devoteam

May 2020

Cybersecurity **for business**

Risk management: essential starting point for effective cybersecurity

Episode 1/3

Creative tech for Better Change

TABLE OF CONTENTS

EDITORIAL

Since 2017, cyber risks, such as attacks or data theft, have been regularly featured in the top 5 of the World Economic Forum's annual Global Risk Barometer, a sign of much welcome awareness among the world's top leaders. In 2020, they disappeared from the ranking, which was established before the Covid-19 pandemic. However, from data leaks to ransomware, the news keeps reminding us that no one is completely safe and that the damage is increasingly heavy. So what has happened? Did companies tackle the problem head-on, to the point where they felt sufficiently protected? Or is there a false sense of security around cybersecurity? If the latter is correct, why and how have CIOs and CISOs failed to maintain their vigilance? It is these questions, among others, that we wanted to answer by launching an EMEA survey on cybersecurity, together with IDC. The study was also carried out before the Covid-19 hit, which makes the results even more valuable.

This dramatic episode has shown us that our resilience is increasingly dependent on digital systems, and therefore on our ability to protect them from the very threats that the crisis is intensifying.

We are publishing the results in a series of three white papers, each focusing on a dimension of the study that we feel is fundamental in exploring these questions fully. The first one concerns risk management and business impact, the second on DevSecOps and operational excellence in security, and the third on the security of digital transformation and the workplace.

In this first part of the series, we address the issue of risk as it is the essential starting point for any responsible and effective approach to cybersecurity. Risk is the prism through which the CISO and the CIO can highlight what's at stake, go beyond the technical dimension and allow management and business line managers to appropriate it. It is through risk management that collaboration between these players is established, a collaboration that digital transformation makes more essential than ever. And it is risk, finally, which gives an indication of the investment that the company must make to conduct its operations with confidence.

Without revealing all the results, which our experts will be discussing at the end of this document, the figures corroborate the lack of maturity that we all too often see in the field. It is true that cybersecurity is no longer ignored but, despite the rhetoric, it is still not treated as a priority issue at the highest level. Change must come from the top, so that everyone understands that cybersecurity is not the responsibility of only a few professionals, but of everyone, and that it is not just a matter of protecting the information system, but the entire company.

Renaud Templier
Group Offer Director
Devoteam

FOREWORD

When the crisis strikes, it sweeps away all the plans. Of course, back-up and business continuity procedures have been planned to save what can be saved and ensure core business gets done. But the challenge for a company is not to limit the damage, but to remain competitive no matter what happens.

In this context, management has to make bold and quick decisions, show a calm and resolute face, instil unity and confidence, but above all they have to face up to their previous decisions. The crisis tests the solidity of the foundations it has been able to put in place: strategy, culture, values. In an uncertain environment, these points - which must be reaffirmed without ambiguity - enable employees to act wisely, almost instinctively, and to make the right decisions. For this to happen, the stability of the strategic framework must be coupled with a significant level of tactical and operational autonomy. No one can claim to know with certainty how things will play out, and it is the people on the ground who will be best able to sense and react to a changing and unpredictable situation.

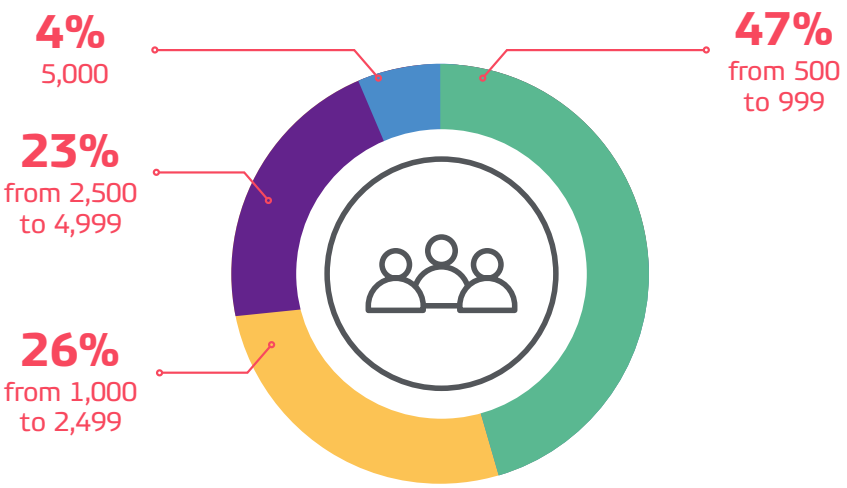
During a crisis, people are the true guardians of a company's resilience and future, and that is why all efforts must be made to enable employees to show their extraordinary capacity to adapt. Above all, we must ensure their safety, their physical and moral integrity, but also provide them with the appropriate framework and tools. Cybersecurity plays a key role in this context. Because in a fragile situation, it gives everyone the reflexes, tools and confidence needed to reinvent the business - without exposing the company any further - and thereby guarantee the company's future.

Sébastien Chevrel
Group COO
Devoteam

METHODOLOGY

On behalf of Devoteam, IDC interviewed 601 decision-makers from European and Middle Eastern companies with more than 500 employees. The interviewees were divided into three distinct populations: Business (CEO, CFO, business managers...), IT (CIO and other IT managers) and Security (CISO and other security managers).

Company size (number of employees)



DIGITAL TRANSFORMATION: ONE PRIORITY, SEVERAL INTERPRETATIONS

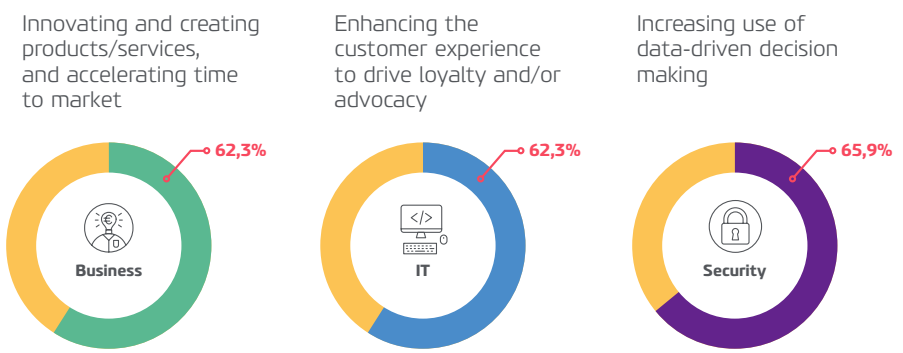
Within companies, there is at least one topic that is no longer subject to debate: the need to transform and go digital in order to take advantage of the opportunities offered by new technologies in terms of innovation, reinventing and optimising processes and improving customer and user experiences. 100% of the companies surveyed declared that they had implemented a digital transformation programme.

Is your organization currently running any digital initiatives within the framework of a digital transformation program?

Yes ! 100%

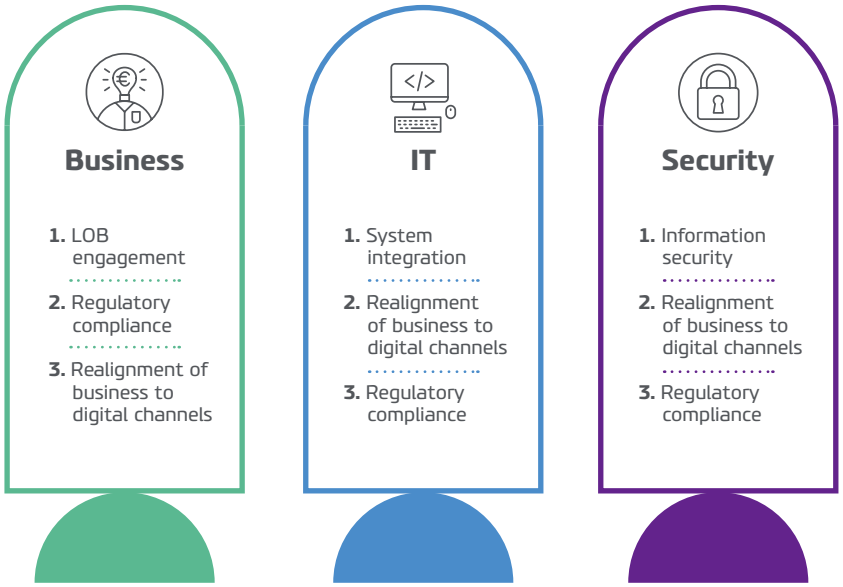
But this unanimity is only superficial because the respondents do not give the same meaning to the term, assigning each a different priority: innovation and time-to-market for Business, user experience and satisfaction for IT, and massive use of data for security

To what extent do you agree that the following are the primary goals of your organization's DX strategy?



These fundamental divergences of interpretation inevitably lead each of us to focus on different concerns, each strongly influenced by its own culture and traditional objectives: mobilization of different business lines to support the operations, systems integration to support IT and information security to support security. This tendency seems quite natural, but it is also a sign that the company has not completely succeeded in breaking down its old silos, which is one of the key aspects of the digital transformation. This misalignment can often be a barrier to the overall success of the strategy.

What are the primary considerations for your organization when it comes to executing your digital strategy?



CYBERSECURITY: A VERY SUPERFICIAL AWARENESS

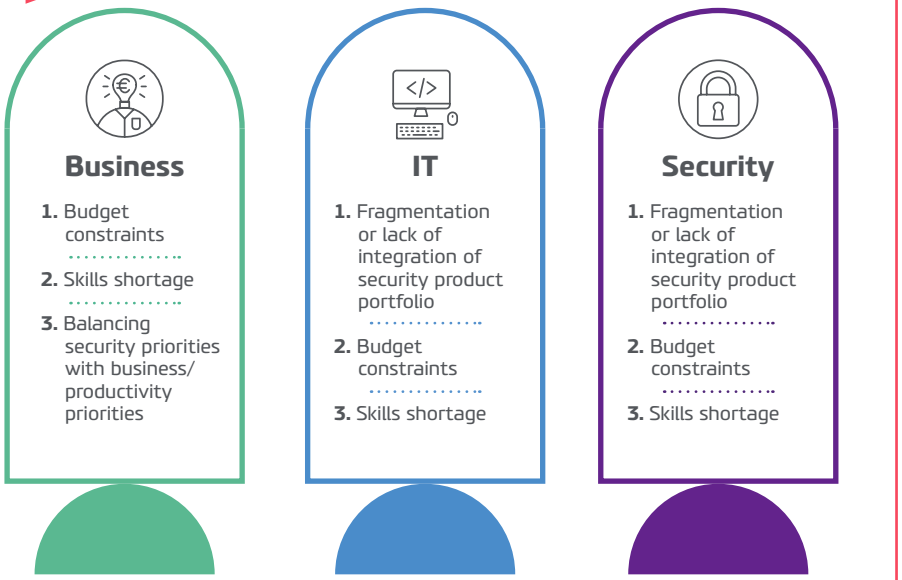
Despite the persistence of internal barriers, the regulatory pressure - including the coming into force of GDPR, and the media coverage of major incidents that have had a positive impact, cybersecurity is now being taken into account by the Business, which is starting to acknowledge its value. However, opinions are still very divided on its main contribution, with none of the various proposals of the survey - improving operational efficiency, reducing operating costs, optimising risk management, compliance and enhancing brand image - standing out among business respondents

What is the primary area in which your organization expects IT security to deliver value?

	Business	IT	Security
Improved operational efficiency	23%	24%	29%
Reduced operating costs	21%	24%	18%
Optimized risk management	19%	17%	27%
Compliance (internal and/or regulatory)	18%	18%	15%
Enhanced brand value/perception	18%	17%	15%

In other words, awareness is still superficial. Security is not deliberately neglected by Business managers, but because they are uncomfortable with the subject and unsure of what it can do for them, they do not consider it a priority and often end up sacrificing it to other issues. In fact, they are the only ones among the profiles surveyed to rank the difficulty of balancing different priorities as one of the top three barriers to improving security

What is mainly limiting your organization's ability to improve its security?



However, all the stakeholders unanimously agree on two major challenges: budgetary constraints and skills shortages. Regarding the first matter, although it is rare to consider ones department sufficiently financed, the lack of funds also reveals that security is not given as much importance in reality as it is in theory. In many cases, only the bare minimum, i.e. what is required by regulations and control authorities, is addressed.

As for the skills shortage, it is probably not so much a question of experts in a particular cybersecurity technology, but rather of having profiles within the business capable of bringing maturity to all organizational levels. Because, as revealed by these results, they are seriously lacking.

ADOPTING A RISK-BASED APPROACH TO MAKE BUSINESS IMPACTS EXPLICIT

In order to effectively strengthen the security of the digital enterprise without overwhelming it with a profusion of technical devices and constraining procedures, it is essential that the solution be proportionate to the probability and extent of possible damage. In other words, to move from the absolute notion of security to the relative notion of risk. Another key advantage of risk is that it can be assessed in terms of its probability and impact on the company, and thus removes the technical dimension in which cybersecurity is too often confined. Translated into risks, IT security is no longer an obscure and costly constraint, but an objective management element. Adopting a risk-based approach makes it possible to clarify the potential impacts on the business. The stakes then become comprehensible to all, measurable and comparable, so that the company can set clear objectives and rules and measure the progress made in relation to the investments made.

For almost all the respondents (92,2 %), a risk framework already guides risk-based investment decisions. More specifically, 81.4% of the companies surveyed believe that their approach to cybersecurity is already aligned with this risk management policy.

Does your organization incorporate risk modeling and risk management into its strategy planning?

Yes! 92,2 %

Is your organization's cybersecurity strategy reflective of the enterprise risk management strategy?

Yes! 81,4 %

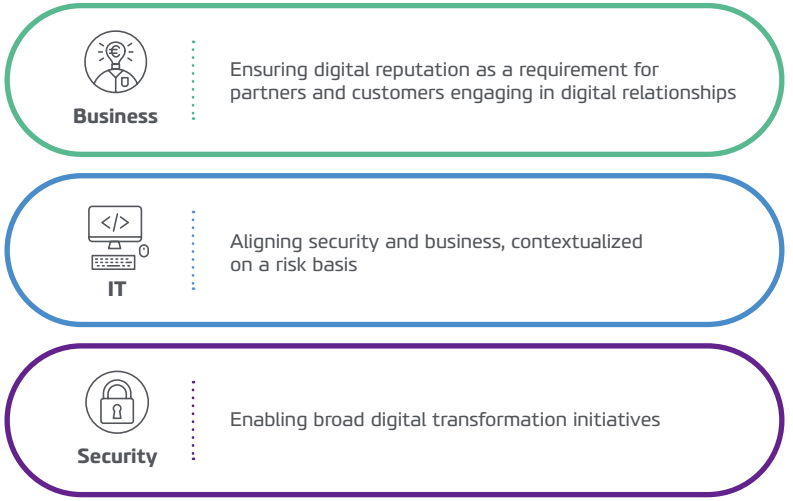
Yet, as we have seen, budgetary constraints and skills shortages remain permanent obstacles to improving security. It is surprising that companies can claim to be so risk-conscious but that it seems so difficult to mobilise the necessary resources. Differences between the different profiles surveyed on the benefits they expect from security or their perception of the operational reality also suggest that cyber risk is not as well understood as some believe. For example, Business decision-makers are convinced that cybersecurity is mostly taken into account at the early stages of a project, whereas IT and Security managers are well aware that this is not the case

To what extent is IT security embedded into new business initiatives in your organization?

	Business	IT	Security
From the planning stage of any new development	38%	23%	27%
During the execution, but prior to launch	31%	34%	35%
As an afterthought (post-release/closure)	24%	35%	32%
Not explicitly invited for participation	8%	8%	6%

The gap between what the profiles expect from the digital trust that cybersecurity can bring is particularly illuminating because it highlights three distinct attitudes towards cybersecurity. Looking ahead, Business decision-makers are anticipating - maybe a little hastily - that an environment of trust will enable them to grow their business within a customer and partner ecosystem. Facilitators by nature, CISOs see security as a lever for digital initiatives. Finally, pragmatic CIOs remind us of the need to align Security and Business, and consider risk as the means to achieve this

What do you consider to be the most critical business outcome that security supports in establishing digital trust?



Such differences of assessment reflect the lack of maturity already observed, and one may, therefore, suspect companies to be under the illusion that they are integrating cyber risk into their risk management policies.

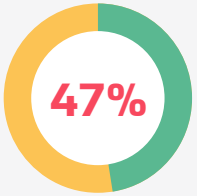
THE CISO MUST DISPEL ILLUSION

And it is on this last point that the CISO is particularly key. Only the CISO is in a position to translate cyber threats into business risks and to recommend suitable solutions. It is their responsibility to carry this risk-based approach of cybersecurity and to spread it to all levels of the organization through tools and, above all, cultural awareness.

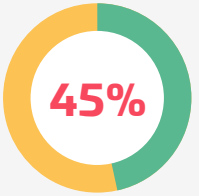
This is, in fact, the role that the decision-makers surveyed assign to them primarily. According to decision-makers, the CISO's main function is precisely to cooperate with the business lines so that they carry out their activities within an acceptable risk framework. A welcome sign of confidence, but which does not mask the enormity of the challenge ahead!

Which of the CISO's various missions is the most important?

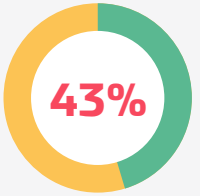
Cooperating with lines of business to encourage activities within an agreed risk posture



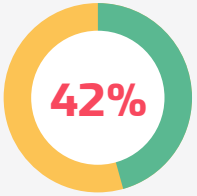
Reducing the likelihood of threats (internal and external) compromising the enterprise and its assets



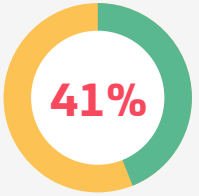
Integrating security with the enterprise environment to drive cost and efficiency benefits



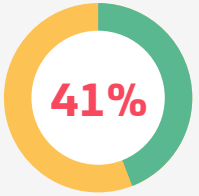
Establishing the enterprise's security risk profile



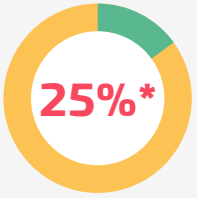
Empowering existing staff to drive improved output



Optimizing the security stack to improve security posture



Enabling the enterprise's digital transformation initiatives (securely)



*(total respondents)

THE DEVOTEAM EXPERTS' POINT OF VIEW

« Rethinking cybersecurity governance. »

The figures show that the leaders are convinced that security is essential and that they have no intention of selling it off, but we can also see that they sometimes lack the maturity to cope with balancing investment decisions and change management priorities. For this reason, they may tend not to accept proposals made to them when they are not supported by a business case and explained convincingly in language they understand. It is therefore crucial that someone makes the connection between the business issue, the business risk and the underlying technology. This should be the role of the CISO, but in many companies, they subordinate to the CIO, who is then ultimately responsible for explaining why IT needs to invest in security. This type of reasoning is not necessarily a strong point of CIOs and it may compete with other IT resources and budget constraints. This is why it is fundamental to rethink the governance of cybersecurity. Separating IT and security roles eliminates such conflicts of interest. The CISO should then be able to directly obtain the necessary buy-in from the business and its executive management. Based on this commitment, the CISO can specify requirements to IT, which can then act as a service provider fulfilling a formal request. CISOs will have to argue by focusing on the notion of risk, which is known and accepted by top management, rather than the more vague and demobilizing notion of security gaps. In addition, the CISO needs to be in a position to put in place business related indicators that measure the level of cybersecurity risk. In the area of cybersecurity, there is a great lack of visibility. This is one of the main factors that blocks making the right decisions at the right time.

Martin Esslinger
Partner
Devoteam

« The CISO must become a business enabler. »

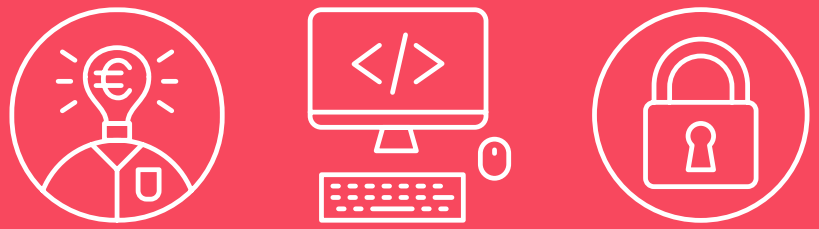
Attached to the CIO, the CISO is obstructed in his actions because, as the study shows, their priorities differ. The first seeks to secure his entire IT system and the second, the activity itself. However, the trend is for the business lines to bear responsibility for securing their developments. The CISO must, therefore, be able to communicate directly with the CIO, raise their awareness, guide them towards appropriate solutions and then justify their investment. Detached from the CIO, the CISO also moves beyond the traditional culture of reducing IT costs, enabling him to show that security is not a cost centre but a lever of value creation. The CISO must become a business facilitator and present as such. In order to do so, they must abandon their «cyber-centrism» and no longer think in terms of potential threats, but in terms of products and services and the associated risks. They are not required to be an expert in all technologies, but the CISO is the person in the organization who understands them and can connect them to business issues. To be convincing, he must be able to demonstrate that the suggested countermeasures will enable business risks to be controlled. Even if things are changing, we are still far from this scenario. In most cases, the CISO is caught up in operational urgency and does not have the means to implement the culture, tools and methods that would make security part of everyday life. They find themselves confined to the role of security guard and firefighter, where his vocation should be to help the company grow.

Jorgen Papadopoulos
Partner
Devoteam

« A wall of incomprehension persists. »

The results of the study show that a wall of misunderstanding persists between cybersecurity professionals and business-line managers, many of whom still perceive security as a constraint. As a result, security is addressed without always attaching enough importance to it or seeing what it could bring in terms of speeding up, building trust and reducing «time to market», for example. Blame for this misunderstanding is shared. On the business side, while the cyber risk is now acknowledged, biases and prejudices remain, which prevent the right measures from being taken. And on the security side, we don't always know how to promote the message and, because of the distance with the business, the stakes for the company are not always properly understood. To tackle this situation responsibly, everyone has to do their part. The key to facilitating collaboration and making it a natural process is to establish a risk metric that is clear, understandable and irrefutable for all. The right balance between risk and operational need can be found by weighing the risk and operational requirements: on the one hand, the contractor knows and assumes the risk he is taking in relation to the issues at stake; on the other hand, Security finds the most appropriate solution in terms of cost, protection and impact on operations. A solution which, in fact, is not necessarily complex. As in the business intelligence sector, cybersecurity is first and foremost a matter of simple precautions taken on a daily basis. It is a culture, a DNA, before being a technological subject.

Benoît Micaud
Partner
Devoteam



ABOUT DEVOTEAM

Devoteam is a leading consulting firm focused on digital strategy, tech platforms and cybersecurity. By combining creativity, tech and data insights, we empower our customers to transform their business and unlock the future.

With 25 years' experience and 8,000 employees across Europe and the Middle East, Devoteam promotes responsible tech for people and works to create better change.

Creative Tech for Better Change

CONTACTS

Renaud Templier
Cybersecurity Group Offer Director
renaud.templier@devoteam.com

Martin Esslinger
Partner, Devoteam
martin.esslinger@devoteam.com

Jørgen Papadopoulos
Partner, Devoteam
jorgen.papadopoulos@devoteam.com

Benoît Micaud
Partner, Devoteam
benoit.micaud@devoteam.com

Creative tech for Better Change