Mini Review

BIOMEDICAL Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717.BJSTR.2019.14.002488

The Consideration of the Human to Protect against Cybercriminals

Nadine Touzeau*

Profiler, Net-Profiler-Behavioral and Environmental Analyst-Researcher, France

***Corresponding author:** Nadine Touzeau, Profiler, Net-Profiler-Behavioral and Environmental Analyst-Researcher, France

ARTICLE INFO

Received: January 24, 2019

Published: February 05, 2019

Citation: Nadine Touzeau. The Consideration of the Human to Protect against Cybercriminals. Biomed J Sci & Tech Res 14(1)-2019. BJSTR. MS.ID.002488.

Keywords: Net-Profiling; Economic Cybercrime; Transverse Zone; Cybersecurity; Virtual Space; Behavioral Differentiation; Avatarization; Virtual Intelligence

ABSTRACT

For years, cybercrime has been secured by antimalware software and digital services, mainly involving engineers with various professional skills in the fields of IT and digital technology. Thus, the company, the administration, the organization feel protected against cybercriminals. It must be said that cybercrime is changing considerably. In a press article and according to serious studies including Norton [1], we talk about 100% growth in cyber-attacks. What company would not wish such economic development. The question that comes back to the mind of structures wanting to protect economic, state, associative and even personal environments is: why don't our antimalware and digital services protect us? One of the answers I would like to give is: have you thought about the human being? Man is at the heart of every act, even virtual ones. However, it is not considered at its right place and value. It is not even integrated into cybersecurity despite the statistics. The prestigious firm Deloitte considers them at 63% (2, 2018). That is 63% of cybercriminal acts are caused by humans, by malice or clumsiness.

Introduction

Safety in France is considered as a right. Concern about implementing it is in fact an overflight, not an in-depth treatment. Contractors, administrations, organizations will rely on law enforcement external to their environment to secure themselves. Faced with cybercriminal threats and the implementation of a law initiated by France to protect internal company data (GRPR, 5), companies are beginning to doubt the usual protections around antimalware and digital services. Being strongly impacted by cyber-attacks, private or state structures are looking for solutions to protect their assets, data, customers, bank accounts, research. Their concern is perceptible (6) as to whether their protection against cyber-attacks is credible, given that humans appear to be the major actors in their cyber concerns.

Considering that the company does not know how to protect itself too well by cultural deficiency and that humans are the main cause of cyber-attacks, it is necessary to question the protection of its environment. In particular, the fact that protections, whether in real or virtual space, favour the use of technology and rarely of the human being. How can we protect ourselves other than through traditional schemes with means? How better detect these cybercriminals? What would be the impact of choosing human protection? Articles are regularly read indicating that leaders are not integrating cybercrime as a priority [1]. Most structures underestimate a cyber-attack, we still have to realize that there's a cyber-attack, even if they have already suffered a cyber attack and even think they can solve it by themselves.

What is even more highly regarded is the transposition into virtual space of crimes committed in real life by adapting them to this cyber environment. Especially since the networks have been organised differently from the real space with synergies of transversal and non-territorial offences, which is a kind of way of living in virtual space. This changes the situation of detections and protections carried out in the real world. But also the understanding of these cyber-crimes committed by humans living in reality and also in virtual space. Humans mutating and activating their mutation through and because of cyber space.

Discussion

The observation is that the Human is at the heart of all acts. Whether he is an initiator, thinker, creator, supporter, etc., at least one brain thinks, acts, decides, instructs, initiates, creates, develops an idea, a tool, a philosophy, an object, etc. However, most problem solving is based on objects, machines, software, tools, or materials. First, because it is more practical to rely on it than on human beings who do not necessarily have the required potential or in limited numbers, and second, because it is considered as a delegation of mission, too often uncontrolled and validated as a given.

If we analyse this method of problem solving, it is considered that to protect ourselves, we must design something with materials. Either one or more brains believe that the tool will meet the need for protection. That's how we protect ourselves today and feel protected. But if you analyse the facts, protection against malware, you will find that it is not possible to protect against them. This implies that the cybercriminal, alone or in a team, which is more likely, has designed a virus or detected a flaw in order to infect information systems, computers,... He therefore took time to design this malware or find the flaw, which probably worked for months or even years without being spotted or massively like Wanna Cry (8). WannaCry has infiltrated a system flaw with thousands of computers and is still active even though Microsoft has fixed the weakness!

The solution of correction or protection with a tool following a cyber-attack cannot be enough to protect oneself. Especially since re- liability is called into question by the results and by the fact that the protection tool is de- signed after having been subjected to the cyber-attack, which, in fact, becomes obsolete. In fact, one cannot consider doing predictive or cyber security on tools created after discovering the cyber-attack. Virus cyber-attacks, a diverse intrusion into the Digital universe, do not represent a significant number in terms of cyber-attacks. As indicated in the introduction, a large majority of cyber-attacks are caused only by humans. Out of clumsiness, out of a desire to do harm.

The risks of infiltration by a person who deliberately wants to harm a company, association, administration, government, etc. are to be considered. Recruitment is one of the sensitive entry points into a company. Recruiters think they can secure their recruitment with external entities, carrying out tests of all kinds. Co-opting promotes the recruiter's lack of time by facilitating recruitment. Analyses of candidates' behaviour on social networks are required with risks that the results may be truncated by different behaviours in real and virtual space. However, it is on these elements that the candidate will be evaluated.

My research work on the Behavioral Differentiations between the Real and the Virtual has revealed in particular that the behaviour of virtual space users changes more or less ac- cording to several criteria such as profile and objective. It is easy to hide behind the screen without feeling apprehensive or committing a major crime against another human being. It is easy to play one or more roles behind the screen. We feel safe, we think we are not being revealed and we react spontaneously and quick- ly often without thinking about the implications. The "Avatarization" [2-5] makes it possible to understand these acts in virtual space, sometimes reproduced in reality. How many fake profiles (Hays, 9) on social networks exist? This article revealing a study is an example illustrating my theory on "Avatarization". Isn't it to play a role? Hide his person and or his intention?

It will enhance its value by revealing confidential information on social network, with- out any intention of harming or on the contrary to destroy his employer, his colleagues, a product, an innovation. This allows you to focus on your work day by revealing information about the team you are working with. This involves criticizing, bullying a person on the Internet. While all these actions would probably not have existed in real space. The screen and feeling hidden behind it promotes "Avatarization". No software or material can protect a company or structure of any kind from such human, malicious or clumsy behaviour.

The cybercriminal uses satiety to hide behind the screen. It is an essence of their activity: not to be seen, not to be spotted and not to work in this way. And above all, to act before others. The French companies do not have the notion of security, which is too often considered as a right. Integrating that the human being is at the heart of any action and must be considered as a priority to protect oneself and associate into Digital protections becomes a complexity to be understood by companies. It is easier to rely on techniques than to raise awareness through training and knowledge among employees. Or detect profiles through profiling

The postponement of being supported, of helping oneself with artificial intelligence is considered as a rescuer. Because we are transferring a human problem solving to technology, again. The difficulty too often encountered is that the data integrated into these Artificial Intelligences are much too generic, not very up- to- date and based on a specific target or a panel can support. The complexity of the human being, in fact, cannot be integrated with regard to the composition of algorithms nowadays. Here again, these Artificial Intelligences are designed by men.

Taking cybersecurity from its environment at its source is a matter of course, since the source is man. Cyber protection must include this. And because cybercriminals are human beings who exist in reality, we must also con- sider protection in real space. Moreover, behavioural differentiations be- tween the real and the virtual cannot be over- looked in cybersecurity and cyberdefence.

Taking cybersecurity from its environment at its source is a matter of course, since the source is man. Cyber protection must include this. And because cybercriminals are human beings who exist in reality, we must also con- sider protection in real space. Moreover, behavioural differentiations be- tween the real and the

virtual cannot be over- looked in cybersecurity and cyberdefence. Internet users, including cybercriminals, are more or less changing their behaviour behind the screen "Avatarize" it [6-8] their own person. Their behaviour and lifestyle, for some, no longer have the same basis as in real space. They evolve in their own universe, more or less mixed with real and virtual "Zone Transverse", Touzeau, 2015, 2018). They have developed new intelligences ("Virtual Intelligence", Touzeau, 2015, 2018).

Web offenders have changed their approach to crime, their synergy of work with other of- fenders in the virtual borderless and therefore uninhabitable world. The modus operandi are transmitted via the web and reproduced by other offenders whose crimes no longer have anything to do with crimes in the true sense of the word. There is not real crime in cyberspace. Crimes are collateral damage resulting from cyberbullying, ransomware, sex tape, terrorism mainly. These cybernetic acts are almost exclusively human in nature. No malware, or detected vulnerabilities, etc.

Thus, in real space, the criminal has a modus operandi that evolves with a signature, in the virtual it is the opposite [6-8]. With people raped, kidnapped, killed by homicide, murder. Not in virtual space. The cybercriminal will be able to sell his success story of delinquency in the dark web for ex- ample, in an unlimited way. So the Modus Operandi is identical, but the signatures change because the actor is a human being and therefore unique. Terrorists make extensive use of this practice. The complexity of apprehending cybercriminals requires to do and think predictive.

The real and the virtual are two different worlds, one of which is constantly changing: the virtual. All are led by men. These same men who have their hands on every act and decide what they will do as crimes. While not being unmasked in real space. For them to be unmasked in this way, wouldn't they first have to be considered?

Conclusion

"We subscribe to the illusion of safety that can be provided by a surveillance system presented as a protection system. Some believe that the transparency of beings and their activities is synonymous with security. To solve anything, it is customary to say that getting to the centre of the problem is making sure to get out. Since man is the actor of every act, he becomes the centre of the problem in the event of delinquency, whether real or virtual. To be concerned about it would make it possible to do preventive, even predictive work. Put the machines back in their context as they are only a support. Not a transposition of our own actions.

This illusion on which we rely does not allow us to think, learn to protect ourselves and even defend ourselves. The tools that are put in place to protect companies, administrations, etc. integrate only too little of the hu- man being and his behaviours in the virtual world that cause harm. Faced with the exponential growth of cyber-attacks and the ingenuity of cybercriminals who surf our cultural faults as well, diverse and varied entities are being disarmed to curb cybercrime. Understanding the virtual space and the hu- man in front of and behind the screen will improve performance of all kinds: human and digital. Without both elements, cybercrime will have a bright future ahead of it. One of the most important flaws in our protection, both in the real and the virtual, is that we rely more on techniques in protection than in the search for evidence. We conceal the hu- man being, which makes it easier to make it difficult or even falsify the file in order to dis- cover the truth. In virtual space, this observation is eloquent and the figures on the growth of cyber-attacks, published in many newspapers, attest to this.

References

1. Touzeau N (2017) Behavioral cybercriminals differentiations between the real world and the virtual space. J Forensic Res 8: 401.
2. Touzeau N (2018) Transposition of modus operandi from the real to the virtual using several signatures: Case of "the drowned of the Garonne" serial crimes in France. Forensic Sci Criminol 7(5).
3. Touzeau N (2018) Avatarization another way to understand cyber bullyers behaviour in the real and the virtual worlds. J Cogn Neuropsychol 2(1): 1-6.
4. Touzeau N (2018) Explanation and definition in comparison with comfort zones. J Forensic Sci & Criminal Invest 9(1): 555753.
5. Touzeau N (2018) Virtual intelligence the ninth family of intelligences to be added to Howard Gardner's list. Crim Forensic studies 1(1): 1-4.
6. Touzeau N (2018) Some behavior differences between bullying and cyber bullying and impacts on adult victims. Crim Forensic studies 1(2).
7. Touzeau N (2018) Can the definition of lying as known in real space be applied to lies perpetuated in the virtual, particularly with regard to the behavioural differentiations that virtual space promotes. Int J Forens Sci 3(2): 1-4.
8. Touzeau N (2018) What could be the concept of time in relation to behavior in the virtual world. COJ Rev & Res 1(5).

ISSN: 2574-1241

DOI: 10.26717.BJSTR.2019.14.002488

Nadine Touzeau. Biomed J Sci & Tech Res