The Company: New Cyber Challenges

Philippe Davadie
Colonel. Gendarmerie Center for Higher Education

May 2014 – Article n° IV.4

This article presents the synopsis of the work published by Philippe Davadie, The Company: New Cyber Challenges, published by Economica, 192 pages, May 2014.

The computerisation of companies happened in a transparent way for the general public, who, for a long time, did not believe they were affected by this phenomenon. Their awareness of the importance of this computerisation goes back to the Year 2000 Issue: while this yearly transition was supposed to be an especially festive occasion, the specialists were predicting that it would be paired with a bug which would turn this festive date into a catastrophe. This transition could have been a chance for a general awareness of the stakes of computer security, but that was not the case as it ended up being only a festive event.

Judging that their efforts had been in vain, companies focused less on computer security, leaving entire aspects of their DP (Data Processing) to develop nearly completely independently. The emerging of cyber criminality didn't alter their behaviour, the forecasted threats being first aimed at individuals.

Along with the appearance of cyber criminality, several phenomena have generated challenges for companies: the rise of personal computing paced its own computerisation as employees expected the company to provide equipment as good as their own. In order to keep up, they came to resort increasingly to service providers with off-the-shelf "solutions", thus accepting *de facto* that part of its computer equipment be operated by someone else.

These DPs which developed independently can be considered orphans, on several grounds. As IT Management was not entrusted with it, it doesn't feel particularly concerned with what happens to it. Moreover, the fact that they seldom break down may give an impression of infallibility. Finally, like the illnesses similarly named , the attacks which target them are diagnosed late and cures are largely undeveloped.

I – Companies' DPs

The great dependence or even the addiction of companies to computers often leads them to believe that a company's computer system is monolithic. When it is mentioned, one thinks almost exclusively of the various processes, the computerisation of which has been much covered by the media. This covers HR, payslip management, equipment accounting, the general management of the company and its online existence.

Largely known and implementing processes for the benefit of the public, the computerisation of these functions owns a media monopoly: mentioning business computerisation often amounts to speaking of the computerisation of those functions. This has led computer security to focus almost exclusively on their problems, and neglect the reflection on other computer aspects.
However, several leaders consider that the space taken by these functions within a company's information system is far from being major.
The first step in order to secure companies is therefore to inventory the number of computer sectors.

Production software, namely all of the computer components (solutions, captors, computers and equipment software) enabling a company to produce the goods they sell to their customers, and control the manufacturing process, is the first that comes to mind. Within this production software, we find the SCADA systems, (*Supervisory Control And Data Acquisition*). Enabling the company to manufacture what it sells, it plays therefore a major part, and it can seem paradoxical that it should be considered "orphan". However, it is a fact that there is not much literature dealing with security, and that only when *Stuxnet* hit did a collective awareness begin to emerge.

Next to production software, we can find remote operation, with which a person outside the physical realm of the company is allowed, via a network that can be the Internet, to take control of another computerised machine, to modify its settings, diagnose a problem or solve it. It is conducted by members of the company, or by service providers. Several important points have to be mentioned when studying these operations. The number of partners, because in addition to the provider and the beneficiary of the service, the telecommunications operator is a part of these operations, which suggests foreseeable difficulties in the search for the responsibility for malfunction in such an operation. Also, it is possible to define the perimeter of production software, but it is impossible to define that of the remote operations, as the path of the information going through the Internet isn't foreseeable.

Perimeter DP falls under the category of orphan DPs. It includes all of the captors and software which enable the detection of any infringement, by a person or a thing, of a given perimeter, in whichever direction, incoming or outgoing, the identification of the transgressor, and help in detecting if this "breach of fencing" is incoming or outgoing. The difference between intrusion and incoming being in the fact that the latter is authorised, whereas the former is unwanted. It includes in particular entrance badges, RFID chips which manage stock, as well as video cameras. The wavelength of their components, often wireless, can be a problem: the theoretical range may lead to the assumption that there is security after a certain distance, when in fact the practical range is often superior.

Last, the *cloud* presented as the answer to mobility and availability needs deserves to be called "orphan" also, as even if it allows the company not to bother with very technical questions for which it doesn't always have the necessary skills, it can be seen as a takeover of the company's vital information by a provider.

In that case it makes sense to define as orphan DP that DP which appeared some time earlier and which, although indispensable to the company, has ceased to seem of interest, both internally for DIS (Directorate of Information System) and externally from a doctrinal point of view, but which continues nonetheless to develop very regularly.

The term "orphan" is of course to be used in the medical sense of "orphan diseases", referring to certain grave and rare illnesses, which do not benefit from sufficient medical research.

II – The reasons for the existence of orphan DPs

The orphan aspect of these DPs is in part the result of History. After mechanisation, companies turned to automation and then computerisation to produce more and faster. As a result of this, the demands for speed have generated a lack of consideration for all of the security aspects. Subsequently, the appearance of DIS and the debates regarding computer security, concentrating on that of management, increased the isolation of these DPs. Last, the *cloud*, inciting companies to focus on their core business, initiated or worsened the lack of investment from companies on subjects that are after all major, such as the degree of sensitivity of information and the rules of access to it. (ne pas souligner senstivity of information)

Other less rational reasons can also explain this virtual abandon. The faith in near-perpetual progress and the power of innovation can lead to thinking that which is beneficial for one DP will be beneficial for another. The low rates of breakdown, the development of computer security and on-board intelligence should be profitable to all the DP which would have started a convergence trend towards each other.

The suppliers of computer products and software also have their share of responsibility. By offering "solutions" which aren't such, because their products don't solve all the security problems, they delude the DIS who, confronted with their management's requirements for results, find the attraction difficult to resist.

However, the convergence trend of the DP mentioned before is not yet on the agenda. If some points may seem to be announcing it (OS, material components and network protocol standardisation notably), differences still remain. The requirements for availability are not the same: production DP needs to be continuously operational, whereas managing DP can be programmed. Industrial production requires real-time performance, which is not the case with management DP. Lastly, the security requirements are different, for if in the case of management, confidentiality prevails, it is availability which is vital for production, whereas integrity is as important for remote operations as it is for perimeter DP.

III – Repercussions of the weaknesses of the orphan DPs on companies.

Despite the fact that they are orphan, these DPs have repercussions on the company's general information system. The *Stuxnet* and *Shamoon* precedents remind us of that fact.

The attacks targeting these DPs have several characteristics. The recent multiplication of alerts and reports from computer "security solutions" providers show the permanent aspect. They can be *destructive* if they aim to alter, paralyse or modify, sometimes radically – up to destruction – a computer system (delete data, modify the behaviour of a production machine), or *acquiring* if their goal is to obtain in a fraudulent manner data or know-how from a competitor, or a company on which the attacker has an eye, or influence a decider or even alter his judgement (subversion). As is the case with attacks aiming management DP, their motivation can be for amusement, for money, for terrorist or strategic purposes, or even multiple or cross-purposed. The increase in the number of Internet users, the increasing ease in accessing tried and tested malware and the connection of DPs to the

internet make the probability of an attack on an orphan DP more and more likely as time goes by. Even if all successes are not advertised in the media, some of those incidents are without question of malicious intent.

As is the case with attacks on management DPs, the attacker can aim at his target directly, or by successive leaps. The attacks becoming more and more sophisticated, they are more and more subjected to the same successive phases: intelligence, planning and conduct. The pathways remain varied, and have no other limits than the attackers' imagination.

The days of security secrecy are over, as are those of security obsoleteness. Orphan DPs are therefore potential targets, and it is necessary to list their vulnerabilities in order to better protect companies. Some are actually inherent, as for example the obsolescence of the Oss, their low securing, as well as those generated by their use constraints (difficulty of applying corrective measures, etc.). Lastly, their connection to one same network weakens them, because their vulnerabilities are therefore accessible to a greater number of people.

Making them secure is a vast project, which can be made even more difficult by the ambiguities of cyberspace. In addition to the difficulty of precisely identifying the attacker, one must add the ambiguity in determining the actual damage (for there can be apparent damage), that of the means used to conduct the attack, and that of its purpose. Because of these ambiguities, it is very difficult to catch the attacker red-handed (flagrante delicto) and impossible to respond in self-defence.

Despite all of this, the effects of the attacks are quite real, and some can easily be imagined. Impairing quality or production rates, people or environment, the acquisition of trade secrets or the company's confidential information, the use of its resources for illegal purposes and damaging reputation are possible by attacking the production DP. Targeting the perimeter DPs can give access to the overall understanding of how the company works, and makes its infrastructures as well as its workers vulnerable. Targeting the cloud enables confidential information acquisition and can also impair vital functions in the company by blocking its access to the essential data. Lastly, targeting remote operations can have more or less the same consequences as targeting the production DP.

IV – Pre-empting the attack

It is therefore essential to pre-empt the attack. In order to do so, several operations are indispensable.

First, and even if this may seem obvious, the sector in which the company navigates must be known. This implies knowing the company, the skills it has on hand, the state of its defence system and their reaction mechanisms, but also the legal and regulatory framework, as well as the hostile and competitive environment.

One must then imagine the crisis by preparing the company, with material and employees. For the material aspect, checklists can be established, but for the second point, it is necessary to pay real attention to the employees. Dialogue within the company and the creation of a climate of trust are indispensable elements for all the employees' involvement in the company's security. These elements are necessary but are not sufficient, the attacker will always have an element of surprise at the moment of attack.

Despite the fact that it is indispensable, preparation will be useless if the company doesn't set up in battle array. In order to do so, the company needs to take a look at the time, the enemy and the field. The earlier the detection happens, the better protection for the company. The company will be even more protected as it will have prepared its IT landscape (VLAN, honey pots, etc.) and will have had up-to-date information on the attackers' modus operandi. However, given that the company doesn't necessarily have the means to react alone, it will be indispensable to constitute a network, which can be mobilised in the event of hardship. It will feature institutional and private sector players, who will either be able to support the company, or assist it in its defensive reaction.

V – After the attack

As thorough as preparation may have been, it may not be enough to counter all the attacks. The company must therefore also know how to react once the aggression is over.

The return to a logical and indispensable operational status, will not be enough and should be paired with precautions. The first one is to ascertain whether the company was the victim of an attack or of negligence. It is a sensitive phase, but it is not impossible. Trustworthy partners can be of assistance in this step. The attacked company can also help limit the spreading of these attacks by broadcasting the characteristics of the attacks.

Subsequently, it is as logical that the company would try to seek redress. Turning to the insurance provider, even though that involves several difficulties, is an option. However, the assessment of risks is still at early stages, and the damage covered, as well as the premium calculation, aren't tied to undisputable assessment grids, which makes the assessment of the damage caused and the payment of compensation uncertain. Another solution is to choose a judicial approach, be it civil or criminal. Each of these options has its advocates, the benefit of choosing criminal proceedings being to obtain the conviction of the perpetrator.

In order to initiate criminal proceedings, the facts which have caused harm to the company must be punishable offences. The Criminal Code defines and punishes in articles 323-1 to 323-3 attacks on the automated processing of data systems, but other offences are possible, depending on the actual damage. In some cases specified by the Criminal Code, attempted attack is also punishable.

If the facts are punishable under criminal law, then the complaint is justified and will allow for the opening of an inquiry which could be preliminary, flagrante delicto or by rogatory commission, depending on the assessment of the magistrate in charge. It isn't indispensable for the company to file. If the company decides to file a complaint, it will be in its interest to cooperate as much as possible with the investigators for the exposition and conviction of the perpetrator.

Conclusion

In conclusion, as is the case with every actor choosing to be present in cyberspace, this presence of the company leads to questioning its way of functioning. Did the company take into account the transformation of the threats it already faced, did it organise consequently, has it given itself the necessary means to avoid turning this presence in cyberspace into a huge disaster?

A great part of the solution is in the company's hands. While partnerships are an option, and steps are being taken to converge security and safety, both of them wil be of help in responding to cyberattacks.