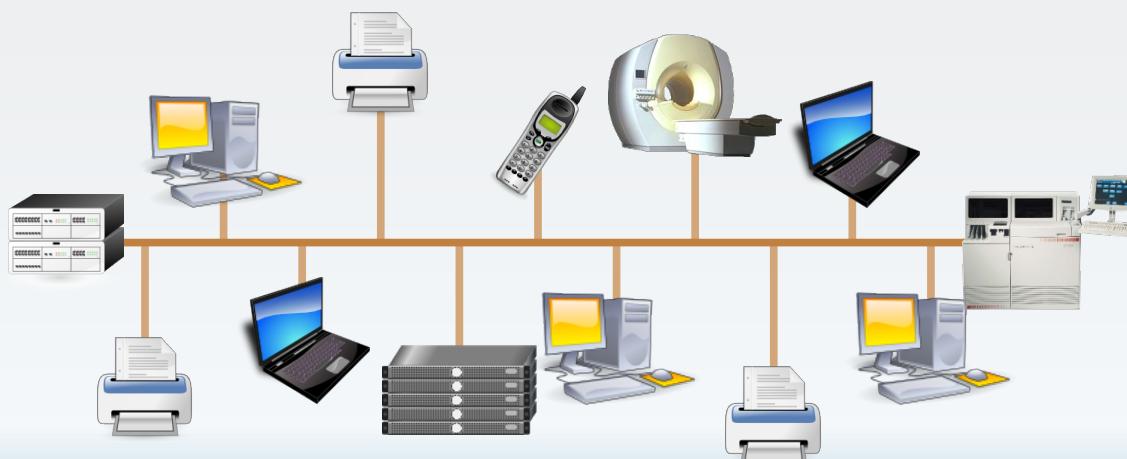
Système d'information

Un **Système d'Information** est un ensemble organisé de ressources matérielles, logicielles et humaines destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.



Système d'information

Concrètement, il s'agit des réseaux informatiques et téléphoniques, des ordinateurs, des serveurs, des autocoms, des téléphones, des télécopieurs, des imprimantes, photocopieurs, des systèmes d'exploitation, des logiciels utilisés sur ces équipements et des personnels qui les administre....



Définitions

Section 8

La cybersécurité



8. La cybersécurité

8.1. Sûreté & Sécurité

La cybersécurité

Sûreté & Sécurité



Sûreté : Ensemble des mesures qui mettent un système et les informations qu'il traite à l'abri de toute **panne**

Virology

Michel Dubois © 2016

85/136

La cybersécurité

Sûreté & Sécurité

საქართველოს პრეზიდენტი

17 დეკემბერი 2008

საქართველოს პრეზიდენტი მიხეილ სააკაშვილი შედგა

18 დეკემბერი 2008

საქართველოს პრეზიდენტი მიხეილ სააკაშვილი განცხადების და მინიჭებულის პაკეტი.

რას უკანასინება ის მოვლენები კვონომიკაში. რომელიც ახასიათებს წევნის ფიციურ ციფრურ მიმღებაში და წევნთვის პრიორიტეტულია. >>

ახალი ამბები

28 დეკემბერი 2008 / 18:00

საქართველოს პრეზიდენტი მიხეილ სააკაშვილმა მინიჭებულის გრძად წლის განმავლობაში გაწეული სამუშაოები შეაჯამა

27 დეკემბერი 2008 / 18:00

საქართველოს პრეზიდენტი მიხეილ სააკაშვილი ბაკურაშვილი ახალი სასტუმრო კომპლექსის გასწონას

Georgian Update

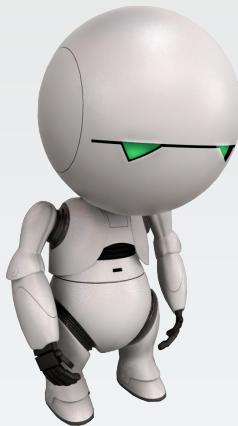
Diversity.ge

Sécurité : Ensemble des mesures qui mettent un système et les informations qu'il traite à l'abri de toute **agression**.

Virology

Michel Dubois © 2016

86/136



8. La cybersécurité

8.2. Sécurité des Systèmes d'Information

La cybersécurité

Sécurité des Systèmes d'Information

La **sécurité des systèmes d'information** recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de **garantir**, au juste niveau requis, **la sécurité des informations** d'un organisme et des systèmes qui en assurent l'élaboration, le traitement, la transmission ou le stockage.

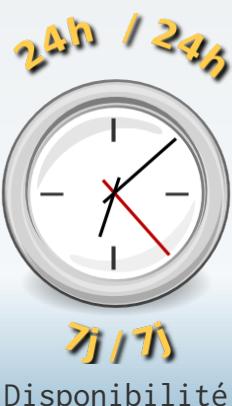
Référentiel général de sécurité



Confidentialité



Intégrité



Disponibilité



Preuve

La cybersécurité

Sécurité des Systèmes d'Information

La confidentialité

Prévention d'une **divulgation** non autorisée de l'information

- ▶ confidentialité des flux d'information dans un réseau
- ▶ **Attaque** : sniffing



Définition ISO 27001

Propriété selon laquelle l'information n'est pas disponible ou divulguée à des individus, entités ou processus non autorisés

La cybersécurité

Sécurité des Systèmes d'Information

L'intégrité

Prévention d'une **modification** non autorisée de l'information

- ▶ intégrité d'une base de données, d'un programme informatique
- ▶ **Attaque** : erreur dans la transmission, écriture illicite.



Définition ISO 27001

Propriété de protection de l'exactitude et de l'exhaustivité des ressources

La cybersécurité

Sécurité des Systèmes d'Information

La disponibilité



Prévention d'un **déni d'accès** à l'information ou à des ressources

- ▶ disponibilité d'un serveur informatique, d'un réseau
- ▶ **Attaque** : DDoS, brouillage de communication radio

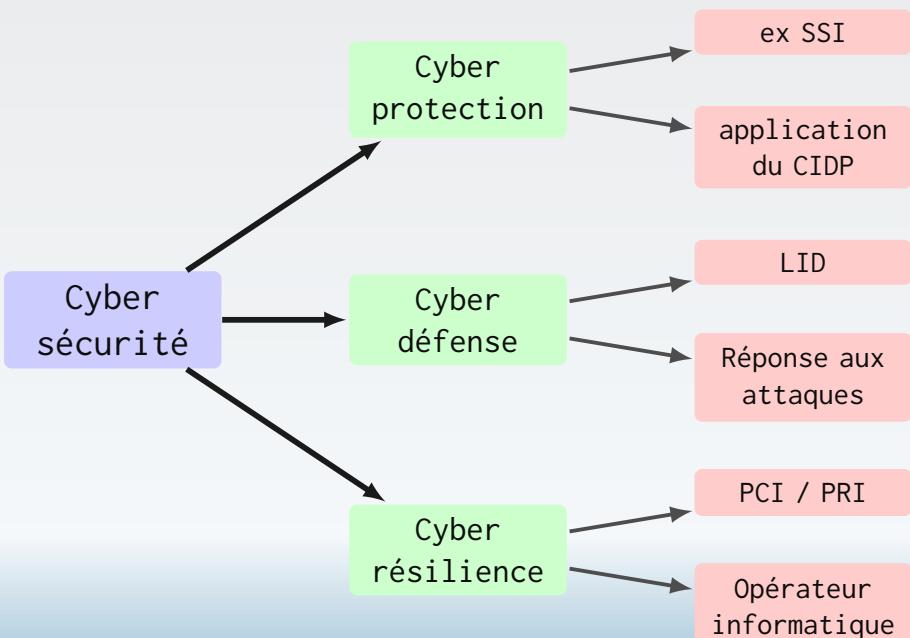
Définition ISO 27001

Propriété d'être accessible et utilisable, à la demande, par une entité autorisée

La cybersécurité

Sécurité des Systèmes d'Information

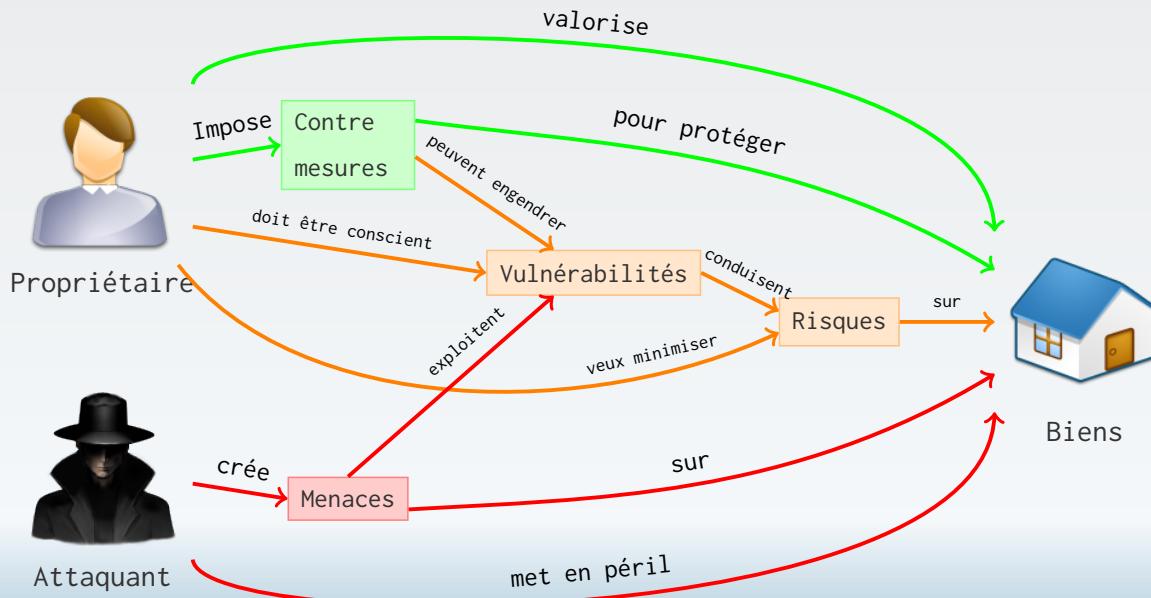
Nouvelle terminologie



La cybersécurité

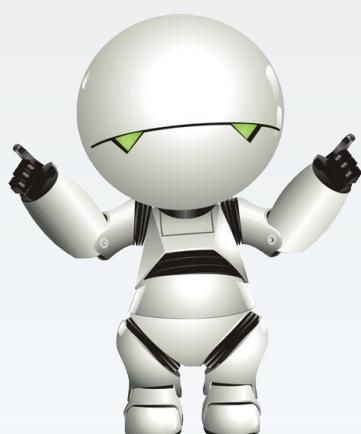
Sécurité des Systèmes d'Information

Le modèle général de sécurité



Partie 3

Le risque informationnel



Le risque informationnel

Section 9

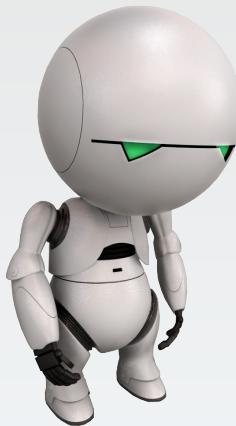
Le risque



Le risque

Sécuriser un **système d'information** revient à essayer de **se protéger contre les risques**, liés à son utilisation et pouvant avoir un impact sur la sécurité de celui-ci, ou des informations qu'il traite.





9. Le risque

9.1. Qu'est ce que le risque ?

Le risque

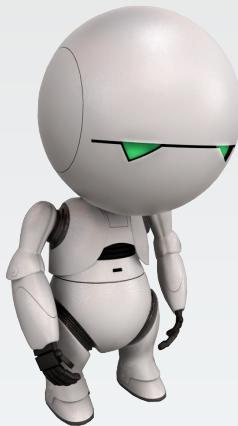
Qu'est ce que le risque ?

Le **risque** est la combinaison d'un évènement redouté et d'un **scénario de menaces**

- ▶ un évènement redouté est un incident susceptible d'avoir un **impact négatif** sur le système d'information
- ▶ un scénario de menace regroupe :
 - ▶ une **menace** susceptible de se concrétiser
 - ▶ une **vulnérabilité** exploitable
 - ▶ une **source de menace** susceptibles d'en être à l'origine

On mesure le niveau du risque en fonction de sa **gravité** et de sa **vraisemblance**

- ▶ la **gravité** d'un risque est mesurée par l'importance de son **impact**
- ▶ la **vraisemblance** d'un risque est sa probabilité d'occurrence



9. Le risque

9.2. Les équations du risque

Le risque

Les équations du risque

Équation mathématique du risque Daniel Bernoulli

Le risque est le produit de la conséquence d'un événement par sa probabilité d'occurrence

- ▶ soit un évènement e avec sa probabilité d'occurrence p et sa conséquence probable c
- ▶ le risque r est alors $r = p \cdot c$
- ▶ Par exemple, si le fait de réaliser l'activité A a une probabilité $p = 0.01$ d'avoir un incident entraînant un coût de $c = 1000$, alors le risque r lié à A est : $r_A = 0.01 \cdot 1000 = 10$.
- ▶ soit une série d'évènements $E = (e_1, \dots, e_i, \dots, e_n)$
- ▶ chaque événement e_i a une probabilité d'occurrence p_i et une conséquence probable c_i
- ▶ le produit $p_i \cdot c_i$ est la valeur de l'alea i
- ▶ le risque résultant R_E est alors $R_E = \sum_{i=1}^n (p_i \cdot c_i)$

Le risque

Les équations du risque

Équation du risque informationnel

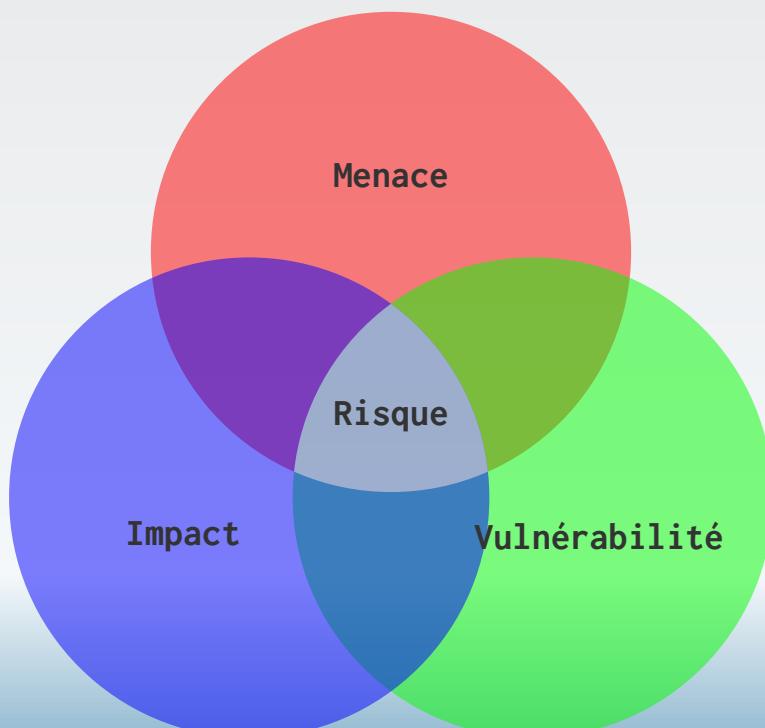
$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité} \times \text{Impact}}{\text{Contre-mesures}}$$

- ▶ La **menace** désigne l'ensemble des éléments, internes et externes, pouvant nuire aux actifs d'une organisation
- ▶ La **vulnérabilité** exprime toutes les faiblesses des ressources qui pourraient être exploitées par des menaces, dans le but de les compromettre
- ▶ L'**impact** est la conséquence de l'exploitation d'une vulnérabilité par une menace

Le risque

Les équations du risque

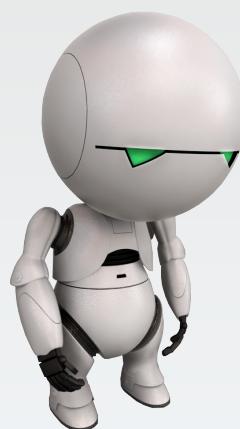
Le risque en résumé



Le risque informationnel

Section 10

La gestion du risque



10. La gestion du risque

10.1. Définitions

La gestion du risque

Définitions

Gestion du risque

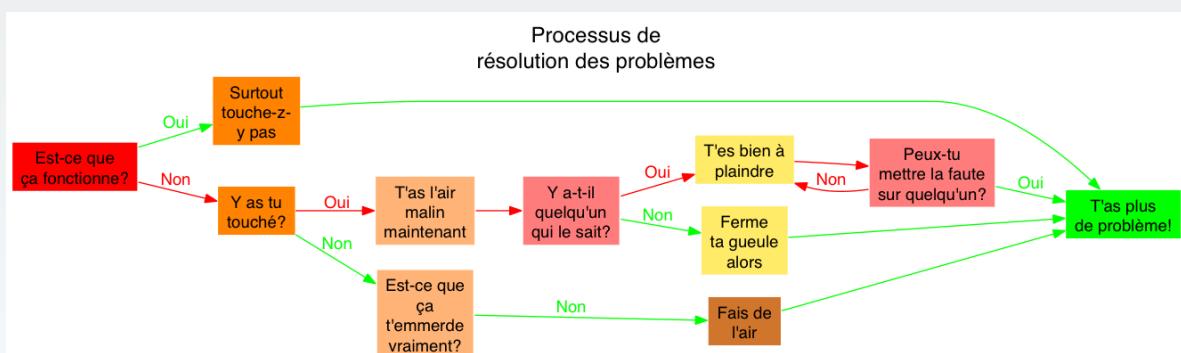
Parallèle à la prise de décision, la **gestion du risque** consiste en :

- ▶ l'**évaluation** et l'**anticipation** des risques
- ▶ la mise en place d'un système de surveillance et de collecte systématique des données pour déclencher les alertes

La gestion du risque

Définitions

Gestion des risques la **mauvaise solution** !



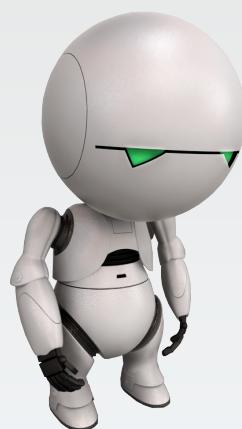
La gestion du risque

Définitions

Les phases de la gestion du risque



1. Établissement du contexte
2. Appréciation du risque
 - ▶ Analyse du risque
 - ▶ Évaluation du risque
3. Traitement du risque
 - ▶ Refus du risque
 - ▶ Optimisation du risque
 - ▶ Transfert du risque
 - ▶ Prise de risque
4. Validation du traitement du risque
 - ▶ Homologation
5. Communication relative au risque
6. Surveillance et revue des risques



10. La gestion du risque

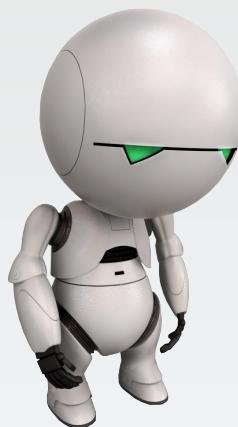
10.2. Établissement du contexte

La gestion du risque

Établissement du contexte

Cette phase permet de **gérer** les risques de façon appropriée, et ainsi de réduire les coûts à ce qui est nécessaire et suffisant au regard de la réalité du sujet étudié

- ▶ **Responsabilité** : Qui pilote le processus ? Qui valide techniquement l'appréciation des risques ? Qui audit le processus ?
- ▶ **Niveaux de risque** : Comment sont-ils définis ? Qui les valide ? Qui décide du niveau de risque acceptable ?
- ▶ **Revue** : À quelle fréquence le processus de gestion du risque est-il revu ? Par qui ?
- ▶ **Traitements du risque** : Quels sont les différents traitements possibles ? Quels sont les critères de décision ? Quelle est la procédure pour accepter ou refuser des risques résiduels ?
- ▶ **Communication** : Comment est assurée la communication entre ceux qui analysent les risques et les parties prenantes ? Sont-ils bien d'accord sur les critères ?
- ▶ **Périmètre** : Quel système d'information ? Quelles contraintes ? Quels enjeux ? Quels biens essentiels ?



10. La gestion du risque

10.3. Appréciation du risque

La gestion du risque

Appréciation du risque

Cette phase représente l'ensemble des processus :

- ▶ d'**analyse** du risque (mise en évidence des composantes)
- ▶ d'**évaluation** du risque (estimation de leur importance)

Les étapes de l'appréciation des risques sont :

- ▶ **Expression des besoins de sécurité** en terme de disponibilité, d'intégrité, de confidentialité et de preuve
- ▶ **Identification et caractérisation** des menaces en termes de gravité et de vraisemblance
- ▶ **Définition des risques** en confrontant les menaces aux besoins de sécurité

La gestion du risque

Appréciation du risque

Niv.	Confidentialité	Intégrité	Disponibilité	Preuve
1	C1 – Public	I1 – Déetectable	D1 – Faible	P1 – Faible
	Le bien essentiel est public	Le bien essentiel peut ne pas être intégrer si l'altération est identifiée	Le bien essentiel peut être indisponible entre 48 heures et une semaine maximum	L'action n'a pas besoin d'être tracée
2	C2 – Restreint	I2 – Maîtrisée	D2 – Importante	P2 – Nécessaire
	le bien essentiel ne doit être accessible qu'au personnel et aux partenaires	le BE peut ne pas être intégrer, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée	le bien essentiel peut être indisponible entre 8 heures et 48 heures maximum	l'action doit être tracée : qui et quand
3	C3 – Confidential	I3 – Intègre	D3 – Critique	P3 – Essentielle
	le bien essentiel ne doit être accessible qu'aux personnes impliquées	le bien essentiel doit être rigoureusement intègre	le bien essentiel peut être indisponible de 2 à 8 heures maximum	l'action doit être tracée : qui, quoi et quand
4	C4 – Secret	I4 – Intègre	D4 – Vitale	P4 – Vitale
	le BE ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître	le bien essentiel doit être rigoureusement intègre et son intégrité doit-être prouvée	le temps d'indisponibilité du bien essentiel ne doit pas dépasser 2 heures	l'action doit être tracée : qui, quoi et quand. L'intégrité des traces est garantie

La gestion du risque

Appréciation du risque

Exemple de typologie des besoins de sécurité

- ▶ **Informations médicales** C3 I3 D2 P3
 - ▶ dossier patient (papier et numérique)
 - ▶ flux de prescriptions
 - ▶ emails échangés avec les médecins de ville
 - ▶ flux de télémédecine
- ▶ **Informations scientifiques** C2 I2 D1 P2
 - ▶ données issues des études statistiques
 - ▶ résultats de travaux de recherche
 - ▶ publications scientifiques
- ▶ **Informations d'administration** C1 I2 D1 P2
 - ▶ dossiers administratifs des personnels
 - ▶ dossiers de notation et travaux d'avancement
 - ▶ budget des établissements, annuaires

La gestion du risque

Appréciation du risque

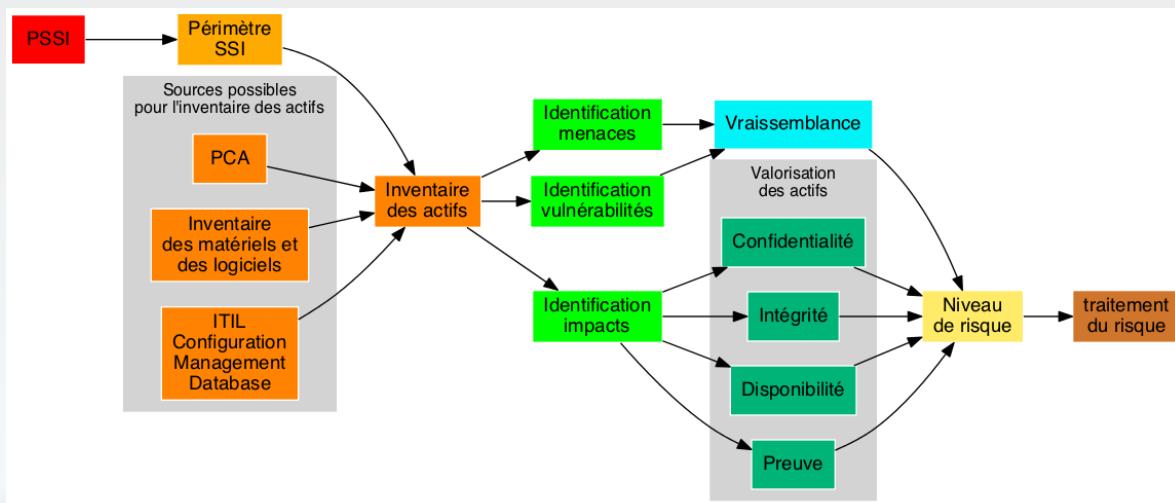
Exemple de typologie des besoins de sécurité

- ▶ **Informations techniques** C1 I2 D1 P2
 - ▶ configurations des équipements
 - ▶ plans d'adresses réseaux
 - ▶ matrices des flux
 - ▶ annuaires techniques
- ▶ **Informations stratégiques** C1 I2 D1 P1
 - ▶ informations d'ordre politique ou stratégique
 - ▶ plans de communication
 - ▶ procédures de gestion de crise

La gestion du risque

Appréciation du risque

Séquence des tâches à effectuer pour l'appréciation des risques



La gestion du risque

Appréciation du risque

Échelle de gravité

Num.	Niveau	Description
1	Faible Perturbation	Dommage non significatif / perturbation Évènement ne risquant pas de provoquer une gêne notable dans le fonctionnement ou les capacités de l'organisme. Cependant, il doit être traité pour rétablir un fonctionnement normal
2	Sensible Dégradation	Dommage important Évènement entraînant des gênes de fonctionnement, susceptible de provoquer une diminution des capacités de l'organisme
3	Critique Arrêt partiel	Dommage grave Évènement entraînant des conséquences graves, avec des conséquences telles que des pertes financières, sanctions administratives, juridiques ou réorganisation majeure
4	Stratégique Arrêt total	Dommage extrêmement grave/inacceptable Évènement susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants ou des pertes financières

La gestion du risque

Appréciation du risque

Échelle de vraisemblance

Num.	Niveau	Description
1	Improbable	L'événement indésirable a peu de chance de se produire
2	Significative	Il existe une faible probabilité que l'événement indésirable survienne
3	Forte	Il existe une probabilité non négligeable que l'événement indésirable survienne et/ou l'événement indésirable c'est déjà produit par le passé
4	Maximale	Il existe une probabilité forte que l'événement indésirable survienne et/ou l'événement indésirable c'est déjà produit à plusieurs reprises par le passé

La gestion du risque

Appréciation du risque

Exemple de résultat obtenu après la phase d'appréciation des risques

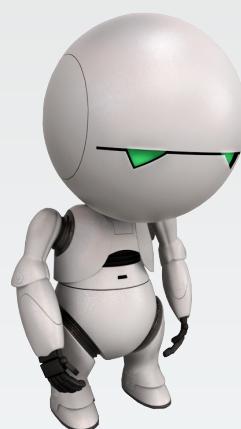
Actif	Responsable	Valorisation				Vulnérabilités	Menaces	G	V	Risque
		C	I	D	P					
Ordinateur portable	Chef de service	4	4	1	1	Équipement léger et peu encombrant	Vol	2	2	4
Serveur BdD	DSI	4	4	4	2	Langage SQL	SQL injection	3	2	6
Local serveurs	DSI	4	1	4	1	Serrure non sécurisée	Intrusion	3	1	4

La gestion du risque

Appréciation du risque

Exemple de tableau pour la classification des risques

Gravité	Vraisemblance			
	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16



10. La gestion du risque

10.4. Traitement du risque

La gestion du risque

Traitemen~~t~~ du risque

Le **traitement du risque** représente le processus de sélection et de mise en œuvre des mesures visant à :

l'**acceptation du risque** l'impact est considéré comme tolérable face au coût des mesures de sécurité

l'évitement du risque la menace est jugée improbable ou l'entité renonce à l'activité source du risque

le transfert du risque par un contrat d'assurance ou par le recours à la sous-traitance

la réduction du risque par la mise en place de mesures de sécurité

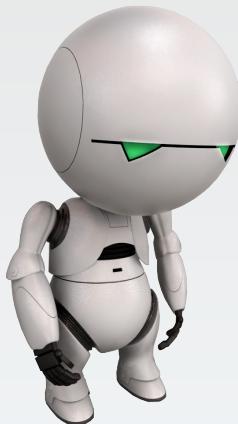
La gestion du risque

Traitemen~~t~~ du risque

À l'issue de cette phase, les risques sont soit **réduits**, soit **transférés vers des tiers** et un ensemble de **risques résiduels** peut subsister.



Nous avons considéré chaque risque potentiel excepté le risque de d'éviter tous les risques.



10. La gestion du risque

10.5. Validation du traitement du risque

La gestion du risque

Validation du traitement du risque

- ▶ Le traitement du risque et les risques résiduels sont **validés formellement**
- ▶ Cette validation correspond à une **homologation de sécurité**
- ▶ L'autorité qui valide le traitement du risque est l'**autorité d'homologation**



La gestion du risque

Validation du traitement du risque

Risque résiduel ?



La gestion du risque

Validation du traitement du risque

L'homologation de sécurité

En s'appuyant sur l'avis des experts, elle permet à un **responsable** de s'**informer** et d'**attester** que les risques qui pèsent sur un SI sont connus et maîtrisés.

La démarche d'homologation

C'est un processus d'**information** et de **responsabilisation** qui aboutit à une **décision** par laquelle le responsable :

- ▶ **atteste** de sa connaissance du SI et des mesures de sécurité mises en œuvre
- ▶ **accepte** les risques résiduels

La gestion du risque

Validation du traitement du risque

Les étapes de la démarche d'homologation

1. Quel SI homologuer et pourquoi ?
2. Quel type de démarche mettre en œuvre ?
3. Qui contribue à la démarche ?
4. Comment organiser le recueil et présenter les informations ?
5. Quels sont les risques pesant sur le système ?
6. La réalité correspond-elle à l'analyse ?
7. Quelles sont les mesures à prendre pour couvrir le risque ?
8. Comment réaliser la décision d'homologation ?
9. Qu'est-il prévu pour maintenir la sécurité et continuer de l'améliorer ?

Le risque informationnel

Section 11

La méthode EBIOS



La méthode EBIOS

Définition

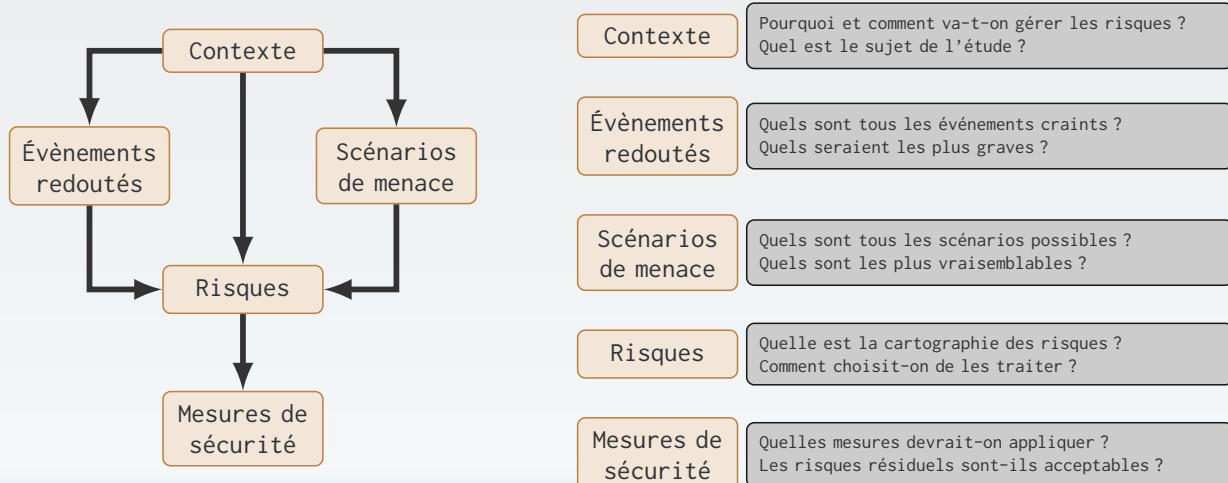
La méthode EBIOS est un outil complet de gestion des risques SSI conforme au RGS et aux dernières normes ISO 27001, 27005 et 31000

Expression des
Besoins et
Identification des
Objectifs de
Sécurité



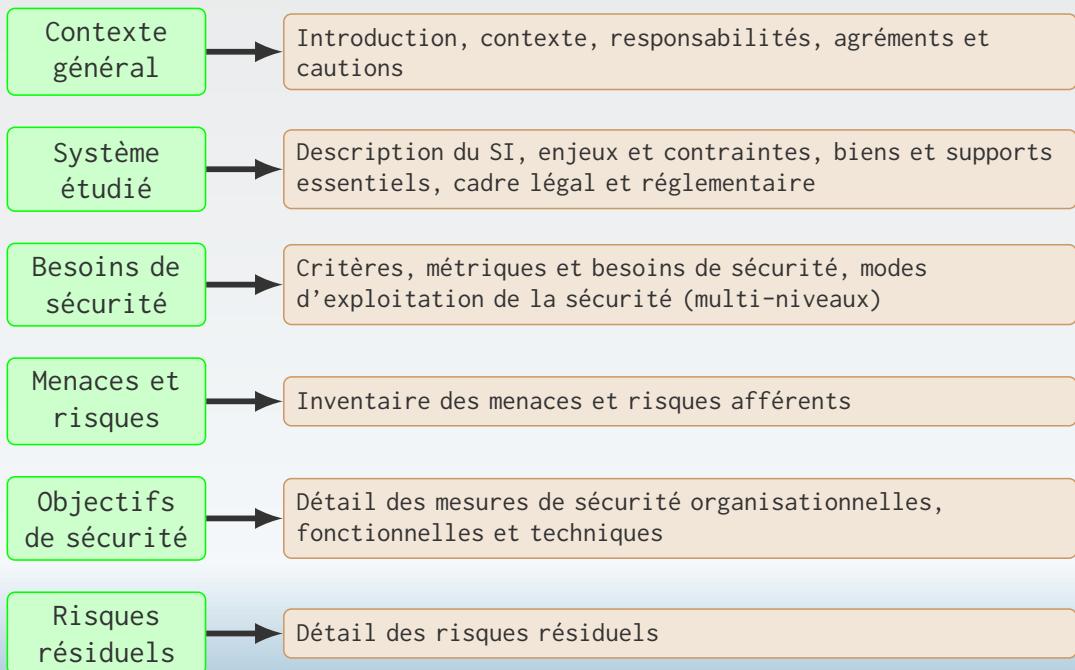
La méthode EBIOS

Les 10 questions essentielles pour gérer le risque



La méthode EBIOS

Fiche d'Expression Rationnelle des Objectifs de Sécurité



Le risque informationnel

Section 12

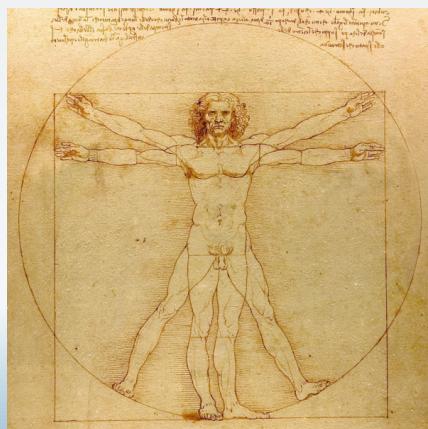
Conclusion



Conclusion

Les cinq commandements de la gestion du risque

1. Il n'y a pas de bonne maîtrise des risques, sans vision prospective
2. Il n'y a pas de gains, sans prise de risques
3. Le traitement d'un risque peut créer un autre risque
4. Plus on complexifie, plus on crée des risques
5. L'homme est au cœur du système.



Conclusion

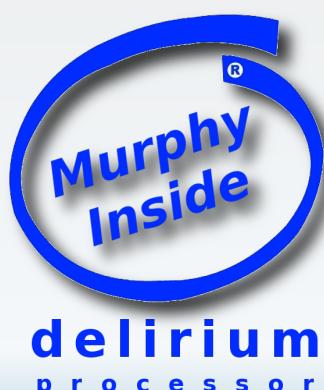
Un risque résiduel spécifique

La loi de Murphy

If anything can possibly go wrong, it will, and at the worst possible time

$$P_M = -K_M \left(e^{-\frac{I*C*U+F}{F_M}} - 1 \right)$$

- ▶ P_M probabilité de Murphy que quelque chose se passe mal
- ▶ K_M constante de Murphy ($K_M = 1$)
- ▶ F_M le facteur de Murphy un très petit nombre calculable uniquement sur une ferme de 386 ordinateurs sous Windows 3.1 ($F_M \approx 0,01$)
- ▶ I est l'importance du résultat
- ▶ C est la complexité du système
- ▶ U est l'urgence & F est la fréquence



source :<http://www.scq.ubc.ca/the-murphys-law-equation/>

Le risque informationnel

Section 13

Licence



Licence

Copyright 2008 - 2016 - Michel Dubois

Paternité



Vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggèrerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre).

Pas d'utilisation commerciale



Vous n'avez pas le droit d'utiliser cette création à des fins commerciales sans autorisation écrite de l'auteur.

Partage des conditions initiales à l'identique



Si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.