STORMSHIELD



Digital transformation of companies:

where does security fit in?

Barometer survey conducted with L'Usine Digitale

December 2018

DIGITAL TRANSFORMATION

The digital transformation of companies is full of promise in terms of agility, innovation, productivity and performance. Currently shaking up all business sectors and professions, it is transforming organisation methods to offer more flexibility, autonomy and cooperation.

The digital transformation of companies has become unavoidable and is a major priority for guaranteeing competitiveness and growth.

Mobility, the cloud, the Internet of Things, artificial intelligence, big data and SaaS applications all make companies more connected, flexible and adaptable. But all these technologies are also breaking up information systems and generating endless new intrusion opportunities.

Stormshield

Stormshield, the European leader in cybersecurity and a wholly-owned subsidiary of Airbus CyberSecurity, offers **reliable solutions** that have been certified and qualified at the highest European level. It is the software publisher that offers the most scope in terms of protection among ANSSI (the French national agency for the security of information systems) Security Visa holders.

How do IT departments, Senior Management and Business Units address this transformation and the risks they present? How can assets and sensitive data be protected in an environment where information is increasingly shared and outsourced, in the face of threats that are becoming more sophisticated by the day?

These are the kind of questions that were sent to over 200 professionals as part of the "Digital transformation of companies: where does security fit in?" barometer survey, conducted by Stormshield and L'Usine Digitale.

Among the **digital transformation projects to be implemented as a priority** according to the barometer results, this white paper highlights three fields which raised particular concern in terms vulnerability for the companies approached.

1

Firstly, the **mobility of employees**, for which they require access to company data and resources from different places (home, co-working areas or on different sites). This constitutes a major risk of information theft, resulting from negligence or insufficient protection.

2

Secondly, **services for sharing documents through the cloud**, such as OneDrive or Dropbox, which serve to store or exchange files easily in areas beyond the company's control.

3

Lastly, the **deployment of new technologies internally**, particularly connected objects, which create new vulnerabilities and are especially difficult to manage when it comes to separating and controlling data.

The results of the barometer survey show that companies are realistic and understand the major impact that digital transformation has on their security. However, they tend to overestimate the protection measures they have already implemented, which are mainly based on traditional technologies that are not in fact capable of protecting all of the extent, infrastructure and data in today's increasingly open and exposed environment.

Companies in the face of digital transformation:

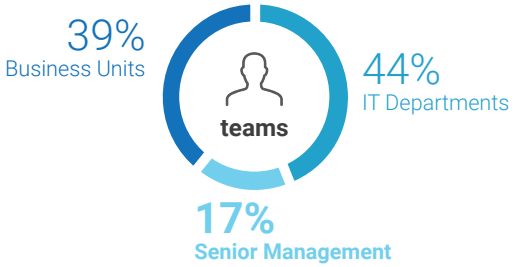
Key figures

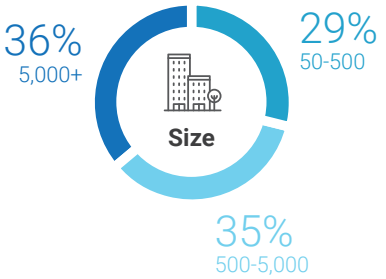
The study conducted by Stormshield and L'Usine Digitale with 200 respondents served to understand the perspective of IT Departments (44%), Business Units (39%) and Senior Management teams (17%) regarding the digital transformation of their company and its impact on security.

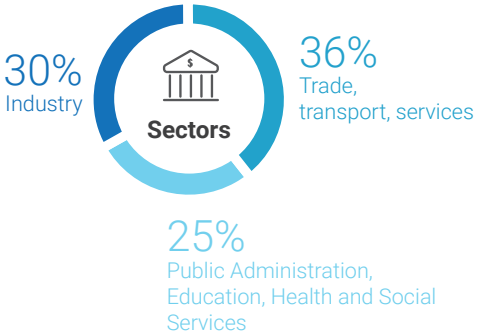
200

ISDS, TM TEAMS AND BUSINESS LINES
OF COMPANIES WITH OVER 50 EMPLOYEES
IN FRANCE









The survey highlights that the **digital transformation of trades and professions is well underway**, but with views varying according to the size of the company and their field of business.

Companies with over 5,000 employees considered themselves to be "ahead" (39%) whereas those from the public sector judged themselves "rather behind" (51%). This gap in perspective was also apparent between the more optimistic Business Units (67% consider themselves ahead or up to standard) and the IT Departments (59%).



Out of all the respondents, 27% of companies considered themselves to be ahead and 31% up to standard in matters of digital transformation.

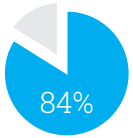
Unified communications platforms tools and collaborative working tools are already largely in use in most companies.

The new stages of digitalisation involve the use of SaaS services (87%) and new digital services (83%), as well as the digitalisation of customer relations (81%) and the introduction of paperless processes and new business applications (80%). On the other hand, companies are more hesitant when it comes to data handling projects, as 30% of IT Departments are not even considering such projects for the time being.



Unified Communications platforms and collaborative working tools already deployed in nearly seven out of ten companies.

However, the impact of these new uses on **the security of information systems and data is difficult to measure**, and perceptions vary: 44% thought that the impact will be positive, 37% did not express an opinion, 14% feared a negative impact and 5% believed that they will have no impact.



84% of respondents stated that the digital transformation has or will have a strong impact on the security of information systems and data.

However, respondents were **confident in their company's level of preparedness** even though the protection measures implemented to support the digital transformation projects remain largely traditional (antivirus for 78%, VPN IPsec or SSL for 76%, physical appliances and anti-spam for 70%) and the budgets allocated to security for these projects being unknown to 48% of the respondents.

6.6/10

This is the average grade given by companies **for their level of preparedness for cyberrisks** associated with digital transformation.



Digital transformation

When increased efficiency penalises security

The respondents questioned confirmed that digital technologies are essential for modernising their companies, but that they pave the way for new security breaches.

"Our employees now have mobile phones, an extranet, a remote meeting platform and other tools at their disposal. And **our main concern is now for the security of information shared** outside the company. We receive an alert reporting a risk of attack about once every three months."

— Representative from a leading brand name

TRANSFORMING YOUR COMPANY TO IMPROVE ITS OPERATIONAL EFFICIENCY...

Digital transformation promises to increase operational performance, save time, and help companies to be more reactive and therefore more efficient. **And the digital revolution currently underway fundamentally transforms the economic processes and models of companies.**

With cloud applications, the IT Department no longer needs to budget for the purchase of servers, nor mobilise and train staff in matters of maintenance. Suppliers of cloud platforms or applications take charge of all technical aspects and so equipping new employees or launching projects now only takes a few hours compared to weeks or sometimes even more before. *"As the collaborative tools hosted on the cloud are globalised, we can work more efficiently with partners located in other countries"*, explained a manager from the tertiary sector.

A further example of efficiency is the mobile equipment and secure remote access that allow employees to work from anywhere and to act remotely with all the necessary information or applications in real time. And further, connected sensors that serve to detect anomalies in a product, a production line or the premises themselves so action can be taken as quickly as possible before the activity is blocked by an incident.

... BUT SECURITY NEEDS TO BE BETTER CONTROLLED

All these new opportunities provided by digitalisation **come hand in hand with a new set of security challenges** that require a better framework. Digital transformation must always be associated with increased security measures and long-term reliability. With equipment and data moving outside the company's internal perimeter and new connected devices not covered by traditional protection procedures, companies must completely change their approach to digital security.

"We now have robots that can be queried by the company's information system. From the IT Department's point of view, this is unacceptable. Moreover, we have to find a way to secure this with intermediaries who are not trained to deal with such issues", complains an industry consultant.

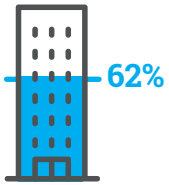
This white paper presents concrete cases regarding the change that companies must undertake as a result of their digital transformation.



Mobile employees

Companies lack control over devices outside their premises

The fact that employees are increasingly working off-site is the main security issue that needs to be addressed for 62% of respondents.



With mobile equipment and corporate data circulating beyond the standard scope of protection, encryption solutions are required to avoid the theft or loss of data.

SECURING REMOTE ACCESS

Teleworking became a right in France in September 2017, and is set out in the French Labour Code[1]. This new regulatory framework requires companies to organise remote access to their information systems if such a facility is not already in place. Accessing the information system from outside the company's premises can constitute a huge security hole if there are no suitable protection mechanisms. **Authenticating employees working remotely, applying access rules on resources available to them and protecting communications** to ensure their confidentiality are basic prerequisites to guarantee secure remote access.

In response to this issue, 76% of the companies surveyed had already setup a remote access system via a VPN (Virtual Private Network) as part of their digital transformation.

Stormshield addresses this issue by giving the user VPN access enabling them to work off-site as if they were on the company's premises. The connection is encrypted to prevent it from being intercepted. The feature includes the authentication of employees, the configuration of access policies (users, time frames, resources made available), as well as the encryption of communications.

Both the physical and virtual appliances of Stormshield Network Security (SNS) offer two types of VPN:

- VPN SSL, which is flexible and simple to use,
- VPN IPsec, which is more reliable as the code is audited as part of the ANSSI qualification.

PROTECTING DATA ON TERMINALS

42% of IT Departments think that terminals should be better secured (computers, tablets or smartphones) when employees use them to work remotely, either on a different site or from home.

"Employees' mobility is problematic insofar as outside the boundaries of their geographical sites, companies can no longer manage its supervision. The equipment is exposed to theft, loss and espionage, and the sensitive data that it hosts can end up in the hands of unknown or malicious third parties", explained Matthieu Bonenfant, Chief Marketing Officer at Stormshield.

In addition to setting up virtual private networks, the content of the hard drive on the customer's device must be encrypted so that if a criminal gains access to it, they will not be able to examine it. This protection mechanism is necessary but not sufficient. "***The manufacturer of professional terminals and computers often offer this option. However this encryption cannot resist a spy who has a software capable of hacking it***", said Jocelyn Krystlik, Data Security Business Unit Manager at Stormshield.

In addition to the default hardware encryption, the publisher recommends using the Stormshield Data Security (SDS) software, which places sensitive files in a container with an additional encryption. As well as the version designed for computers, SDS is also available for smartphones and tablets. It acts as an alternative browser which, once the user is authenticated, can be used to access files on the terminal just like those hosted on a cloud storage service.

"Files secured by SDS cannot be accessed through traditional tools, but SDS can access all peripheral devices. It is therefore possible to encrypt a photo directly, which is very much appreciated in an industry where images are used to assess critical parts", concluded Mr Krystlik.

(1) Ruling No. 2017-1387 of 22 September 2017 relating to the foreseeability and securing of work relations (official journal of 23 September 2017) states that a company's refusal to allow teleworking must be justified.



Sharing Documents

The challenge of protecting confidential data in a public place

Even though services for sharing documents online are making exchanges easier and increasing employees' agility, the company should still be able to control the confidentiality of information.

Today, these sharing tools embody the fears of IT Departments, as 48% of them consider that such SaaS applications present a high risk.



ONLINE SHARING
THAT IS TOO EASY TO ACCESS

Among the new collaborative features, services for sharing documents online, such as OneDrive, Google Drive or Dropbox, cause particular concern to companies, who believe that the protection level of these transformation elements needs to be increased as a priority.

"Online sharing and storage must be secured urgently because the Business Units of companies, particularly in the industrial sector, need it immediately. There are indeed very attractive group rates available for this type of service, compared with the actual cost of their file servers. However, they cannot accept their data being stored unencrypted on a platform operated by a third party accessible by anybody", explained Mr Krystlik, Data Security Business Unit Manager at Stormshield.

GIVING CONTROL TO THE USER
WHILE MANAGING SECURITY

Suppliers of cloud-based document sharing services usually provide the option of encrypting data so that only users with the appropriate access rights can read them. But Mr Krystlik highlights a problem: *"These access rights can only be managed by security managers, which generates a work overload and considerable latency times for processing requests"*. But for the collaboration to remain prompt, the users themselves - as the owners of the data - need to be able to assign accesses to the employees of their choice.

"On the other hand, employees are in no way entitled to share documents on platforms out of the company's control without first implementing safeguards. The users therefore need to access the authorisation features from their terminals, but all activity records must be reported to the monitoring dashboard of the security teams", he explained.

To resolve this issue, the software publisher offers SDS (Stormshield Data Security), a tool which integrates with leading email and cloud sharing services clients. SDS includes all the features for managing data access (data criticality level, selection of authorised employees, etc.) from the user's interface. SDS is based on a mechanism for encrypting files end-to-end, from the sender's terminal to the recipient's terminal. The administrators define the identities and rules of use without being able to access the data.



Technological developments and the Internet of Things

Protection against the unknown

The digital transformation of companies involves continuous technological developments and the deployment of connected objects. The frantic race for innovation often forces software publishers and manufacturers to focus on miniaturisation, performance, and the reduction of development cycles rather than on the security of their products. These technical components are not always properly controlled and do not natively integrate enough security mechanisms (automatic updates, authentication, encryption of communications, etc.).

Although the study indicates that companies have a high level of confidence in the protection of their infrastructure (87% of them consider that their networks are well protected), it also reveals that the adaptation of security measures to encompass the constant technological changes to their information systems is a matter of concern. So how can this new equipment, recently integrated in the IT network, be secured?



CONNECTED OBJECTS AS AN ENTRY POINT

CCTV cameras, probes and sensors, connected tools, vehicles and autonomous systems now make buildings, towns and factories smart. **These connected objects are a pillar of the digital transformation** as they form a link between the physical and digital world. Their exponential development is a true challenge for digital security.

"We are unfamiliar with these IoT environments and usually less able to secure them than servers or workstations, but they remain nevertheless targets for hackers", explained Mr Bonenfant, Chief Marketing Officer at Stormshield.

Let's take the example of the infamous Botnet Mirai, which managed to take control of 500,000 connected objects, mainly CCTV cameras, using default login IDs and passwords. In 2016, the equipment contaminated by Mirai was coordinated to trigger two massive cyberattacks against the supplier of OVH cloud and DynDNS services, which many websites depend on, including GitHub, Twitter, Netflix and Airbnb. Technically, hackers could also very well steal data from these devices, including CCTV images.



ACTING AT THE FIREWALL LEVEL

To prevent connected objects from acting against their owners or being misused, Mr Bonenfant recommends **implementing the "Zero Trust" policy**, which involves isolating these components from the rest of the information system using a filter. Network segmentation in zones of trust serves to control all connections between zones or via the Internet. ***"Regarding connected objects, it is possible to find out which kinds of connections are legitimate. The best practice is therefore to use white lists and to only authorise certain actions such as connecting an object to its cloud management platform. This makes it easier to control objects that have been hacked"***, he explained.

Stormshield offers solutions to solve these issues through its range of Stormshield Network Security (SNS) firewalls. The advantage of this solution is that a single appliance can create up to 50 different physical zones and filter all exchanges between these zones. Moreover, the high-end SNS boxes can evolve, because their chassis allows them to acquire additional connection modules as zones are added to the network. "It is one of the principles of digital transformation: to become more agile, companies need to be able to adapt their investment dynamically based on their immediate needs," concluded Mr Bonenfant.



STORMSHIELD

Stormshield, the European leader in cybersecurity and a wholly-owned subsidiary of Airbus CyberSecurity, offers communicative, intelligent solutions for anticipating attacks and protecting digital infrastructure.

Its mission is to ensure cybersecurity and protect the data of organisations and of their employees and customers.

Stormshield's expertise is spread over three complementary product ranges for utmost security:

- Protection of IT and industrial networks (Stormshield Network Security);
- Protection of workstations and servers (Stormshield Endpoint Security);
- Protection of data (Stormshield Data Security).

Interaction between these three products strengthens the level of protection of IT, OT and cloud environments whatever the point of attack.

These cutting-edge and reliable solutions are certified at the highest European levels (EU Restricted, NATO Restricted, ANSSI EAL3+/EAL4+).

Present in over 40 countries via a network of distribution partners, Stormshield ensures the protection of strategic information belonging to companies of all sizes, public institutions and defence organisations all over the world.

www.stormshield.com



Version 1.0 - Copyright Stormshield 2019