

GEORGES ATAYA (SBS-EM)
26 Octobre 2017

Cybersécurité, protection des données et autres **'BUSINESS AS USUAL'** pour PME



WANNACRY

On May 12 a strain of ransomware called WannaCry spread around the world, walloping hundreds of thousands of targets, including public utilities and large corporations.



PETYA

A month or so after WannaCry, another wave of ransomware infections that partially leveraged Shadow Brokers Windows exploits hit targets worldwide.



Macron Campaign Hack

Two days before France's presidential runoff in May, hackers dumped a 9GB trove of leaked emails from the party of left-leaning front-runner (now French president) Emmanuel Macron.

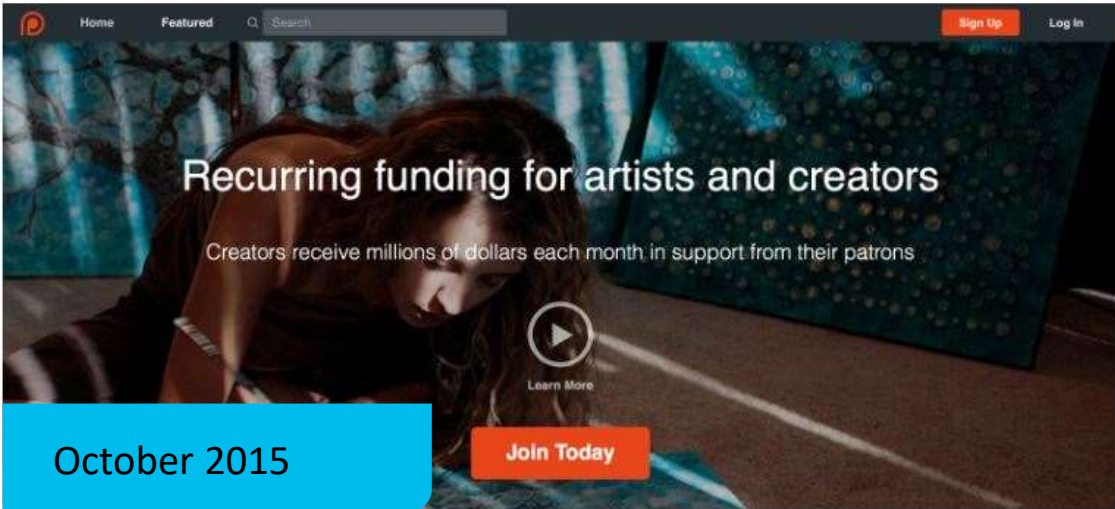


On-line business

Hackers Dump Entire Database of Artist Crowdfunding Website Patreon Online

Chris Mills
Filed to: SECURITY 10/02/15 1:00am

7,591 🔥 4 ☆



October 2015

Impact Team hack could cost Ashley Madison £1.2bn in UK alone

Details of 32 million people that signed up to use the adultery website have been published online.

By Sam Shead | Aug 20, 2015



ASHLEY MADISON®
Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

See Your Matches »

Over 37,765,000 anonymous members!

August 2015

Some examples in Belgium

Cyberattaque à la SNCB: pas de surtaxe à bord jusqu'à vendredi midi

BELGA Publié le jeudi 06 août 2015 à 17h21 - Mis à jour le jeudi 06 août 2015 à 17h22



Recommander Partager 2 Tweeter 9 G+ 0

BELGIQUE Le système de paiement de la SNCB connaît des problèmes depuis jeudi matin 8h30 et ce, tant au niveau du site internet que des automates et guichets en gare.

August 2015

10 November 2017

Piratage de la base de données de Mensura : les données de centaines de travailleurs sur le net



Stagiaire Le Vif

21/11/14 à 14:59 - Mise à jour à 14:59
Source : Rtbf

La société, ayant refusé le chantage des pirates, ne peut que constater la mise en ligne de données de plusieurs centaines de travailleurs.

November 2014

La base de données pour les passeports à nouveau consultable

Accueil - Belgique - lundi 12 mai 2014 19h56 - Belge



(illustration)-Frog 974 - Fotolia

Hacker hielp drugsbende in Antwerpse haven

do 17/10/2013 - 17:50 Wouter Carton

In Antwerpen heeft de politie een man opgepakt die als hacker een internationale drugsbende bijstond. De 30-jarige verdachte kraakte de computers van enkele grote havenbedrijven.

October 2013

La base de données du SPF Affaires étrangères, inaccessible lundi en raison de la remise en état du système informatique du SPF après un piratage constaté il y a quelques jours, est à nouveau consultable, indique le cabinet du ministre des Affaires étrangères Didier Reynders lundi soir.

May 2014

You all remember....

Belgium's telecoms firm Belgacom hacked; officials suspect state-sponsored cyber-espionage

Belgium's largest Telcom 'Belgacom' hacked; NSA could be behind the Attack

by Mohit Kumar on Monday, September 16, 2013

Like 396 Share 405 LinkedIn Share 19 Reddit 8 Buffer 3 Tweet 218 +1 82



Who bugged Belgacom?



Credit reporting firm Equifax says data breach could potentially affect 143 million US consumers

- Equifax said data on 143 million U.S. customers was obtained in a breach.
- The breach was discovered July 29.
- Personal data including birth dates, credit card numbers and more were obtained in the breach.
- Three Equifax executives sold shares in the company days after the breach was discovered.

Todd Haselton | @robotodd

Published 4:34 PM ET Thu, 7 Sept 2017 | Updated 3:25 PM ET Fri, 8 Sept 2017



riminals gained access to certain files in the company's system from mid-June to July by exploiting a weak point in website software, according to an investigation by Equifax and security consultants. The company said that it discovered the intrusion on July 29 and has since found no evidence of unauthorized activity on its main consumer or commercial credit reporting databases.

In addition to the other material, hackers were also able to retrieve names, birth dates and addresses. Credit card numbers for 209,000 consumers were stolen, while documents with personal information used in disputes for 182,000 people were also taken.

Other cyberattacks, such as [the two breaches](#) that Yahoo announced in 2016, have eclipsed the penetration at Equifax in sheer size, but the Equifax attack is worse in terms of severity. Thieves were able to siphon far more personal information — the keys that unlock consumers' medical histories, bank accounts and employee accounts.

Massive Cyber Attack Could Affect 143 Million Americans: Report

Indo-Asian News Service | Friday September 8, 2017



Hackers exploited a vulnerability in the company's website application from mid-May through June. A range of consumer information, the company said.

Hackers Gain Entry Into US and European Energy Sectors, Warns Symantec

Reuters | Wednesday September 6, 2017



Malicious email campaigns have been used to gain entry into organisations in the US, Turkey, and other countries well, Symantec said.

Google Removes Nearly 300 Apps From Play Store That Hijacked Android Devices for DDoS

Shubham Verma | Tuesday August 29, 2017



Akamai has joined hands with major companies such as Google, Cloudflare, Flashpoint, Oracle and Cymru among others to combat cyber threat.

Some India Security Agencies Hit by Cyber Spying Malware: Symantec

Gadgets 360 Staff With Inputs From Reuters | Monday August 28, 2017



Symantec said the online espionage effort dated back to October 2016, according to news agencies.

Airtel, Symantec Partner on Cyber-Security Solutions for Businesses

Press Trust of India | Monday August 28, 2017



The Airtel, Symantec partnership will target the IT security requirements of large enterprises, small businesses, as well as the government.

Popular Robots Are Dangerously Easy to Hack, Researchers Say

Jeremy Kahn, Bloomberg | Wednesday August 23, 2017



These vulnerabilities could allow the robots to be turned into surveillance devices, surreptitiously

US Government Websites Hacked With Pro-Islamic State Rant Attacking Trump

Associated Press | Monday June 26, 2017



A message posted on the website of Governor John Kasich said, "You will be held accountable Trump, you and all your people for every drop of blood flowing in Muslim countries."

UK Parliament Under Cyber Attack

World News | Agence France-Presse | Saturday June 24, 2017



British lawmakers on Saturday said they were unable to access their e-mail accounts remotely as parliament's security team battled against a cyber attack.

CIA Reveals It Was Hacked by an Insider Network of Snack Thieves

Agence France-Presse | Friday June 23, 2017



A report released this week shows the CIA discovered that insider hackers had stolen more than \$3,300 worth of potato chips, chocolate bars and other snacks from its vending machines.

Cybercrime-Related Losses Rose 24 Percent in 2016, Says FBI

Reuters | Thursday June 22, 2017



The FBI's Internet Crime Complaint Center, which was set up in 2000 to receive complaints of Internet crime, received 300,000 complaints during the year from hacking victims.

Qatar Accuses 'Neighbours' Over Hacking That Led To Crisis

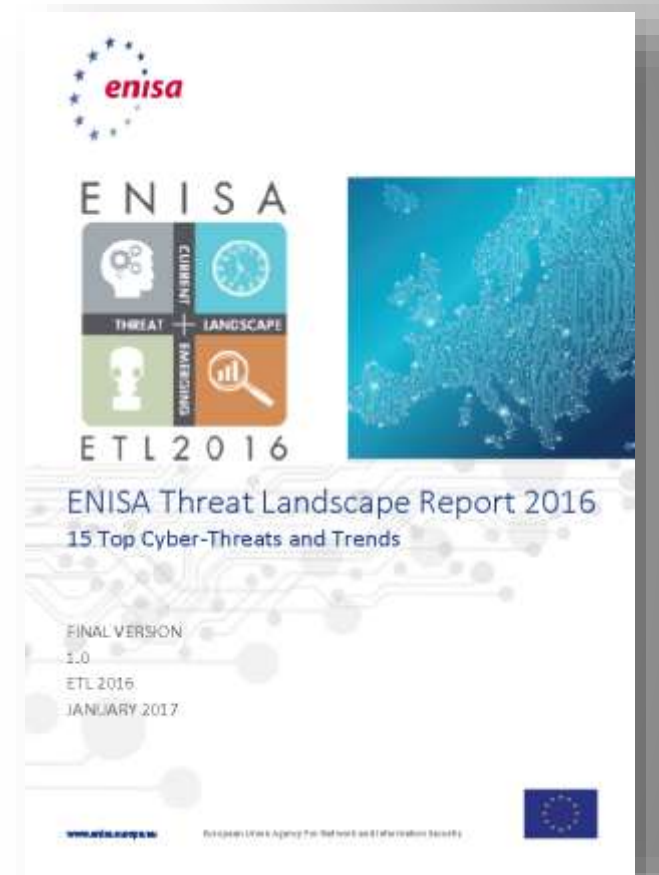
World News | Agence France-Presse | Wednesday June 21, 2017



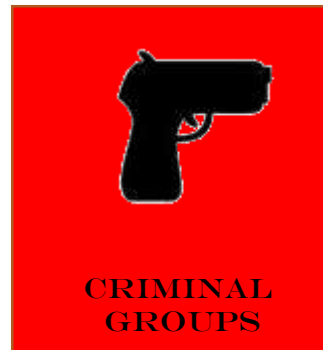
Qatar on Tuesday accused "neighbouring countries", which have cut ties with it, of being behind the alleged cyber attack on Doha's state media which set into motion the current diplomatic crisis.

Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	↑	1. Malware	↑	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Denial of service	↑	↑
5. Denial of service	↑	5. Botnets	↑	↓
6. Physical damage/theft/loss	→	6. Phishing	→	↑
7. Insider threat (malicious, accidental)	↑	7. Spam	↓	↑
8. Phishing	→	8. Ransomware	→	↑
9. Spam	↓	9. Insider threat (malicious, accidental)	→	↓
10. Exploit kits	↑	10. Physical manipulation/damage/theft/loss	↑	↓
11. Data breaches	→	11. Exploit kits	↑	↓
12. Identity theft	→	12. Data breaches	↑	↓
13. Information leakage	↑	13. Identity theft	↓	↓
14. Ransomware	↑	14. Information leakage	↑	↓
15. Cyber espionage	↑	15. Cyber espionage	↓	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down



Sources of external threat



Threat	What They Seek	Business Impact
Intelligence agencies	Political, defense or commercial trade secrets	Loss of trade secrets or commercial, competitive advantage
Criminal groups	Money transfers, extortion opportunities, personal identity information or any secrets for potential onward sale	Financial loss, large-scale customer data breach or loss of trade secrets
Terrorist groups	Production of widespread terror through death, destruction and disruption	Loss of production and services, stock market irregularities, and potential risk to human life
Activist groups	Confidential information or disruption of services	Major data breach or loss of service
Armed forces	Intelligence or positioning to support future attacks on critical national infrastructure	Serious damage to facilities in the event of a military conflict



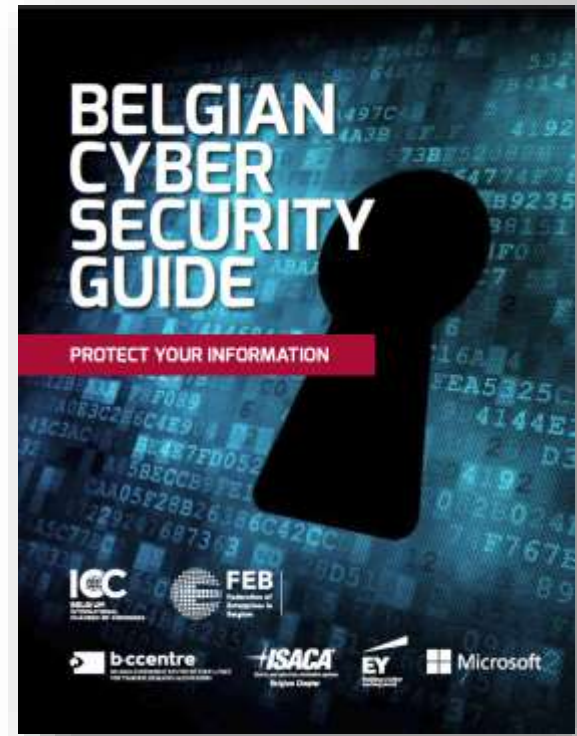
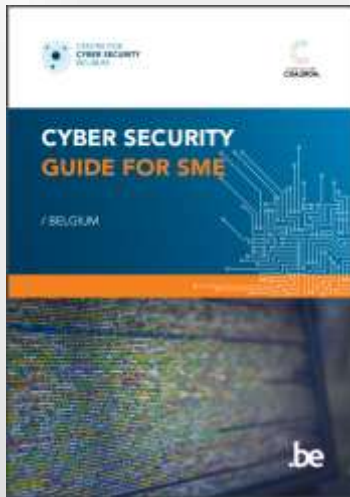

GDPR

General Data Protection Regulation



NIS

New EU cyber security regulations



Awareness Campaigns



**RÉCUPERONS
INTERNET**

 **6,491,641**
BELGES AIDENT LES CYBERCRIMINELS

**Nettoyez votre
appareil ici.**

 **Safeonweb^{be}**

 **.be**



 **Safeonweb^{be}**

Check out the national campaign about strong passwords and participate:

Dutch: www.safeonweb.be/nl/campagnemateriaal
French: www.safeonweb.be/fr/materieldecampagne

THE COALITION

- Cross sector collaboration, uniting **Academic, Public & Private** sectors
- Focus on:
 - **experience sharing**
 - **collaboration**
 - **exchange with peers on actionable, concrete topics**
- Non-profit (by and for members)
- Close collaboration with **Centrum for Cyber Security Belgium**





OUR MISSION

Raise member's cyber security capabilities through cooperation



Experience Sharing

Sharing knowledge, best practices, threats & opportunities.



Operational Collaboration

Peer-to-peer collaboration in a trusted community.



Policy Recommendations

Issuing recommendations for more efficient regulations and policies.



Raising Awareness

Campaigns to raise awareness amongst citizens and organizations.



Conclusions

Cyber threats present
a clear, large and growing risk

Opportunity costs may well
outsize the cost of cyber crime

To achieve digital resilience
collaboration is necessary



CYBER SECURITY
COALITION_{bc}





Executive Education in Digital and IT Management

Executive Master and
Executive Programmes in

- . CIO Practices
- . CIO Leadership
- . IT Business Agility
- . Enterprise and IT Architecture
- . IT Sourcing
- . IT Management Consulting



Solvay Brussels School
Executive Education

Executive Education in Information Security Management

Executive Master in Information
Risk and Cybersecurity

Executive Programmes in

- . Security Governance
- . Information Security
- . Cybersecurity

EDITION FACTS

1.

LEGAL AND MANAGEMENT REQUIREMENTS

Business objectives are combined with applicable legislation to identify Data Protection requirements.

- Data Protection Act 1998
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)



2.

RISK AND IMPACT ASSESSMENT

Risk Assessment and Data Protection Impact Assessment exercises shape the transformation activity.

- Data Protection Impact Assessment (DPIA)
- Data Protection Impact Assessment (DPIA)
- Data Protection Impact Assessment (DPIA)
- Data Protection Impact Assessment (DPIA)
- Data Protection Impact Assessment (DPIA)
- Data Protection Impact Assessment (DPIA)
- Data Protection Impact Assessment (DPIA)
- Data Protection Impact Assessment (DPIA)
- Data Protection Impact Assessment (DPIA)
- Data Protection Impact Assessment (DPIA)
- Data Protection Impact Assessment (DPIA)



5.

SECURITY & BREACH MANAGEMENT

Response management and breach handling activities require due care and adequate preparation.

- Incident Response Plan (IRP)
- Incident Response Plan (IRP)
- Incident Response Plan (IRP)
- Incident Response Plan (IRP)
- Incident Response Plan (IRP)
- Incident Response Plan (IRP)
- Incident Response Plan (IRP)
- Incident Response Plan (IRP)
- Incident Response Plan (IRP)
- Incident Response Plan (IRP)



3.

COMPLIANCE TRANSFORMATION

Transformation includes program and project management, process improvement and the implementation of adequate controls to target protection levels.

- Data Protection Act 1998
- Data Protection Act 2018
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)
- Data Protection Act 2018 (EU Data Protection Act 2018)



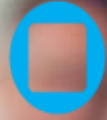
4.

INFORMATION SECURITY AND PRIVACY

Build the secure platform with several architectural layers.

- Information Security and Privacy
- Information Security and Privacy
- Information Security and Privacy
- Information Security and Privacy
- Information Security and Privacy
- Information Security and Privacy
- Information Security and Privacy
- Information Security and Privacy
- Information Security and Privacy
- Information Security and Privacy





ICT CONTROL

Your Trusted Advisor

DPO Mentoring
and support

Management Dashboard

GDPR implementation
activities

Training and Awareness

gdpr@ictc.eu



DPO Circle – Data Protection Association

GET IN TOUCH

European data Protection professionals



Can a CISO act as a DPO?
Georges Ataya on LinkedIn

gataya@solway.edu

[linkedin.com/in/ataya/](https://www.linkedin.com/in/ataya/)

Georges Ataya

gataya@solvay.edu – solvay.edu/it – www.Ataya.info



Career Summary

- Professor, founder and Academic Director of Digital and information security management at SBS-EM
- Managing Director ICT Control advisory firm
- Founded IT Management Academy
- Past International Vice President at ISACA
- Past Partner Ernst & Young
- Past Deputy International CIO ITT World Directories
- Previously Project Manager and Senior IT Auditor

Expertise Summary

- IT Governance (development of Cobit 4 and COBIT 5)
- IT Governance and Value governance (co-author VALIT and supervision CGEIT BOK)
- Information Security Management (Co-author CISM Body of Knowledge)
- IT Audit and Governance
- Information security and risk
- Strategy and Enterprise Architecture and IT Sourcing
- Keynote speaker
- Lecturer at inno.com, Transconstallation academy, Error Management, etc.

Education/ Certification

- Master in Computer Science (faculty of Sciences ULB)
- Postgraduate in Management (Solvay Brussels School ULB)
- Certified Information Systems Auditor (CISA); Certified Information security Manager (CISM); Certified in Risk and control (CRISC); Certified Information Systems Security Professional (CISSP); Certified in Governance of Enterprise IT (CGEIT)

THANKS
DREAM. LEARN. LEAD.



Solvay Brussels School
Economics & Management