



STORMSHIELD

CYBERSECURITY

CISO: A PROFESSION ON A KNIFE EDGE

Victor Poitevin
Digital Manager,
Stormshield

They've paid a personal price during the pandemic. On the front line of the Covid-19 crisis, unhappiness among CISOs – torn between urgent internal demands and long-term security requirements – seems to have risen to new heights. To such an extent, in fact, that the topic of burnout is now no longer a taboo in the sector. We find out more.

In November 2019, the CISO Stress Report, based on a survey of over 800 Chief Information Security Officers (CISOs) and company leaders in the United States and the United Kingdom, painted a bleak picture of one of today's most in-demand jobs. And it revealed some alarming figures: 88% of the CISOs surveyed considered themselves to be "*moderately or extremely stressed*", 48% said that their stress levels had an impact on their mental health, and 23% admitted that they had turned to medication or alcohol. With long working hours, limited budgets, recruitment difficulties, and a lack of representation on boards of directors, the situation is hardly promising, while at the same time employees and business teams require IT tools to offer ever-greater speed and fluidity. And there's also the constant stress as a result of the acceleration of new cyber threats, coupled with the fear of being held liable in the event of mishaps... **So what's the situation in terms of CISOs' mental health?** What approaches can be taken to improve things?





THE CULTURE AT THE ROOT OF THE PROBLEM

Above all, CISOs suffer from being misunderstood. Yohann, who is looking for a job after leaving his former role to avoid burnout, explains: *"What's frustrating is that when we do our work well, no-one sees it."* Which makes it difficult to showcase your value as a cybersecurity expert... And yet **the role of CISO is a role for people who are passionate** about new technologies, and for many of them it's much more than a job. *"The field of IT security is so huge that you can never do enough – we do it out of professional ethics and out of love for our work, but it can become exhausting"*, he adds. The CISO Stress Report clearly highlights the weight of the responsibility that these IT security experts shoulder: 44% of respondents said that the main reason for their unhappiness was single-handedly being responsible for their company's cybersecurity in a world that fails to recognise the severity of the challenges they face. And for 35% of those surveyed, the level of stress is so great that it affects their physical health. Following its publication, the study received mass coverage, and **Russell Haworth**, CEO of Nominet and the study's sponsor, reported receiving many messages from CISOs and cybersecurity experts confessing that they recognised themselves in the study's results..

"The field of IT security is so huge that you can never do enough – we do it out of professional ethics and out of love for our work, but it can become exhausting."

The study was based on professionals in the United States and the United Kingdom, but the situation doesn't seem much better in France either. However, the scope of the problem differs as a result of different cultural characteristics: it seems that France places little value on those with *"technical"* profiles. **Alice Louis**, an IP/IT lawyer and expert in information asset governance, recalls the exemplary case of **Louis Pouzin**. *"A brilliant researcher and engineer and a Polytechnique graduate, he is recognised globally as being one of the founding fathers of the internet. The Cyclades project, which he led in the 1970s, resulted in significant advances in the field of network architecture. The Americans, who were in the midst of the Cold War at the time, soon saw the strategic benefits, while the French government decided to focus on Minitel. I'm stunned to see just how unable we are to learn from the lessons of the past! France has many talents, and French genius also shows itself in the form of information and communication technology."* But this attitude isn't present across the pond. *"If you take the top 10 listed companies, three quarters of them are run by engineers or coders. This is absolutely not the case in France, where the engineering culture we take so much pride in is nothing more than a fantasy. There are no Polytechnique graduates in top state roles, only ENA graduates"*, says **Fabrice Epelboin**, an entrepreneur and teacher at Sciences Po.





In his eyes, IT is still viewed with a certain level of contempt, and he responds to this with provocation: *"Within companies, people don't know the name of their IS Director, and so they have nothing to do with them. For big French companies, the IS Director is a housewife – a well-paid one, yes, but someone in a position of a simple underling who you call when you have a problem."* So what about CISOs, who are themselves subordinate to the IS Director? In the 2018 edition of the *"IT Threats and Security Practices in France"* study by Clusif, 77% of CISOs at the biggest companies reported that they were part of the IS Department. Meanwhile, in companies of fewer than 1000 employees, 55% reported directly to management.

In the United States and the majority of English-speaking countries, the CISO is increasingly part of the management committee. But in France, they are overlooked within their companies. *"It's to do with the fact that fundamentally, a CISO is a hacker. They don't come from the prestigious universities we value, and they aren't familiar with their codes of behaviour, otherwise they would have become an engineer"*, Fabrice Epelboin adds. And as a result, CISOs are perceived as holding simple support roles.


CISOs IN CRISIS BEFORE THE CRISIS

Especially because, isolated and alone, CISOs aren't lucky enough to enjoy a support system within their company – in fact, the very opposite is true. *"It's a product of the organisational structure"*, says Yohann. *"We're seen as a necessary evil. Our missions clash not only with those of other departments, but also with the missions of the IS Director, our line manager, whose goals of ensuring infrastructure availability and ability to cope with loads are the opposite of our own."* When the two clash heads, the CISO – whose budget is nothing but crumbs and who often has a small team – must sometimes accommodate a bending of security practices in the name of the business's needs.

"CISOs are seen as a necessary evil."

Jérémy, another CISO who agreed to tell us his story, shares this view. *"We're caught between the IS Director, the management committee, and the users, who don't understand why we impose security standards. By going along with what IS departments want, we're often forced to approve dangerous situations and accept the risk of it coming crashing down on us."* With a wry laugh, he repeats a well-worn phrase among CISOs: *"The IS Director is management's fall guy, and the CISO is the IS Director's fall guy."* If a problem arises, the CISO will soon be blamed – or even sacrificed.

"We're caught between the IS Director, the management committee, and the users, who don't understand why we impose security standards."



And to top off this precarious position, along came the Covid-19 crisis to add to the friction. *"The sole aim in many executive committees at the moment is to survive, and that comes at the expense of the security standards we recommend"*, says Jérémy. Rolling out remote working for the entire company by generalising BYOD has opened up a number of weak points in IT security while also increasing the workload of already overworked CISOs. *"Everything had to change overnight. And no company was prepared"*, says Jérémy. *"For employees, there was no issue, because their work didn't change, whereas on our side it required a complete reconfiguration."* In the wake of these practices, new threats, such as shadow IT, are arising as a result of the use of applications and services alongside those offered by the IT department. *"By pulling out all the stops, CISOs were nonetheless able to quickly and successfully implement a number of initiatives. But this success was a double-edged sword: it hid the complexity and difficulties of our task"*, Jérémy adds.

And the cost of succeeding in this difficult balancing act can be the implosion of your personal life. *"I come home late from the office, I grab something to eat, and I get back to work until 1 am. I no longer have weekends"*, says Yohann. In English-speaking countries, the CISO Stress Report reveals the same unease: 95% of respondents reported working more than their contract requires, and 39% said they had missed a family member's wedding or even holidays because of their work.

HOW CAN YOU LOOK AFTER YOUR CISO?

From within and without, CISOs are besieged from all sides. But they aren't doomed to their fate, and a number of solutions can be considered.

Yohann and Jérémy are unanimous: CISOs should no longer be subordinate to the IS Director. *"This relationship prevents the CISO from properly fulfilling their role as a cybersecurity expert and a counter-power that can only be achieved with independence"*, explains Jérémy. To do this, a more American cultural approach is required – one which is more open to delegating responsibility. *"The CISO also needs to be closer to the top management team and incorporated into the Executive Committee. Once they're on an even footing with the IS Director, they will be able to defend their positions in full transparency"*, adds Yohann. This would allow decisions to be made with full knowledge of the facts.

And at the employee level, one solution could be to organise educational workshops. *"In employees' minds, moving people to remote working is simple because they don't understand that this means protecting a different network with new concentrator flows. If only they knew"*, sighs Yohann. Establishing workshops to raise awareness of digital well-being would also help employees understand why certain best practices (no longer simply having an eight-character password, only using the recommended tools, etc.) are necessary. Because **at a time when the boundaries between personal and professional lives are becoming blurred** and when digital attacks are becoming increasingly common

and increasingly sophisticated, employees haven't yet truly understood the scope of the risks they face. According to the *CISO Stress Report*, just 15% of respondents believe that the topic of cybersecurity is consistently discussed at meetings attended by company managers. And this means that the CISO, in their capacity as an IT security expert, must also become a teacher.

Another approach supported by **Alice Louis**, who champions interdisciplinarity, is "managing knowledge networks – in particular, networks of ethical hackers", who are culturally closer to CISOs than IS Directors. Ethical hackers "could be clear allies for organisations", helping to **shift the balance of power in favour of cybersecurity**. These trusted hackers, who are sometimes more likely to be listened to, could play an important role in today's companies, becoming extensions of in-house security teams. **Frans Rosén**, a hacker from the HackerOne community, wrote in a press release published at the end of May: "Some of my favourite highlights are [the] reactions to some of the bugs I've found. When the [IS Director] of a company calls me up in the middle of the night to understand the severity and panics when he realizes the impact."

While Yohann and Jérémy have seen improvements to the situation, they nonetheless fear the role that Covid-19 could play. The epidemic could roll back what little progress they have witnessed in people's understanding of the role of CISO. So will the crisis accelerate progress or drive it back to the bad old days? It's still too soon to tell.



STORMSHIELD

All around the world, companies, governmental institutions and defence organisations need to guarantee cybersecurity for their critical infrastructure, their sensitive data and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission: to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy and the services provided to our populations. When you choose Stormshield, you are choosing a trusted European cybersecurity provider. Further information: www.stormshield.com