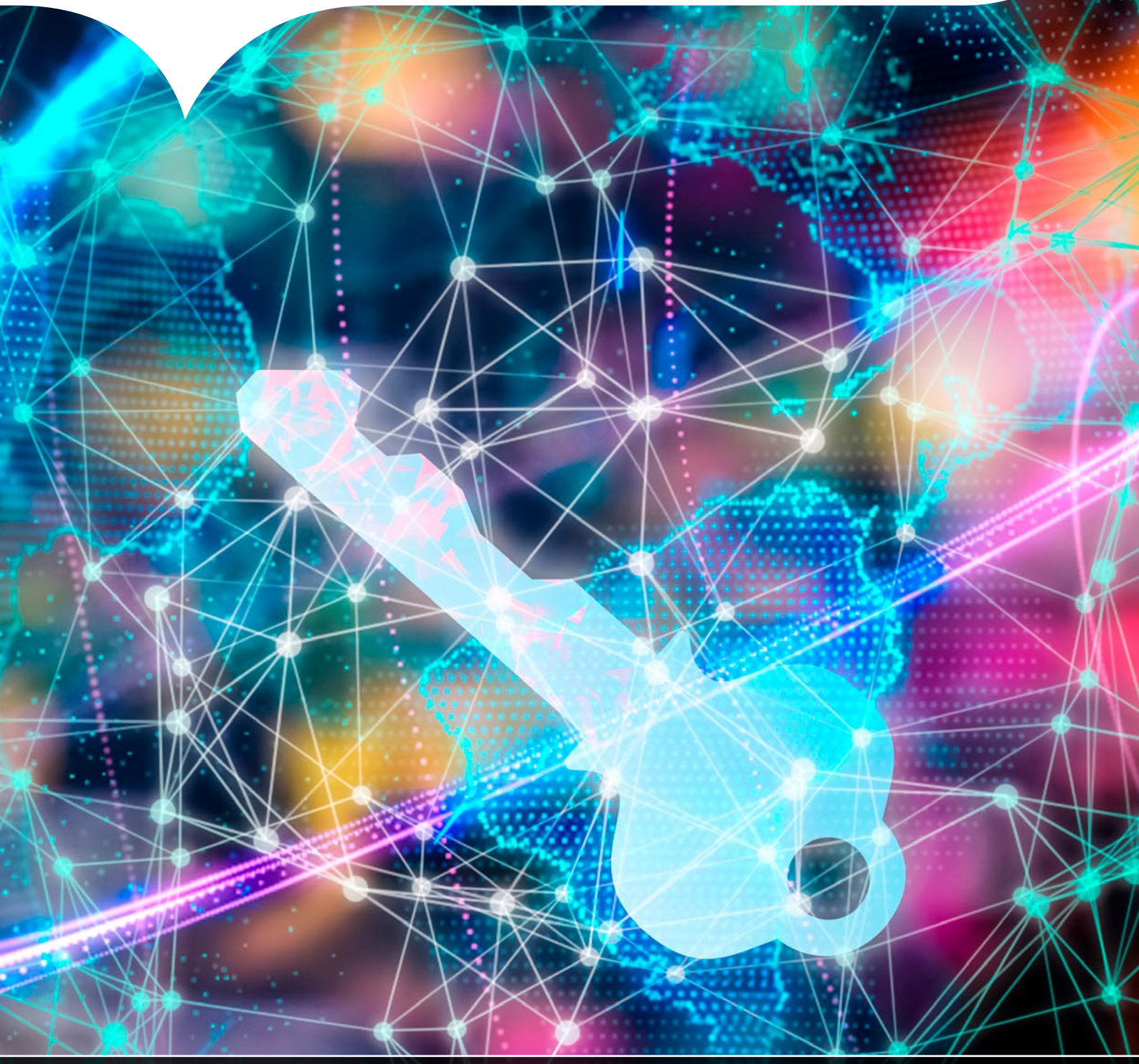
Capgemini Consulting



Information Security Benchmarking 2017

Enabling business ambitions, cost efficiency and resilience with strategies for tackling Cybersecurity challenges

CONTENT


DATABASE
CLIENT
COMPUTER
SYSTEM
THORIZATIO
OBILITY
ERVER
SSIBILITY
ORMATI

I. MANAGEMENT SUMMARY

STUDY DESIGN AND APPROACH

- The rapid adoption of social, mobility, analytics, cloud and the "Internet of Things" (SMACT) technologies introduces new risks to organizations' sensitive assets and their business activities. As a result, companies and governments are eager to find answers to omnipresent Cybersecurity questions.
- The understanding of how other peers implement Information Security to protect their assets and integrate security into daily business is essential. Such insights are not only helpful in discerning hot trends and best practices but also enable the quick identification of individual strengths, improvement potentials and enable the benchmarking across the organizations' peer group.
- In Q2 2017, Capgemini Consulting conducted a global Information Security benchmarking study among companies and organizations around the globe. The 101 respondents from various industry sectors provided their views on emerging trends and delivered information on topics such as their security budget, organization structures or breach costs.
- This year's study puts particular emphasis on three prevailing topics of today's information security landscape: EU General Data Protection Regulations (GDPR), Cloud Security and DevOps.
- The Information Security assessment is based on a detailed maturity model. Using this model, survey contributors evaluated their security practice in the domains "Strategy & Governance", "Organization & People", "Processes" and "Technology".
- Capgemini Consulting 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 challenges, trends, risks, organization structures and budgets.
  - An individual assessment for each participant where individual answers are discussed and compared against their industry peer group.

KEY INSIGHTS

Information Security Risks – 90% of the participants state that the protection of information and data is the most important driver for information security, followed by compliance with security requirements (64%) imposed by authorities.

More Severe Security Breaches – Even though the number of security breaches decreased, the cost per security breach faced by our participants is significantly higher than in last year's study. Costs inccurred due to a single security breach range between 99.000€ and 416.000€.

Information Security Driver – 90% of the participants state that the protection of information and data is the most important driver for information security, also compliance to exogenously imposed regulations is vitally influencing.

Know Your Crown Jewels – 70% of the respondents state customer data as the most critical asset, besides personal information and password credentials are regarded as essential crown jewels.

Increasing Security Budgets – Although companies on average currently only dedicate about 6.2% of their IT Budget to security, 90% indicate an increase of their security expenses in the next fiscal year.

Budget Constraints Impeding Security Contributions – About one third of the participants designate budget constraints as the prime obstacle which challenges information security contribution. 32% state that information security does not meet their organization's needs.

Lack of Employee Awareness – While most companies indicate board attention and knowledge in general as their top strength, employee awareness is regarded as the main improvement field.

Lack of Detection Capabilities – While most participants employ procedures to detect security incidents, roughly 25% do not have realtime detection capabilities in place.

Lack of EU GDPR Compliance, Cloud Security & DevSecOps Adoption – By today, only 6% of the respondents fully comply with EU GDPR regulations. 73% lack of a proper cloud service utilization. Further, 46% of the respondents do not have DevOps in place yet or struggle to implement adaquate security mechanisms.

No Correlation between Budgets and Security Maturity – Multiple participants spend more budget on Information Security than their peers but achieve a security maturity level below average. Strategic investment in the proper domains is key as demonstrated by the Security Masters.

Characteristics of Security Masters – participants with an efficient investment strategy - i.e. low Information Security budget and high overall security level - indicate above average maturity in the areas: security governance, IT risk management, audits, awareness & expert training, threat management and network intrusion detection.

II. PARTICIPANTS' INFORMATION

OBJECTIVES AND STRUCTURE

The strong reliance of today's companies on technology and a sharp increase in the number as well as the severity of Information Security breaches underline the growing importance for an organization to establish effective Information Security capabilities. A comprehensive understanding of these capabilities assets can, therefore help to identify necessary improvement fields. Benchmarking your organization against your direct competitors by the use of Capgemini's annual Information Security Benchmarking is a good starting point to approach.

Structured into six major parts, this report presents the following findings:

- After a short introduction of this year's participants, the first section provides indepth insights into the impact of Information Security, illustrating risks, drivers and critical assets.
- The Information Security Benchmark following focuses in the second section on the structure of the contributors' Information Security organizations, including budgets, personnel and planned improvement initiatives.
- The third section of the report puts emphasis on the strengths and improvement fields of this year's respondents.
- Hereafter, the report examines participants' practices in case of security breaches and identifies the most common measures to counteract cyberattacks.
- In the fifth section three prevailing topics are discussed: EU GDPR, Cloud Security and DevOps.
- The core element of the study is the Information Security maturity assessment of the participating organizations, which concludes this report.

STRUCTURE OF ANALYZED ORGANIZATIONS

Based on the statements of 101 participants, this year's Information Security Benchmark does not only provide general information of the latest state of Information Securitybut also distinguishes four characteristics of the participating organizations, enable the study to derive more focused insights. These characteristics are the contributors' origin, industry sector, size of the organization, as well as the respondent's role in their organization.

Participants' origin – The analyzed organizations cover a broad range of countries and industries. While most participants (69%) represent companies based in the DACH region (Germany, Austria and Switzerland) the remaining respondents (31%) are mainly located in other parts of Europe (Fig. 1).

Figure 1: Participants' origin

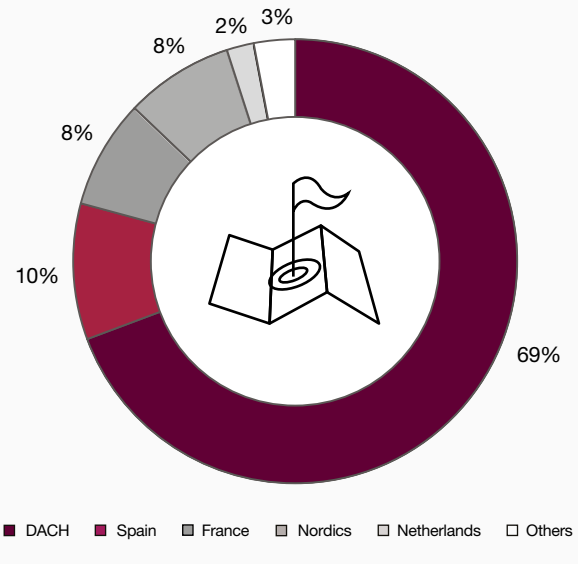
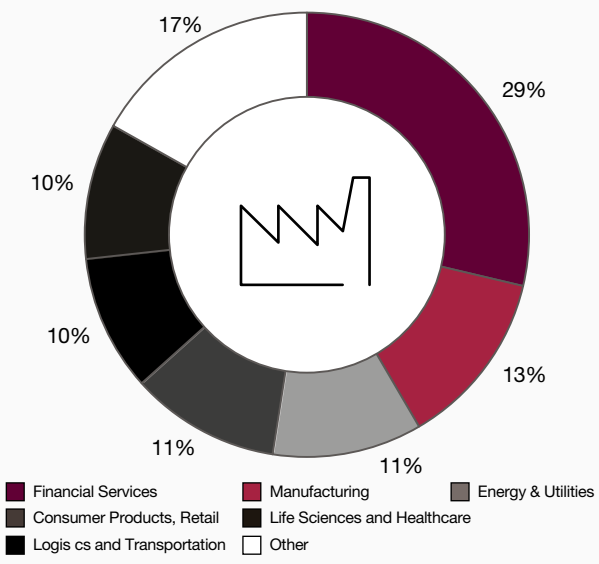


Figure 2: Participants' industry sectors



Participants' industry sectors – Our benchmark compares seven industry peer groups. Particularly, participants operate within the sectors: Financial Services (29%), Manufacturing (13%), Energy & Utilities (11%), Consumer Products & Retail (11%), Life Sciences & Healthcare (10%), Logistics & Transportation (10%) as well as other industries (17%) (Fig. 2).

Organization size – Looking at the size of the organizations, onethird of the participants (34%) represent largesized organizations with more than 15.000 emplyees. Most of the participants (67%) constitute mediumsized organizations comprising up to 15.000 employees (Fig. 3).

Overall, this year's Information Security Benchmarking Study provides a balanced view of various-sized participants and therefore presents a holistic overview of organizations' state of information security, strengths and weaknesses, as well as future desires.

Figure 3: Organization size (number of employees)

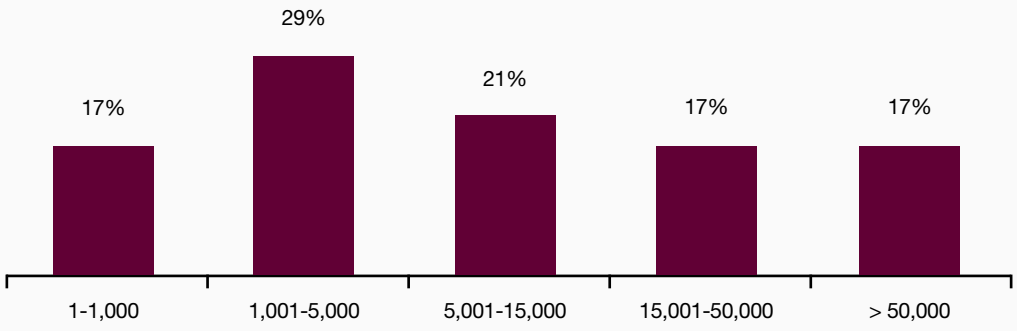
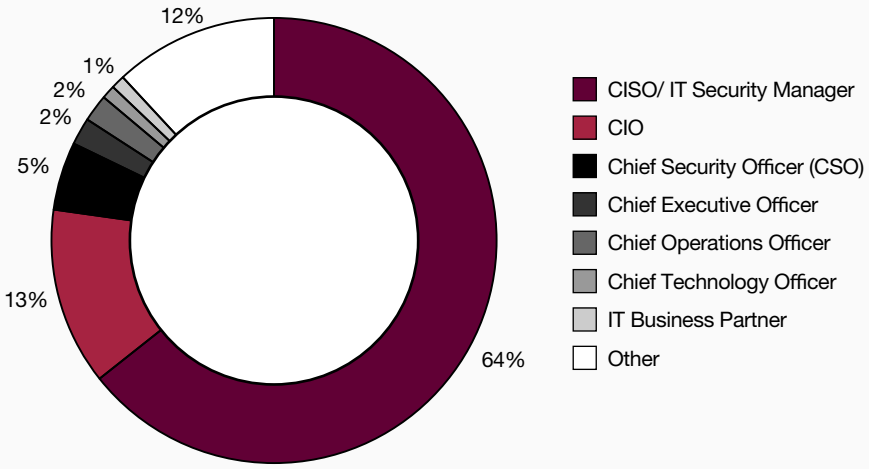


Figure 4: Role of Participants



Role of Participants – Based on the role the respondents hold in their organization, the benchmark also provides several perspectives. The majority of the participants (64%) act as Chief Information Security Officers (CISO) in their company, while the remaining contributors hold positions such as Chief Information Officers (CIO) or act in a related role within the IT division.

III. CROWN JEWELS, RISKS AND DRIVERS

CRITICAL ASSETS AT RISK

The Information Security Benchmark 2017 asked participants for their critical assets at risk – socalled "crown jewels". In order to make appropriate invest its daily business, suitable protection mechanisms should be considered as an integral element of operations. Crown jewels at risk ranked by the respondents across all industry sectors are displayed in Fig. 5.

67% of the contributors across all industries name customer data as their most important crown jewel. Not significantly less crucial are personal information (61%) plus password credentials (59%). Taking data privacy regulations, as well as the growing organizational dependence on digitally embedded systems and procedures these critical assets become even more vital.

In addition, noticeable crown jewels named by participants are strategic business information, intellectual property and financial transactions. In general, the answers given by the respondents indicate that not only personally related data is of growing importance, but also other types of business data are at risk. There are considerable differences between industry setors. For example: participants within "Energy & Utilities" and "Logistics & Transportation" stated "Operations Data" most frequently as a crown jewel at risk.

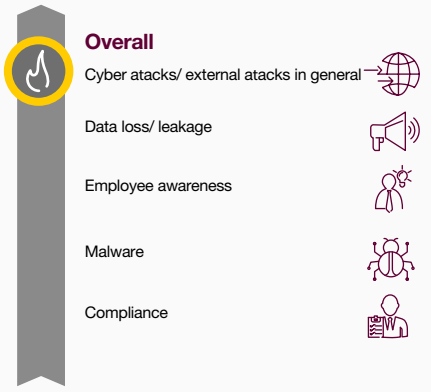
Respondents from the "Manufacturing" sector name intellectual property along with customer data as the most critical assets, while in "Life Sciences & Healthcare" data related to persons is essential.

Figure 5: Critical assets at risk

INFORMATION SECURITY RISKS

The number of Cybersecurity threats across all industries around the world is increasing tremendously. Today's organizations predominantly struggle with the protection of their aforementioned critical assets against these hazards.

Figure 6: Ranked Top Risks



When asked to build a Top 3 ranking of prevalent information security risks, participants reported external cyber attacks as the most severe one, followed by the loss and/ or leakage of crucial data.

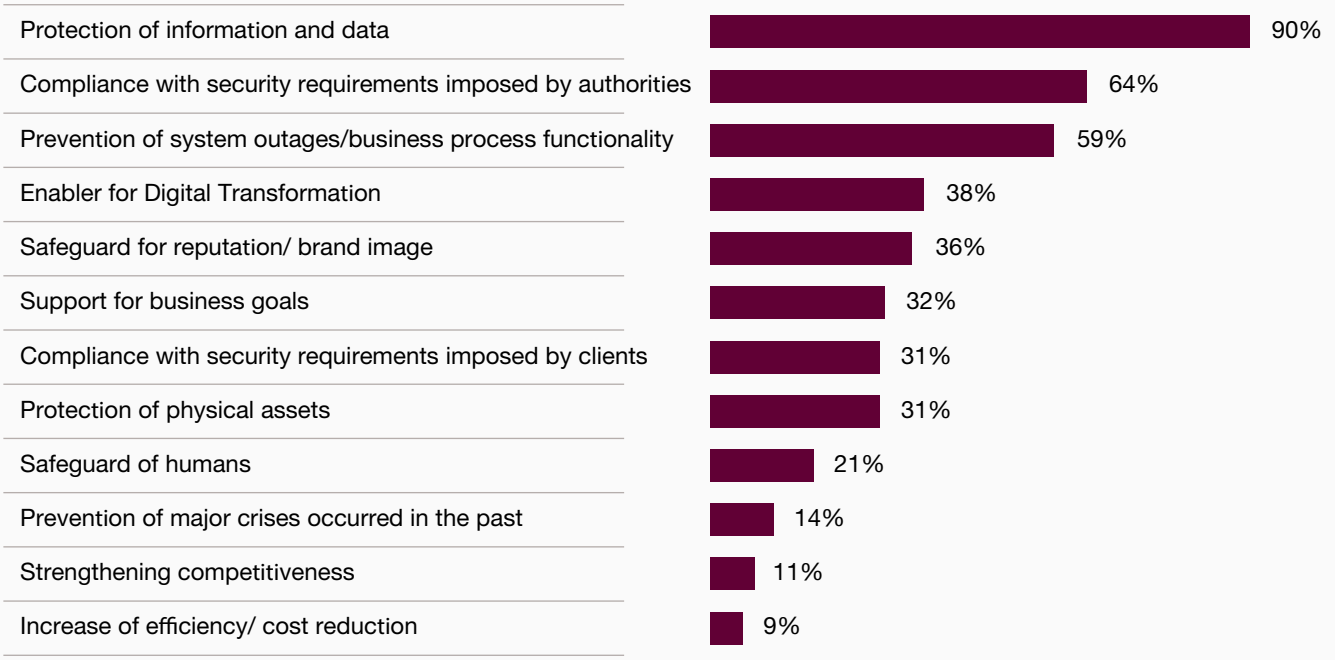
Often, these two risks trigger each other, which again fosters the need for effective protection. Awareness of employees is considered as the third critical hazard. Social engineering is one of the most common reasons for security breaches in today's organizations. These attacks are often realized by wellorganized professionals, turning them even more dangerous.

DRIVERS FOR INFORMATION SECURITY

The most important driver for organizations to increase Information Security investments is to protect the formerly mentioned crown jewels. Therefore, it is not surprising that the most frequently mentioned driver is by far the protection of information and data (90%). In the light of the new EU GDPR regulations, participants consider compliance with security requirements imposed by authorities as the second most crucial driver for Information Security (64%) (Fig. 7).

Surprisingly, only 32% state the support of business goals as a booster. Strengthening the organization's competitiveness is only relevant for 11% of the respondents in the context of information security.

Figure 7: Drivers for Information Security



IV. INFORMATION SECURITY BUDGET AND ORGANIZATION

INFORMATION SECURITY BUDGET

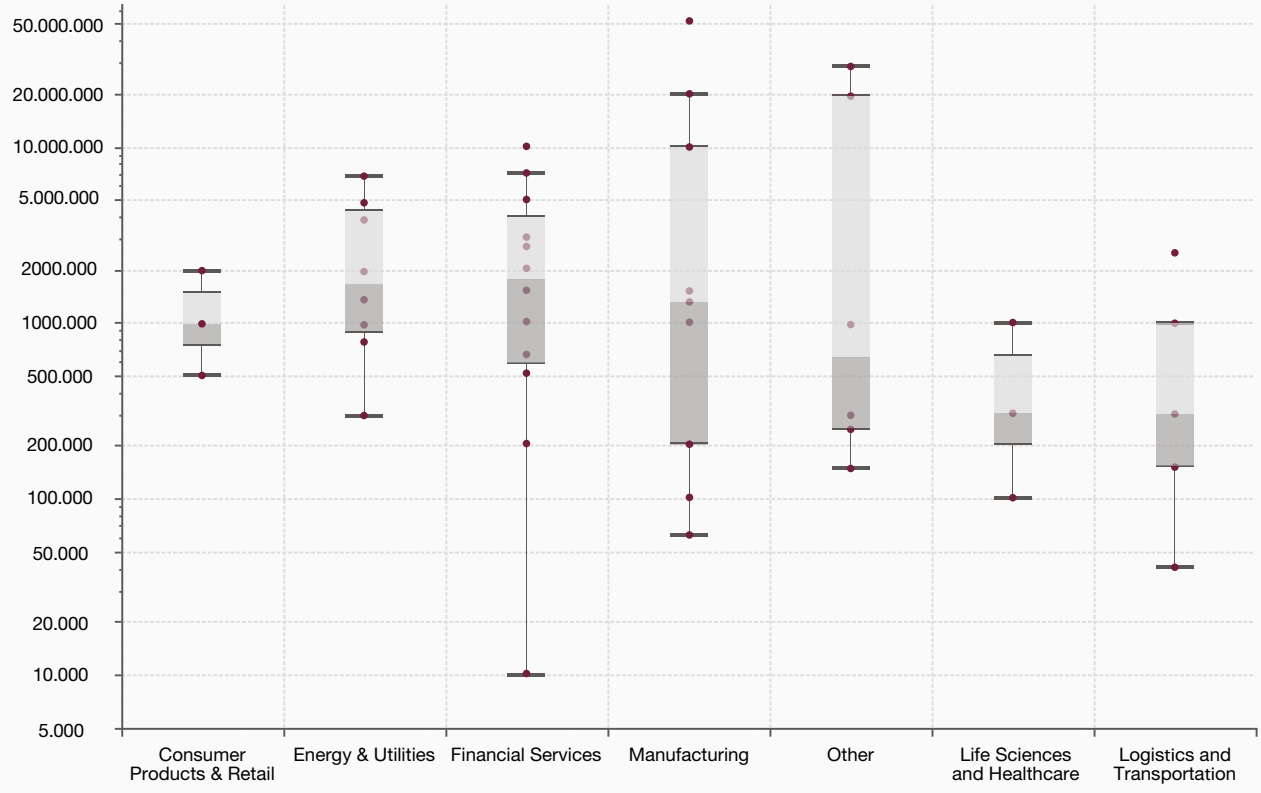
Companies need to allocate their overall IT budget effectively in order to have financial resources for counteracting security breaches. Therefore, it is necessary for companies to not underestimate the magnitude of necessary investments in Information Security and recognize it as an essential part of the business.

In this year's study, participating companies stated various budgets reaching from 10k € up to 50m €. Across all sectors, the respondents report an average security budget of about 4.2m €. Results, however are varying significantly across industries: While the peer group "Manufacturing" states an average amount of 9.2m € as security budget, participants from the peer group "Financial Services" report 2.8m €. Individual values are displayed in Fig. 8.

On average, contributors declare 6.2% of their overall IT budget dedicated to Infor-mation Security. The mean of the participants from the peer group "Life Sciences & Healthcare" allocate about 10.2% of their IT expenses to security, which is the largest amount of all peer groups.

Although the numbers are relatively low at this point in time, 90% of the participants across all peer groups expect to increase their Information Security budget in the next fiscal year. Comparing this figure to last year's perception (45%) it is obvious that security topics' relevance for organizations has grown significantly and is anticipated to grow further prospectively. last year's perception (45%) it is obvious that security topics' relevance for organizations has grown significantly and is anticipated to grow further prospectively.

Figure 8: Information Security Budget (in €)



We asked participants to allocate their Information Security budget in four categories: Prevention, Protection, Detection and Response & Recovery. Compared to last year's study, the amounts dispensed to Detection (14.6% in 2016) and Response & Recovery (11.5% in 2016) receive greater attention due to higher investments. Finding appropriate responses becomes more and more important for organizations due to increased complexity, cross-linked systems and higher degrees of dependency on digital infrastructures. For example, companies are investing in Security Operations Centers (SOC) and Intrusion Detection Systems (IDS) to reveal (potential) security breaches.

INFORMATION SECURITY ORGANIZATION

As against last year's study, medium as well as large-sized companies raised their information security personnel. Especially for large organizations, the increase is significant (14.2 FTEs in 2016 vs. 36 FTEs in 2017). Results for specific peer groups are even more meaningful: Large-sized companies from the peer group "Financial Services" reported that on average 23.3 FTEs are outsourced while for "Logistics & Transportation" this figure accounts only for 2.2 FTEs. Large-sized companies from the peer group "Manufacturing" report the highest number of in-house Operational Technical FTEs across all peer groups (21.0).

Figure 9: Information Security Budget - Investment areas

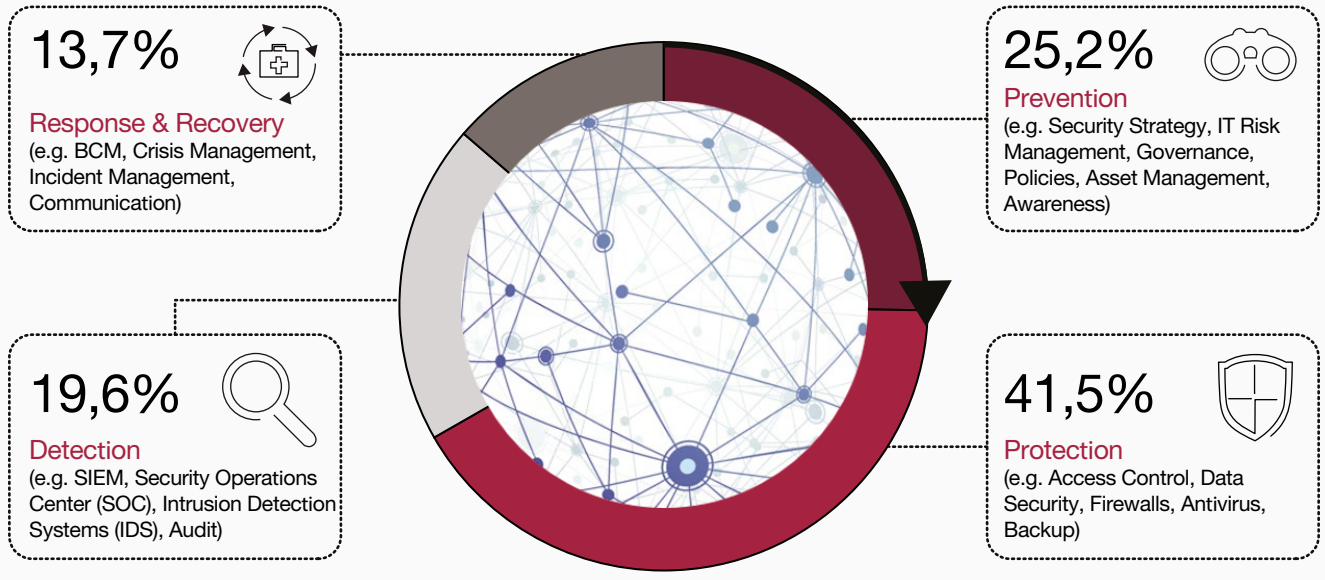
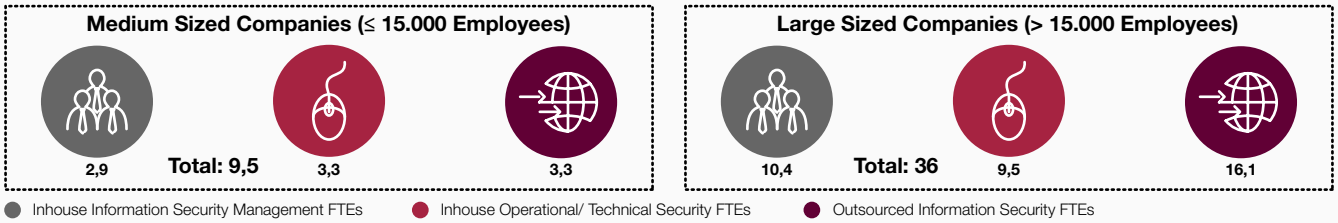


Figure 10: Information Security Organization Size (Full Time Equivalents)



V. STRENGTHS & IMPROVEMENT FIELDS

Finding an efficient approach to Information Security that ideally protects critical assets and infrastructures against cyber threats is the focus of organizations' interests. This approach is manifested in governance, organizational structure, perceived improvement fields as well as in its budgets and targeted investments.

Organizations have to know their strengths and weaknesses in order to make necessary investments to change or maintain the status quo of their operations.

STRENGTHS AND IMPROVEMENT FIELDS

There are different strengths and improvement fields which are influenced by the organizational structure. When participants ranked their top strengths and improvement fields of Information Security, board attention/ awareness of management was named as the top strengths while employee awareness was stated as the top improvement field. These results lead to the assumption that holistic awareness initiatives throughout the entire organization are essential in order to minimize the opportunities for criminals to implant malware in the organizations' infrastructure.

In line with current developments is the importance of Information Security governance. While some companies emphasize it as a major strength, others perceive it as a key improvement field. Especially in the light of EU GDPR, the significance of governance and compliance is expected to grow further prospectively.

Yet, the involvement of Information Security in business decisions is a key improvement field which organizations should not underestimate. It is crucial to emphasize security measures not only in IT specific dimensions of the organizationbut also to implement a coherent security concept throughout the company.

Figure 11: Strengths and Improvement Fields

MEETING ORGANIZATION NEEDS

In every organization, the security function's significance for daily procedures is growing. A well-suited integration of the function in business operations is required in order to ensure a holistic security approach across all peer groups, about one third of the respondents state that their security funtion merely occasionally or in no sense meets their organization's (Fig. 12).

Observing specific peer groups, it stands out that 57% of participants from the peer group "Manufacturing" state "Sometimes". In contrast, respondents from the peer group "Energy & Utilities" are more satisfied with their security function. All of the respondents in this peer group state that their needs are met in leastwise most of the cases. An effective coordination between the security function and other parts of the organization is necessary to mitigate risks thoroughly.

MAIN OBSTACLES

There are various factors impeding the sufficient financial contribution to an organization's security function. Across all peer groups, 34% of participants perceive budget constraints in general as the major obstacle. Referring back to the respondents' expected security budget increase in the next fiscal year, companies aim to tackle this drawback. Of further importance are management and governance issues (20%). Governance requirements imposed by authorities will play a major role in organizations security structures in the near future.

In certain peer groups, the results are more expressive. Thus, 43% of the participants from "Life Sciences & Healthcare" and "Consumer Products & Retail" report budget constraints as their main obstacles.

Surprisingly, the lack of skilled resources is only concerned as a minor barrier to impede contribution, which is contradictory to personnel increases during the last year. Beyond, it is a dissent to low employee awareness, which participants stated as one of the major improvement fields in the future.

Figure 12: Security Function meets organization's needs

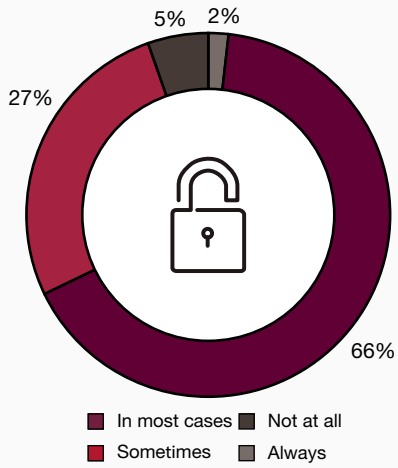
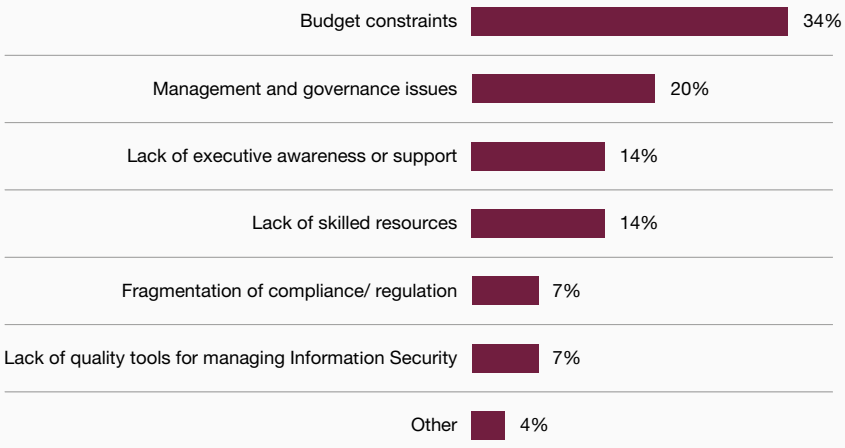


Figure 13: Main Obstacles



VI. INFORMATION SECURITY INCIDENT HANDLING & BREACHES

NUMBER AND COST OF SECURITY BREACHES

Across all peer groups, the participants report an average number of security breaches per year of about 12. Unexpectedly, the number of breaches compared to last year's study. On average, respondents from the peer group "Energy & Utilities" state only 2-3 violations per year while it is even less for the peer group "Life Sciences & Healthcare" (1 to 2).

However, the cost of breaches is significantly greater compared to last year's study. While medium and small-sized companies (<15.000 employees) report average costs of 99.000€ per breach, large-sized companies (>15.000 employees) state an average damage of 416.000€.

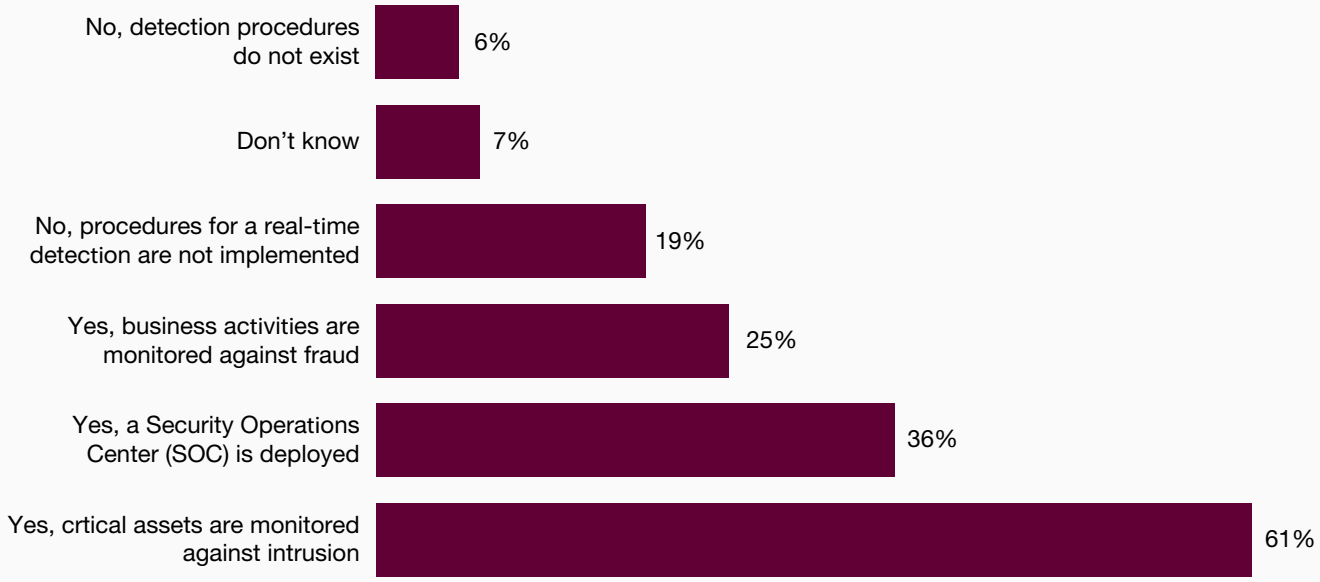
This fact leads to the interpretation that although the number of breaches is not necessarily increasing, their severity is.

Organizations have to prepare their critical assets and infrastructures for major breaches in order to minimize financial impacts.

DETECTION MECHANISMS

In line with the relatively low share of investment made in the detection of malicious behavior stated in the previous paragraph (19%), companies struggle to implement mechanisms to detect/ monitor external

Figure 14: Ability to detect malicious behavior



25%

of overall participants do not employ detection mechanisms

threats. Merely about one third of the participants have a Security Operations Center in place and about 61% monitor their critical assets against intrusion by now. Nonetheless, 25% of the participants indicate that they do not have detection mechanisms implemented at all and, thus carelessly expose their company to extenal threats.

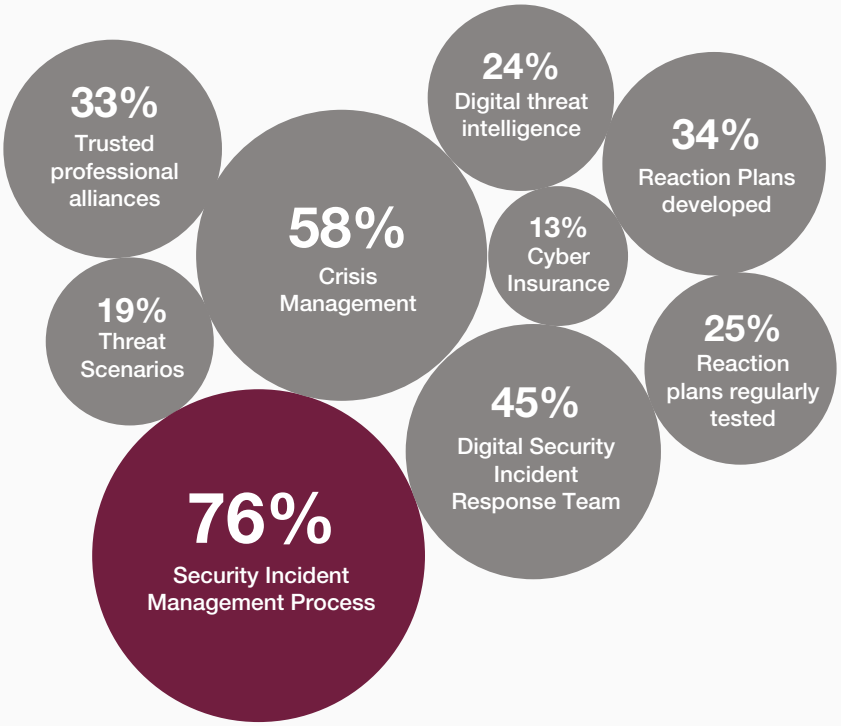
Taking a look at specific industries, it stands out that 38% of the participants from "Financial Services" lack realtime detection mechanisms, which is extremely negligent due to strictly confidential personal data being processed in these organizations. Respondents from the "Energy & Utilities" as well as "Life Sciences & Healthcare" sector show the highest values regarding realtime detection with 75% each. Organizations should follow the overall trend and increase their investments in detection and monitoring mechanisms. Adopting Security Operations Centers is necessary in order to expeditiously identify external threats and respond accordingly mitigating harm to critical business operations.

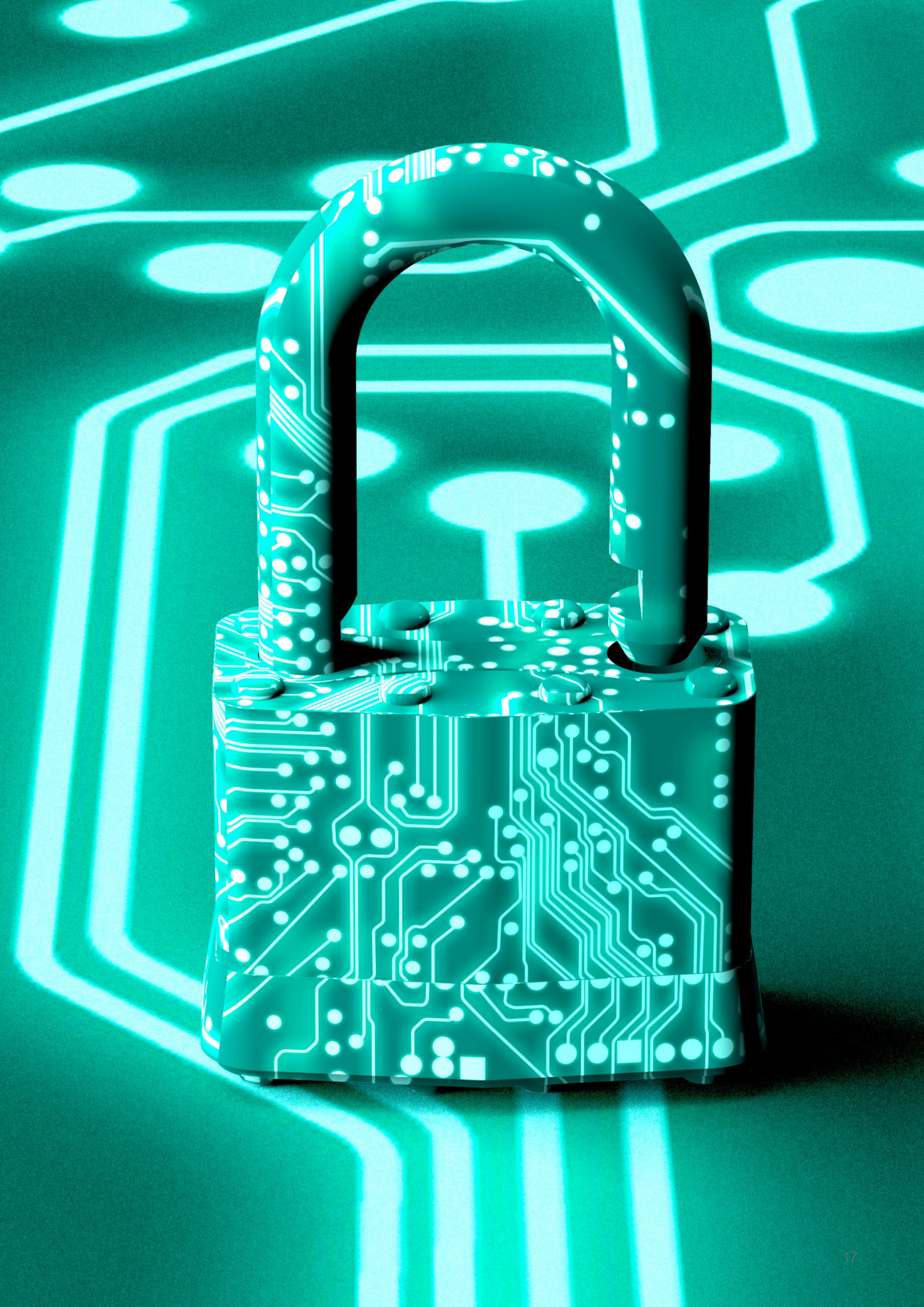
REACTION TO SECURITY BREACHES

In many cases, it is not feasible to protect against all types of security threats leading to security breaches simultaneously. Breaches are defined as external events that circumvent active security policies, practices or procedures and harm the confidentiality, integrity or availability of critical assets. It is the main objective to avoid security violations by proactively ensuring the resilience of business operations and, thereby preserving company reputation.

Compared to last year's study (42%), about 76% of the participants have Security Incident Management processes in place to counteract security breaches. This significant increase underlines the need for organizations to prepare against possible violations. In line with this, 45% of the participants have dedicated teams in place who are responsible for managing security incidents. Surprisingly, only 13% of the respondents are insured against cyber attacks.

Figure 15: Reactivity and crisis management in place





VII. FOCUS TOPICS

EU GDPR COMPLIANCE

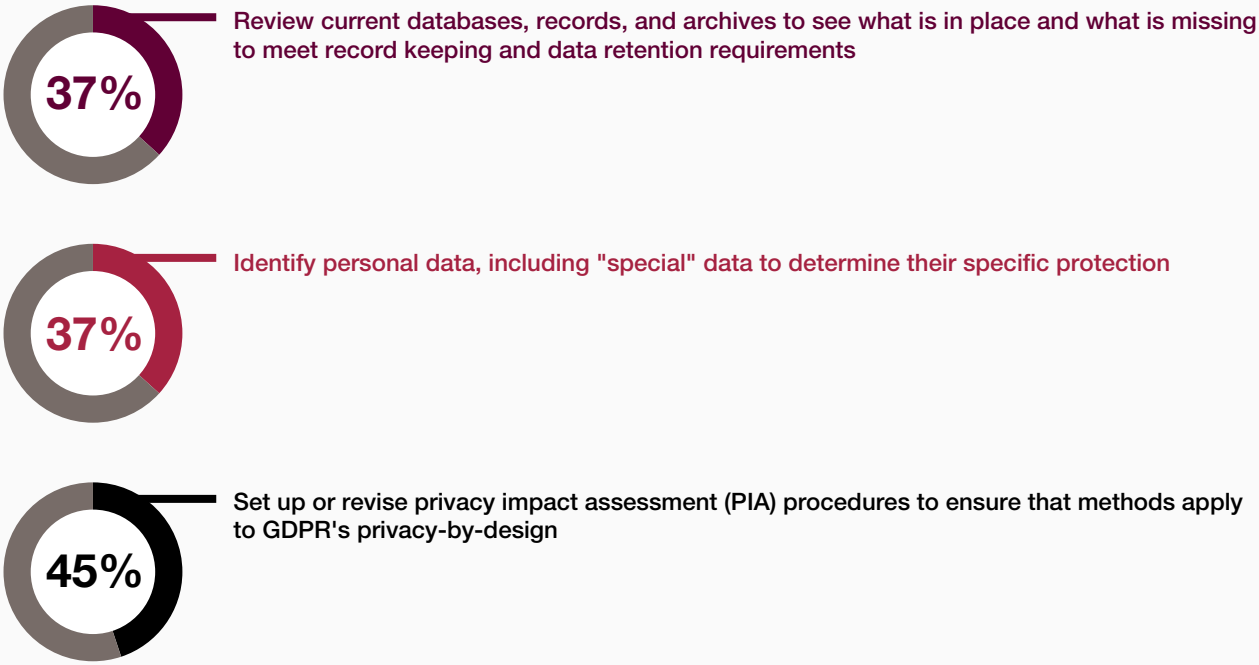
The General Data Protection Regulation (GDPR) will come into effect on May 25th 2018. The regulations aim to improve consumer privacy by giving customers more control over their data. This is done by granting customers the right to see what information companies collected about them, for which purposes it is used and to whom it has been given for further processing. On the one hand, this results in enormous pressure coming from the need for implementation, on the other hand it offers a chance for companies to implment a comprehensive privacy risk assessment. In this year's Benchmarking study we asked participants how far they already comply with existing regulations. About 50% feel comfortable, whereas the other 50% massively lack of compliance. Only 6% stated full adherence with regulations.

MEASURES TO ENSURE EU GDPR COMPLIANCE

Across all industries, 45% of the participants chose Privacy Impact Assessment (PIA) procedures as the dominant measure to ensure GDPR compliance.

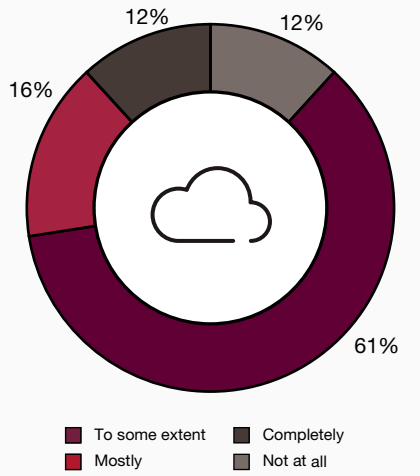
Taking a closer look at specific peer groups, it stands out that for "Consumer Products & Retail" the most relevant measure is the review of current databases, records and archives to examine what is in place and what is missing to meet record keeping as well as data retention requirements (86%). Participants from the peer group "Life Sciences & Healthcare" mainly chose the identification of personal data for the purpose ofdetermining their specific protection (83%). In preparation for GDPR requirements, companies already document every step they take to be forearmed for compliance. Nevertheless, most companies struggle to implement a comprehensive strategy that counteracts privacy risks.

Figure 16: Measures to ensure compliance with EU GDP



CLOUD SECURITY

Figure 17: Degree of Cloud usage



Most of the study participants across all industries merely use cloud services to a certain extent. Considering respondents from the peer group "Financial Services" 25% indicate not to use cloud services at all. Even more severe is the share of participants from "Manufactures" that forego opportunities of cloud integration in daily business operations (33%).

MEASURES TO ENSURE CLOUD SECURITY

The general acceptance of performing business operations in the cloud is growing rapidly. Nevertheless, security concerns are rising and organizations pose the question how to secure their cloud effectively. We asked participants which types of operations they run in the cloud and which measures they undertake to ensure the usage of cloud services.

Most respondents state "IT" as the prevailing operation in the cloud (53%) followed by "Marketing and Sales" (35%). "IT" is also the dominant operation for each individual peer group except for "Financial Services". Participants from this sector mainly state that they do not run any operation in the cloud.

In order to ensure the security of cloud services, 59% of the participants screen their cloud service providers. Furthermore, 50% state that encryption of data plays a major role to secure operations in the cloud.

DEVSECOPS

Development to Operations (DevOps) will have an enormous impact on the global IT sector in the near future. DevOps aims to reduce inefficiencies in current IT projects through the unification of software development and software operation. For today's organizations, DevOps offers the opportunity to increase overall efficiency.

At the time of data collection, however, 54% of the participants across all industries reported that they do not employ DevOps in their company. This is a fairly high amount taking into account the advantages DevOps implementation brings along for organizations. It remains to be bided, whether future IT investments will also increase DevOps adoption.

Figure 19: DevOps adoption rate

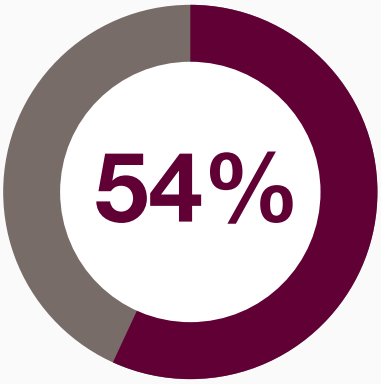


Figure 18: How Cloud Security is ensured

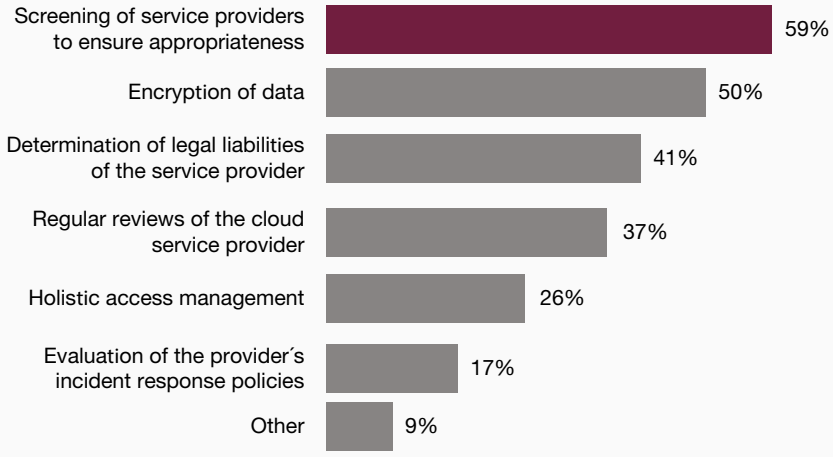
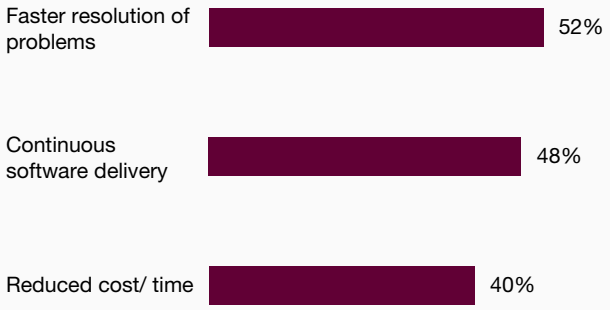
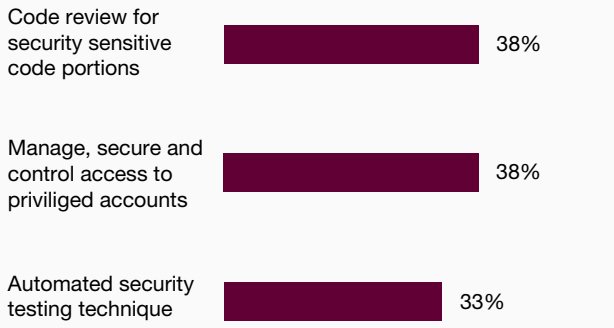


Figure 20: Reason to adopt DevOps



Considering the Top 3 reasons why companies adopt DevOps, it is noteworthy that all rea-sons include time issues, which points out the major advantage DevOps offers. A well-suited implementation of DevOps can reduce cycle times remarkably and, thereby increase organ-izational efficiency.

Figure 21: Integrated security controls



In order to ensure appropriate security, participants have integrated security steering into DevOps. Code reviews (38%) as well as the management of access controls to privileged accounts are major controls. Furthermore, one third of the respondents state to have automated security testing techniques (33%) in place to mitigate risks.

VIII. INFORMATION SECURITY MATURITY ASSESSMENTS

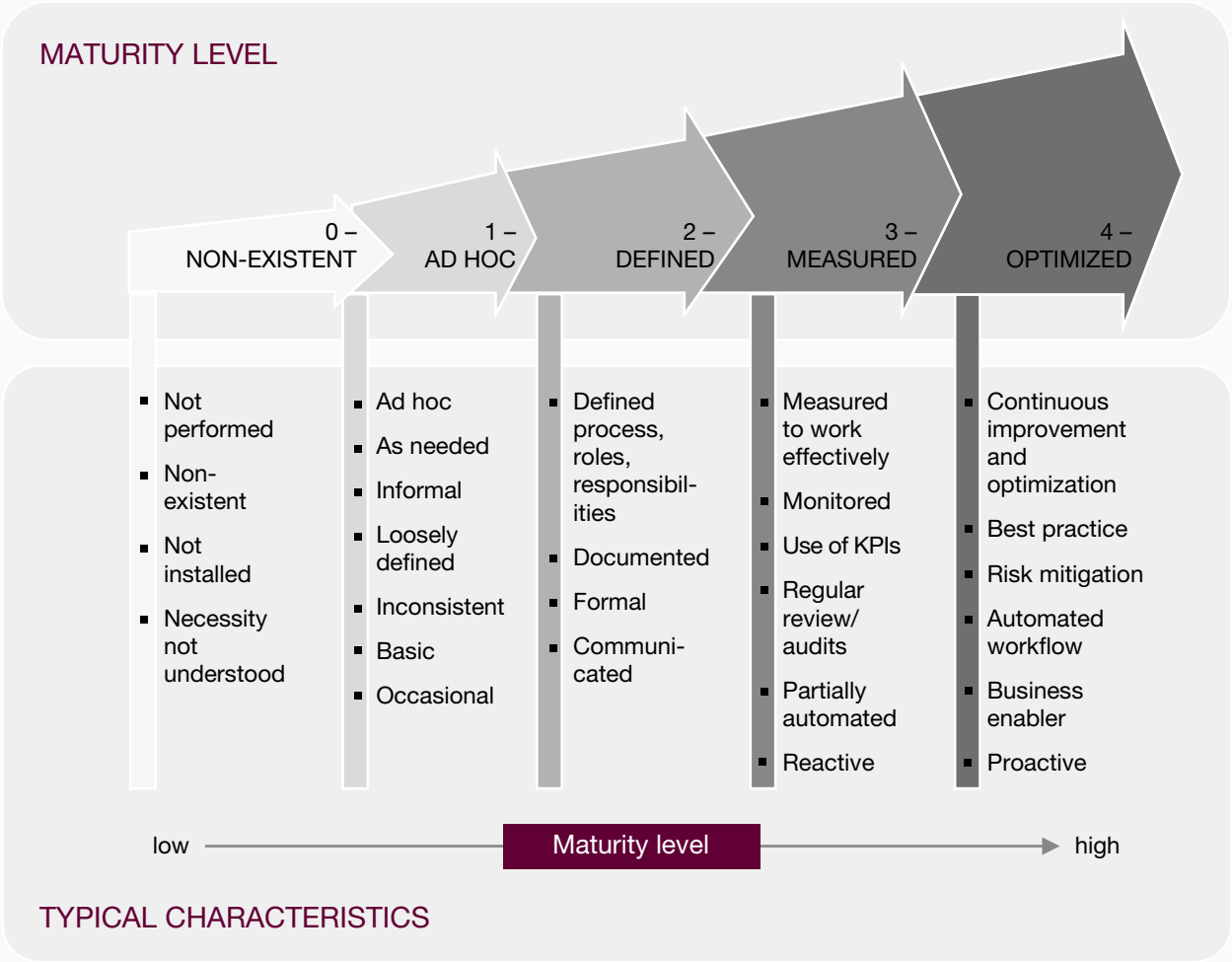
SELF ASSESSMENT USING A STANDARDIZED QUESTIONNAIRE

Besides the general questions on Information Security evaluated above, the benchmark assesses the participants' security level based on Capgemini Consulting's Information Security maturity model. This approach (Fig. 22) distinguishes five 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.

To achieve reliable results, the survey aims at an objective and repeatable security maturity assessment of all participants.

Figure 22: Definition of maturity level



OVERALL SECURITY MATURITY ASSESSMENT

The overall security maturity assessment summarizes the maturity level of all peer groups based on four assessment categories. These categories are:

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

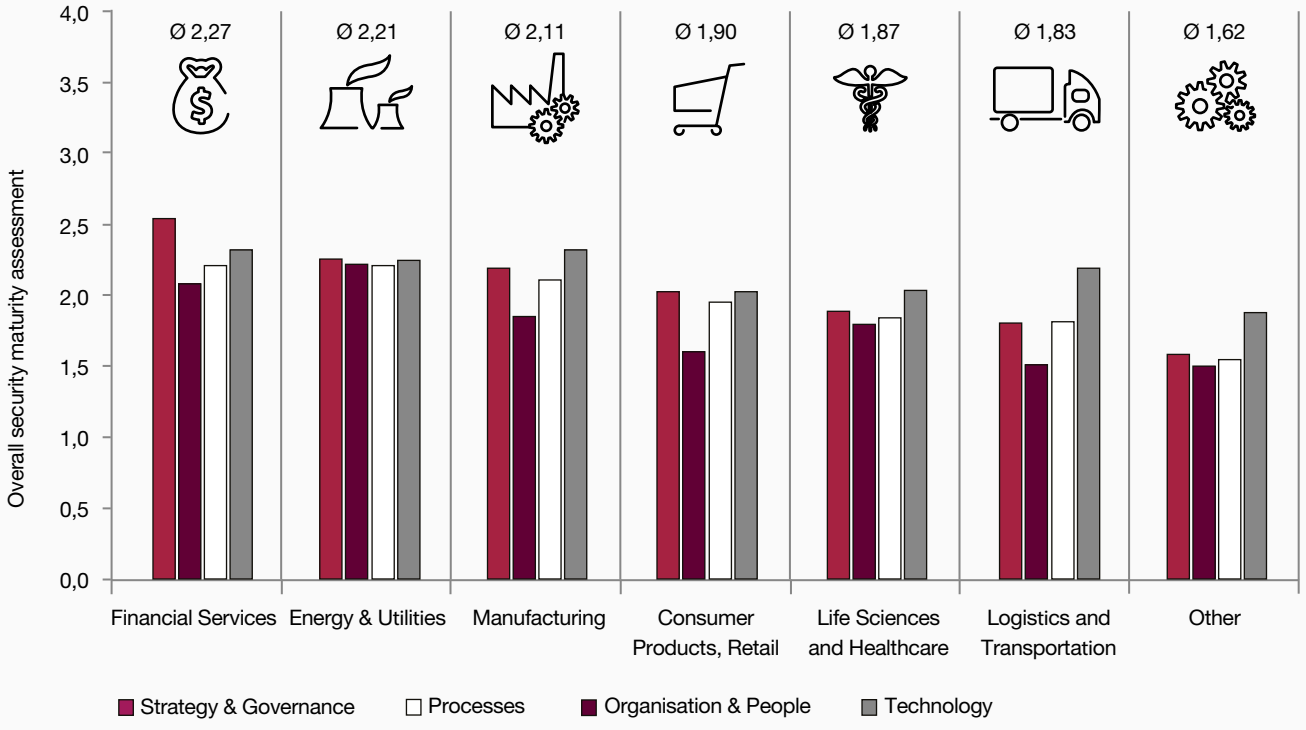
The average overall security maturity level accounts to a score of 1.97. According to the maturity level (Fig. 23), it can be interpreted that organizations have a level of "defined" Information Security on average (processes, roles, responsibilities of Information Security are defined, documented and communicated). In general, all sectors show a relatively good maturity in the domain "Technology", while the highest improvement potentials can be monitored in the "Organization & People" domain.

Comparing the peer groups among themselves, participants within the "Financial Services" and "Energy & Utilities" sector show the highest maturity level close to an average of 2.27 and 2.21. Respectively, while participants within the "Logistics & Transportation" peer group represent the lowest level, with an average maturity of 1.83.

Furthermore, it is noteworthy that some peer groups indicate major discrepancies of maturity in different categories. For example, the maturity in the category "Strategy & Governance" is considerably higher than the maturity in "Organization & People" for four out of the seven observed peer groups.

Participants within the peer group "Energy & Utilities" show an evenly spaced maturity across all four categories. This fact can be interpreted as an indicator for a coherent Information Security approach throughout the entire organization.

Figure 23: Overall security maturity assessment



MATURITY LEVEL VS. BUDGET

Taking the maturity level and the percentage of participants' IT budget spent on Information Security, the peer groups can be clustered into four categories (Fig. 22):

- Security Masters
- The Innocent
- Cost-intensive Security Showpieces
- Security Pretenders

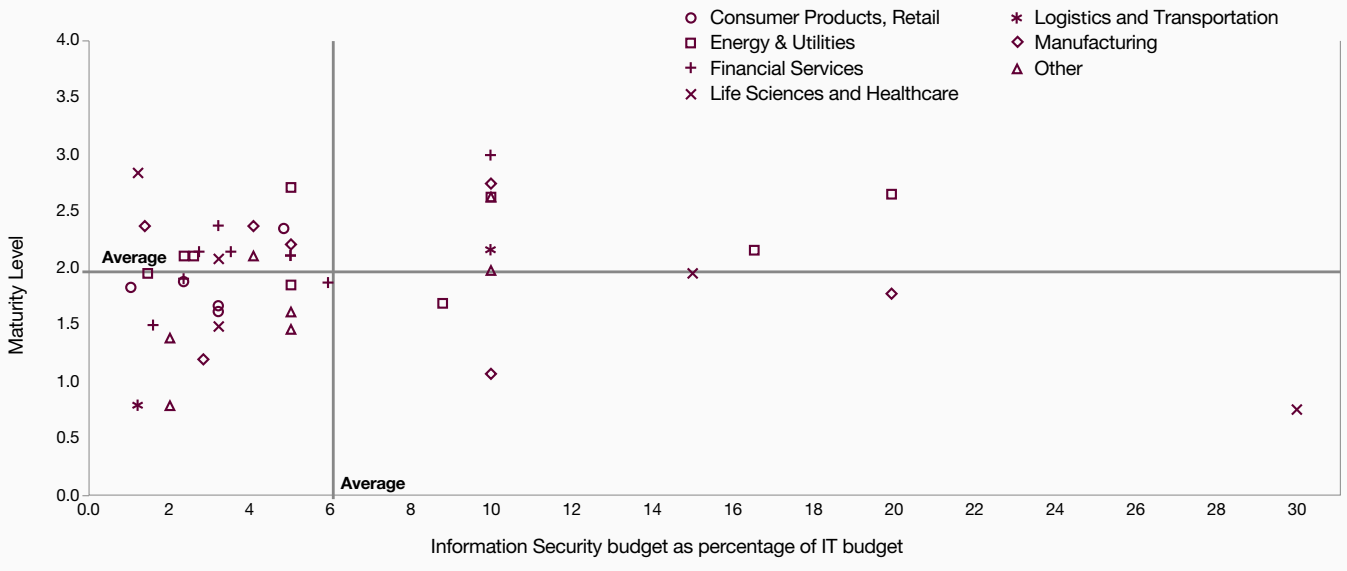
Respondents are called "Security Masters", when they spend a relatively low percentage of their IT budget on Information Secrity (below 6.15%) but achieve a relatively high maturity level, greater than 1.97. "The Innocent" participants have a relatively low Information Security budget and, therefore achieving a maturity level below average.

In regard to the right-hand side of Fig. 24, "security pretenders" are participants with higher budgets spent on Information Security than the two previous groups but achieve a maturity level below average. On the contrary, a couple of the respondents achieved an above-average maturity level with cost-intensive investments. In general, a correlation between the Information Security budget as a percentage of the IT budget and the maturity level could not be detected, i.e. spending a high budget on Information Security does not directly translates into a higher Information Security maturity.

However, for Security Masters the following areas indicate a high maturity level and might be the key success factors for an effective Information Security:

- Security Governance
- IT Risk Management
- Audits
- Awareness & Expert Training
- Threat Management & Network Intrusion Detection.

Figure 24: Maturity Level vs. budget



IX. CONCLUSION

Organizations from various industries and regions are shaping their business models as well as their internal structures to take ad-vantage of the Digital Transformation. Even though wide-ranging opportunities are emerg-ing from technological advancements, the derivations entail threats. As a result, today's organizations are more than ever determined to find answers to omnipresent security questions.

Capgemini's Information Security Bench-mark-ing Study 2017 provides detailed insights in organizations' security meas-ures, their strengths and weaknesses concerning the detection and protection of security breaches, plus the allocation of their IT budgets. 90% of the participants expect to increase their Information Secu-rity budget in the next fiscal year, which emphasizes the growing importance of security issues within organiza-tions.

A key result of the study is the lack of employee awareness within organizations. While the expertise of the top management is perceived as the key strength, knowl-edge among employees is stated as the major weakness. Today's organizations need to implement awareness programs across all hierarchy levels in order to ensure a holistic security approach and comply with increasing governmental regulations.

On average, the participants report a lower number of security breaches compared to last year's study. However, due to the fact that many respondents lack sufficient detection mechanisms, the actual number of security breaches might be higher than reported. Moreover, the severity of breaches is increasing substantially. While in 2016 the average cost for a security violation at medium-sized companies was 21k €, it amounts to 99k € in 2017.

Capgemini's Information Security Bench-marking Study 2017 aims to provide inter-ested organizations with detailed insights about the current states of Information Security across several peer groups. The findings facilitate companies to set purposeful priorities for future investments and to prepare for the growing challenges of the ongoing Digital Transformation.


DNA ANALYSIS
19%
57%
24%
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep

X. CAPGEMINI CYBERSECURITY PORTFOLIO

OUR EXPERTISE

OUR **STRATEGIC CYBERSECURITY CONSULTING** ADDRESSES C-LEVEL AND BUSINESS CONCERNS TO ENABLE A SECURE DIGITAL TRANSFORMATION.

Strategy Development and Innovation

Maturity Assessment and Digital Risk

Governance, Organization and Professionalization

Response and Recovery

Data Protection and Privacy

Acculturation and Change Management

Cloud Security, Architecture and Automation

WHY CAPGEMINI CONSULTING?

1. **Structured, proven approaches** to setup or optimize your Cybersecurity capabilities
2. **Flexible and easy-to-adopt solutions** for an accelerated increase of Information Security based on your needs
3. **Benchmarking data** derived from previous projects and our ”Informarion Security Benchmarking” study to compare with industry peers
4. **Measuarable impact** based on implemented KPIs
5. Extensive knowledge in **project, change and communication management**
6. **Global Capgemini network** of over 2,500 security and communication experts

YOUR CONTACT PERSONS

Capgemini Consulting

Dr. Guido Kamann
Vice President
Head of Business & Technology Innovation

Capgemini Consulting
Phone: +49 151 4025 2115
E-Mail: guido.kamann@capgemini.com

Capgemini Consulting

Dr. Paul Lokuciejewski
Senior Manager
Lead Cybersecurity Consulting

Capgemini Consulting
Phone: +49 151 4025 0855
E-Mail: paul.lokuciejewski@capgemini.com

Capgemini Consulting

Sebastian Heierhoff
Manager
Cybersecurity Expert

Capgemini Consulting
Phone: +49 151 4025 0133
E-Mail: sebastian.heierhoff@capgemini.com

Capgemini Consulting

Luca Thun
Cybersecurity Expert

Capgemini Consulting
Phone: +49 178 144 5240
E-Mail: luca.thun@capgemini.com

Strategic Cybersecurity Consulting

www.capgemini.com/consulting-de/service/cybersecurity/

Capgemini Consulting

About Capgemini Consulting

Capgemini Consulting is the global strategy and transformation consulting organization of the Capgemini Group, specializing in advising and supporting enterprises in significant transformation, from innovative strategy to execution and with an unstinting focus on results. With the new digital economy creating significant disruptions and opportunities, our global team of over 3,600 talented individuals work with leading companies and governments to master Digital Transformation, drawing on our understanding of the digital economy and our leadership in business transformation and organizational change.

Learn more about us at

www.capgemini.com/consulting-de

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini 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 200,000 team members in over 40 countries. The Group reported 2016 global revenues of EUR 12.5 billion.

Visit us at

www.capgemini.com