#3

STORMSHIELD



Corporate digital transformation:

putting maturity to the test?

Corporate digital transformation barometer produced in partnership with L'Usine Digitale
2020 edition

Just as we have done every year for the past three years, we have been interviewing **companies and organisations,** large, small and medium-sized, to find out more about their digital projects and security.

So, has this year been just like every other year? Hardly, as you can imagine. 2020 has already been – and will remain – a remarkable year in every way.

That's why, in this third edition of the Digital Transformation Barometer, we'll give a more detailed interpretation of the short- and medium-term effects of current events.

Contents

4 **Preamble: has the "forced-march" digital transformation really happened?**

8 **When current events affect our perception of digital transformation**

13 **Cybersecurity: automated systems in place, despite difficulties**

19 **A strategy of contrasting resources**

25 **Conclusion**

Preamble

Has the "forced-march" digital transformation really happened?

What with the massive strike in French transport at the end of 2019, the international Covid-19 health crisis and the organisational and security issues linked to the lockdown(s), the last twelve months have really put companies and organisations to the test.

We have sought to highlight the latest advances in terms of the digital transformation of these structures, and examined links with this year's events, which have simultaneously slowed down many activities and led to widespread teleworking.

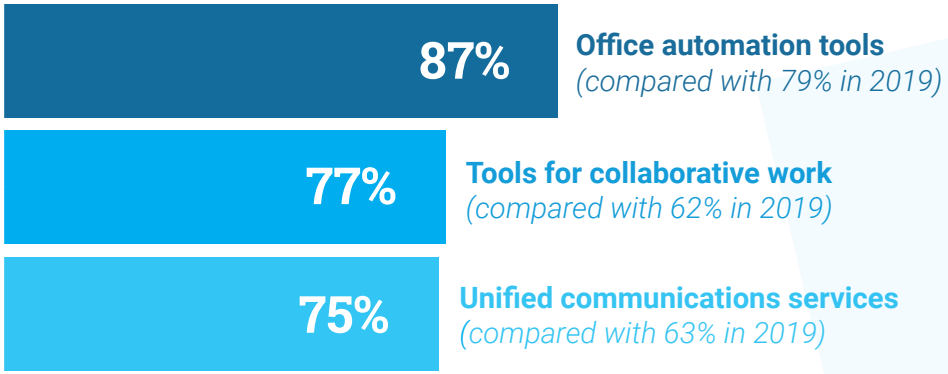
We've talked a lot about a “forced-march” digital transition, but does this phrase accurately describe what we have experienced? For companies that are considered to be digitally “mature”, was this not more in the nature of a test?

The results of our survey, and the various interviews conducted to shed light on those results, do indeed depict very different realities. It is therefore difficult to apply a one-size-fits-all label, let alone a definitive one, to the year 2020.

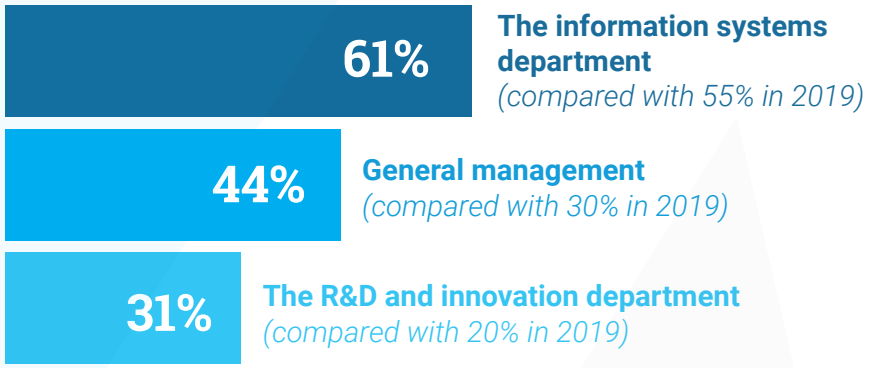
Nevertheless, we hope to provide some keys to understanding to help us draw a few early lessons from a crisis that is still unfolding at the time of writing.

Key figures for 2020

What are the most widely-deployed transformation projects?

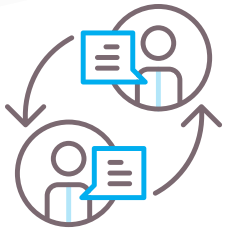


Who leads corporate digital projects?



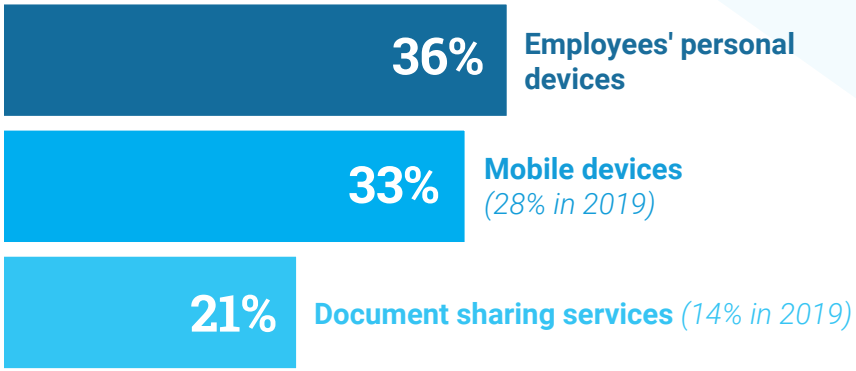
Public bodies invest (at last) in collaborative solutions

37% of respondents from public bodies stated that they had urgently introduced collaborative work tools during the events (compared with 20% of the overall sample). This discrepancy can be explained by a **significant delay in the digital transformation of the French public sector**, as reported by one in three public officials.



Key figures for 2020

What are the most vulnerable elements of cybersecurity?



What corporate security solutions have been implemented?



More than 1 company in 2
reports using a Web Application Firewall (WAF) solution



More than half of the sample
has a file encryption solution. Email encryption is being used by 39% of respondents, with 17% considering it.

90%

The deployment rate for antivirus, antispam or anti-phishing, network and VPN protection is now approaching or exceeding 90%.

Key figures for 2020



Vulnerability of employees' personal devices

The urgent need to implement teleworking has forced some companies to accept the use of employees' personal devices. This creates a genuine security issue, as confirmed by 36% of respondents.



Industrial and operational infra-structure on the right track

Although among the most vulnerable elements in our previous edition, the security of these infrastructures has increased by 13 points this year, so that 66% of respondents now consider them to be fairly or completely secure.

Would you like to find out more about the security solutions being considered or deployed in companies and organisations?

Go to page 17!

Part 1

When current events affect our perception of digital transformation

The news of the last twelve months has highlighted the social and economic inequalities that permeate our society. According to the World Economic Forum[1], one of these challenges is the ever-widening digital divide: the reality of the lockdowns will have been quite different depending on the standard of computer equipment, the quality of the Internet connection or simply the ability or inability to carry out business activities remotely.

Our study reveals that there are also inequalities in terms of perceptions. When asked how their company or organisation has changed in terms of digital transformation this year, 70% of respondents believe that it has improved. Particularly in the retail sector, which has been forced to reinvent itself as a result of successive crises... caused in France by the social movements and transport strikes, and internationally by the Covid-19 crisis.

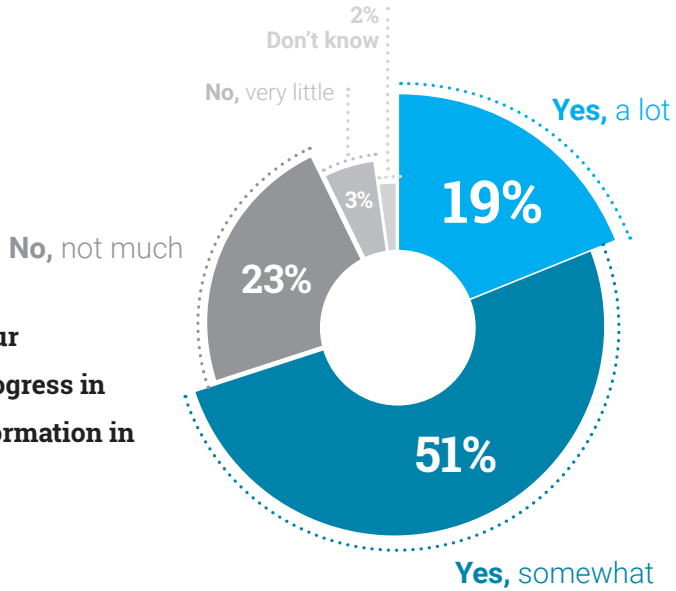
However, this was not the case for public bodies, where 44% of respondents replied in the negative... with the exception of teaching, where a majority of respondents perceived an improvement that some might describe as "remedial" or "catching up".

70%

of respondents believe that their business or organisation has made progress in terms of digital transformation

The proportion of respondents who consider themselves to be ahead of the curve in terms of digital transformation is up almost 10 points compared to last year, although more in the opinion of general management (51%) than of CIOs, who remain more cautious (25%). Of these optimists, 44% operate within the industry. What if the lockdowns – a real "crash test" of digital transformation – had not provided companies in this sector with a chance to assess their level of transformation and reassurance as to their preparedness?

Would you say that your company has made progress in terms of digital transformation in 2019 and early 2020?



[1] www.weforum.org/agenda/2020/08/5-things-covid-19-has-taught-us-about-inequality/

When current events affect our perception of digital transformation

It isn't all due to the virus or strikes

61% of respondents acknowledge that recent events (social unrest, the health crisis) have changed the perception of the key role of digital transformation in ensuring business continuity. And this growing awareness is not unrelated to messages shared by CIOs during the implementation of teleworking, for example.

The health crisis therefore seems to have accelerated digital transformation in public administration, health and social work. On the industry side, Yann Bourjault – Director of Digital Transformation and Cybersecurity France at Schneider Electric – adds that *"more than anything, the health situation has brought a realisation that most manufacturers did not have the ability to supervise their factories remotely."*

Charles Blanc-Rolin, Chief Information Systems Officer (CISO) & Data *Protection Officer (DPO)* for the ***Groupement Hospitalier du Territoire Cantal*** hospital group, muses: "For a *number of management bodies, particularly in the hospital sector, the priority in 2020 was clearly not digital projects or security for them*."

This year also sees an increased **perception of the security function as a "policeman"**. While almost half of the business departments surveyed in 2019 felt that the security function acted as an "advisor", this proportion fell by 11 points in 2020. 37% now see it as playing the role of a policeman (compared to 26% in 2019).

Nevertheless, 57% of those surveyed said that changes in their organisational structure with regard to digital transformation were not due to the health crisis. We must therefore be careful not to attribute all the year's developments to social or health news.

For example, Frédéric Leblond, CISO at the Port of Boulogne and Calais, rolled out a new VPN solution at the end of last year. "We *had the tools to deal with the situation in the spring of 2020,"* he explains.

What form does this progress take?

In the ranking of the types of projects deployed, the top three places remain unchanged from our 2019 barometer: office automation, unified communications and collaborative solutions.

The most noteworthy improvements include:

- mobile applications, where roll-outs increased by 18 points,
- paperless digital solutions, which have become a reality for 54% of respondents (also up 18 points),
- the digital transformation of customer relations, which has increased by 16 points.

Data exploitation (39%) and business platforms (36%) are the most popular solutions being considered or rolled out.

We should remember that companies and organisations have to deal with a lack of clarity made more difficult by uncertainty around current events, which has a certain impact on investment choices. For Frédéric Leblond, CISO of the Port of Boulogne and Calais, this could mean *"focusing in 2021 on setting up a local computer network as part of port extension work"*.

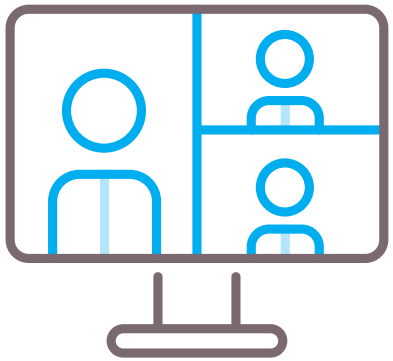
Yann Bourjault, Director of Digital Transformation and Cybersecurity France at Schneider Electric, has observed significant investments in office automation in response to the need to enable teleworking. *"In industrial computing, companies have also invested to enable factories to be operated remotely, because the connectivity of production tools is an issue which has an impact not only on business continuity, but also on competitiveness. This takes the form of the implementation of secure remote access mechanisms, including VPNs, firewalls, PAM (Privileged* Access Management) *solutions, etc."*

When current events affect our perception of digital transformation

Is digital transformation linear?

Not according to the experts interviewed, who point out that it can be quickly reversed. Sébastien Viou, Cyber Evangelist Consultant at Stormshield, does not foresee the universal adoption of all things digital. "*The implementation of teleworking has quickly gone mainstream in France. Teleworking has brought a degree of freedom, which has often been the experience in IT departments, but in companies as well as in schools, many reverted to the old ways as soon as they could.*"

Frédéric Leblond, CISO of the Port of Boulogne and Calais, confirms this view: "*We have been forced to introduce teleworking to ensure business continuity, but it still hasn't become a real habit.*"



However, digital transformation is not limited to teleworking, and some changes may be long-term. For example, Sébastien Viou points to an "*acceleration in sectors that are not really under competitive pressure to change. For example, some municipal council sessions have been held in videoconference form, as have the general meetings of co-ownership associations. The remote signing of notarial deeds has also been authorised*".

Part 2

Cybersecurity: automated systems in place, despite difficulties

Current threat levels

"*Cybercrime and cyber-attacks are on the rise, motivated by the lure of profit. The increase in online shopping and teleworking has increased the attack surface, but cyber criminals are also playing on users' nervousness in these anxious times,*" laments Sébastien Viou, Cyber-Evangelist Consultant at Stormshield.

Indeed, despite the crises, cyber attacks have continued to increase and become more sophisticated in 2020. For example, France's ANSSI cybersecurity agency describes twice as many ransomware cases as there were in 2019, with a peak of 28 cases in one week in June.

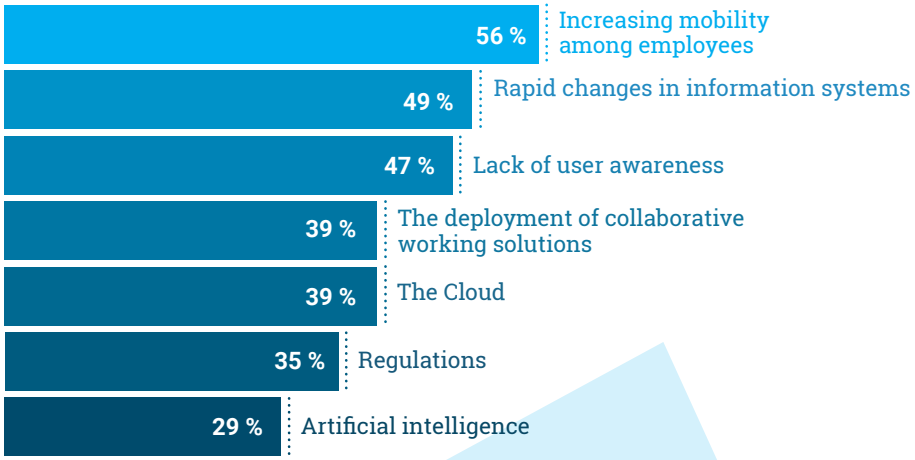
Phishing continues to be popular, although Charles Blanc-Rolin, CISO & DPO at the GHT Cantal hospital group, emphasises that attacks are being tailored to the current situation: "*The attackers are clearly watching the news closely. What with all the misleading statistics on the growth of the epidemic, the fake online mask shops and the vaccine sale scams, we've all had to be especially careful when opening our inboxes!*"

Alongside these rather opportunistic attacks, Jérémy – the CIO of an agri-food group in West Africa – adds: "*Cyber attackers are increasingly well organised. They have more resources at their disposal and are using greater and greater numbers of zero-day exploits.*"

Meanwhile, Yann Bourjault, Director of Digital Transformation and Cybersecurity France at Schneider Electric, observes that cyber attacks in an industrial environment "*are getting closer to the actual machines. Structures of all sizes fear the damage that these increasingly complex attacks could inflict – not only on production tools, but also on the victim's reputation.*"

Apart from attacks, other cyber challenges are of concern to companies

Employee mobility is cited as the top cyber security challenge for the coming years, up 11 points from last year. 49% of respondents also mention rapid changes in information systems (+9 points). **Lack of user knowledge** comes in third place, followed by the deployment of **collaborative working** solutions, in joint fourth place along with the **cloud** (39% of responses).



What are the main cybersecurity challenges your company will have to face in the years to come?

The results show that in the public sector, more than elsewhere, there is **a difficulty in defining individual staff roles** (40% compared with 26% in the full sample). At the same time, 21% of the overall sample report **a lack of financial resources** (a number that climbs to 41% for respondents who felt they were lagging behind in digital transformation).

These medium-term cyber challenges have been compounded this year by some very practical difficulties:

- unsuitable Internet connection in the case of nearly 40% of respondents,
- access problems to business applications for more than one in five respondents,
- access problems to and ability to use communication and work organisation solutions for a third of respondents (46% on this last item among general management).

Not forgetting the delicate balance between remote working and personal life, including childcare.

The study reveals that a quarter of organisations had no choice but to make concessions on cybersecurity to ensure business continuity.

These include a majority of government organisations. Charles Blanc-Rolin, CISO & DPO of GHT Cantal, confirms that *"some healthcare establishments found themselves in critical situations after opening their infrastructures in emergency situations. Fortunately, we make use of collaborative intelligence in our sector, and we were able to escalate a large number of vulnerabilities to the* ***Agence du Numérique en Santé*** *(ANS, "digital health agency")"*.

Another encouraging indicator is that the proportion of respondents declaring that "security" considerations were consistently taken into account in advance of a project has increased from 70% in 2019 to 82% this year. Some automated systems are therefore being implemented.

1 company in 4

reports having made cybersecurity compromises to ensure business continuity.

What security solutions are being introduced for digital transformation projects?

The increase in employee mobility this year is undoubtedly linked to the acceleration of the "**Zero Trust**" approach, which is being considered or deployed in nearly one in five of the organisations surveyed. This strategy is based on the principle of never giving trust by default and therefore always verifying the identity of individuals before granting them any access whatsoever.

Cloud access security brokers (CASBs) had won the business of nearly 20% of respondents in 2019. Enthusiasm is much more moderate this year, with only 7% (compared to 43% of respondents who have no plans to deploy it).

However, organisations and businesses are considering implementing **advanced two-factor authentication** (29%), data loss prevention (**DLP**, 22%) and **email encryption** (17%).



Jérémy, CIO of an agri-food group in West Africa, says there is no shortage of projects: "*We will be implementing new firewalls, multi-factor authentication (MFA), vulnerability scanning and an SOC.*"

Emergency deployments are few in number, with the exception of VPNs, even to a lesser extent (4%). This is undoubtedly explained by the fact that security projects and crisis management tend to follow different timescales. The only certainty at this stage is that we have not seen the last of the crisis yet, hence the importance of anticipating and preparing for different scenarios in order to reduce the threat posed by increased mobility of employees and the use of their personal equipment.

The rating given to the degree of cyber-risk preparedness by the entire sample is 6.6 out of 10, which is stable compared to last year (6.5). It is even reassuring to note that it has risen among IS departments (from 6.1 to 6.6).

6.6/10

as an average score for assessing the degree of preparedness of companies and organisations for the cyber-risks presented by digital transformation

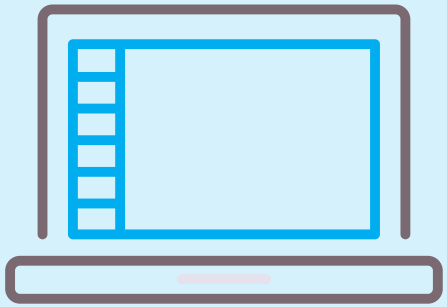
Part 3

A strategy of contrasting resources

New digital tools requiring security

As already pointed out last year, the survey group gave low security ratings to mobile devices and document sharing services (33% and 21% respectively). However, **fears this year are focused on a new item: employees' personal devices (36%)**. These results show that employee mobility – which has generally been imposed on staff this year – remains an area in which the security of digital tools is important.

In terms of improvements, it should be noted that the perceived security of industrial or operational infrastructure has increased by 13 points and that the perceived security of network infrastructure has increased by 19 points, as has business application security.



The SOC: a rising star among resources employed to guarantee information security?

Raising awareness of IT security remains the No.1 priority action recommended by respondents to improve cyber security within companies and organisations. Efforts are already under way in 68% of the surveyed organisations, and 17% are planning to do so.

However, the proportion of companies with no plans for IT security awareness initiatives has increased from 2% in 2019 to 9%. Is this a reflection of corporate priorities in this extraordinary year, or the impact of the cancellation of face-to-face training courses?

Almost half of the respondents said they were considering, or had opted for, the Security Operations Centre (SOC). As Sébastien Viou, Stormshield Cyber-Evangelist Consultant, explains, "*the SOC is involved in the detection phase: it is an organisation, in the process sense, that oversees the security of the information system and identifies threats. It advises the response teams on possible fixes.*"

These IS control towers have been widely deployed in major groups and for critical infrastructures in the wake of the adoption of the General Data Protection Regulation (GDPR), the French Military Programming Law (LPM) and the Network and Information Security (NIS) directive. But smaller structures can also benefit from the services of a pooled SOC.

The use of **consultancy firms specialising** in cybersecurity has more than doubled, now covering 46% of respondents. Conversely, the forecast for **recruiting specialised profiles** has fallen by 13 percentage points from last year. Beyond the budget issues involved, we can see this as a sign of a sector that is still in need of talent. These recruitment difficulties are confirmed by Yann Bourjault, Director of Digital Transformation and Cybersecurity France at Schneider Electric: *"it's already hard enough to find experts in cybersecurity; and even harder in industrial cybersecurity! An understanding of the world of industry, from priorities through to production, to how a programmable controller works, is a particularly rare dual skillset."*

Finally, almost a third of respondents plan to **rethink processes for updating workstations**. One company in five is planning to incorporate security issues into its planning for new digital transformation projects, to set up a cybersecurity **automation platform** or to **redefine its network and security architecture**.



Budgets: always at the heart of security discussions

Budgetary trends are very dependent on the sector of activity and, of course, on the way that sector has been impacted by the crisis. Some sectors have continued to invest in the image of the agro-food industry, at least the segments which distribute essential products to households, or the automotive sector, which has experienced a net rebound after coming out of the first lockdown. On the other hand, it is easy to understand why there has been little or no investment on the part of the players in the hotel and catering industry or airports, for example.

Yann Bourjault, Director of Digital Transformation and Cybersecurity France at Schneider Electric, continues: "*Companies have allocated their budgets to increasing office IT security as part of the widespread switch to teleworking. From the point of view of industrial technologies, the only budgets on the rise are for cybersecurity in factories.*"

This observation echoes the 27% of respondents who stated that their company had released significant extraordinary funds for digital technology and its security in this context.

Priority has been given to digital transformation in the short term, but there seems to be a willingness to invest more in security in the medium term, with 49% of respondents saying that the cybersecurity budget will increase.



It is to be hoped that companies and organisations have the means to take action.

Faced with the problems of financing the public sector, and the hospital sector in particular, it is clear that managing its ageing IT architectures and obsolescence in its software does not rank high on the list of priorities. The investment of 2 billion euros in digital technology planned by the ***Ségur de la Santé*** health consultation body is therefore to be applauded. However, Charles Blanc-Rolin, CISO & DPO of the GHT Cantal hospital group, tempers any such enthusiasm: "*Yes, it's historic, but these agreements make no provision for maintaining these investments*"[1].

Budgetary difficulties also affect the private sector. In July, nearly half of CAC 40[2] companies were preparing to stabilise their cyber security budgets, and 25% to reduce them.

Jérémy, CIO of an agri-food group in West Africa, is therefore something of an exception. "*While others have seen their entire budget eaten up by security and/or remediation measures, my budget has seen very little impact and we will be able to maintain the investment roadmap,*" he confides, aware of his good fortune.

[1] esante.gouv.fr/node/3641

[2] www.lesechos.fr/tech-medias/hightech/cybersecurite-en-difficulte-le-cac-40-reduit-ses-budgets-1221700

Conclusion

In the digital world, as in other areas of our societies, the crises have accentuated inequalities of access, resources and digital skills between the various players. Yann Bourjault, Director of Digital Transformation and Cybersecurity France at Schneider Electric, confirms this: "*Cyber threats are increasing and growing in complexity much faster than computer security is improving: the gap is widening*."

2020 has also been an "*extraordinary lab experiment for large-scale out-of-office work and teleworking*"[1]. According to Jérémy, CIO of an agri-food group in West Africa, "*teleworking will have made a lot of companies aware this year that IT was vital and that IT and cyber budgets should be reassessed accordingly*".

At individual level, the personal infrastructure of the employee becomes the concern of the company. With the spread of teleworking, cyber responsibility tends to shift to employees. Are they ready to assume that responsibility?

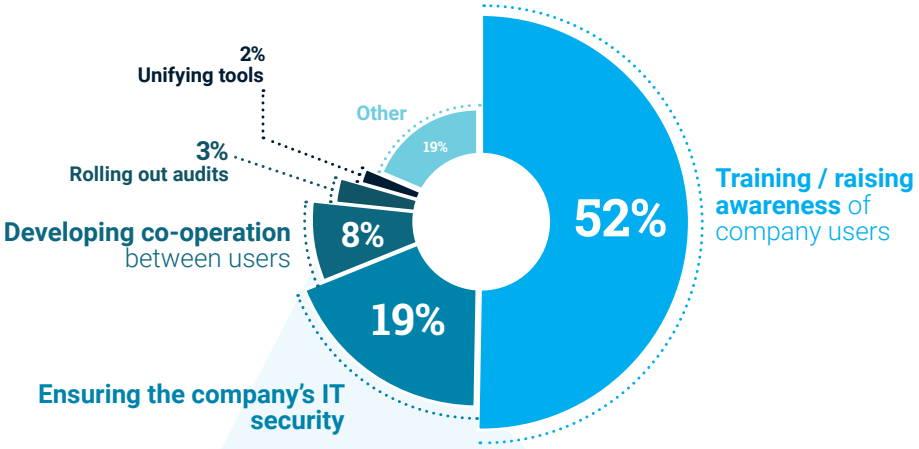
At least, that's the question being asked by Sébastien Viou, Cyber-Evangelist Consultant at Stormshield: "*The whole company must be involved in improving cybersecurity. For example, the IT team could set up the tools and then delegate day-to-day management to managers*." It's a model that requires a sustained effort to raise awareness among all audiences.

[1] CLUSIF, *Teleworking, Cybersecurity and Employees: the new balances,* October 2020

Continuing to experiment to improve cyber security

Charles Blanc-Rolin, CISO & DPO of GHT Cantal, is continuing to fulfil his mission: "*passing on information with the goal of changing working practices*." To this end, he shares information on current events, threats and incidents observed in his sector. "*Despite the situation, we have user feedback, alerts, etc; things are positive*."

And he is not the only one to have opted for the communication route.



What would be your main ideas for improving the cybersecurity of your company?

For almost a year now, Frédéric Leblond, CISO of the Port of Boulogne and Calais, publishes a monthly newsletter that has captured the attention of its audience. And a programme of webinars enabled Schneider Electric to continue its mission of evangelisation to raise security levels across the entire ecosystem, despite the cancellation of face-to-face training sessions.

This is undoubtedly a positive point to emerge from this unusual year: the incredible number of resources shared to build collective intelligence... and the world of tomorrow.

Sources and references

Digital transformation and cybersecurity barometer 2020 Stormshield/L'UsineDigitale

Methodology:

Self-administered online questionnaire, completed between 16 July and 07 September 2020 by 217 decision-makers in the IT/Digital sector and business units, from all sectors of activity and all sizes of company.



STORMSHIELD

Around the world, companies, government institutions and defence organisations need to ensure the digital security of their critical infrastructures, sensitive data and operational environments. Stormshield technologies are certified and qualified at the highest European level to meet the challenges of IT and OT and protect their business activities. Our mission: to give our clients peace of mind concerning cyber risks so that they can concentrate on their core business, which is so crucial to the smooth running of our institutions, our economy and the services provided to people. Choosing Stormshield means opting for trusted European cybersecurity.

www.stormshield.com