devoteam

October 2020

# Cybersecurity for business

Security by design, SecDevOps :
security upstream !

Episode 3/3

**Creative tech for Better Change**

# TABLE OF CONTENTS

# FOREWORD

When the crisis strikes, it sweeps away all plans. Of course, back-up and business continuity procedures will have been put in place 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 firm and fast decisions, show a calm and resolute face, instil unity and confidence, but above all they have to face up to their previous decisions. A crisis tests the solidity of the company's existing foundations: 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, as long as we can test and learn from it.

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 - therefore guaranteeing the company's future. The more cybersecurity is embedded within formalized policies and best practices, the more efficiently it will be addressed in both regular times as well as in times of crisis.

**Sébastien Chevrel**
**Group COO**
Devoteam



# 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 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. After addressing risk management and the business impacts of cybersecurity, and then looking more specifically at the case of workplace and digital transformation security, this third and final issue focuses on Operational Excellence in IT security.

While the IDC survey results have highlighted a number of unfortunate shortcomings and obstacles, they have also confirmed that perceptions of cyber-security have changed significantly. The same survey carried out some ten years ago would certainly have revealed low appreciation and interest in the subject at that time. Today, even if an organisation has not yet made all the improvements on their list, particularly in terms of resources, everyone agrees that cybersecurity is a major issue that contributes directly to value creation.

The challenge for companies is to capitalize on this change of mindset both in organisational and operational terms. How can we ensure that cybersecurity is no longer a matter for specialists, to be dealt with separately, but rather a matter for everyone, effectively integrated into daily processes? It is this question of security management and its operational excellence that we are addressing here.

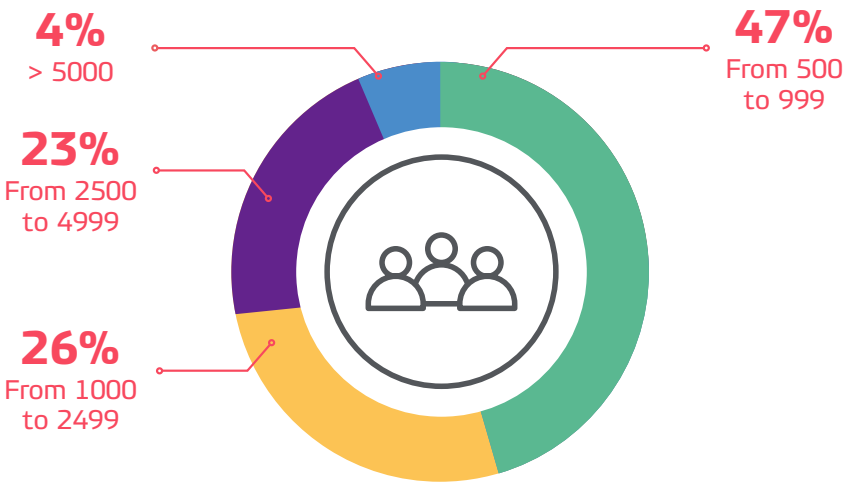
Without entering into the details of the results, which our experts will discuss in detail at the end of this document, the answer to this question largely involves «shifting-left». This will mean approaching cybersecurity more upstream of projects, first through a security policy whose formal framework will be imposed to everyone, then through approaches such as Security by Design and DevSecOps, which reconcile the needs for agility, efficiency and security on a practical level. It is at this fragile point of balance, between rigour and flexibility, that the operational excellence of cybersecurity lies.

**Renaud Templier**
**Group Offer Director**
Devoteam

# METHODOLOGY OF THE STUDY

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.

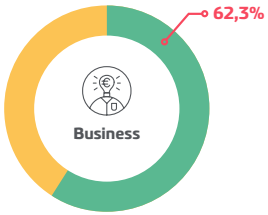
Is your organization currently running any digital initiatives within the framework of a digital transformation program?

YES ! 100%

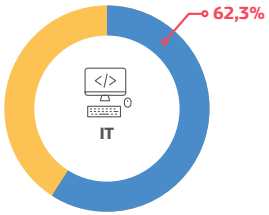
But this unanimity is only superficial because the respondents do not ascribe the same meaning to the term, assigning each a different priority: innovation and time-to-market for Business, user experience and satisfaction for IT, and massive use of data for Security.

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

Innovating and creating products/services, and accelerating time to market




Enhancing the customer experience to drive loyalty and/or advocacy




Increasing use of data-driven decision making

These fundamental differences reveal that the digital transformation has not always been precisely defined. Everyone therefore gives their own interpretation of it, in which the end goal (what the company is meant to become) very often disappears behind the means (the digital). Under these conditions, security is only one priority among others, relegated during implementation behind the realignment of business to digital channels, regulatory compliance and systems integration.

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

1. Realignment of business to digital channels
2. Regulatory compliance
3. System integration
4. Information security


# SECURITY, A LEVER FOR OPERATIONAL EFFICIENCY

Despite these differences of appreciation, cybersecurity is nonetheless perceived by all respondents as a lever for value creation. Contrary to popular belief, cybersecurity is not seen as an obstacle to the fluidity and agility of operations, but first and foremost as a means of improving operational efficiency, for example through automated controls or Single Sign-On (SSO), which both secures and simplifies access. Although the figures are relatively modest and fairly evenly spread between the different suggestions, they reflect a genuine awareness.

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

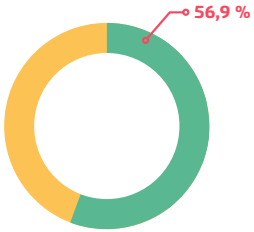
| | Business | IT | Security | Total |
|---|---|---|---|---|
| Improved operational efficiency | 23% | 24% | 29% | 25% |
| Reduced operating costs | 21% | 24% | 18% | 19% |
| Optimized risk management | 19% | 17% | 27% | 21% |
| Compliance (internal and/or regulatory) | 18% | 18% | 15% | 17% |
| Enhanced brand value/perception | 18% | 17% | 15% | 17% |

# FOCUS ON ORGANIZATIONAL MEASURES

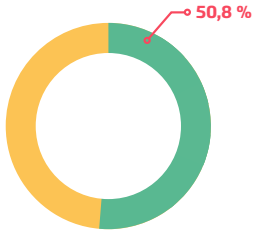
This potential is now recognised, but it still needs to materialise. To ensure that security delivers the expected value, Business decision-makers favour the principles of Security by Design/Security by Default (56.9%) and the implementation of a formal enterprise-wide security programme (50.8%). For them, the most substantial improvements are therefore not due to a question of tools, but to organisational and managerial measures. It seems obvious to them that safety will be better taken into account and more value-creating if everyone has, early on, clear guidelines to follow.

**Where can the organization gain the most value from improving security operations management within the context of digital business? (Business)**

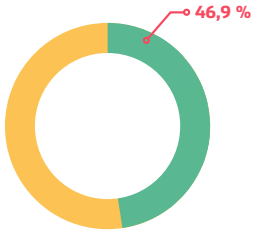
Incorporating security by design and security by default as an enterprise principle




Implementing a formal security program




Optimizing and integrating security to seamlessly support business operations




CIOs and CISOs agree with Business decision-makers on the need to set up a formal security programme - limited, for them, to development. But they do not forget about the challenges specific to their job: while the CIOs remain particularly attentive to the integration of security rules and systems into business operations, CISOs remind us of the need to have adequate resources: skills, tools, suppliers... It is not enough for them to have their role recognised: they want the means to follow.

**How important are the following for managing security operations within the context of your digital business?**

| | | |
|---|---|---|
| Security | 1. Implementing a formal secure development program | 63,1 % |
| | 2. Facilitating enterprise-wide security integration | 59,7 % |
| | 3. Optimizing and integrating security to seamlessly support business operations | 59,3 % |
| IT | 1. Recruiting and retaining a security team | 64,4 % |
| | 2. Implementing a formal secure development program | 63,4 % |
| | 3. Rationalizing the security products and suppliers used | 62,9 % |

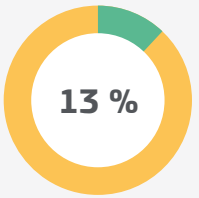
# SECURITY BY DESIGN, A SCATTERED ADOPTION

Among the possible measures, Security by Design[1] appears in the Business profiles as the top solution to the digital transformation security challenges. Solid conviction or just a fad? It is difficult to say because, in reality, very few of those surveyed have any real experience of it. Only 13% of companies have adopted Security by Design as a business principle. On the other hand, almost half have adopted it partially or specifically. The discrepancy between the stated desire and this scattered adoption betrays a certain lack of maturity on the subject with, possibly, a mismatch between the idealised vision of the managers and the pragmatism of the teams on the ground, who apply "Security by Design" without giving it a name.

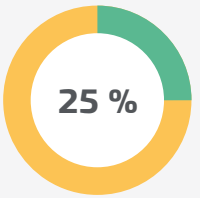
[1] Taking into account the notion of risk from the design stage.

Does your organization incorporate any security by design principles in its planning and processes across the organization? (total respondents)

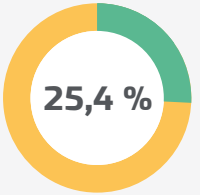
Yes, we have adopted security by design as an enterprise-wide principle



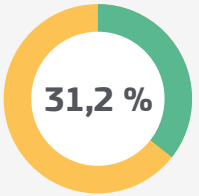

We use security by design in appropriate areas



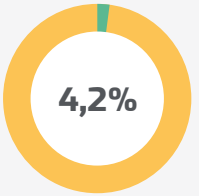

No formal adoption of security by design, but we follow some ad hoc practices



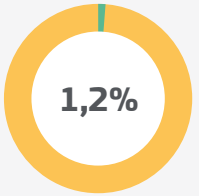

No formal adoption of security by design, but plan to start in the next 12 months




No formal adoption of security by design, and no plans to start




I don't have a clear idea of the security by design concepts

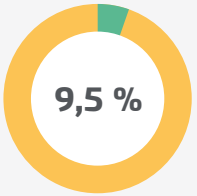


# SECDEVOPS IN SMALL STEPS

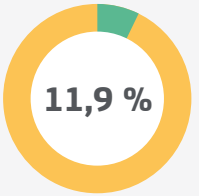
Similarly, while CIOs and CISOs point out the importance of a formal security programme for development, a SecDevOps approach is only implemented in less than one company in 10 ( and under construction in just a few more). However, DevOps alone is already present in almost 80% of companies, and the experience of this transformation should serve as a springboard for wider adoption of SecDevOps.

Which of the following best describes the situation at your organization regarding the adoption of DevOps or SecDevOps program(s)? ? (respondents: IT and Security)

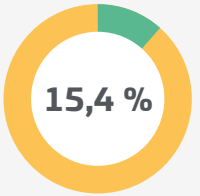
We have fully implemented a running SecDevOps program



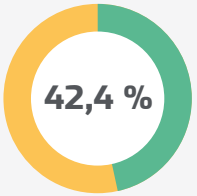

We are actively working on merging security and DevOps, but it is not yet enterprise-wide



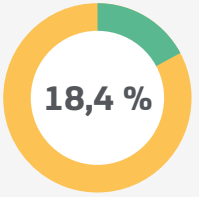

We have adopted DevOps, but only run training/awareness programs for security among our DevOps stakeholders



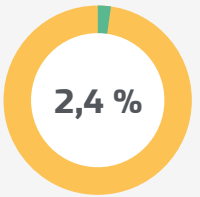

We have adopted DevOps, but security is not formally incorporated within the program




We don't have any DevOps or SecDevOps program yet, but plan to start in the next 12 months




We don't have any DevOps or SecDevOps program



# “SHIFT-LEFT”, A CONCEPT TAKING SOME TIME TO MATERIALIZE

Security by Design and SecDevOps are the two approaches that best embody the concept of «shift-left», i.e. shifting the focus of security considerations upstream of projects. Involving security at the earliest possible stage and making all the players aware of their responsibilities makes it possible, on one hand, to make technical and functional choices that minimise risks (e.g. dispensing, to the extent possible, with certain personal data) and, on the other hand, to remedy without delay vulnerabilities that would be more complex (and more costly) to process later. Based on a formalised security programme implemented by the IT Department, this «shift-left» principle is one of the keys to operational excellence in cybersecurity.

However, despite the enthusiasm shown, the «shift-left» has been slow to materialise. According to Business decision-makers, who are the most optimistic on the matter, less than 4 out of 10 companies are concerned about security right from the planning phase of new projects. Only 23% of CIOs consider that it is (correctly) addressed at this stage.

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 prerelease | 31 % | 34 % | 35 % |
| Only post-release/closure | 24 % | 35 % | 32 % |
| Not explicitly invited for participation | 8 % | 8 % | 6 % |

This difference between the respondent groups on the early consideration of security betrays three distinct positions within the company.

Business profiles are **optimistic** and convinced of the merits and effectiveness of «shift-left», but they appear to neglect what remains to be done downstream to control countless and changing risks.

**Realistic** and **pragmatic**, CISOs consider that it is not necessarily relevant to talk about risks too early and that they are dealt with more effectively when the specifications are advanced enough to identify and qualify them.

Finally, CIOs could be accused of **pessimism**, stating that the constant evolution of the information system, technologies, uses and threats will, in any case, require them to deal with security problems after the launch.

Despite their differences, these three points of view hold some of the truth about cybersecurity. The challenge of operational excellence is to reconcile them in a formalised and coordinated approach.

# THE EXPERTS' POINT OF VIEW

***« The global security plan must be an operational tool. »***

The global security plan sets out a number of requirements, standards, roles and processes applicable throughout the company. It is a referential that must remain dynamic, in order to integrate the rapid evolution of risks, technologies and uses, but it must also be an operational tool. To spread best practices and incarnate the security vision approved and supported by the Executive management, it must be intelligible, accessible and anchored in the business lines. This requires a maturity that is not found in all sectors, banking and insurance being the most advanced ones.

Another obstacle is the compartmentalisation of organisations, inherited from mergers and acquisitions or generated by the development of parallel activities such as e-commerce and physical sales. Filling cultural gaps in security is rarely a priority in the merging process and the persistence of different perceptions is a barrier to a globalized approach.

Finally, a last difficulty, identified by the study, concerns budgets. A formal plan provides a clear, multi-year strategy, which makes it possible to set priorities as well as to spread out investments.

Today, it is estimated that companies still only devote 3% to 5% of their turnover to cybersecurity, whereas the ANSSI (French National Cybersecurity Agency) recommends 5% to 20% depending on the sector. This discrepancy is mainly due to the fact that the information system is often considered as a support means and not as a business enabler, which introduces a bias in the risk assessment and therefore in the allocation of resources. It is crucial for the CISO to be able to demonstrate the justification for their expenditure. They must argue that today it is impossible to conduct business without trust between partners, whether B2B or B2C, and that they are in a position to provide many guarantees to strengthen this trust, including in new areas such as compliance with security laws (GDPR, Network and Security Information Directive, etc.), standards (PCI-DSS, ISO 27001, etc.) and sectoral regulations (e.g. the monetary and financial code).

**Vincent Gervais**
**Cybersecurity Expert**

***« SecDevOps has undeniably proved its worth, but beware of false starts! »***

For a majority of the CIOs questioned, security is only addressed once the new projects are in production. Such pessimism is a little surprising - and regrettable - when SecDevOps approach makes it possible to include it very effectively beforehand and at a lower cost. Admittedly, this method is recent, which explains why it is much less widespread than DevOps, but it has undoubtedly proven its worth.

To begin with, carrying out a PoC on small projects with motivated teams' support is the best. In the organisation, we often meet a team/squad that is aware of the security issues and feels the need to be better geared to deal with them. These employees can be the pioneers of this approach, which requires a certain amount of investment at the beginning, but quickly pays off after a few weeks. The challenge is then to go at scale, because this requires getting everyone on board and coordinating everyone, at all levels of the organisation, even though the maturities are very heterogeneous. Apart from the support of external professionals, having previously set up a global safety programme is an undeniable asset.

More than a methodology, it is a culture that needs to be adopted, and the programme facilitates this by setting out a framework of responsibilities at company level. The risk, on the other hand, is to reduce the SecDevOps to its tooling. If the developer is not supported to face his first code reviews, generally full of vulnerabilities, this will only reinforce his reticence: the feeling that one is interfering in his work, that one devalues it, and that security is just another chore that will prevent him from achieving his objectives. Despite changing attitudes, cybersecurity remains a slippery slope. For any project, nothing is more difficult to catch up with than this kind of false start. SecDevOps is no exception.

**Laurent Lajugie**
**SecDevOps Offer Leader**

# 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

**Vincent Gervais**
**Cybersecurity Expert**
vincent.gervais@devoteam.com

**Laurent Lajugie**
**SecDevOps Offer Leader**
laurent.lajugie@devoteam.com


Creative tech for Better Change