Punish and Perish : The Human Factor in Cybersecurity

Didier Danet[1]

[1] *Saint-Cyr Military Academy, Guer, 56380, France*

Abstract

According to many prominent experts, IT users are the “weakest link” in cyber-security chain. This assumption has important consequences on the definition of cyber-security policies which are often rooted in the fear of sanctions. We argue in this paper that such policies miss the point of security because they create wrong incentives for users who make mistakes or undergo the maneuvers of social engineers. Doing so, most cyber-security policies are in fact scapegoat processes more that effective guidelines for fighting cyber attacks. We argue that alternative cyber security policies, breaking up with the "Weakest Link" paradigm, are required in order to make significant improvements in facing cyber threats, especially in times of COVID-19.

Keywords

Human Factor, Cyber-attack, IT Charter, Prevention Policy

1. Introduction

In a recent paper, Jim Boehm, James Kaplan and Wolf Richter address the issue of Cyber-security in times of Covid-19 [1] They adequately point out that "Changes in working conditions have made it harder for companies to maintain security. Large-scale adoption of work-from-home technologies, heightened activity on customer-facing networks, and greater use of online services all present fresh openings, which cyberattackers have been quick to exploit." Businesses and administration as well, civilian organisations and the military, all of them are under the threat of cyber-attacks or accidents which could result in outages or even collapse of IT systems.

Among the many sources of issues raised by the COVID-19 pandemic, shifting to work-from-home arrangements increases the risk of cyber-attacks. Boehm and alii identify three main vectors of accidents and attacks. First, changes in app-access rights. Remote working may require widen access rights and, possibly, enabling off-site access to more people or to more critical applications and data. Second, scarcity of computer resources has lead many businesses to allow the use of personal devices, introducing non centrally controlled computers in professional systems and sharing data through unsecured networks. Last, phishing campaigns are made more efficient since isolated employees can not benefit from "human protection system" which refers to asking co-workers about suspicious e-mails.

Not surprisingly, cybersecurity issues are more relevant and challenging than ever. Since many efforts have already been made, which priorities should be set? Most experts suggest putting people first as a security priority throughout the organization. According to a survey by Accenture, organizations have experienced sizable increases in phishing and social engineering attack, ransomware and stolen devices. [2] This statement is consistent with the very common opinion that the user is the weakest link in the chain of cyber-security. This paper is about the "Weakest Link" paradigm, its practical declination in IT charters, its harmful consequences for cyber-security and the alternative policy which is required to implement effective answers to the increased threat of phishing and social engineering attacks.

ITASEC21, April 07–09, 2021, Roma, Italy
EMAIL: didier.danet@st-cyr.terre-net.defense.gouv.fr
ORCID: 0000-0001-6554-3370


2. Punishing the Weakest Link

2.1. The Weakest Link Paradigm

From initial statements of prominent experts such as Schneier, [3] Singer and Friedman [4] or Mitnick and Simon [5] to nowadays numerous contributors, cybersecurity issues are dominated by the "Human Factor" or "Weakest Link" paradigm. According to Aldawood and Skinner, "even in situations where different organizations have polished procedures and sophisticated technology, the weakest link still lies in the human personnel in the process." [6] The Human Factor refers to the negative role that people play in the security process while using the information systems they are given access to. Because human beings have limited memory, do not pay enough attention to security requirements or appear easily gullible, they make mistakes that undermine information systems integrity. Such mistakes include using easy to guess passwords, sharing them with colleagues, opening emails from unknown senders and downloading their allegedly "unbelievable" attachments... A survey by Kaspersky concludes that a majority of businesses see their own employees as "the biggest chinks in their armor against cyber-attacks". The top three cyber threats are related to human factor. Businesses "worry most about employees sharing inappropriate data via mobile devices (47%), the physical loss of mobile devices exposing their company to risk (46%) and the use of inappropriate IT resources by employees (44%)." [7]

The human weaknesses, such as recklessness or negligence, can cause even greater damage when exploited by unscrupulous attackers. Mitnick, again, explained that most cyber-attacks begin with an important phase of "social engineering". Gaining access to the IT system or escalating privileges would not be possible if critical information were not available through open-source intelligence techniques. The most sophisticated scams, such as “Fake CEO Scam”, [8] entirely depends on the collection of trust signals, both human and organizational, that the victim will rely on to transfer the requested funds. To this regard, the greatest danger for information systems security is the "Insider Threat" which gave rise to an abundant literature. [9]–[11]

Fifteen years after his famous "On security", which highlighted the human factor as the most important flaw in IT systems security, Bruce Schneier is even more pessimistic. Looking to six aspects of the human problem such as "the futility of asking people to make intelligent security decisions, the dangers of malicious insiders or Social engineering, and why it is so easy for an attacker to simply ask for secret information", his conclusion is "It's not going to be pretty." [12] In spite of dissent opinions, especially coming from social scientists, the "Human Factor" paradigm is widely shared among IT systems scientists and engineers.[13]

2.2. IT Charter : When ISS meets the Law

Under the "Human Factor" paradigm, the security of information systems is considered in jeopardy each time the system has "to interact with users in some way, at some time, for some reason". [12] In other words, because information systems are socio-technical systems, each and every existing computer in the world is at risk every day. How to face this challenge ? Since the implementation of technical solutions does not solve human weaknesses, alternate remedies are required to enforce user’s compliance with IT security rules.

Basically, the issue may be defined as a specific case of the general problem of organizational compliance that Amitai Etzioni explored in "Comparative Analysis of Complex Organisations". [14] The general framework by Etzioni provides us with theoretical concepts and tools which could be relevant to frame security policies really dealing with the fact that IT systems are more than just technical systems flawed by human deviant behaviors. According to Etzioni, compliance is a universal stake in organizations and generally refers to members of organizations acting as per their organizational values and directives. In order to enforce compliant behaviors, three forms of control may be used, most often in combination one with others.

Normative power rests on the allocation and manipulation of symbolic rewards and deprivations: allocation of prestige, esteem or influence... Normative incentives aim at developing compliance thanks to intrinsic rewards that generate a positive moral involvement of high intensity. Examples given by Etzioni, the parishioner or the devoted member of a party, suggest that normative power is ill suited with such prosaic requirements as computer security norms.

Remunerative power is based on control over material resources and rewards through allocation of salaries and wages, commissions and contributions, "fringe benefits," services and commodities. The use of remunerative power could enforce IT systems security through utilitarian incentives and a calculative involvement by the users. An obvious limit to such utilitarian calculus would be that IT security becomes a matter of costs and benefits which can lead users to dangerous behaviors if they spare enough time, budget or efforts by not applying rules.

Coercive power rests on the application, or the threat of application, of physical sanctions such as infliction of pain, deformity, or death. As far as computer security is at stake, the nature of sanctions is not so radical but it may involve penalties under criminal law. No symbolic reward or monetary benefit is awaited; compliance is expected from the alienative involvement that users will follow security rules because they fear to be hurt by the organization if they do not.

Many IT charters each of us signed before being granted access to IT system, are perfect examples of coercive power in action. Let us consider the example of this military academy. The IT charter is written on a doubled-sided sheet. The first one states that the user is gaining access to a monitored information system and must use it for professional reasons. The charter defines the limited list of permitted usages and stipulates that all other manipulations are forbidden. Then security measures are listed such as probihition of software installation by user or plugging of USB devices which are not checked in "white stations". Disciplinary sanctions are defined for non-compliant behaviors. On the backside of the charter are widely quoted the provisions of French criminal law in relation with computer fraud (articles 323-1 and following) Criminal penalties (fines and imprisonment) are explicitly mentioned. A more detailed example of IT charter is given in the appendix. This charter, used in the French National Center for Scientific Research (CNRS) is based on the same principles and goes further in detailing definitions, authorized and forbidden behaviors…

Using such explicit coercive power to enforce compliance with IT security rules could be considered as "normal" in a military academy where obeying orders is a basic of training programs. The question is: does coercive power work? Do cadets of the Military Academy behave compliantly and make less mistakes? Does IT Charter contribute to a more secure IT system? An experience lead by one of our Post Master Degree trainees clearly shows that the answer is negative.

3. The Failure of Punishment Policies

3.1. The Result: Punish & Perish

In an insightful thesis paper, Jean-Philippe Perrottet analyzes individual behaviors when cadets are trapped during an experimental phishing campaign. [15] An e-mail is sent to two groups of cadets, inviting them to click on a formally suspicious link which is supposed to provide them with information about the new wage bonusses for junior officers. Once trapped, a certain amount of time is given to the cadets so that they can implement the alert procedure and, after this while, they receive a message explaining the issue and asking them to fill in a questionnaire which aim is to understand their behavior and to prevent attacks in the future.

Among the conclusions of the survey, three may be highlighted. First, even if dedicated training programs are delivered on a yearly basis, cadets make mistakes. They do pay less attention to the suspicious sender's address than to the interesting topic of the mail. 20% of them click on the link. No simple relation can be established between the age or academic degree or experience of social networks. Of greater interest seem to be factors such as the hour of the reading (more clicks by the end of the day), or the informal communication between cadets (most of the clicks are registered one day after the message has been sent but, four days after, no cadet is trapped anymore) The second interesting point is precisely that informal circuits of communication are important in fighting cyber - attacks. This point is of utmost importance since the third conclusion is very worrying. Too few cadets who are trapped do not report on the incident. They are frightened by disciplinary sanctions

and adopt a "hide and seek" behavior. Very few of them even answer the questionnaire which is sent in order to explain them that the trap was not a real one but an academic experience. This conclusions fits with Kasperski's one: "Such policies only foster fears, and leave employees with just one option — to avoid punishment whatever it takes." [7]

This result is all but a surprise. The survey by Kaspersky shows that in 40% of businesses, employees hide an incident when it happens with growing percentages in relation with the size of the firm. The consequences are utmost damageable. Unreported events give the attacker the opportunity and time to spread in the system and escalate privileges so that he can take a greater control. Worse, the victim may try to deliberately erase clues, tracks and evidences in order to escape disciplinary sanctions. Doing so, digital forensics is made more complicated. In some cases, unaware user simply plugs off the machine, losing the web pages or messages that could help digital forensic experts. More concerning are cases in which the user is skilled in computer technology and is able to destroy more evidences and tracks of his deviant behavior.

3.2. Why Punishment Policies are Counter-Productive

If most computer security policies are based on the punishment principle, the reason is that coercive power perfectly meets a certain set of assumptions related to IT users and a significant lack of knowledge in social sciences : people are negligent, ignorant of technical matters, disdainful for businesses interest... Only threat of sanctions seems to be efficient in order to prevent human negligence and poor attention to security requirements. A moralistic approach to the issue only makes the problem even worse: it seems to be "fair" that disciplinary sanctions apply to "reckless" behaviors. Computer engineers would not understand that mistakes or errors undermining the security of information systems were not to be punished. Legal officers would not understand that disciplinary rules or criminal provisions would not to be applied in case of damageable behaviors. Even cadets who did not click on the fraudulent link spontaneously suggest to increase penalties in order to fight their peers' deviant behaviors. The general principle of General Deterrence Theory is deeply rooted in our collective mindset and businesses cultures as well.[16]–[19]

General Deterrence Theory assumes that as punishment certainty and severity increase, deviant behaviors can be deterred; the fear of a certain and severe punishment should balance the poor interest computers' users pay to following the rules established by the people who know how not to put the information system at risk. The very simple model in which the deterrence effect depends on two variables (certainty of control * severity of punishment) pleases common sense but its empirical validity is discussed. The literature review by Chen et alii finds disputed results. [20] D'Arcy [21] or Straub both conclude in the same way. " Deterrent administrative procedures that focused on disincentives or sanctions against computer abuse resulted in significantly lower computer abuse". [22] On the contrary, other scholars put emphasis on non-significant [23] or only temporary effects. [24]

Our point is not related to disputing the more or less significant or temporary effects which can result from a purely punishment policy or a policy combining punishment and rewards. We argue that information security policies which rely on General Deterrence Theory are creating vulnerabilities because of the adaptive behaviors when facing a threat or a reward. Because information systems are not purely technical systems but socio-technical ones, the common sense or moral considerations must be put aside and the complex human dimension of the problem must not be over-simplified just like the General Deterrence Theory does. Disciplinary or criminal punishments are counterproductive under the criteria of computer security effectiveness. We suggest that this kind of policy is not effective because of the following two considerations:

The threat of punishment, or real sanctions, do not prevent mistakes or errors which, in most cases, do not proceed from deliberate calculus; every IT user, even computer scientists, is likely to make a mistake out of fatigue or lack of attention;

The fear of punishment strongly incents user who makes a mistake to "hide and seek" behavior instead of alerting immediately IT specialists who address the problem too late and with crippled information.

4. A New Culture in Cybersecurity

Based on the very simple observation that “computer hygiene” campaigns do not work and that standard IT charters make the problem worse than fix it, we suggest to reverse the principles of IT security policies, aiming at one principal goal: to create a set of incentives that motivate people who make mistakes to report them so that the attacker does not have time to spread in the IT system. Even better, the goal should include not only reporting actual mistakes but also "near mistakes experience", which are, by comparison with “near death experiences", mistakes that people have almost made but avoided and which others might make.

4.1. The Non-Punishment Principle

Thanks to police series, everyone knows the "Miranda Rights" that detectives ritually state to the criminals they arrest: " You have the right to remain silent. If you give up that right, anything you say can and will be used against you in a court of law." Any experimented criminal knows that he must not talk without the assistance of a counsel because he may incriminate himself by giving too much information. In applying this Punishment Principle to IT users who make mistakes, IT Charters generate both silent and noise which hamper cyber-attack problem solving.

Punishment Principle is “mother of silence”: When punishment principle is implemented, mistakes become crimes and users' priority is to avoid sanctions. Accordingly to Miranda's rights, they remain silent and, as far as possible, they try to cover their tracks. This is not a proper way to solve the problem which is: how to contain the attack and avoid a deeper intrusion in our IT system? Because the Punishment Principle encourages silence, the problem is made more serious and applying personal sanctions will not solve it.[25]

Paradoxically, the Punishment Principle which is mother of silence, also creates noise in the Signal Theory meaning of the word. Punishing someone requires procedures which are all the more rigorous and subject to cancellation for procedural defect that disciplinary or criminal sanctions are at stake. So, the investigations will take time and will require formalities of all kinds in order to bring legally admissible evidence which will support sanctions. Instead of going straight to the most important questions and freely exchange with the user to clarify the problem, investigators will have to define who exactly did what so that he may be charged with a specific crime under the provisions of legal procedures. Time is lost; data are hidden. Investigators are focusing on individual responsibilities, not in problem assessment and solving. In some cases, noise becomes din because the punishment principle prevents admitting that there may not be individual responsibility but a systemic error. Prosecuting people would then be unfair and exemplary of scapegoat processes.

Two more consequences should lead to definitely get rid of the Punishment Principle. First, it is a strong incentive to disempowerment of users since not being involved in a cyber-incident is the best way not to be suspected or incriminated; users that are aware of a problem will stay apart of it and will not report to IT services. Second, the fear of being involved in an investigation will refrain them from reporting "Near Mistake Experiences" since they will fear to be charged with possible disciplinary sanctions. Yet, no highly reliable organisation would exist without an individual and collective attention to these problems which did not really occur but could have. By examining and fixing these problems which could have been, organisations become safer and cyber-attacks are made more complicated. [26], [27]

IT charters should definitely promote some kind of New “Miranda Rights”, proclaiming the exact opposite of existing ones: "You have the right to remain silent. If you give up that right, NOTHING you say can and will be used against you in a court of law. Conversely, any information you would keep secret or hidden may be used against you if a damage were to be.”

This non punishment principle will shock both IT engineers, legal advisers and bureaucrats. It means that the weakest link is protected against sanctions if he voluntarily reports mistakes. However, the goal is not retribution but efficiency: the non-punishment principle prioritizes cyber-attacks containment and organizational resilience over chasing supposed culprits.

The main benefit of this new cyber security policy would be to allow the emergence of a "Highly Reliable Organisation" culture. Because people would not fear sanctions anymore, they would be keen to report failures or mistakes. Because people are usually aware of stakes and threats of cyber-attacks (even if they do not master technical details) and they easily understand that their own sake is to protect businesses they are working for, they would do it even in "Near Mistake Experiences". Individual behaviors would tend towards alertness and reporting which is a basic condition to increase the capability of organisations to face hazards and threats of digital space. IT services would finally be informed of incidents in real time and they would receive complete information from users providing them with many data they would have to sort and rate. Not looking for faults and culprits would allow IT experts to focus on facts, not on people, with the help of users willingly cooperating to the process.

4.2. The Exception

Just like every principle, the non-punishment principle is subject to limits and exceptions.

A first exception is written into the body of the "New Miranda Rights": mistakes or errors are not punished if the user is reporting it and gives all relevant information to the IT services who will be therefore capable to fight the cyber-attack as soon as possible. In the absence or reporting or concealment of relevant data, the non-punishment principle does not prevail and action will be taken against guilty silence or lie.

It is also obvious that the non-punishment principle applies to mistakes or errors occurring "in good faith", not to intentional or inexcusable deviant behaviors. Foe example, it does not prevail if a user voluntarily introduces a virus in the IT system to get revenge on a promotion refusal. The same if a employee steals data in order to sell them to a competitor. The same again if an employee uses the login and password he stole from a colleague to enter the information system and falsify R&D results. In all these cases, the deviant behavior cannot be labelled "mistake" but espionage or sabotage and the perpetrator not only will be sanctioned but also prosecuted under the provisions of criminal law.

One could argue that a thin red line will be difficult to draw between different kind of errors, from the simple mistake (such as clicking on a link which is a perfect copy of a genuine institutional website) to the deviant but usual behaviors (such as plugging on a USB key which has not been checked) and to the insider who is consciously helping an attack against the company he is working for.

In some cases, labelling deviant behaviors (venial, serious, inexcusable, deliberate) will be tricky. But, it may be considered that these difficult cases will be only very few and solutions exist in order to deal with them. Most of deviant behaviors in using IT systems are mistakes not frauds. Even if computers fraud is a real threat to organisations, fraudulent behavior aiming at criminal goals are a small percent in all daily breaches to IT security. Within these mistakes, some criteria may be used in order to distinguish between venial and serious errors. According to Christian Morel, airlines companies combine two questions in processes of this kind. [25] First, did the pilot repeatedly made the error? The severity of the error increases as it is repeated. Second, in the same circumstances, would a pilot with the same experience have made the same error? (*in concreto* assessment) Answering yes to the question means that punishment is not justified. A huge corpus of courts decisions is available to define guidelines in companies. A small bunch of really complicated cases will probably occur and be addressed as previously described on a yearly basis. Above all, the benefits inherent to the application of the Non-Punishment Principle in terms of security exceed by far the marginal cost of the very few difficult cases related to the thin red line.

4.3. IT Charters

What would an IT Charter based on the Non-Punishment Principle look like? To our opinion, the Charter should deal with three main points.

First, considering that IT users are moderately capable but widely honest, the importance of IT systems and informational assets (data, reputation, ideas...) for the sake of the company need to be explained. The idea is basic but it may be recalled in order to make people aware of their responsibility to themselves and to others. People should not be threatened but empowered so that the weakest link becomes an asset in the socio-technical IT system. In Etzioni's framework, this first part refers to normative power and seeks to generate a positive moral involvement of higher intensity than the usual consideration for bureaucratic constraints that prevent users from working or impose impossible requirements such as random twelve characters passwords to be changed monthly.

In the second point, the charter should state the most important rules the user needs to comply with. The goal is not to specify a strictly limited list of what is authorized but to give users an insight of what he should use the IT system for. Then, once the compliant behavior explained, the charter should lay down the Non-Punishment Principle. All errors but inexcusable deviant behaviors and intentional frauds, benefit from immunity and are not to be prosecuted and sanctioned under the condition that the user report as soon as possible and in a complete way the incident or quasi-incident which occurred when using IT system.

The third part of the charter should explain the difference between venial and inexcusable errors under the two criteria of repetition and *in concreto* assessment. Here too, the goal is not to provide people with a detailed list of what they should do or not do. Users know that plugging a USB device may be dangerous but they do it because they are late or they forget; the goal here is not to prevent them from ever doing so but to reduce such behaviors (repetition criterium) and, mostly, to report quickly and explain completely if a problem occurs (Non-Punishment Benefit associated with a "normal deviant behavior")

5. Conclusion

The "Weakest link" paradigm has widely been proved unable to create the security climate which is required for any organisation to survive in the digital world. The assets and competitiveness of administrations and businesses as well are jeopardized and exposed to cyber-attacks lead by criminal organisations pursuing their own benefits or state sponsored groups who steal information to gain advantage in the competition. Both threats are vital and require a renewal of theories, concepts and tools of IT security. In this paper, we have argued that the fear of sanctions is a primitive and inadequate foundation of computer security. Primitive because IT user is not an irresponsible and ignorant busybody who pays strictly no attention to security concerns; this is why normative power should get a much greater place in security policies. Inadequate because sanctions deal with designating a culprit, not facing an attack. Moreover, fear of sanctions gives totally wrong incents in most frequent cases where the user made a forgivable mistake which quickly reported can be fixed, preventing a possible attacker to invade the IT system. Only the Non-Punishment Principle is capable of significantly enforcing IT security in the years to come. In the next edition of "On Security", Bruce Schneier may revise his current statement: "It is not going to be pretty".

[1] J. Boehm, J. Kaplan, et W. Richter, « Safeguarding against cyberattack in an increasingly digital world », McKinsey Digital, Insights, juin 2020. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/safeguarding-against-cyberattack-in-an-increasingly-digital-world (consulté le févr. 08, 2021).

[2] K. Bissell, R. M. Lasalle, et P. Dal Cin, « 2019 Cost of Cybercrime Study | 9th Annual », mars 06, 2019. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (consulté le févr. 08, 2021).

[3] B. Schneier, Schneier on security. John Wiley & Sons, 2009.

[4] P. W. Singer et A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know®, 1 edition. Oxford ; New York: Oxford University Press, 2014.

[5] K. D. Mitnick et W. L. Simon, The art of deception: Controlling the human element of security. John Wiley & Sons, 2003.
[6] H. Aldawood et G. Skinner, « Educating and raising awareness on cyber security social engineering: A literature review », in 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 2018, p. 62-68.
[7] Kaspersky Lab., « The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within | Kaspersky Lab official blog », 2017. https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (consulté le mai 25, 2019).
[8] M. Dhooge, « Fraude au Faux Président: la sensibilisation reste la meilleure parade! », Securite et strategie, vol. 23, nº 3, p. 66-67, 2016.
[9] P. Chattopadhyay, L. Wang, et Y.-P. Tan, « Scenario-based insider threat detection from cyber activities », IEEE Transactions on Computational Social Systems, vol. 5, nº 3, p. 660-675, 2018.
[10] M. Mylrea, S. N. G. Gourisetti, C. Larimer, et C. Noonan, « Insider threat cybersecurity framework webtool & methodology: Defending against complex cyber-physical threats », in 2018 IEEE Security and Privacy Workshops (SPW), 2018, p. 207-216.
[11] C. W. Probst, J. Hunker, M. Bishop, et D. Gollmann, Insider threats in cyber security, vol. 49. Springer, 2010.
[12] B. Schneier, Secrets and lies: digital security in a networked world. John Wiley & Sons, 2015.
[13] C. Mc Mahon, « In defence of the human factor », Frontiers in Psychology, vol. 11, p. 1390, 2020.
[14] A. Etzioni, Comparative analysis of complex organizations. Simon and Schuster, 1975.
[15] J.-P. Perrottet, « Le facteur humain dans l'espace nuumérique : l'acculturation cyber au sein d'une population de l'armée de Terre », Thèse professionnelle Mastère Spécialisé, Ecoles de Saint-Cyr Coëtquidan, Guer, 2017.
[16] L. Cheng, W. Li, Q. Zhai, et R. Smyth, « Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory », Computers in Human Behavior, vol. 38, p. 220-228, 2014.
[17] J. D'arcy et T. Herath, « A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings », European Journal of Information Systems, vol. 20, nº 6, p. 643-658, 2011.
[18] S. M. Lee, S.-G. Lee, et S. Yoo, « An integrative model of computer abuse based on social control and general deterrence theories », Information & management, vol. 41, nº 6, p. 707-718, 2004.
[19] D. S. Nagin et G. Pogarsky, « Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence », Criminology, vol. 39, nº 4, p. 865-892, 2001.
[20] Y. Chen, K. Ramamurthy, et K.-W. Wen, « Organizations' information security policy compliance: Stick or carrot approach? », Journal of Management Information Systems, vol. 29, nº 3, p. 157-188, 2012.
[21] J. D'Arcy, A. Hovav, et D. Galletta, « User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach », Information systems research, vol. 20, nº 1, p. 79-98, 2009.
[22] D. W. Straub Jr, « Effective IS security: An empirical study », Information Systems Research, vol. 1, nº 3, p. 255-276, 1990.
[23] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, et R. W. Boss, « If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security », European Journal of Information Systems, vol. 18, nº 2, p. 151-164, 2009.
[24] E. Fehr et K. M. Schmidt, « Adding a stick to the carrot? the interaction of bonuses and fines », American Economic Review, vol. 97, nº 2, p. 177-181, 2007.
[25] C. Morel, Les décisions absurdes, vol. 2. Paris: Editions Gallimard, Folio, 2012.
[26] K. H. Roberts, « Some characteristics of one type of high reliability organization », Organization Science, vol. 1, nº 2, p. 160-176, 1990.
[27] K. E. Weick, « The collapse of sensemaking in organizations: The Mann Gulch disaster. », Administrative science quarterly, vol. 38, nº 4, p. 628-652, 1993.