Capgemini invent

# INFORMATION SECURITY BENCHMARK 2019

A balanced view on the Information Security landscape

# CONTENTS

# MANAGEMENT SUMMARY

To a large extent, the Digital Transformation is being challenged by how organizations are seizing and transforming new opportunities without compromising critical assets. Therefore, companies and governments are eager to find answers to omnipresent Cybersecurity questions. Companies around the globe have invested significant amounts of money into programs to improve their Cybersecurity, face new requirements and trends, protect sensitive data from organized cybercrime, and increase employees' Cybersecurity know-how.

In Q3 2018, Capgemini Invent conducted an Information Security Benchmark Study among companies and organizations with various backgrounds. The 105 respondents from diverse industry sectors provided their view on emerging trends and delivered information on topics such as their security budget, organization structures as well as the top security trends.

With Agile Security as the focus topic, this year's study emphasizes a trend we as Capgemini Invent observe in the market.

For participants, Capgemini Invent analyzed the respondents' answers and presents the study results from two different points of view:

- Overall results across all participants to provide a thorough and balanced view of the current state of Information Security including current risks and trends, organization structures, and budgets
- An individual assessment for each participant in which answers are discussed and compared against the participant's industry peer group average

## Key takeaways and insights

- Information Security risks - participants consider social engineering (78%), malware/ ransomware (60%) and advanced persistent threats (44%) as the prevalent risks for Information Security
- Allocation of Information Security budget - participants spend the largest share of their budget (41%) on protection (e.g. access controls, data security, firewalls or backups). Surprisingly, only 15% are spent on response and recovery mechanism (e.g. BCM, crises simulation, or incident management)
- Information Security budget (% of IT budget) - on average, participants across all peer groups dedicate 7.2% of their IT budget to Information Security
- Top security trends - the top 3 security trends participating organizations are dealing with are building a cyber risk culture (52%), enhancing cloud security (41%), and managing known vulnerabilities (41%)
- Information Security function meeting organizational needs - participants predominantly state that the Information Security function meets organizational requirements "In most cases"
- High demand for agile Information Security - fast reaction to security requirements (71%) and the establishment of security as a daily operation (63%) are important reasons why Information Security needs to become agile
- Integration of Information Security into agile projects - participants state that a successful integration requires the formation of interdisciplinary teams (63%) and an implementation of security and privacy by design (63%)
- Requirements to operate Information Security in a more agile way - participants state that sufficient skills and talent (49%), as well as Cybersecurity empowerment (46%) are needed to make their Information Security function more agile

# INTRODUCTION

New digital trends and extensive regulatory requirements, such as to increase the connectivity of ecosystems and to ensure EU General Data Protection Regulation (GDPR) compliance, can lead to severe business disruptions as well as financial damage. Moreover, organized cybercrime and sophisticated attacks, paired with a lack of Cybersecurity know-how put the whole success of the Digital Transformation at risk.

For the reasons stated above, and thus as a starting point to ensure a secure Digital Transformation, Capgemini Invent's Information Security Benchmark evaluates all relevant security aspects of the participants' organizations and provides valuable insights into Information Security in general.

Furthermore, the detailed security benchmark indicates the participant's maturity level compared to the corresponding peer group average. It serves as an orientation as well as self-reflection for decision-makers and highlights necessary improvement fields of the organizations.

The understanding of how other peers implement Information Security and integrate security into their daily business can serve as guidance. Such benchmarking across an organization's peer group is not only helpful in recognizing hot trends and best practices, it also enables the quick identification of individual strengths and improvement potentials.

## Study design and structure

Structured into five major parts, this report represents the following sections:

- A short introduction of this year's study participants
- The assessment of top security risks and the composition of the participants' Information Security budget to mitigate identified risks
- An overview of top security trends and a peer group-specific comparison of the Information Security function
- A closer look at this year's focus topic Agile Security to highlight its relevance, outline integration approaches and requirements in detail
- The core element of the benchmark, the Information Security maturity assessment of participating organizations

# PARTICIPANTS' INFORMATION

This year's Information Security Benchmark is based on the statements of 105 participants and hence is not limited to drawing a general picture of the state of Information Security. On the contrary, the participants cover a wide range of industries, sizes of the organizations and roles enabling the study to gain from meaningful and focused insights.

Participants' industry sectors – the Information Security Benchmark compares five industry peer groups. Most of this year's participants belong to the peer groups Financial Services (34%) and Manufacturing (28%). However, the participants also operate within the sectors Consumer Products & Retail (11%) and Energy & Utilities (11%). This variety of organizations from different industries and origins allows for a balanced view of the security landscape (Figure 1).

Organizations' size – regarding the size of the participants' organization, this year's sample is evenly distributed. Altogether, 30% of the participants represent large-sized companies with more than 15,000 employees. Medium-sized companies with a headcount of more than 1,000 to a total of 15,000 have a share of 45%, while small-sized companies represent 26% of the participants (Figure 2).

**Figure 1: Most of this year's participants belong to the peer groups Financial Services and Manufacturing**

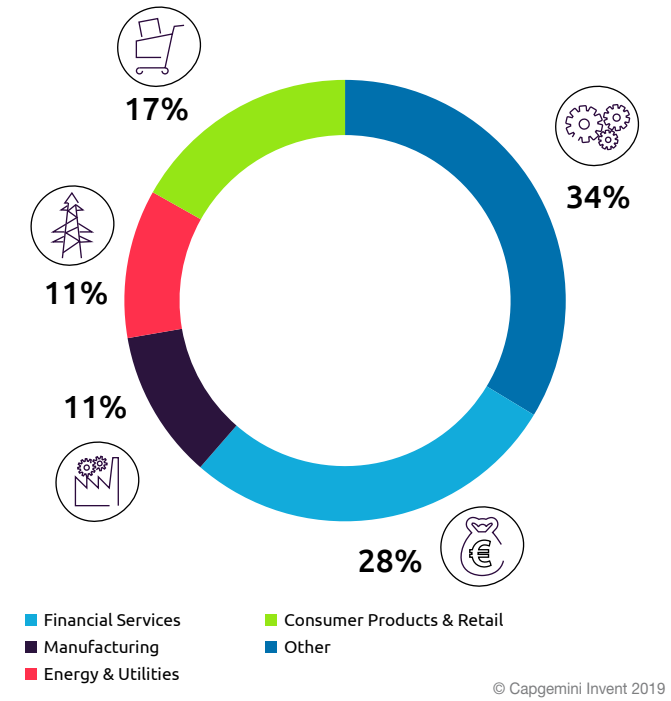
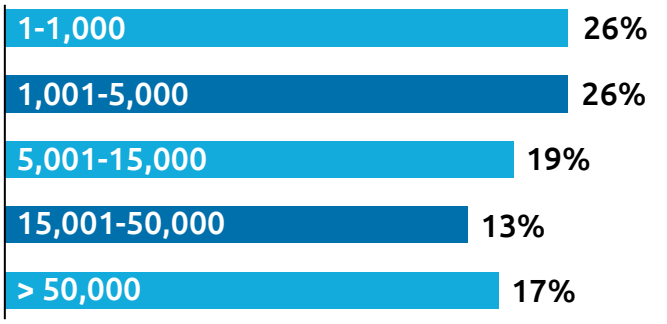




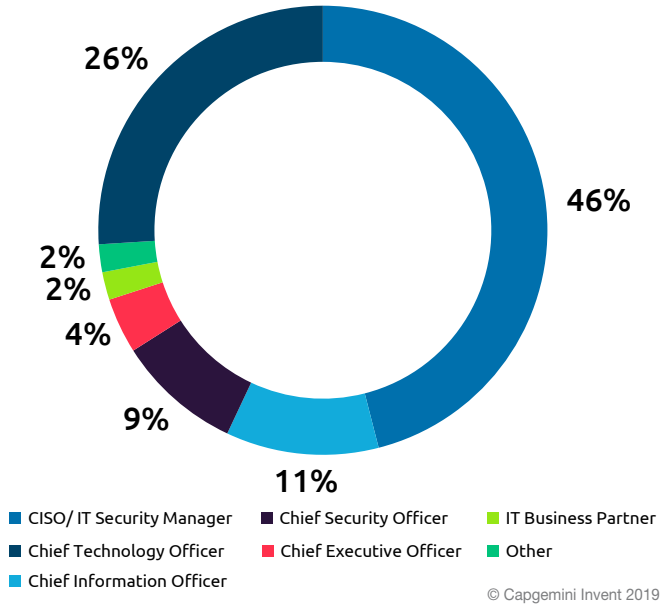

**Figure 2: The size of the participating companies is evenly distributed**






Role of the participants – concerning their role, most of the participants (46%) act as Chief Information Security Officers (CISOs) and IT Security Managers. The remaining contributors occupy positions such as Chief Information Officers (CIOs) or act in a role within the IT division. Given the different perspectives of the roles, the Information Security Benchmarking allows divergent insights (Figure 3).

**Figure 3: Most of the participants act as CISOs in their company**



# INFORMATION SECURITY RISKS

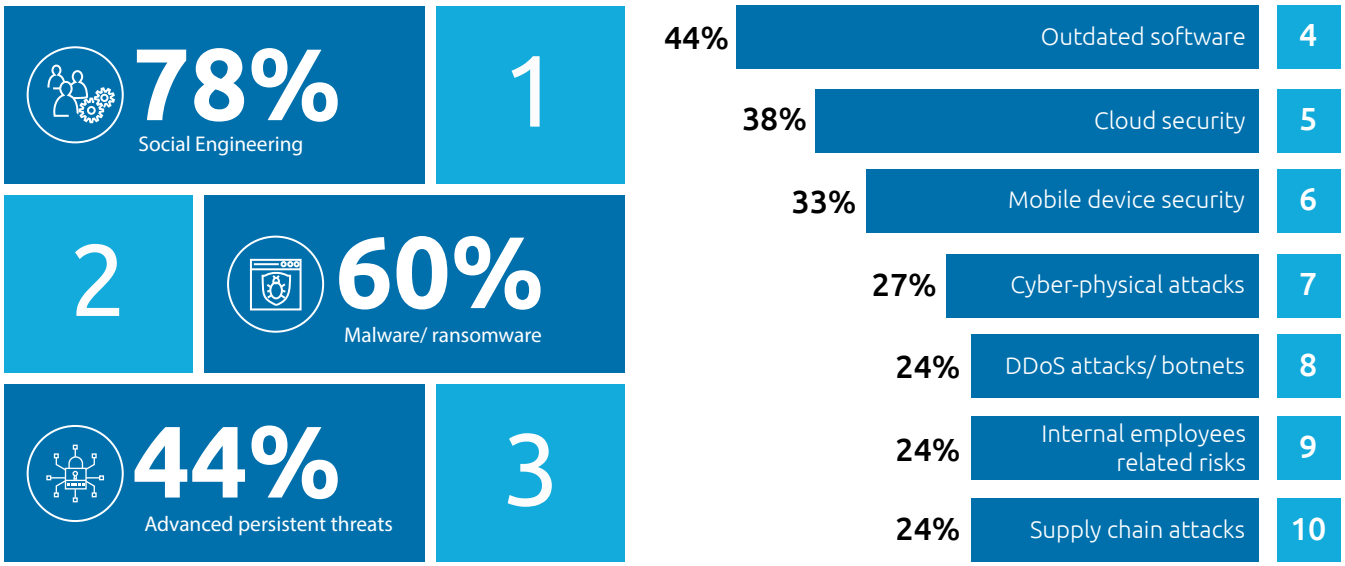
## Information Security risks

CxOs across all industries want to keep abreast of developments regarding Information Security risks to seize new opportunities as well as to protect their critical assets. This year's Information Security Benchmarking asked the participants which Information Security risks they currently consider as most critical. These Information Security risks are displayed in Figure 4.

Across all peer groups, social engineering is the most important Information Security risk to tackle with a share of 78%. Not significantly less recognized are malware/ ransomware (60%) as well as advanced persistent threats (44%). In addition, noticeable current risks are outdated software (44%), cloud security (38%), and mobile device security (33%).

However, there are substantial differences regarding the ranking of the Information Security risks throughout the industries. While participants' organizations from Financial Services rank malware/ ransomware as their top security issue, the sector Manufacturing sector views outdated software as the most serious threat.

**Figure 4: 78% across all peer groups in the study chose social engineering as the most important Information Security risk to tackle**



# INFORMATION SECURITY BUDGETS

## Information Security budgets

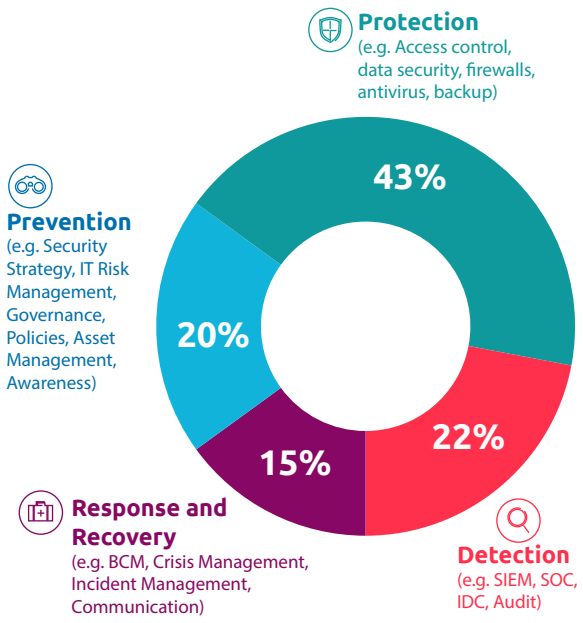
It is essential that companies and governments allocate a significant share of their overall IT budget to Information Security to have the financial resources for improving their defences and counteracting security breaches. Thereby, it is crucial not to underestimate the magnitude of vital investments in Information Security and recognize it as a crucial part of the business. The budget composition of participating companies is displayed in Figure 5.

In this year's study we asked the participants which percentage of the total annual IT budget accounts for the Information Security budget. Across all peer groups, organizations on average dedicate 7.2% of their IT budget to Information Security which represents an increase of one percentage point compared to last year's study. Frontrunners are organizations from the Financial Services with a share of 10.2%, followed by Manufacturing (5.5%), Energy & Utilities (5.4%) and Consumer Products & Retail (4.0%). Considering current hazards and Cybersecurity trends, from our point of view both organizations and governments continue to devote too little attention to the issue.

Furthermore, we asked our participants to allocate their Information Security budget in four categories: prevention (e.g. security strategy, IT risk management), protection (e.g. access control, data security), detection (e.g. SIEM, SOC), and response & recovery (e.g. BCM, crisis management). On average, contributors spend 20% on prevention (25% in 2017), 43% on protection (43% in 2017), 22% on detection (20% in 2017) and 15% on response & recovery (14% in 2017).

Finally, we analyzed the participants' distribution between internal (e.g. own security staff) and external (e.g. service providers) Information Security resources. In all sectors, most participants spend the same proportion of their budget on internal and external resources. This budget distribution also indicates that the market for security talent is currently highly competitive.

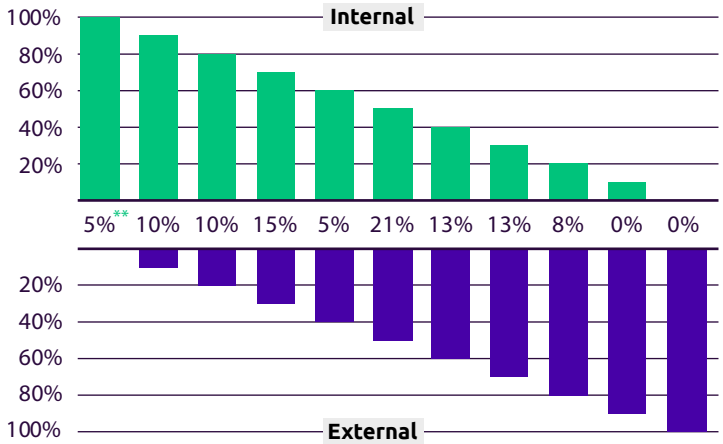
**Figure 5: The participating organizations spend almost two thirds of their Information Security budget on prevention and protection**




*Values might be subject to negligible rounding errors

On average, participants across all peer groups in the study dedicate **7.2%** of their IT budget to Information Security

The graph explains the distribution between **internal** (e.g. own security staff) and **external** (e.g. service providers) Information Security budget




**Answers from participants, e.g. 5% indicates that the Information Security budget is fully distributed to internal FTEs

# INFORMATION SECURITY TRENDS

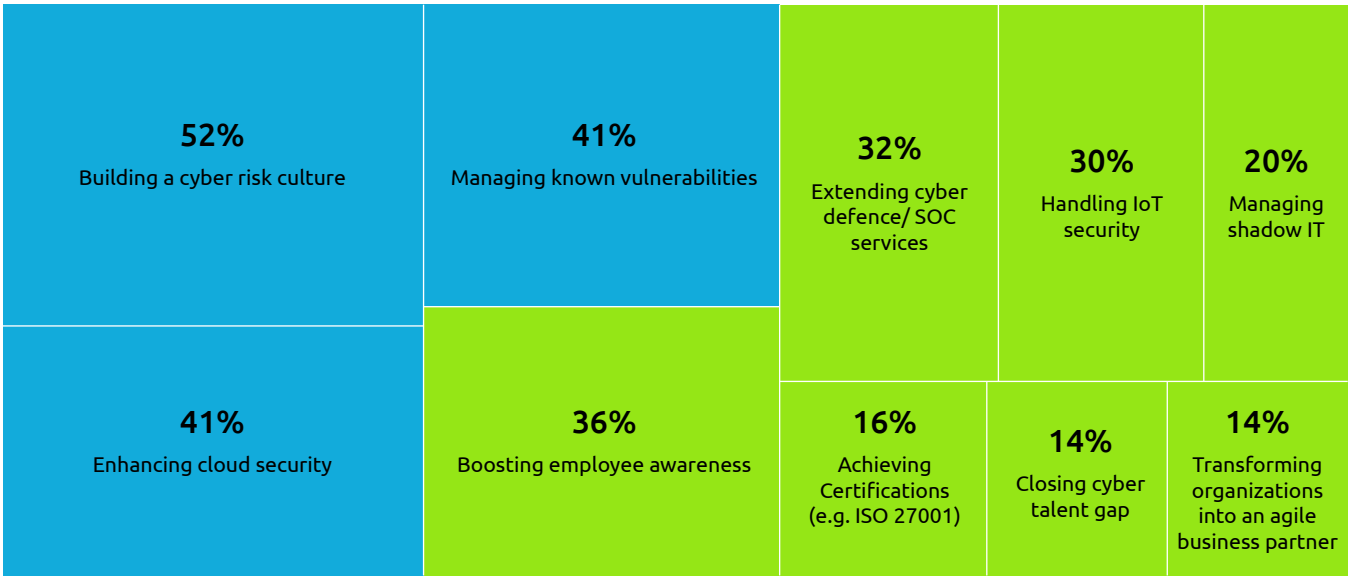
## Top Information Security trends

Furthermore, to not just identify the current risks but to display future trends regarding Information Security, Capgemini Invent asked the participants to identify what will be the top 3 security trends for their organization next year. Given that the number of Cybersecurity threats is increasing across all industries around the globe, it is vital for today's organizations to secure their critical assets against these hazards. The most recognized security trends are displayed in Figure 6.

Across all industries, the participants' top trend (52%) is to establish a cyber risk culture. Given the fact human errors are currently the leading cause for cyber breaches, the participants are consequently intrigued in establishing a cyber-sensitive culture amongst their employees. Enhancing cloud security (41%) and to manage known vulnerabilities (41%) are also central security trends across all industries. Nonetheless, there are several other noticeable trends, namely to boost employee awareness (36%), to extend cyber defence/ SOC services (32%) as well as to handle IoT security (30%).

Differences between the industry sectors could also be identified. On the one hand, the sectors Consumer Products & Retail as well as Energy & Utilities both identify enhancing cloud security (80%) as their top trend, and on the other hand, Manufacturing focuses on handling IoT security (45%). Financial Services, on the contrary, favours to establish a cyber risk culture by a large majority (80%).

**Figure 6: The top 3 trends of this year's study are to establish a cyber risk culture, enhancing cloud security, and the management of known vulnerabilities**



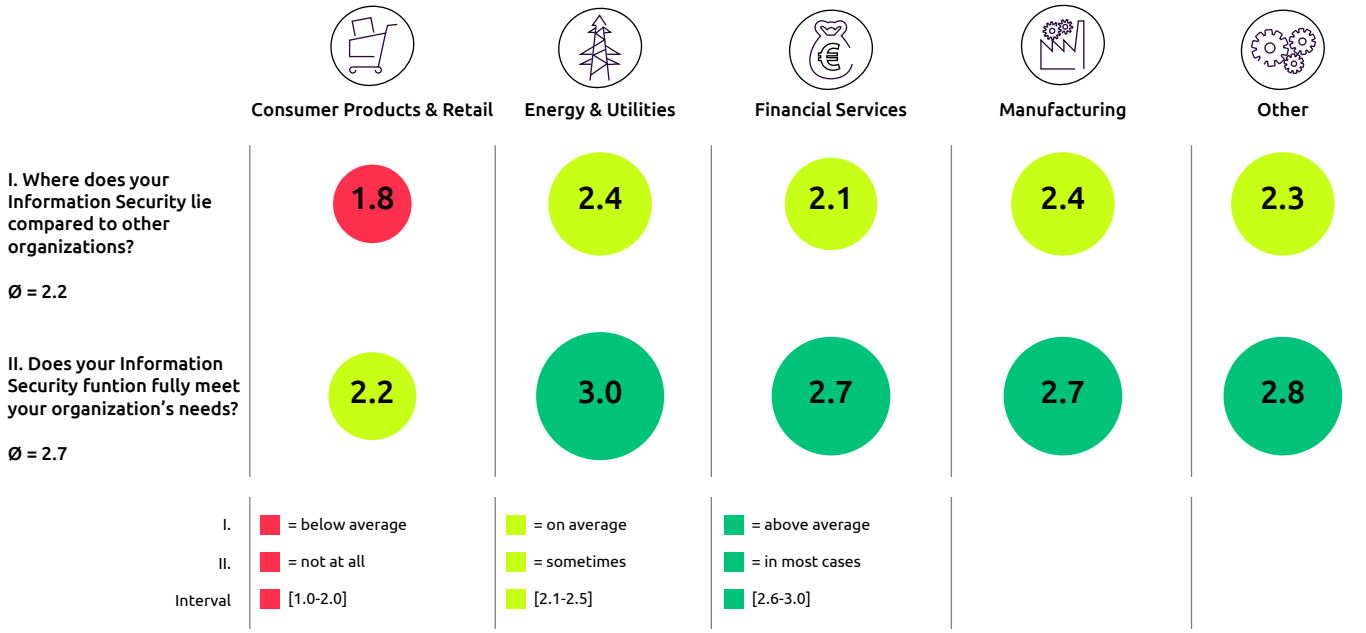
## Comparison of Information Security function

In this year's Information Security Benchmarking, the participants were also asked to conduct a self-assessment of their Information Security function. The results are displayed in Figure 7.

First, the study looks at how the participants compare their Information Security with other organizations. All in all, participants across all industries perceive their level of Information Security to be on average compared to their peers. Only organizations from the sector Consumer Products & Retail assess their Information Security to be below the average compared to their peers. From this it could be concluded that the sector Consumer Products & Retail has so far invested too little and therefore has a great need for action in order to keep pace with other sectors.

Next, the participants were asked whether their Information Security function fully meets organizational needs. Participants from the sectors Energy & Utilities, Financial Services and Manufacturing are mostly satisfied with their Information Security function (above 2.5), whereas the Consumer Products & Retail sector states that their Information Security function only meets their needs "Sometimes" (2.2).

**Figure 7: This year's participants largely rated their own Information Security as average compared to other companies**



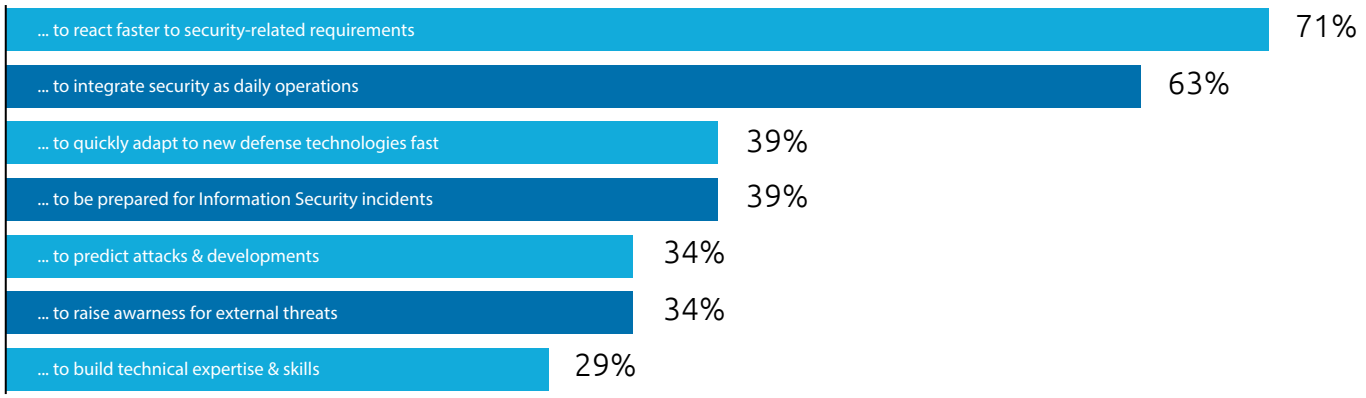
# FOCUS TOPIC: AGILE SECURITY

Today, organizations in all kinds of industries are subject to fast evolving changes in a multi-facetted world. This acceleration of businesses goes hand in hand with the need of quicker reaction time as well as the ability to implement initiatives within shorter timeframes. To be able to still consider Information Security it is essential to keep the Information Security up-to-date to increase adaptivity. Therefore, it is essential to respond to this trend with a consequent transformation into agile ways of working and integrating Cybersecurity into products by design.

## Reasons for Agile Security

First, the participants were asked for their general opinion on the relevance of an agile Information Security. Overall, a fast reaction to security-related requirements (71%) and to integrate Information Security as a daily operation (63%) are considered as the most important reasons (Figure 8). In addition, important reasons are the fast adaption of new defence technologies (39%), the preparation for Information Security incidents (39%), as well as to predict attacks and developments (34%).

**Figure 8: Fast reaction to security requirements and the integration of security as a daily operation are important reasons why security needs to become agile**



## Integration of Information Security into agile projects

However, to find quick responses to newly developing cyber-threats and hazards, it is essential to integrate Information Security and infuse all agile projects with Information Security requirements from the start. Therefore, the participants were asked for their opinion regarding what the most essential requirements are to ensure that Information Security is well-integrated into agile projects (Figure 9).

Across all sectors, a successful integration of Information Security into agile projects calls for the formation of interdisciplinary project teams (63%) as well as an integration of security and privacy by design (63%). Furthermore, fostering awareness for Cybersecurity and data privacy (54%), the inclusion of Information Security requirements in all projects (51%), and the establishment of a pragmatic cyber risk management (41%) are a priority for the participants.

**Figure 9: An integration of Information Security in agile projects requires the formation of interdisciplinary teams and the establishment of security and privacy by design**

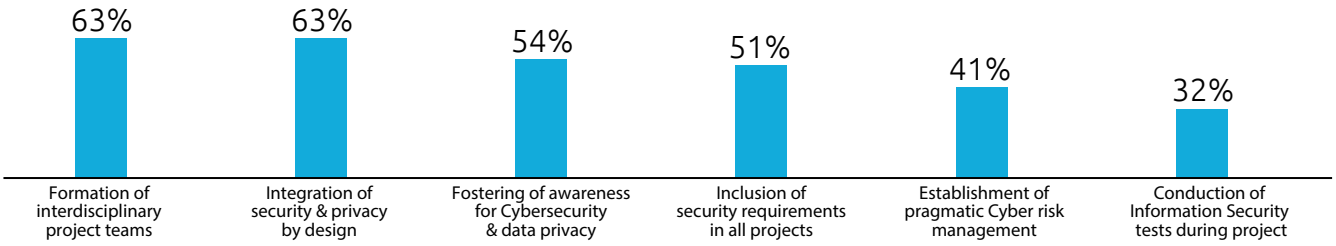
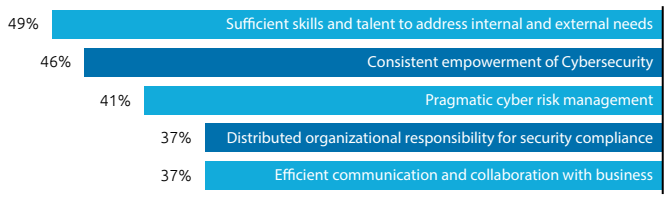





**Figure 10: Organizations require skilled employees and consistent empowerment of Cybersecurity to make their Information Security organization more agile**






## Requirements to operate Information Security in a more agile way

At the end of this year's focus topic, the participants were asked what is necessary to achieve a sufficient level of agile security. In most cases companies suffer from a lack of professional competence and are therefore constantly looking for skilled employees to meet internal and external needs (49%) and a consistent empowerment of Cybersecurity (46%) to make their whole Information Security organization more agile (Figure 10).

# INFORMATION SECURITY MATURITY ASSESSMENT

## Overall security maturity assessment

The overall security maturity assessment summarizes the maturity level of all peer groups based on four assessment domains (Figure 11). These domains are:

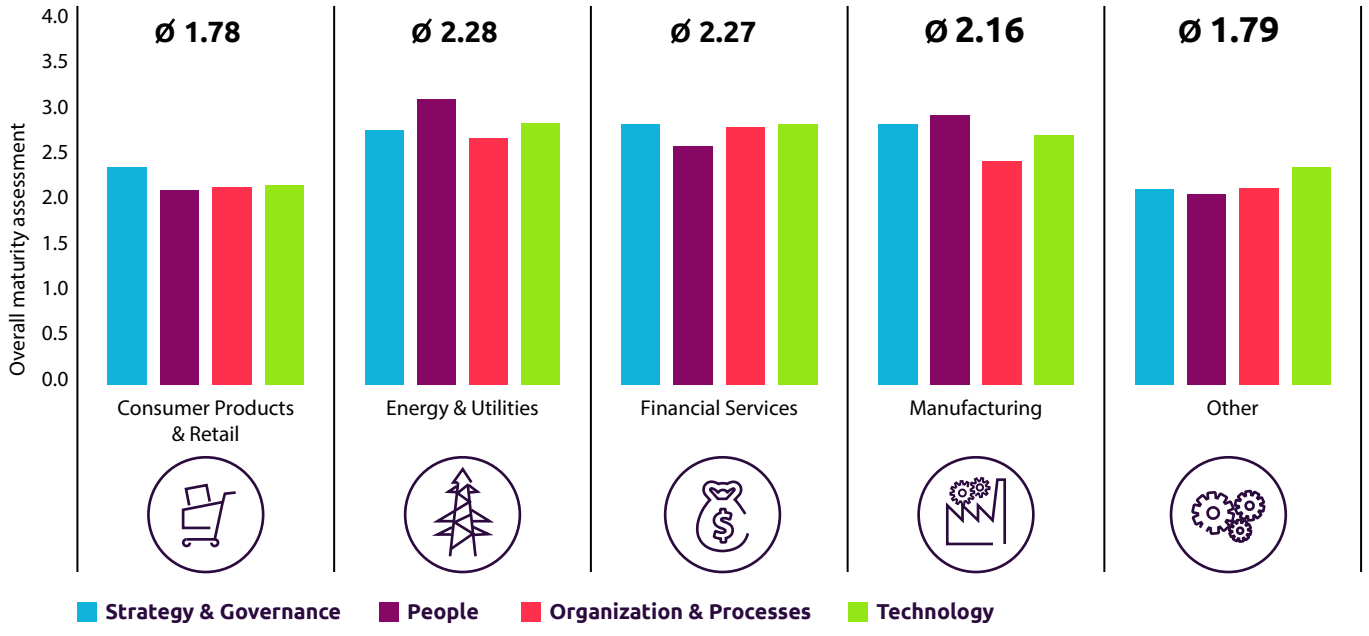
1. Strategy and Governance
2. People
3. Organization & Processes
4. Technology

The overall security maturity level as measured by the Information Security Benchmark accounts to a score of 2.06. Therefore, the security maturity level of this year's participants can be interpreted as "defined" which means that processes, roles and responsibilities of Information Security are defined, documented and communicated, but important characteristics such as regular reviews and audits and continuous improvement and optimization are still missing. Also, the score is slightly higher than it was in the last Information Security Benchmark (1.97 in 2017).

Comparing the peer groups among themselves, participants within the Energy & Utilities sector (2.28) as well as the Financial Services (2.27) show the highest maturity level. While organizations from the Financial Services kept their maturity level (2.27 in 2017), participants from Energy & Utilities are now the new frontrunners in the overall assessment (2.21 in 2017). Organizations with a manufacturing background score a solid 2.16 and show a slight increase compared to our last benchmark (2.11 in 2017). However, participants from the sector Consumer Products & Retail (1.80) do not only score far behind the average, their score also decreased not insignificantly (1.90 in 2017).

Furthermore, while organizations from Manufacturing and Energy & Utilities show differences of maturity across domains, participants from Financial Services and Consumer Products & Retail show a more even maturity across all domains. This fact can be interpreted as an indicator for a coherent Information Security approach throughout the entire organization.

**Figure 11: In general, all sectors show a high average maturity; with "Organization & Processes", being the domain with the highest improvement potential**



## Maturity level vs. budget

Our benchmark clusters the peer groups into four classes (Figure 12) by setting the security maturity level and the percentage of participants' IT budget spent on Information Security into relation:

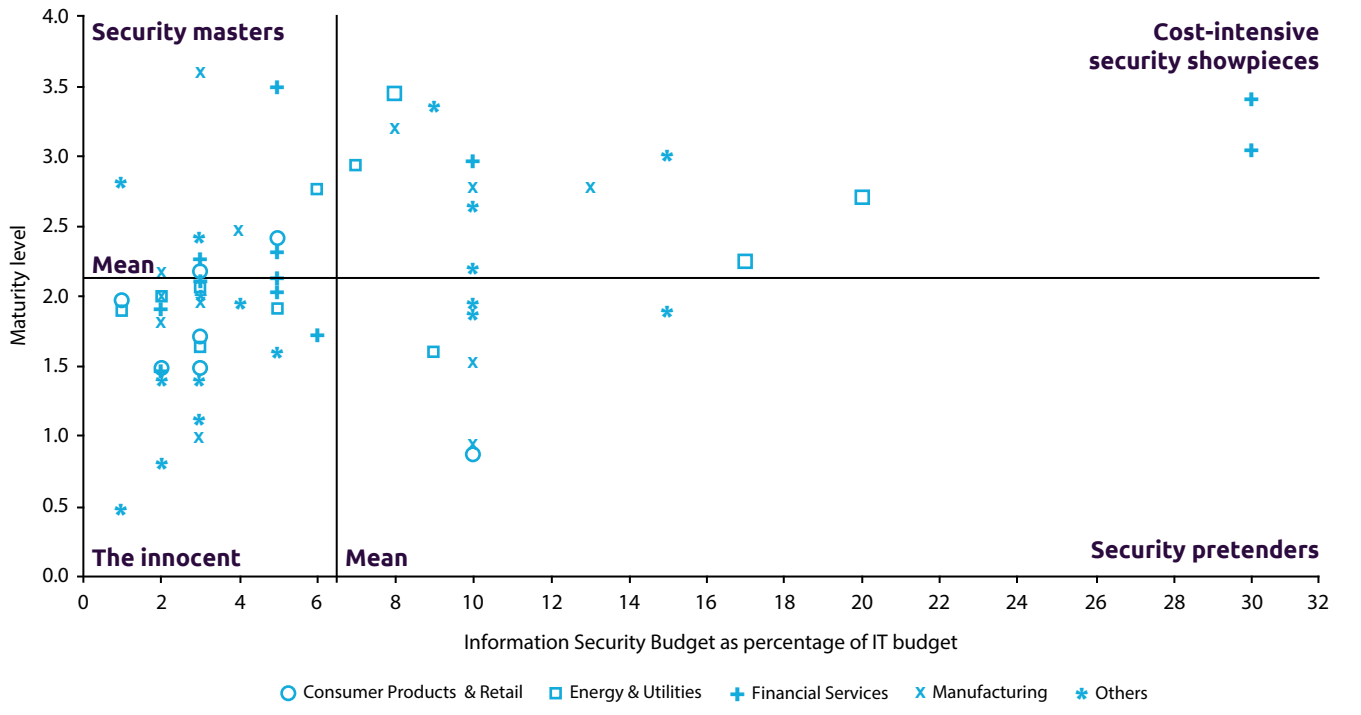
1. Security masters
2. The innocent
3. Cost-intensive security showpieces
4. Security pretenders

Respondents are classified as "security masters", when they spend a relatively low percentage of their IT budget on Information Security (below 6.5%), but achieve a relatively high maturity level, greater than 2.06. Compared to last year, these two thresholds have increased: the budget for Information Security from 6.15% to 6.5% and the maturity level from 1.97 to 2.06. It can also be observed that the share of "security masters" has decreased from 13% to 11%.

"The innocent" participants have a relatively low Information Security budget and at the same time achieve a maturity level below average. As depicted on the right-hand side of Figure 12, "security pretenders" are participants with higher budgets spent on Information Security than the two previous classes but achieve a maturity level below average. Last but not least, a couple of the respondents achieved an above-average maturity level with cost-intensive investments.

To sum up, a correlation between the Information Security budget as a percentage of the IT budget and the maturity level could not be detected. Consequently, spending a high budget on Information Security does not directly translate into a higher Information Security maturity – even with a small budget, high maturity levels can indeed be achieved.

**Figure 12: A correlation between budget and the maturity level could not be detected - even with a small budget, high maturity levels can be achieved**



# CONCLUSION

In the digital age the risk potential of cyber-attacks is enormously high, and the rapid adoption of new digital technologies continuously introduces new risks to organizations' sensitive assets and their business activities. As a result, today's organizations are more than ever determined to find answers to omnipresent Information Security threats. Besides a peer group comparison, a look at the current state of Information Security in other sectors can help to identify best practices.

Capgemini Invent's Information Security Benchmark Study 2019 provides detailed insights into organizations' IT security landscape and measures. The questionnaire used identifies the current hazards & future trends and reviews the participants' budgeting regarding Information Security. Moreover, the objective and repeatable Information Security maturity assessment compares the Information Security maturity across several peer groups to identify strengths and weaknesses.

In hindsight, the necessity for Agile Security as well as the integration of Information Security into agile projects is one of the key findings of this year's Information Security Benchmark. Furthermore, the lack of employee awareness within organizations needs to be addressed to ensure a holistic security approach. However, it is surprising that despite new extensive regulations like the GDPR the overall security maturity level has changed only insignificantly since the last benchmark in 2017. Nevertheless, the findings help companies to set purposeful priorities for future investments and to prepare for the growing challenges of the ongoing Digital Transformation.

# CAPGEMINI INVENT CYBERSECURITY PORTFOLIO

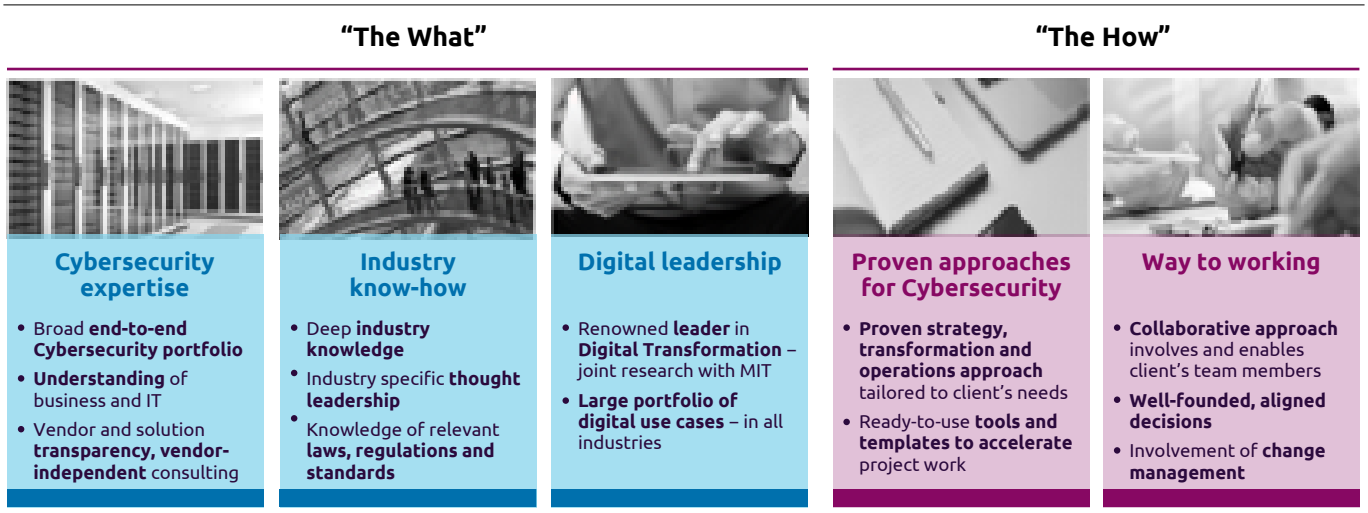
## What we do and how we do it

Capgemini Invent offers a wide-ranging portfolio of Cybersecurity consulting services. Our strategic Cybersecurity consulting takes a C-Level and business perspective to enable a secure Digital Transformation. Our service portfolio combines profound Cybersecurity and industry expertise with best practice methods.

**Figure 13: Capgemini Invent's broad portfolio of consulting services**




**Figure 14: Capgemini Invent combines profound Cybersecurity and industry expertise with best practice methods**



## Our Cybersecurity experts

Your organization benefits from our Cybersecurity experts' extensive experience from consulting projects in various industries.


**Dr. Guido Kamann**
Head of Future of Technology DACH
Leutschenbachstrasse 95
CH-8050 Zürich
guido.kamann@capgemini.com
Mob.: +41 44 5602 400



**Dr. Paul Lokuciejewski**
Principal | Cybersecurity Consulting
Mainzer Landstraße 178 – 190
D-60327 Frankfurt am Main
paul.lokuciejewski@capgemini.com
Mob.: +49 151 4025 0855



**Frank Hebestreit**
Principal | Cybersecurity Consulting
Potsdamer Platz 5
D-10785 Berlin
frank.hebestreit@capgemini.com
Mob.: +49 151 4025 1341



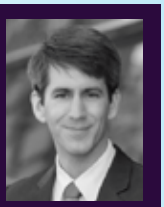
**André Hohner**
Principal | Cybersecurity Consulting
Mainzer Landstraße 178 – 190
D-60327 Frankfurt am Main
andre.hohner@capgemini.com
Mob.: +49 151 1137 4431



**Werner Held**
Principal | Cybersecurity Consulting
Leutschenbachstrasse 95
CH-8050 Zürich
werner.held@capgemini.com
Mob.: +41 7966 95559



**Sebastian Heierhoff**
Manager | Cybersecurity Consulting
Gustav-Heinemann-Ufer 72a
D-50968 Köln
sebastian.heierhoff@capgemini.com
Mob.: +49 151 4025 0133

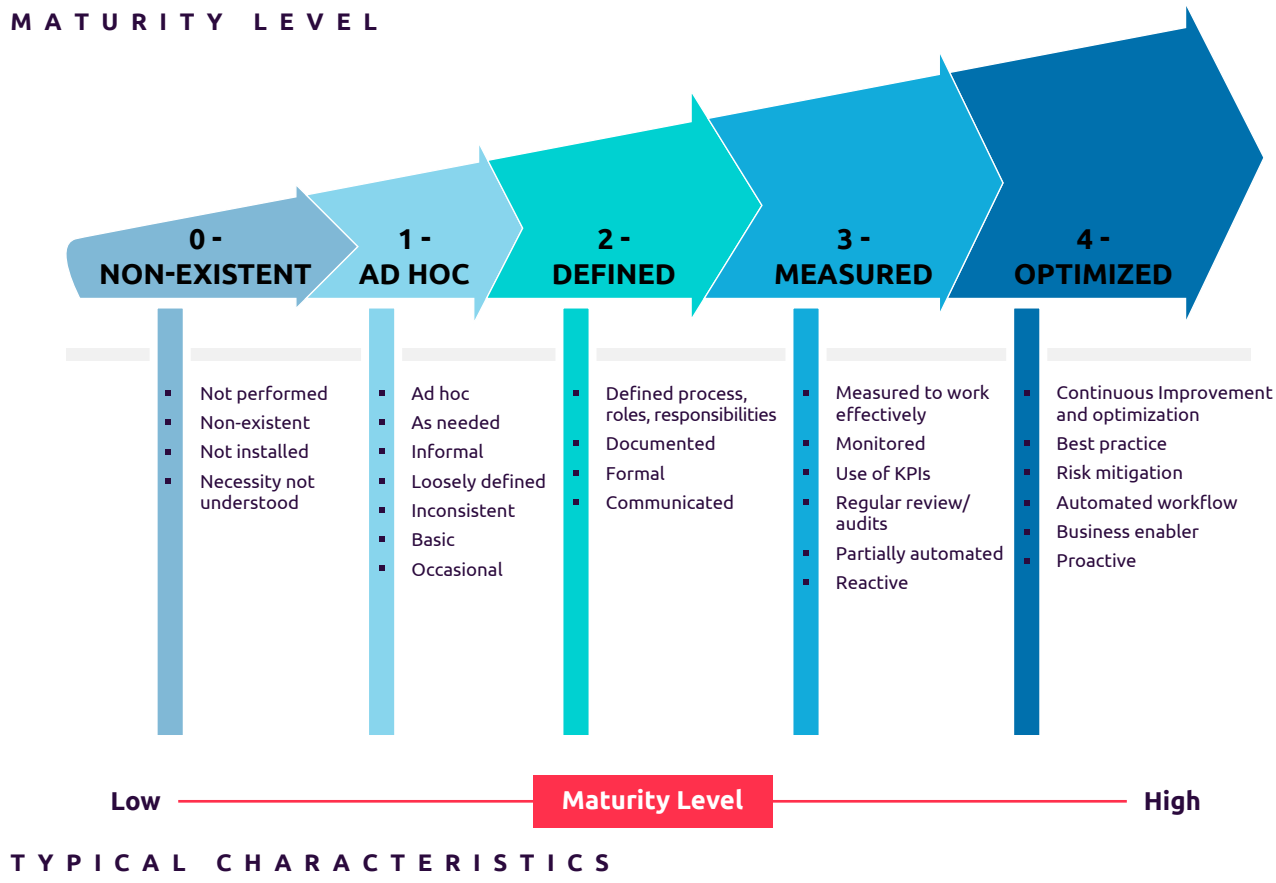
# APPENDIX

## Design principles

Capgemini Invent's maturity level assessment thoroughly evaluates participants' level of Information Security. To achieve reliable results, our study aims at an objective and repeatable security maturity assessment of all participants. We ensure objectivity by assessing each Information Security component based on a clearly defined 5-level maturity model. This approach (Figure 15) can be considered as proven, as it has been used successfully several times in both our study as well as projects and distinguishes the following levels of Information Security Maturity:

- Maturity level 0: Information Security is non-existent, and the necessity is not understood.
- Maturity level 1: Basic Information Security actions and methods are used ad hoc when required.
- Maturity level 2: Processes, roles, and responsibilities of Information Security are defined, documented and communicated.
- Maturity level 3: Information Security is measured to work effectively. Processes are monitored, reviewed and partially automated.
- Maturity level 4: Information Security is improved and optimized continuously.

**Figure 15: The Maturity Level Assessment thoroughly evaluates participants current level of Information Security**



# About
## Capgemini Invent

As the digital innovation, consulting and transformation brand of the Capgemini Group, Capgemini Invent helps CxOs envision and build what's next for their organizations. Located in more than 30 offices and 22 creative studios around the world, its 6,000+ strong team combines strategy, technology, data science and creative design with deep industry expertise and insights, to develop new digital solutions and business models of the future.

Capgemini Invent is an integral part of Capgemini, a global leader in consulting, technology services and digital transformation. The Group is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Visit us at

www.capgemini.com/invent

**People matter, results count**

Capgemini invent