GLOBAL CYBER SECURITY CENTER

Newsletter

2018 July August

Cyber Security is our mission

editorial

Invisible security

In these days, I was reading an article by Bruce Schneier "The psychiatric of Securtiy" where I found one of his affirmations more and more current: “But security is also a feeling, based not on probabilities and mathematical calculations, but on your psychological reactions to both risks and countermeasures”. The article touches some aspects that imply the human factor and how much it counts in the choices that we often have to make in our digital life.
For example, we know that when people are under time pressure, they tend to focus more on the losses affecting their immediate task, therefore take shortcuts and ignore policies.
Furthermore, we have reached a point where we expect that the cyber security issue is now applied by companies and then applied by design.
Instead, today the security approach is often an “add-on” and we are very far from the most reasonable approach that is "built-in" function.
I think that for a large percentage of end users would be to make the security aspects and interactions of today disappear from their view, avoiding the user involvement. So, we must to continue the pursuit of secure system development, patching, configuration, and operation as required, but do so without any action required from the users. Security should become invisible and we have just to continue to talk and increase user awareness. We have to bear in mind that complexity for end users is an enemy of strong security.
Implementing an invisible security could be simpler for the user if it reduced or eliminated complex security configurations and user interactions.
Security must evolve along with the systems, with the advantage that users would not need to master the new terms and concepts. Of course, we must consider that there are risks with invisible security that we have to mitigate.
Implementing automated updates, we need to know that they could interfere with other software or generate other issues. We will need mechanisms to verify that the invisible security is enabled and working in a proper way.
Today we have a situation of poor security adoption and practice, that interact with human nature, that scenario requires the next step; offering automated, invisible cyber security as widely as possible. I believe that now is time to consider seriously this approach. So, let's go on vacation with these reflections, enjoy reading and have fun ...

Enjoy your reading

Nicola Sotira
General Manager GCSEC

events

BlackHat USA 2018

Location: Las Vegas, Nevada
Date: August 4-9, 2018
https://www.blackhat.com/us-18/

Now in its 21st year, Black Hat USA is the world's leading information security event, providing attendees with the very latest in research, development and trends. Black Hat USA 2018 opens with four days of technical Trainings (August 4 – 7) followed by the two-day main conference (August 8 – 9) featuring Briefings, Arsenal, Business Hall, and more.

Def Con 26

Location: Las Vegas, Nevada
Date: August 9-12, 2018
https://www.defcon.org/html/defcon-26/dc-26-index.html

DEF CON is one of the oldest continuously running hacker conventions around, and also one of the largest. DEF CON is a unique experience for each con-goer. Speechs, contests, movie marathons, scavenger hunts, music events. DEF CON is what the attendees make of it.

Artificial Intelligence, Robotics & IoT

Location: Marne La Vallée, France
Date: August 21-22, 2018
https://artificialintelligence-iot.enggconferences.com/

Artificial Intelligence, Robotics &Internet of Things (IoT) is the latest trending technology in many fields. AI & IoT 2018 will be a common platform to gain knowledge and share new ideas amongst the Technologist, Professionals, Industrialists, Researchers, Innovators and students from research area of Artificial Intelligence, Robotics and Internet of Things. Experts will share their research experiences and engage in many interactive discussions at the event.
This European AI & IoT 2018 Conference guarantees that offering the thoughts and ideas will enable and secure you the theme: AI & IoT: The Real Race for Future.

in this issue

Switzerland a land where Data Protection rules become a (paying) real asset for individuals

by Laurent Chrzanovski – School of Social Sciences at the University of Sibiu

Following – and even enhancing – European Union's GDPR framework, Switzerland adapted and buffed up its Federal Law on Data Protection.

In most of the European countries, compliance to the GDPR is seen with worry by companies which handle personal data, as the fines in case of data breach will be up to 4% of their yearly incomes. But for the private citizen, GDPR looks like an "after-crash" parachute in case of violation of his/her privacy with, depending of the countries, some ways to receive indemnities from the guilty company or to sue it in courts.

On the contrary, Switzerland – besides adopting the same sanctions and fines for breached data holders – proposed a proactive system to all the inhabitants of the country desiring to anticipate and buff up the protection of their data, through public-private partnerships such as the Swiss Internet Security Alliance.

As a consequence, a whole range of free-of-charge services to citizens has been set up (free hotlines in case of phishing, identity theft, encryption viruses etc.), yet the most visible and interesting effect of this 6-months (r)evolution has been the birth of innumerable cheap and well-thought out "individual/family internet protection" contracts proposed as an additional service by all kind of Swiss Insurance Companies.

A person with Swiss residence can now add to their Civil Responsibility, Car, Home or Health insurance the "Internet Protection" extension, with yearly fees starting as low as 4 CHF (3.2 EUR) and rising to a maximum of 100 CHF (85 EUR) per year according to the coverage the customer desires.

The whole Swiss system is based on an individual compulsory and free-of-charge inscription on the website IDprotect.ch, a service created by I-surance.ch and financed by the insurances fees.

There, each individual – and not his insurance – chooses which data he desires to be protected – personal / intimate pictures, texts, passport/ID card numbers, Credit/Debit card numbers and so on.

EUROSCIPY 2018

Location: Trento, Italy
Date: August 28-September 1, 2018
https://www.researchitaly.it/en/events/euroscipy-2018/

The event is an interdisciplinary meeting focused on the use and development of the Python language in scientific research. It aims at bringing together users and developers of scientific tools, as well as academic research and industry state of the art.

ACS 2018

Location: Trento, Italy
Date: September 3, 2018
https://acs2018-200606.appspot.com//

In Conjunction with the 15th IEEE International Conference on Autonomic Computing (ICAC 2018) and the 12th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO 2018).

The workshop aims to bring the research community together in exploring the use of autonomic computing techniques to address cloud security, as well as techniques and approaches for securing cloud-based autonomic systems.

6th Central European Cybersecurity Congress

Location: Sibiu, Romania
Date: September 13-14, 2018
https://cybersecurity-romania.ro

The only ITU-backed non-governmental yearly cybersecurity eventi in Europe and one of the only non-technical, non-marketing congresses in cybersecurity, awarded the title of "best practices example for Europe", the congress is thought and managed, since its beginning, to allow a perfect interaction between the speakers and the audience.

5th World Machine Learning and Deep Learning Congress

Location: Dubai, UAE
Date: September 30-31, 2018
https://machinelearning.conferenceseries.com/

This conference aimed to expand its coverage in the areas of Machine Learning and Deep Learning where expert talks, young researcher's presentations will be placed in every session of the meeting will be inspired and keep up your enthusiasm. We feel our expert Organizing Committee is our major asset, however Speakers are what make events stand out. World Machine Learning and Deep Learning Congress is bringing the most innovative minds, practitioners, experts and thinkers to inspire and present to the delegates new innovative ways to work and innovate through their data

The role of IDprotect.ch, placed under very strict Federal rules on data confidentiality, is to scan 24/365 the deep web to see if those data are to be found, meaning that they have been compromised. The customer is then immediately called and advised on the procedures to follow and attitude to adopt.

As on the net everything is about time, the team at IDprotect will immediately start to deal with the most urgent technical and juridical aspects (fraud, identity theft, client's assistant to data recovery in case of crypto-ransomware, direct medical assistance in case of a child or teen in the family is victim of grooming/bullying, a.s.o.).

An amazing element, if we take the mid-level and top-level contracts is that for less than a hundred Euros a year an individual is insured as follows:

1. World coverage
2. Help in eliminating all private data leaked
3. Up to 5000 CHF directly paid to replace the damaged device(s)
4. Up to 1000 CHF for undelivered online purchased goods (min. 200 CHF value)
5. Up to one million CHF (850'000 EUR) for lawyer's costs – free choice of the lawyer –, court costs, forensics costs*
6. Indemnity for direct financial losses (for private professionals) and reputation loss
7. Health expenses unlimited coverage in case of psychological consequences for 5 years
8. 300'000 CHF in case of partial invalidity caused by an attack (blackmailing, etc.)
9. 150'000 CHF to the family in case of death (suicide)

* The list of cases covered is impressive:

- Abusive use of identity
- Abusive use of bank / credit card credentials
- Victim of phishing
- Victim of hacking
- Victim of blackmailing or threatening to the individual or his family
- Victim of sexting, grooming, bullying
- Victim of stolen virtual property: intellectual property, author's rights, trade marks and names registered individually, stealth or unauthorized use of private images or confidential texts, a.s.o.

The most important aspect of the new insurance services proposed in Switzerland is the forecasted ability for individuals to obtain (at their choice) a full protection to fit the possible extent of damages and a constant challenge service (except in the USA or some advanced Asian countries) for Company Insurances.

As an example, a "cyber security" insurance for a company in France or Italy, is still based on the gross incomes of the contract buyer, is generally very expensive, and covers a maximum of some millions in case of damage, which is far below the real financial consequences of the most recent global attacks. The reason of this "half-blind" system is that neither the insurance companies nor the companies buying insurance have strict and uniform standards to evaluate the resilience of the infrastructures, the employees' capacities in security basic knowledge and the effectiveness of the CISO/CSO department.

The lack of awareness of the majority of the companies' boards forms the base of the compulsory under-evaluation extent of the damages. Security being immature as a whole, national insurances cannot reward companies which do perfectly comply to all NIST / GDPR frameworks with fair yearly fees and very high refunds in case of attack, pushing several sectors (banking, finance, critical infrastructures) to contract, where possible, an overseas insurance company.

Why is this new-born service predicted to have such a shiny future?

There are many simple reasons creating the ecosystem where insurance

news

The dirty secret about Bitcoin: It's amplifying ransomware, cybercrime, and more
https://www.techrepublic.com/article/the-dirty-secret-about-bitcoin-its-amplifying-ransomware-cybercrime-and-more/
Cryptocurrency is on the rise and creating a lot of potential benefits, but one can't ignore the startling dark side and risks associated with it as well.

Despite potential benefits, cryptocurrency often gets a bad rap. Cybercriminals are drawn to Bitcoin and other currencies like it due to its anonymity and decentralized system, as reported in a new NullTX infographic.

Hide-N-Seek IoT Botnet Starts Infecting Database Servers
https://securityboulevard.com/2018/07/hide-n-seek-iot-botnet-starts-infecting-database-servers/
Hide 'N Seek (HNS), an IoT botnet known for infecting home routers, IP cameras and digital video recorders, has recently started compromising NoSQL database servers.

HNS was discovered by researchers from antivirus firm Bitdefender in January and stood out among other IoT threats due to its use of peer-to-peer communications and its attempt to gain persistence on infected devices.

Popular apps may secretly take screenshots of your activity
https://cio.economictimes.indiatimes.com/news/enterprise-services-and-applications/popular-apps-may-secretly-take-screenshots-of-your-activity/64912573
Some popular smartphone apps may be secretly taking screenshots of your activity and sending them to third parties, a study has found.

This is particularly disturbing because these screenshots - and videos of your activity on the screen - could include usernames, passwords, credit card numbers, and other important personal information, researchers said.

Hidden malware in Fortnite cheating app shells gamers with barrage of ads
https://www.scmagazine.com/hidden-malware-in-fortnite-cheating-app-shells-gamers-with-barrage-of-ads/article/778386/
Gamers who recently downloaded a Fortnite cheating app in order to gain an unfair advantage over fellow players found they had a hard time surviving a barrage of malicious ads that followed.

Andrew Sampson, CEO of the game streaming app Rainway, revealed the scam in a July 2 Medium blog post, noting that the malicious app was downloaded 78,000 can engage at a fair price and high refunds without risk, and all of them are met in the 26-Cantons country.

1) Swiss citizens are often mocked as being "over-insured", which is partially true yet has to be seen, not as a fear but as a knowledge of the costs in case of problems. Civil responsibility protection, healthcare insurance, car insurance, home insurance and many more are compulsory and privately-handled. Among them, the only public one, healthcare, became private - under State supervision for fixing the annual raising of fees, (after a popular referendum held in 1996). State-managed insurance programmes are only the loss of job insurance and the invalidity insurance as well as a small pension fund, to be completed with private ones.

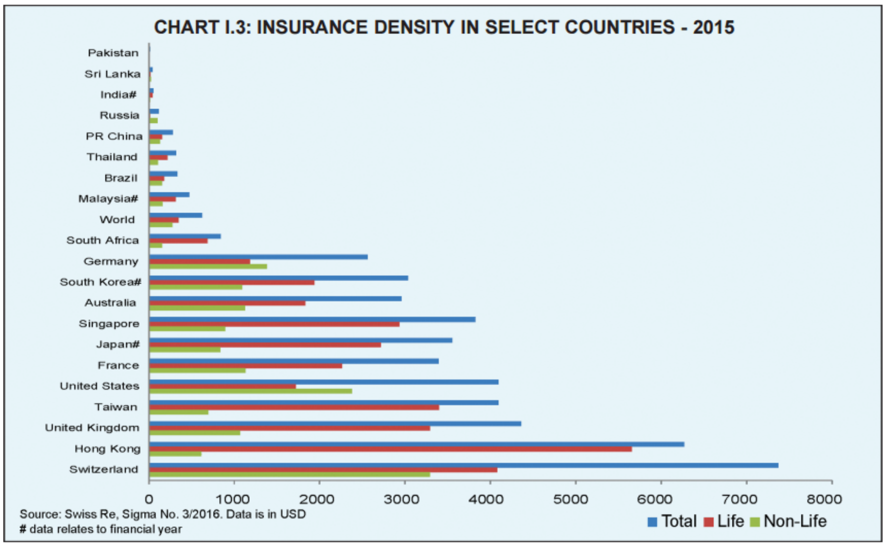


CHART I.3: INSURANCE DENSITY IN SELECT COUNTRIES - 2015

Source: Swiss Re, Sigma No. 3/2016. Data is in USD
# data relates to financial year

2) As a consequence of "everybody being insured" and a general mentality of being collectively responsible of being honest with the insurances, the companies of this sector are fully beneficiary and provide customers several bonuses, which are almost an exclusive Swiss privilege. E.g. we can quote the full refund of broken glass in a ca (no matter the cause: urban violence or simple driving incident), without any "bonus reduction" on the next yearly fee.

Another example is the optional hand-luggage full insurance valid everywhere (bus, train, plane) for less than 50 CHF per year – we were stolen once, and the insurance refunded us in a week not only the full price of the of the photo machine which was inside, but also of the cabin trolley!

3) Being proposed for a very reasonable price as a "plus" to an already contracted - and compulsory by law - healthcare, car or home insurance, the cyber-insurance is ready at a click, benefitting in marketing terms of an already "captive customer" (bonuses) having a long-term relationship with the company.

4) With a knowledge and free choice of "which data to protect" the trust and collaboration between the customer and the insurance is total. Moreover, the insurance platform can use all its assets to scan the net in search of very precise items and reduce at a maximum the duplication of leaked/stolen data when they appear.

5) Without being naïve, several of the services offered are already packed in the compulsory insurances (illnesses, invalidity, death) or in the financial terms most Swiss Banks offer (full credit card data stealth coverage, very limited fee to pay if debit card stolen with PIN, a.s.o.)

Anyway, these new insurances will make some companies (like aggressive ecommerce ones) very careful with Swiss data of unknown provenience or bought on the grey market. The possibility for Swiss citizens to easily benefit from coverage of lawyer and court costs up to one million CHF will give to Swiss citizens the capacity to sue, if needed, a US company in a US court, an action which is financially impossible to any normal European citizen.

times by the time his team reported the issue to the file host and had the app removed from its platform.

Hacker Puts Airport's Security System Access On Dark Web Sale For Just $10
https://thehackernews.com/2018/07/rdp-shop-dark-web.html
If you can't find it on Google, you will definitely find it on the Dark Web.
Black markets on the Dark web are not known for just buying drugs, it is a massive hidden network where you can buy pretty much anything you can imagine—from pornography, weapon, and counterfeit currencies, to hacking tools, exploits, malware, and zero-days.
One such type of underground marketplace on Dark Web is RDP Shop, a platform from where anyone can buy RDP access (remote desktop protocol) to thousands of hacked machines for a small fee.

Attacking hard disk drives using ultrasonic sounds
https://www.helpnetsecurity.com/2018/05/30/attacking-hard-disk-drives/
Another group of researchers has demonstrated that hard disk drives (HDDs) can be interfered with through sound waves, but they've also shown that ultrasonic signals (i.e., sounds inaudible to the human ear) can be used to damage their integrity and availability.

They showed that vibrations caused by specially crafted acoustic signals can cause significant vibrations in HDDs' internal components and therefore negatively influence the performance of HDDs embedded in real-world systems

Timehop discovers hackers swiped even more data than updates, notifications
https://www.scmagazineuk.com/timehop-discovers-hackers-swiped-even-data-updates-notifications/article/1487589
Intruders who infiltrated Timehop's cloud infrastructure came in through an admin account not protected with two-factor authentication and exfiltrated access keys removed more data than originally believed.

The additional user data stolen included dates of birth, gender and country, the company's COO Rick Webb told SC Media.

IoT Robot Vacuum Vulnerabilities Let Hackers Spy on Victims
https://threatpost.com/iot-robot-vacuum-vulnerabilities-let-hackers-spy-on-victims/134179/
Researchers have uncovered vulnerabilities in a connected vacuum cleaner lineup that could allow attackers to eavesdrop, perform video surveillance and steal private data from victims.

Two vulnerabilities were discovered in Dongguan Diqee 360 vacuum cleaners, which tout Wi-Fi capabilities, a webcam with night vision, and smartphone-controlled navigation controls. These would allow control over the device as well as the ability to intercept data on a home Wi-Fi network.

Fake News: What's going on?

by Gianluca Bocci – CERT, Poste Italiane

Politics always tried to regulate the correct use of media, to protect citizens, companies and the Government: in the last years, this applies also to digital media, which provides access to largest number of every kind of information, like social platforms (chat services, blogs, forums, social networks).

With the Net we have overcome traditional communication, and people can now share experiences, opinions and sensations, but for the first time we must also face a new kind of problem, as, first of all: how reliable are the news, which could have been manipulated or altered (fake news)?

For these reasons, new rules and strategies for a quality information on the Internet are increasingly necessary.

Last year, Germany passed a law obliging social network with over two millions users to remove inciting hatred contents and to block offensive and violent fanpages.

In the same year, in Italy, the Parliament has introduced a draft bill about fake news and incitement to hatred on the Internet.

In the meantime, Internet tycoons are trying to establish their responsibilities for information dissemination: false ones, which conflict with their policies, or national and international laws, are removed. This goes smoothly. But there is a grey area where action could be tricky and there is a risk of impacting on one's personal freedom. We are talking about those information which distort the true picture but are also personal opinions: they could be matter of criticism, nevertheless are the result of that freedom of speech that must always been protected and defended.

Facebook is currently working on this issue, with communication professional help: they are trying to improve the platform, removing fake news and deleting fake accounts reported by users but also with Machine Learning techniques, offering customized information, so as to become a reliable source of information.

A the end of 2016, Germany, France, the United Kingdom, and Netherlands, have started experimenting these new processes, engaging the so called fact checking organizations: when a user finds what he considers fake news, he reports it to Facebook, which forwards it to one of these organizations and waits for its response. Facebook is, as well, are boosting the related articles: links provided to the users that redirect to articles about the same subject, so as to deepen the information the user looked for.

It is therefore obvious that things are happening in this field: there is still much to be done, in terms both of law regulations and of technical developments, for instance making use of machine learning much more and raising awareness among users.

The impact of the disinformation on the stock market

by Massimo Cappelli - GCSEC

This article intends to share a reflection more than to provide answers, as it raises a number of interrogations any responsible of Information Security should ask himself in short and long terms.The Information Security is defined as a whole made of processes and methodologies, designed and implemented to protect private information, sensitive or confidential, may they be digital, printed, or in any other form, against the unauthorized access of their use, misuse, divulgation, destruction, modification or damage.

Often, the Information Security is identified with the IT security, yet the last concerns only a part of the activities to be done, as the information travels through different means and not only through digital networks. The evaluation of the risk pending on information should not be based only on considerations of merely "IT type", but has to be a process including the evaluation of places as well as persons too. This has been clearly demonstrated by Kevin D. Mitnick in his 2001 best-seller "The art of deception", where he shows a series of cases where it is possible to recover useful information for one's own goals, simply speaking with people and collecting parts of information which, once brought together, create a solid base of credentials enabling the access to further information. For this, in some realities, we use the term of "information protection", exactly to indicate those processes and methodologies included within Information Security, but with a much wider perimeter in comparison to IT security.

In the biggest part of the cases, the protected informations are those of the company. Our attention is looking inwards: information on clients, contracts, strategies, brevets and so on. The first question is then to define the perimeter of competency. Is it sufficient to monitoring the use and the protection of the internal information? Probably not. To protect one's own company, it is compulsory to look also outwards, to those threats which could anyway harm the reputation of our brand or of our business. Some examples to be used could be the phishing websites or the profiles of fake consultants pretending to be belong to the company in order to steal information or credentials from the client. All the banking institutions do monitor the web to spot and block the phishing websites, i.e. they look outwards the perimeter to block any toxic news for the company. But is it sufficient to monitor and to verify only the unauthorized use or the abuse of the trademark? Or do we have other aspects to take into consideration?

In the last years, the newspapers were flooded by articles, discussions and declarations on the “fake news” phenomenon, used for disinformation, mainly in the political field or for direct economic gains. As an example, the "endorsement" of Pope Francisc of the candidate Donald Trump was shared and commented more than 960.000 times on Facebook. Who knows if this small element did have an influence on the candidate's election or not?

It happened to all of us to see that a friend or a colleague was reporting to us a fake news. Probably, we also were victims and unconscious transmitters of at least one fake news, read on social network, quickly, between a croissant bite and a coffee sip at the bar.

Disinformation can occur through an incomplete representation of the facts, a fake representation of the facts or a manipulated representation of the facts. The objective of the agent spreading the disinformation is to push the news as far as possible on all communication means, driving the readers into a precise conviction.

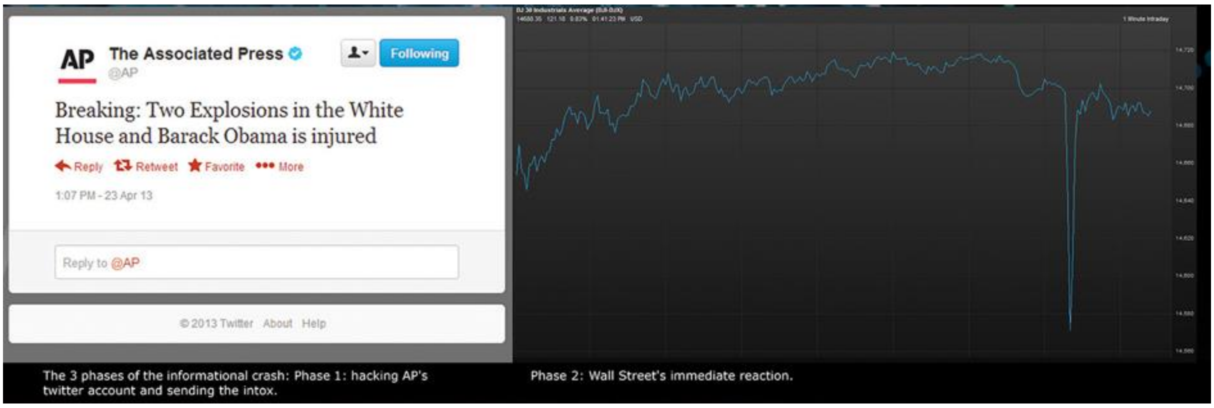
Disinformation has a simple scope: to address the reader to a determinate position, may it be in favor or against an argument. It is created to generate a feeling of empathy or of repulsion. This feeling, sometimes, can lead to concrete actions such as protests, boycotts or manifestations.

If we stay focused on the last American elections, we can give as an example a soft drink case. On mid-November 2016, a blog of American conservatives reported an interview to the CEO of the society producing this soft drink, in which he would have declared (obviously at the conditional form): “CEO Tells Trump Supporters to Take Their Business Elsewhere”. The news was completely distorted both from its source and by who forwarded it, but its impact on the company seems to have been real, both in terms of appreciation of the company and in terms of value of its title on the stock exchange. The agreement ranking (sentiment) towards the company sunk by 35%. The title price, the same day of the "news" publication, sunk by 3,75% and by more than 5% in the range of the whole months. It is still possible that the two reactions could have been dissociated, yet it remains a very important study case for the analysts of brand reputation and communication.

Out of the electoral context, another case which made history was the one who concerned a pharma company we will name XY. In January 2012, an article appeared on Seeking Alpha, a finance-specialized website. It stated that the company XY, listed on Wall Street, was working on the development of a treatment against cancer, cheaper and more competitive than the ones of its concurrence. In five months, the company's title totalized an increase of 263% of its value, maybe because of the publication of that news. The SEC (Security & Exchange Commission) discovered that in fact the article had been commissioned by the same pharma company XY, through an indirect payment. As a result, the stock exchange rate of the title sunk abruptly.

This technique, in the past, was known as “Pump & Dump”, which meant to "pump" the title value thanks to fake news leaving to understand that huge increases of the value will take place, and then "dumping" it once the desired value was reached. It is one example of financial fraud where the worse informed people pay the consequences.

Another case, in 2013, had a systemic impact. The Tweet published on the Associated Press (AP) account, stating that an attack took place at the White House and that President Obama was wounded, "burnt" more than 130 billion USD in the NY stock exchange, before it has made been public that the AP account had been hacked.


AP The Associated Press
@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

1:07 PM - 23 Apr 13

Reply to @AP

© 2013 Twitter About Help

The 3 phases of the informational crash: Phase 1: hacking AP's twitter account and sending the intox.

Phase 2: Wall Street's immediate reaction.

Let us suppose, hypothetically, that we are company Beta, desirable on the market as we are present in various geographic areas, we have consolidated infrastructures with solid trade deals and a monopolistic position on some markets. The title value is high and potential variations could be very costly to the actual stock-holders. If the Alpha company would be interested in the Beta one, wishing, with unfair means, to buy a part of my titles to have influence on my strategies or to consolidate its own presence inside Beta, could it use disinformation to lower the value of my title and buy more of them?

Disinformation activities can be on short or on long term. Probably, if we were speaking with an English CEO or with an Asiatic CEO, even their own conceptions of "short" and "long" terms would raise not a few questions.

Option 1: If I was the Alpha company, I could make publish from several sources a fake declaration of the Beta Company's CEO, like in the case of the soft drink we quoted before. This initiative could lead to a lower value of the Beta company stock title. The Alpha company could then profit of the moment to buy a part of the titles for a ca. 5% cheaper price than the normal one, buying them indirectly and at different moments not to raise the attention.

Option 2: If I was, again, the Alpha company, I could also make publish information on the Beta company, similar to those we saw on the pharma company case. In this option, the objective would still be to buy titles, but through a process of discredit of the targeted company. Investors could lose their trust after reading fake news on the future winning strategies of the company, then denied, and hence make the speculation bubble explode. There are various controls of the vigilance commissions, but I bet that with due precautions and, if well planned, different modes to buy, even indirectly, titles, without being unveiled do exist, even more if they are backed by governments.

Option 3: The disinformation activity could also be led on the long term, using fake profiles. Let us suppose we can dispose of a certain quantity of fake profiles on diverse social media and let us suppose that those fake profiles start to share not very fine information on the Beta company: service disruptions, mediocre quality of the products, untrusty employees, management scandals. Those fake news, as many little drops, would be massively reversed into an ocean of information, polluting it. These information quantity is hard to cream off. We can remember the sentiment analysis that could bring the fake news, sinking the trust on the products and hence their sales. The products sold on eCommerce websites do bear all the client's "recensions". So we can defy anyone not to think twice before buying a product after reading two positive and one negative recension, or the way other. The negative recension will influence the reader's psyche much more than the positive ones.

And if, instead of a company, it was a country? A country which could be, logistically speaking, a ramp for economic initiatives or for the transit of important international infrastructures. To discredit the country's reliability as well as the one of its rulers could happen through disinformation campaigns on fiscal politics, low quality tourism, to put it shortly on all those indicators which could help destabilizing or impoverishing that country, allowing then a "sacking" of its resources or infrastructures. Its GDP would fall because of the lack of tourism revenues or of the internal investments into productive activities. The GDP fall leads to a fall of the tax incomes, which leads to a lack of covering the costs of infrastructure maintenance. But to cover this lack of covering and to maintain its infrastructure, the country is obliged either to sell a part (or all) of it or to take further debts. All that being, of course, a work hypothesis.

The financial market is subject to key information it receives and tries to convert into value. We must also think to the High Frequency Trading systems using mathematic algorithms; some of them are already equipped with capacities of quantitative Big Data analysis and of news parsing system to monitor the news in real time and adjust the values of the transactions, taking into account also other information than the merely financial ones.

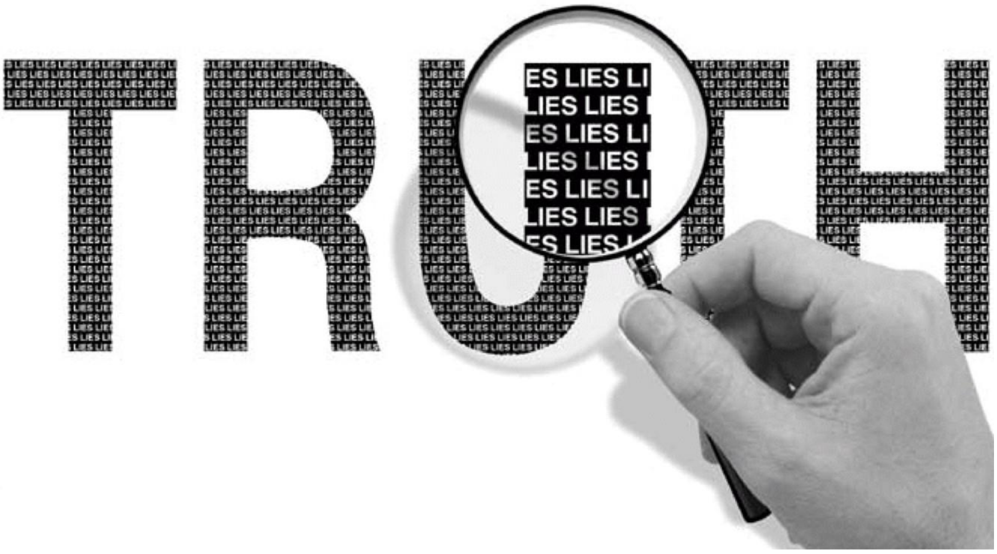
The presence of outnumbered information which reliability is not verified and whose source is not classified according to its own reliability can lead, in the future, to bigger and bigger distortions of the market, as well as politics of expansion - even geo-economical - through the use of information. The High Frequency Trading systems will be more powerful even and will be more and more confident on their own analysis and judgements made on Big Data.

If we add that, in a nearby future, even the individual investors will have a broadened possibility to invest with higher frequencies, we can only deduce that a correct use of information has become vital for the markets.

How to protect ourselves? This is the last interrogation we raise in our essay.

Certainly, all actors should take part into the protection of the financial system. To blame and prosecute the publishers of "fake news" is an activity, by itself commendable, but which would request timeframes which are not in accordance with the markets' volatility.

Certainly, it would be possible to impose some rules on the selection of the sources by the High Frequency Trading systems, through a reliability certification based on the reliability of the information issued by a source during the time. In this way, we could avoid to run the risk of impacting with polluting sources but we would not solve the potential problems of compromised accounts such as in the Associated Press case.



From a company point of view, a fundamental rule is to "communicate first". It is the basic rule to manage a crisis but in a society so invaded by information, it must become a daily activity. In the book “*Deception – Disinformazione e propaganda nelle moderne società di massa*”, the author argues that "the speed is an essential element, because what matters is the first affirmation: all further denials have no efficacy".

It is hence urgent that companies start to build structures able to monitor social media, to analyse information published there and to verify their potential impact on the company in order to make anticipated moves through press communiqués devoted to define clearly the position of the company. By monitoring the social media, we do not mean only the "classical social media". The analysis must be led also on a multi-dimensional level, i.e. by verifying that there are no diverse ties leading back to the same nest, the very source of a disinformation attack.

We do not have to pursue the news to confine it, deny it or correct it. A badly dealt information can quickly transform into a Hydra of Lerna. A clear, official position of the company, well structured and widely diffused, get take stakeholders rid of doubts and uncertainties. In order to do this, we have to build a capillary communication system able to catch all the levels of stakeholders. The information must be simple, linear and easy to understand, with different levels of detail based on the needs of the stakeholders we want to reach: financial analysts, consumers' associations, consumers, vigilance institutions and so on. In the information era, the very same information is the best weapon we can use.

Thus, the perimeter of the protection of the information, for the companies, could be widely broadened. This could ask for additional efforts and always more transversal competences, with quick-response teams delivering not only technical but also communication solutions, helping the press office and the communication office to lead information operations in order to contrast disinformation.