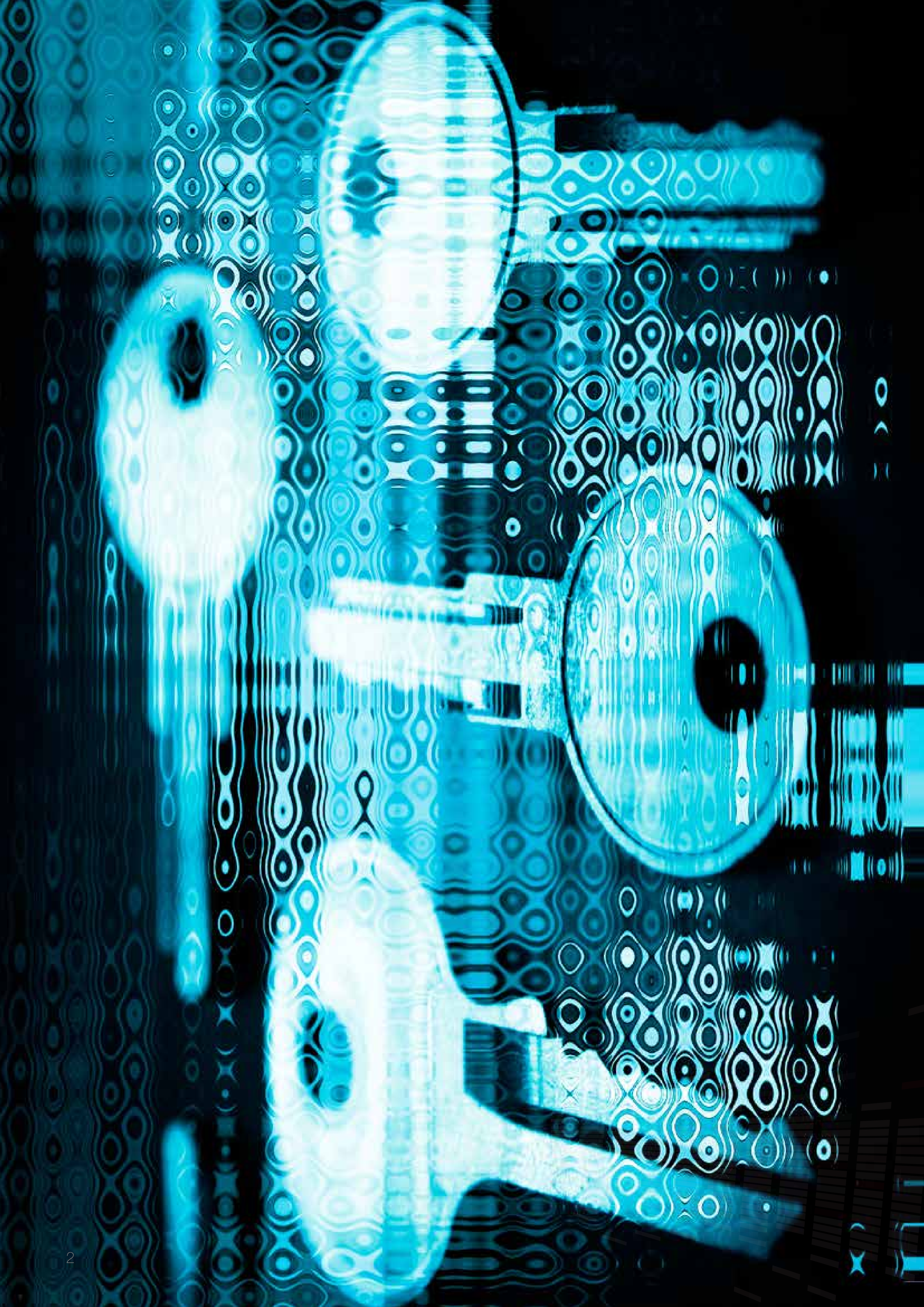
Capgemini Consulting

Information Security Benchmarking 2016

Leading the way in Information Security



CONTENT

Management Summary 05

Introduction 06

Critical Assets – Risks And Impact Of Breaches 09

Best Practices For Effective Information Security 13

How Can You Become a Security Master? 21

Conclusion 24

Capgemini Cybersecurity Portfolio 26

PASSWORD
LOGIN
LOGIN
PASSWORD

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, businesses and governments are looking for answers to omnipresent security questions today more than ever.
- Understanding how other peers implement Information Security to protect their assets and integrate security into daily business is key. Such insights are not only helpful in recognizing current trends and best practices, but also enable rapid identification of individual strengths and areas which require improvement and allow for benchmarking across the organization's peer group.
- In Q4 2015, Capgemini Consulting conducted a global Information Security benchmarking study of companies and organizations around the world. The 86 respondents from various industry sectors provided their views on upcoming trends, and delivered information on topics such as their security budget, organization structures or breach costs.
- The Information Security assessment was conducted based on a detailed maturity model. Using this model, study participants evaluated their security practice in the domains "Strategy & Governance", "Organization & People", "Processes" and "Technology".
- Capgemini evaluated the respondents' answers and is presenting 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

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

Know your crown jewels – 60% of the respondents consider customer data as their most critical asset, further crown jewels are personal information, strategic business information and intellectual property.

Rising costs of information security breaches – large-scale companies estimate the costs for major security breaches of being up to EUR 900,000, for mediumsized companies the breach costs may reach EUR 100,000.

Need for organizational evolution – 43% of the respondents believe that a member of the executive committee should lead Information Security to leverage the over-arching protection of digital organizations.

Increasing board awareness – 85% of participants value a medium or high level of attention for Information Security from top management, which is an increase of 10% compared to the results from the previous year.

Weak integration of security into business – only 20% of the participating companies have achieved effective integration of security behaviors into business activities and 37% of management is still not aware of Information Security risks.

Lack of effective intrusion detection – only 29% of participants monitor their critical IT assets against intrusion, leaving a majority of systems unmonitored.

Increasing security budgets – 45% of the respondents believe that their Information Security budget will increase in 2016; on average, security budgets translate into 4.0% of the annual IT budget.

No correlation between budgets and security maturity – multiple participants spend a greater amount of their budget on Information Security than their peers, but achieve a below-average security maturity level. Strategic investment into the right areas is key, as demonstrated by the security masters.

INTRODUCTION

OBJECTIVES AND STRUCTURE

A strong reliance on technology on the one hand, and a dramatic increase of the frequency and severity of Information Security breaches on the other, underline the importance for an organization to establish an effective Information Security function. A profound understanding of the state of this function can therefore help to identify areas which require improvement. Comparing yourself with others, for example through the use of a benchmarking study like the Capgemini Consulting Information Security Benchmarking 2016, is a good starting point for doing so.

Divided into three sections, this report summarizes this year's findings:

- After a short introduction of the benchmark's participants, the first section gives in-depth insights into the impact of Information Security, illustrating risks, drivers, breaches and costs.
- The Information Security benchmark then focuses on the structure of the participants' Information Security organizations, including budgets and planned improvement initiatives.
- One core element of the study is the participating organizations' Information Security maturity assessment, which concludes this report.

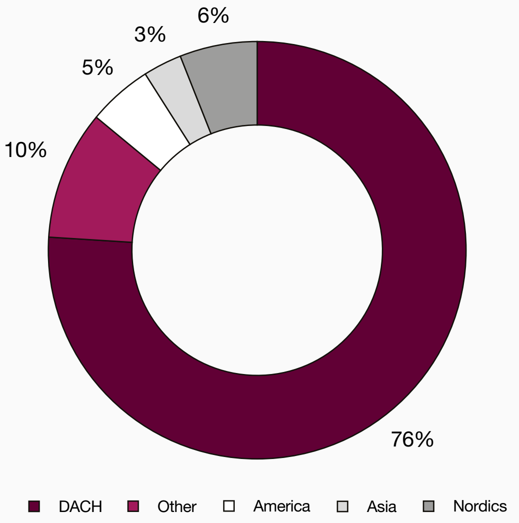
STRUCTURE OF ANALYZED ORGANIZATIONS

Based on the opinion of 86 participants, this year's Information Security Benchmark is not limited to drawing a general picture of the state of Information Security.

By distinguishing four characteristics the participating organizations share, the benchmarking study is able to derive more detailed insights. These characteristics are the participants' origin, industry sector, size of the organization, and the respondent's role in his/ her organization.

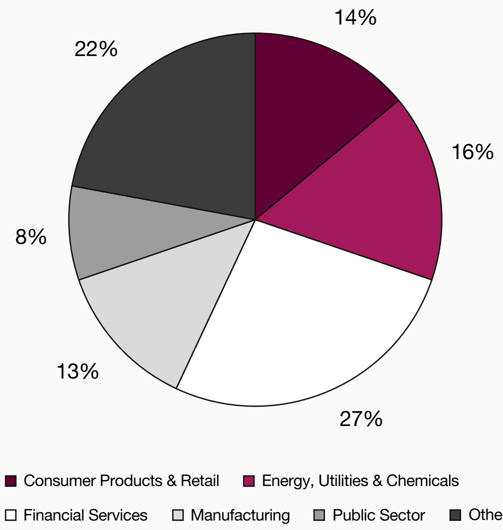
Participants' origin – The analyzed organizations cover a broad range of countries and industries. While most participants (76%) represent organizations based in Germany, Austria and Switzerland, nearly a quarter of organizations (24%) are based in other countries, primarily America, Asia and Northern Europe (Fig. 1).

Figure 1: Participants' origin

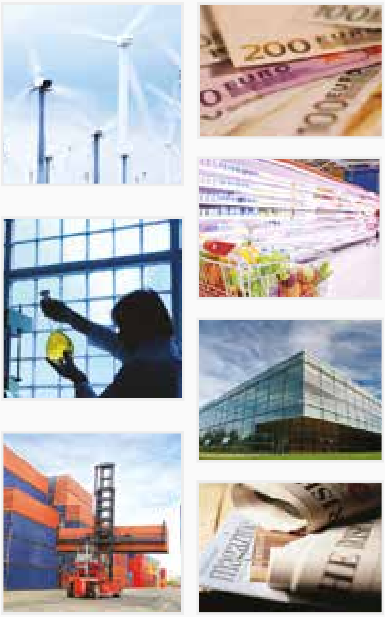


© Capgemini Consulting 2016

Figure 2: Participants' industry sectors



© Capgemini Consulting 2016



Energy, Utilities & Chemicals
Leading and market-listed energy and chemical companies from several countries and international utilities

Financial Services
Major global banks, leading insurance companies and international service providers for financial institutes

Manufacturing
Large market-leading manufacturers and international hidden champions with global orientation

Consumer Products & Retail
Global consumer product companies and major international retailers

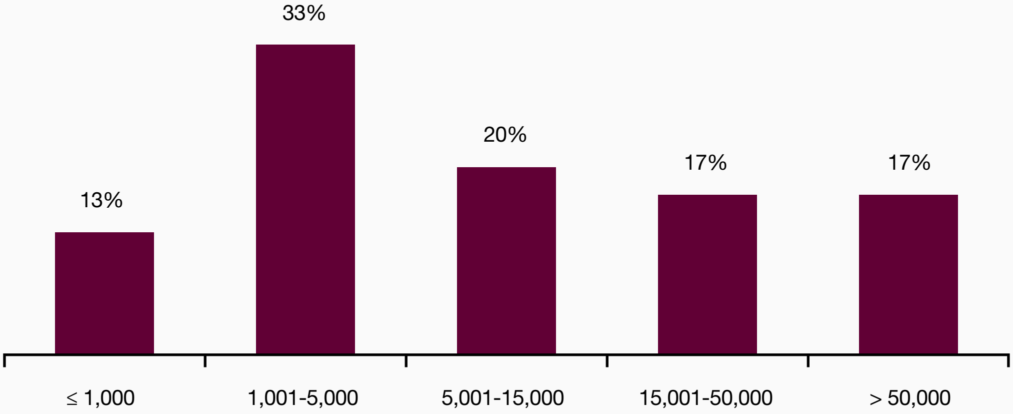
Public Sector
Major federal authorities and ministries, infrastructure operators and competence centers for municipals

Other Industries
Leading international logistic, telco, media and car supplier companies from several countries

Participants' industry sectors – Our benchmark compares six industry peer groups. In particular, participants operate within the sectors Financial Services (27%), Energy, Utilities & Chemicals (16%), Consumer Products & Retail (14%) and Manufacturing (13%) (Fig. 2).

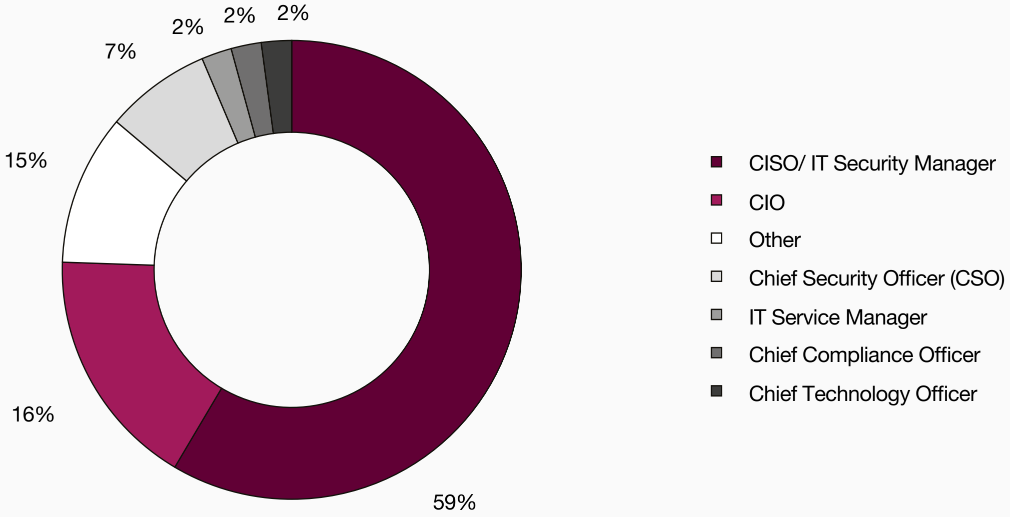
Organization size – Looking at the size of the organizations, one-third of the participants (34%) represent large-sized organizations with more than 15.000 employees. Most participants (66 %) represent medium-sized organizations with up to 15.000 employees (Fig. 3).

Figure 3: Organization size (number of employees)



© Capgemini Consulting 2016

Figure 4: Participants' role



© Capgemini Consulting 2016

Participants' role – Based on the role respondents hold in the organization, the benchmark also provides various perspectives. About one half of the participants (59%) act as Chief Information Security Officer or IT Security Manager in their company, while the other half are Chief Information Officers (CIO) or act in a nearby role within the IT division (Fig. 4).

CRITICAL ASSETS – RISKS AND IMPACT OF BREACHES

CRITICAL ASSETS AT RISK

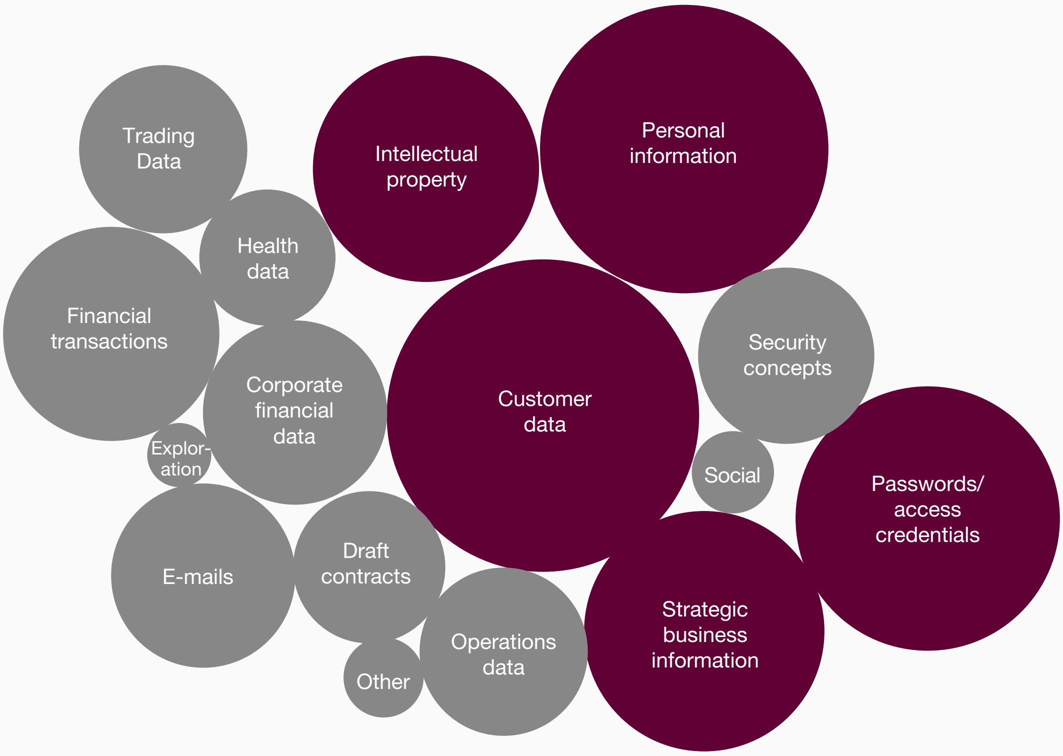
To prioritize investments in Information Security, it is crucial for an organization to understand what is at stake. Information resources have to be considered as critical assets, essential in the support of business operations. If an organization's assets are affected by risks of any kind, protecting them should be seen as an integral element of operational management and strategic planning. Critical assets at risk ranked by participants over all industry sectors are shown in Figure 5.

Organizations use customer data to tailor relevant advertisements, offers and other products and services to consumers, as well as to provide them with a personalized experience based on individual preferences. 60% of participants consider customer data as the most critical asset. Protection of personal client data becomes even more important when taking new developments in data privacy regulations into account.

Further noticeable critical assets named by participants are personal information (e. g. HR data), intellectual property (e. g. inventions, literary or artistic works, symbols, names and images used in commerce), strategic business (e.g. long-term strategic plans) as well as passwords and access data.

Differences between the industry sectors can be observed. For example: participants within the Manufacturing sector named intellectual property (e. g. inventions) most frequently as an asset at risk, whereas the most critical assets within the Financial Services Sector are personal information, customer data and financial transactions.

Figure 5: Critical assets at risk

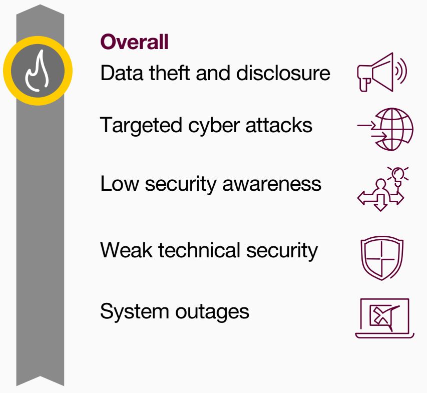


© Capgemini Consulting 2016

INFORMATION SECURITY RISKS

As security threats are multiplying, organizations are facing an increasing level of Information Security risks and organizations are struggling to protect the aformentioned assets.

When asked to rank these risks in the Information Security Benchmark, 28% of overall participants named data theft and disclosure as the major Information Security risk. Targeted cyber attacks have been reported as the second biggest risk. These attacks are often realized by well-organized groups, making them more dangerous. The lack of employees' knowledge and understanding of Information Security leads to the third most frequently mentioned risk – low security awareness. Technical security (e. g. security of mobile devices or within a cloud) is considered to be a less important Information Security risk.



Overall

Data theft and disclosure

Targeted cyber attacks

Low security awareness

Weak technical security

System outages

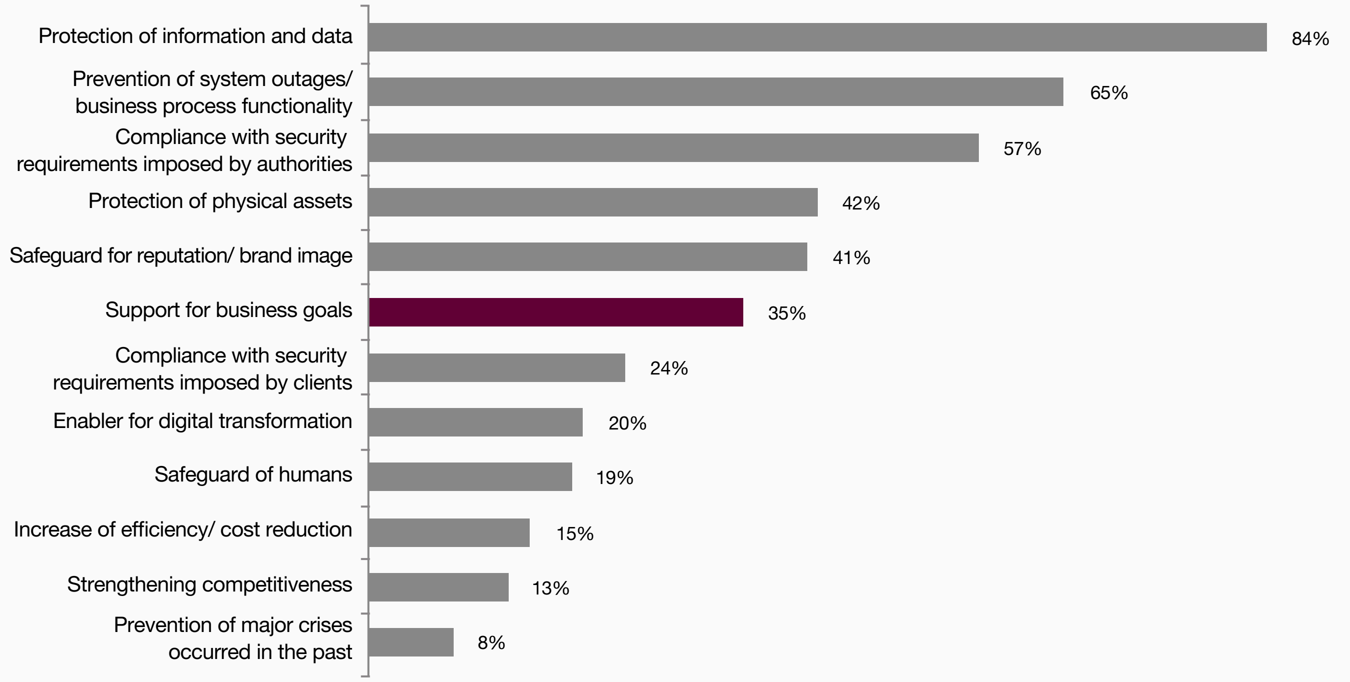
In contrast to the previous year's study, system outages (e.g. those prevented by high availability of systems) are becoming less prominent, highlighing the focal shift from availability to confidentiality.

DRIVERS FOR INFORMATION SECURITY

The obvious key driver for an organization to invest in Information Security is to protect its crown jewels from these risks. The most frequently named key driver for Information Security is the protection of information and data (84%). Further key drivers are the prevention of system outages (65%) and compliance with security requirements imposed by authorities (57%).

In contrast, only 35% of the participants state the support of business goals as a driver for their security practice (Fig. 6).

Figure 6: Drivers for Information Security



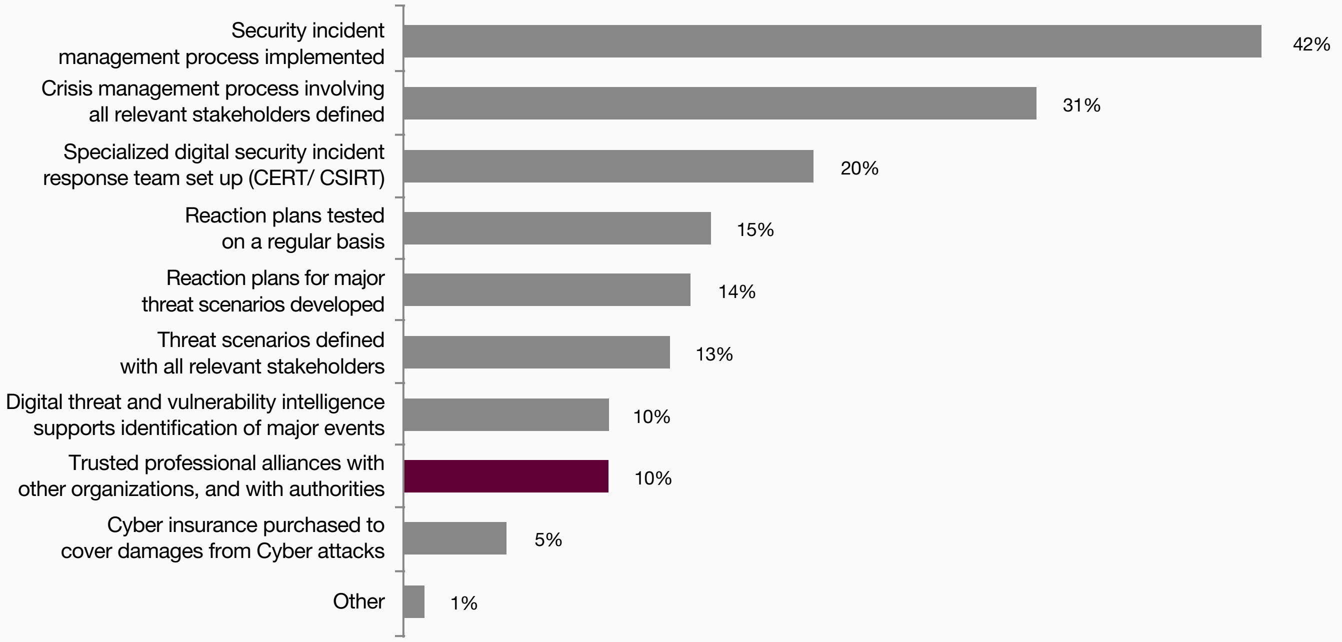
© Capgemini Consulting 2016

REACTION TO SECURITY BREACHES

Not all security threats can be prevented at all times, and may result in a security breach. The latter are defined as external events that by-pass security policies, practices, or procedures and violate the confidentiality, integrity or availability of critical assets. Avoiding security breaches is the main objective, as doing so ensures business operations and competitiveness and preserves reputation.

Individual organizations' reactions and crisis management strategies differ in the face of security breaches. While 42% have a security incident management process in place, the number of participants with a specialized digital security incident response team which can react appropriately is rather low (20%). Only 10% of participants have trusted professional alliances with other organizations and with authorities. Participant answers confirm that, at present, organizations underachieve when implementing effective reactivity and crisis management (Fig. 7).

Figure 7: Reactivity and crisis management in place



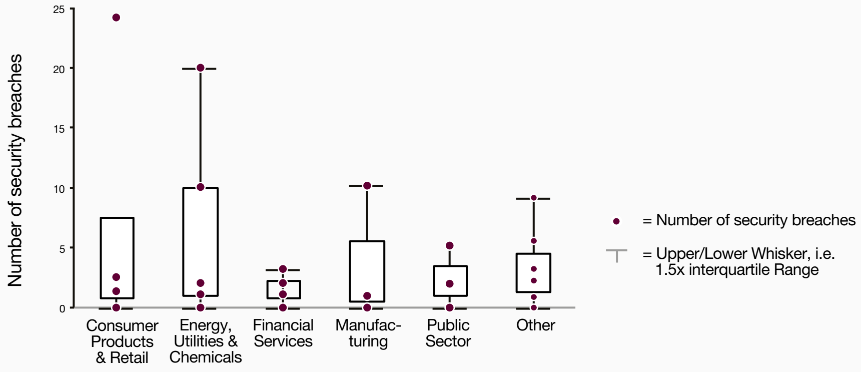
© Capgemini Consulting 2016

NUMBER OF SECURITY BREACHES

Our question regarding the number of annual security breaches per industry sector showed quite a different picture per industry peer group. The highest number of security breaches was reported from participants belonging to the peer groups “Consumer Products & Retail” and “Energy, Utilities & Chemicals”, who faced up to 24 and 20 security breaches respectively. Regarding the Information Security maturity level (explained later on), organizations of these two peer groups show the lowest maturity level across all industries and therefore the high number of breaches is not surprising.

Organizations within the Manufacturing Sector have reported up to 10 annual security breaches, followed by participants of the Public Sector with up to 5 annual security breaches on average. The lowest number of breaches was reported by organizations of the Financial Services Sector, which faced 3 annual security breaches. Organizations within these sectors show a higher Information Security maturity level, which cuts the number of breaches by half, compared to the sectors named above (Fig. 8).

Figure 8: Number of annual breaches per industry



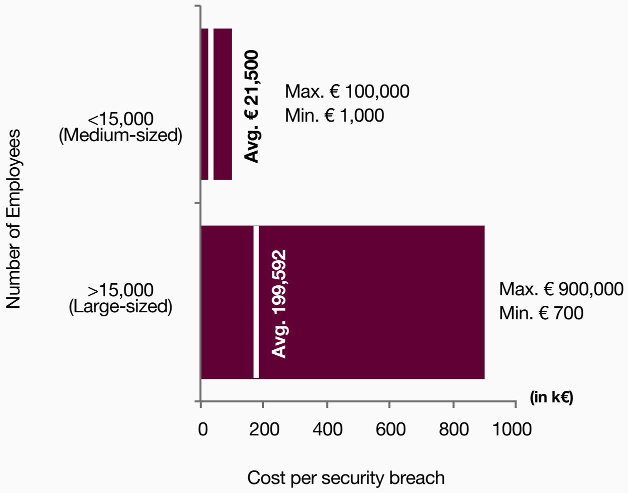
© Capgemini Consulting 2016

COSTS OF SECURITY BREACHES

In addition to the number of security breaches, the benchmark provides data about the cost per security breach including e.g. cost of service unavailability, forensics, reparation/ recovery, fines and notification costs.

These costs correspond to the size of an organization. Medium-sized organizations have lower cost per security breach than large-sized organizations. Whereas the average cost per security breach in medium-sized organizations is EUR 21,500, it reaches up to EUR 200,000 in large-sized organizations. As shown in Figure 9, the maximum cost per security breach for a medium-sized organization was stated to be EUR 100,000, while it was reported to be up to EUR 900,000 for a large-sized organization.

Figure 9: Cost per security breach



© Capgemini Consulting 2016

BEST PRACTICES FOR EFFECTIVE INFORMATION SECURITY

Finding an efficient approach to Information Security which prevents security breaches and protects the organization's critical assets is currently the main objective. This approach is manifested in governance, organizational structure, perceived strengths and improvement fields as well as an organization's budget and planned investment.

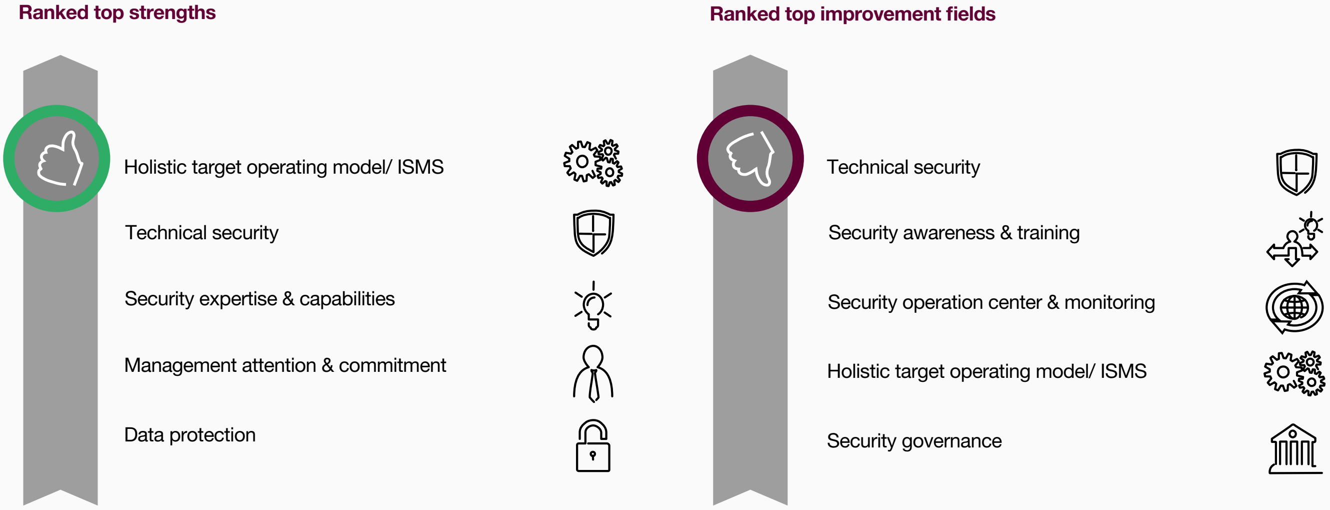
In the end, the organizational structure and the available budget have to support the implementation of necessary changes and the operationalization of an Information Security approach.

STRENGTHS AND IMPROVEMENT FIELDS

Different strengths and improvement fields which are influenced by the organizational structure in different ways. When participants ranked their top strengths and improvement fields around Information Security, technical security (e.g. mobile device or cloud security) was named as both the improvement field with the greatest priority, as well as one of the top strengths. These results lead to the assumption that once an adequate level of technical security is achieved, this level can be retained and is therefore seen as a top strength. Otherwise, if organizations struggle to implement technical security, it is named as the most important field that needs to be improved by the organization.

The improvement field named by participants as holding the seconds highest rank was security awareness. Security awareness is – as explained below in more detail – one of the most effective ways to prevent security breaches, and therefore a cornerstone for effective protection of information.

Figure 10: Strengths and improvement fields of participants' Information Security

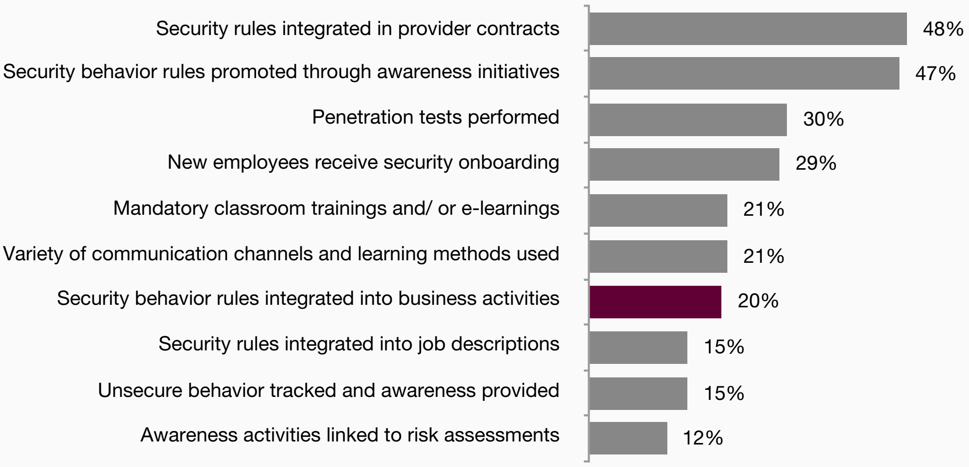

Ranked top strengths
Holistic target operating model/ ISMS
Technical security
Security expertise & capabilities
Management attention & commitment
Data protection
Ranked top improvement fields
Technical security
Security awareness & training
Security operation center & monitoring
Holistic target operating model/ ISMS
Security governance

AWARENESS INITIATIVES

Security awareness was ranked by participants as among the top priorities regarding improvement fields. An important aspect is approaching a higher Information Security maturity level, as employees are involved in up to 40% of all security attacks as stated by various studies. Effective awareness initiatives help organizations to prevent most security breaches.

As shown in Figure 11, the benchmark evidences the as-is situation of present awareness initiatives named by participants. The results of the study indicate that most of the organizations have “security rules integrated in provider contracts” (48%) and “security behavior rules are promoted through awareness initiatives” (47%). Notable is the low number of participants who answered that “security behavior rules are integrated into business activities” (20%), which confirms the statement above.

Figure 11: Awareness initiatives (Top 10)



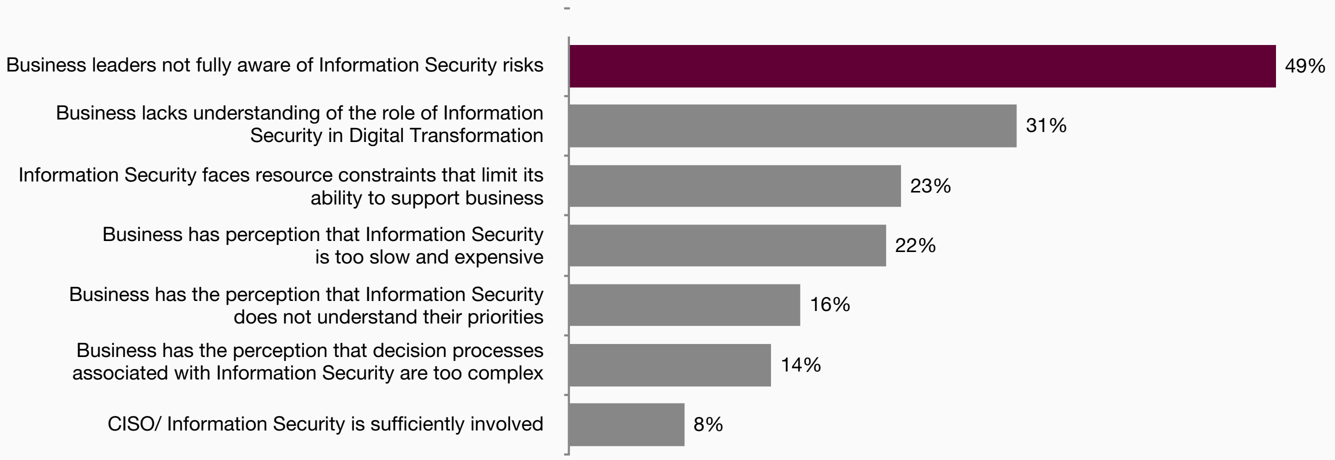
INSUFFICIENT BUSINESS INVOLVEMENT

Results of the question on participants' awareness initiatives confirm that security behavior rules are insufficiently integrated into business operations. Implementing Information Security is often seen as a matter of minor significance by organizations' employees, especially by business leaders.

Participant's most frequently named answer (49%) regarding the reason for insufficient business involvement underlines that "business leaders within the organization are not fully aware of Information Security risks" (Fig. 12).

Furthermore, 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. By implementing SMACT technologies in the face of Digital Transformation, the role of Information Security is often underestimated. This underestimation is illustrated by the second most frequently named reason (31%): "business lacks understanding of the role of Information Security in Digital Transformation".

Figure 12: Reasons for insufficient business involvement



© Capgemini Consulting 2016

SIZING OF INFORMATION SECURITY

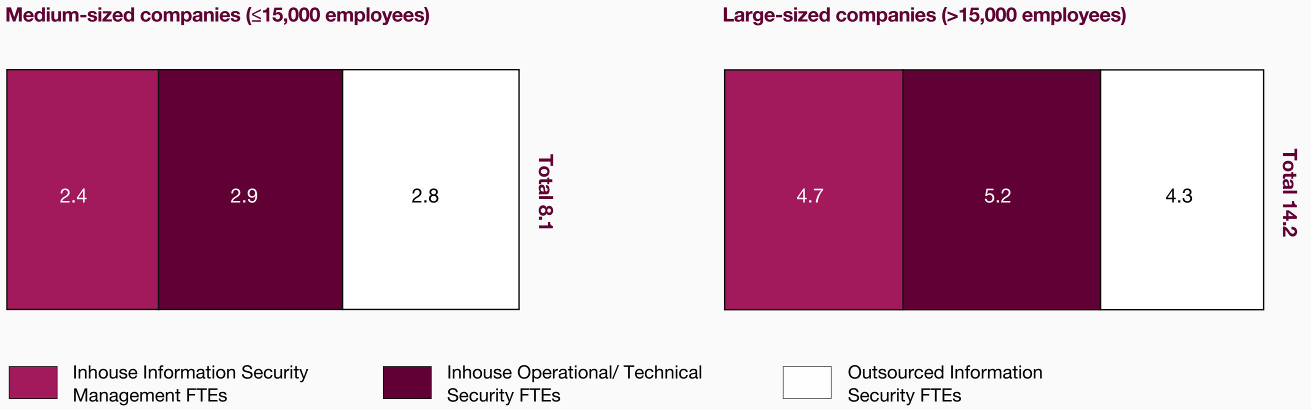
Implementing Information Security requires an Information Security department within the organization that is equipped with the right resources. Our benchmark delivers indicative numbers of employees working on Information Security. The sizing of Information Security can be measured by the number of employees, quantified by the number of full-time equivalents.

In medium-sized organizations (<15,000 employees) there are on average 8.1 FTEs responsible for Information Security, whereas in large-sized organizations (>15,000 employees) 14.2 FTEs on average are dedicated to the same (Fig. 13).

The sizing also varies among the industries. The smallest teams were observed in "Consumer Products & Retail" with 4.0 FTE and 9.0 FTE for medium-sized and large-sized companies, respectively. At the other end of the spectrum, "Financial Services" employs 10.3 FTE and 50.5 FTE for medium-sized and largesized companies.

These departments differ in the proportion of FTEs dedicated to in-house and outsourced resources. Across all industry sectors, two-thirds of FTEs are dedicated to In-house Information Security Management and In-house Technical Security, whereas one-third of FTEs are dedicated to outsourced Information Security services.

Figure 13: Organization of Information Security – sizing



© Capgemini Consulting 2016

ORGANIZATIONAL EVOLUTION OF INFORMATION SECURITY

Due to a growing relevance of Information Security issues, respondents believe that members of the executive board or the CISO will take over responsibility of the Information Security strategy. Our benchmark 2016 confirms that successful implementation of Information Security requires great attention from management boards.

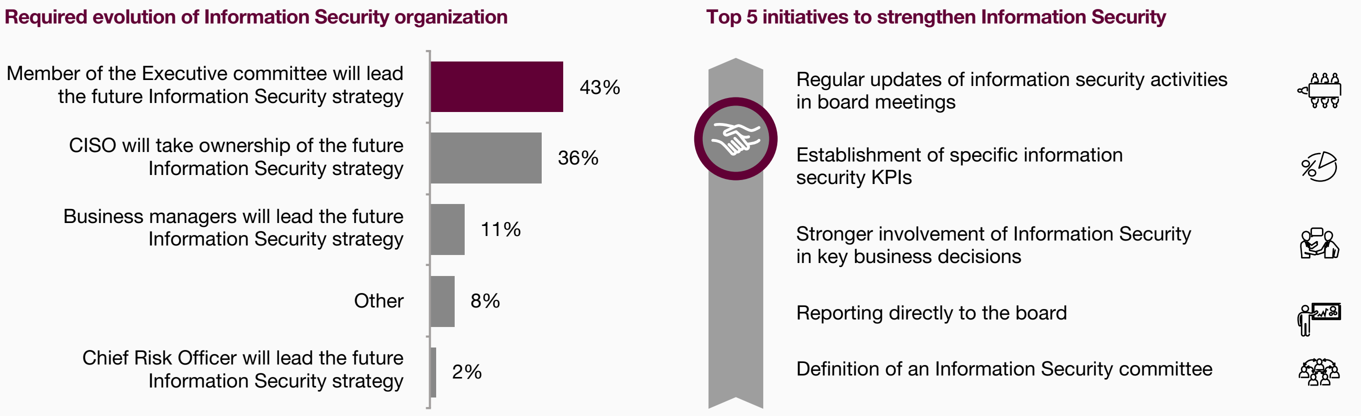
When participants were asked who they think take over full responsibility for future Information Security strategies, 43% of all participants responded that a "member of the executive committee will lead the future Information Security strategy", whereas 36% answered that the "CISO will take ownership of the future Information Security strategy". These results support the statement that participants understand the necessity for an evolution of Information Security organization.

HOW TO STRENGTHEN INFORMATION SECURITY

There are multiple solutions in terms of leveraging the Information Security function. In order to achieve a holistic security culture – a main field that must be improved – specific initiatives are considered by the respondents to be most effective.

Implementing the TOP 5 initiatives – shown in Figure 14 – helps organizations to strengthen the security improvement fields. With regard to the figure, the initiatives are primarily targeted at implementing organizational structures, involving various employees from different units and hierarchy levels as well as the establishment of specific Information Security KPIs.

Figure 14: Reasons for insufficient business involvement



Regular updates of information security activities in board meetings

Establishment of specific information security KPIs

Stronger involvement of Information Security in key business decisions

Reporting directly to the board

Definition of an Information Security committee

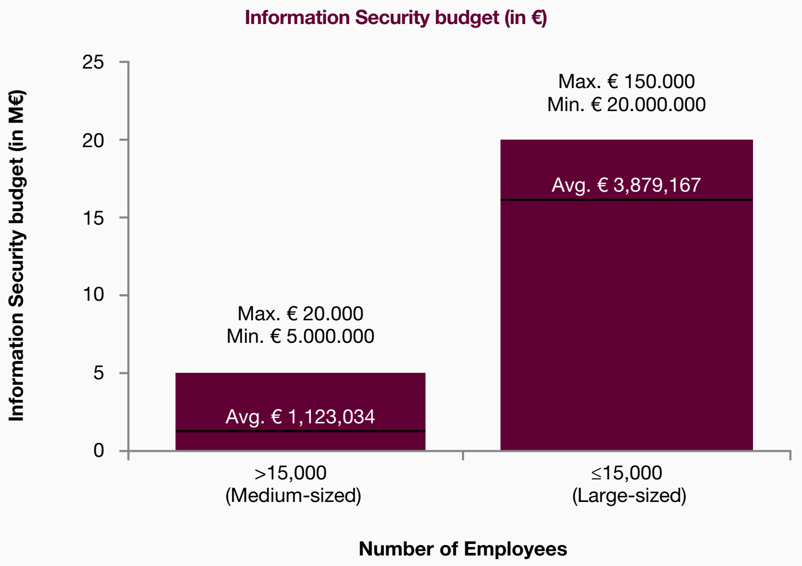
© Capgemini Consulting 2016

INFORMATION SECURITY BUDGET

Budgets correspond to the size of organizations. The budget of medium-sized organizations is naturally lower than the existing budget of large-sized organizations. The average budget (including e.g. HR, budget for consulting, projects, operations) invested in Information Security in large-sized organizations is 3.5 times higher than in medium-sized organizations. Large-sized organizations' budget is nearly EUR 4 million on average, whereas the average budget of a medium-sized organization is EUR 1.1m.

As shown in Figure 15, the budget range of large-sized organizations reaches from EUR 150,000 up to EUR 20m, whereas the budget range of medium-sized organizations spans EUR 20,000 up to EUR 5m. The spread of these security budgets is extremely wide, which leads to the hypothesis that the Information Security maturity levels of the participants significantly differ from each other as well.

Figure 15: Information Security budget in €



EVOLUTION OF INFORMATION SECURITY BUDGET

The implementation of Information Security is essential in supporting business operations. Organizations have recognized the importance of investing in this area, and their planned investments will increasing in the near future.

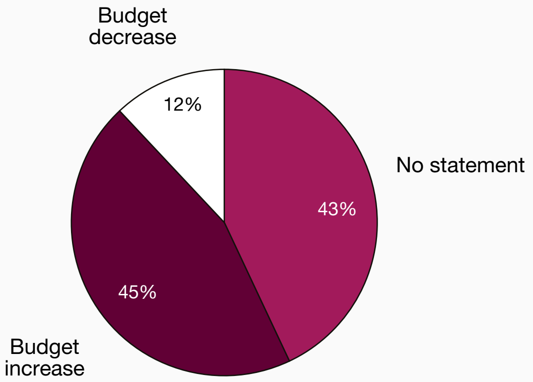
This is a strong statement based on the results of this year's benchmark. Although 43% did not to reveal their investment plans, 45% of all participants answered that their Information Security budget will increase in the future, while only 12% of the participants answered that the budget will decrease (Figure 16).

Considering the current budgets of medium- and large-sized organization, further answers to our benchmark show which proportion of the Information Security budget is invested compared to an organizations' entire IT budget.

As shown in Figure 17, different organizations' Information Security budgets – as a percentage of the entire IT budget – ranged from 0% up to 10%. The evaluation has shown that on average 4.0% of the IT budget is invested in Information Security.

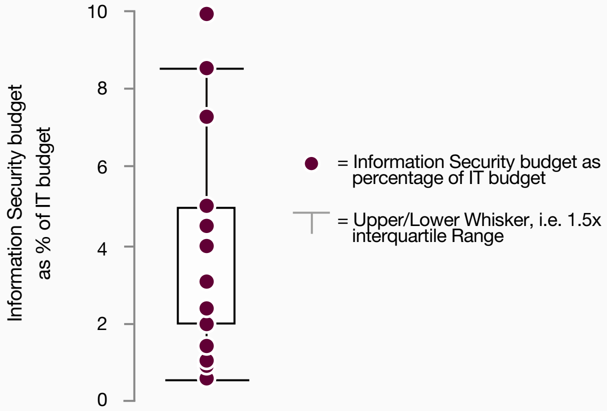
The smallest relative Information Security budgets were observed for "Manufacturing" with 3.1% of the IT budget, while the "Public Sector" with 6% seems to have the largest relative budget for Information Security.

Figure 16: Evolution of Information Security budget



© Capgemini Consulting 2016

Figure 17: Evolution of Information Security budget



© Capgemini Consulting 2016

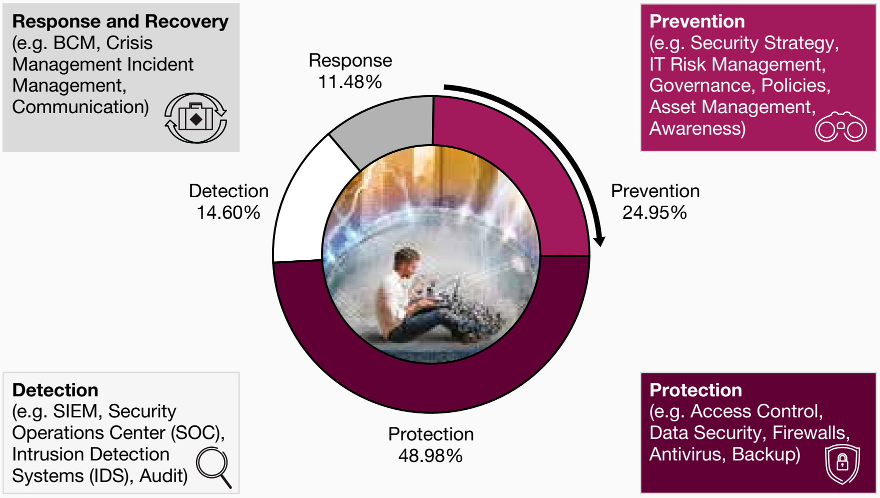
INVESTMENT AREAS

Going into detail of organization budgets, participants were asked to allocate their budget to four investment areas. These investment areas are:

- **Prevention:** e. g. security strategy, IT risk management, governance, policies, asset management, awareness
- **Protection:** e. g. access control, data security, firewalls, antivirus, backup
- **Detection:** e. g. SIEM, Security Operations Center (SOC), Intrusion Detection Systems (IDS), audit
- **Response & Recovery:** e. g. BCM, crisis management, incident management, communication

The amount of the invested Information Security budgets differs in these areas. On average, 25% of the overall budget is invested in preventing security breaches, whereas 49% of the budget is invested in protecting critical assets. Nearly 15% of the budget is invested in the detection of security breaches. Organizations invest 11% of their entire budget for responding to security breaches and recovering in the aftermath.

Figure 18: Evolution of Information Security budget



© Capgemini Consulting 2016

Compared to the past years, the amount spent on detection activities is increasing. For example, organizations are investing in Security Operations Centers (SOC) and Intrusion Detection Systems (IDS) to detect (potential) security breaches. The main reason for this trend seems to be linked to a growing technical complexity, cross-linked systems and the high number of communication channels used by organizations today. The number of potential risks is growing tremendously as a result.

Furthermore, organizations fear past security breaches, which either were not detected or only detected after several days. Due to the investments in the area of detection, planned investments in "response & recovery" will increase as well in order to be able to react appropriately to detected security breaches.

HOW CAN YOU BECOME A SECURITY MASTER?

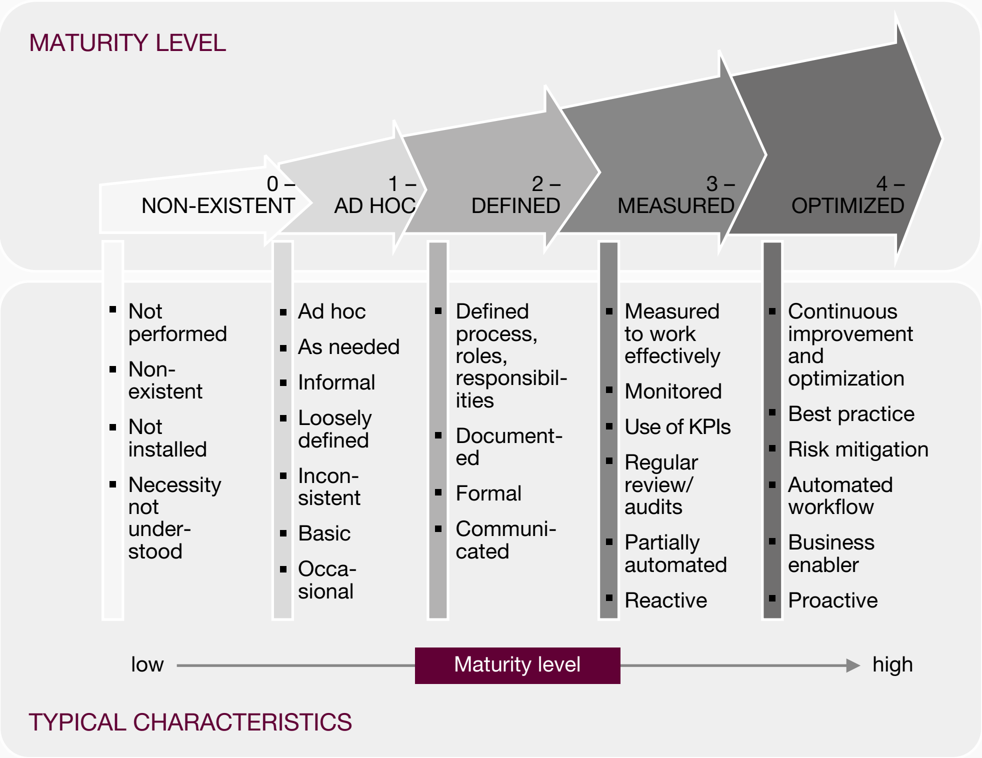
SELF ASSESSMENT USING STANDARDIZED QUESTIONNAIRE

Besides the general questions on Information Security evaluated above, the benchmark assesses participants security based on Capgemini Consulting's Information Security maturity model (Fig. 19), which distinguishes between 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 activities and methods are used ad hoc when needed.
- Financial Services Sector are personal information, customer data and financial transactions.
- Maturity Level 2: Processes, roles, 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 study aims at an objective and repeatable security maturity assessment of all participants.

Figure 19: Definition of maturity level



0 – NON-EXISTENT	1 – AD HOC	2 – DEFINED	3 – MEASURED	4 – OPTIMIZED
▪ Not performed ▪ Non-existent ▪ Not installed ▪ Necessity not understood	▪ Ad hoc ▪ As needed ▪ Informal ▪ Loosely defined ▪ Inconsistent ▪ Basic ▪ Occasional	▪ Defined process, roles, responsibilities ▪ Documented ▪ Formal ▪ Communicated	▪ Measured to work effectively ▪ Monitored ▪ Use of KPIs ▪ Regular review/audits ▪ Partially automated ▪ Reactive	▪ Continuous improvement and optimization ▪ Best practice ▪ Risk mitigation ▪ Automated workflow ▪ Business enabler ▪ Proactive

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:

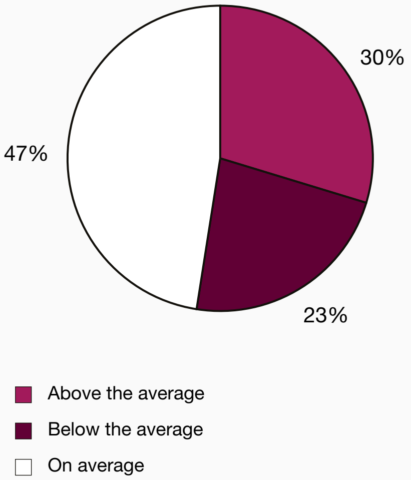
1. Strategy & Governance
2. Organization & People
3. Processes
4. Technology

The average overall security maturity level amounts to 1.97. According to the maturity level (Fig. 19), the result states 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 Public and Manufacturing Sector show the highest maturity level at an average of 2.33 and 2.28 respectively, while participants within the Consumer Product and Retail peer group show the lowest level, with an average maturity of 1.62. (Fig 20)

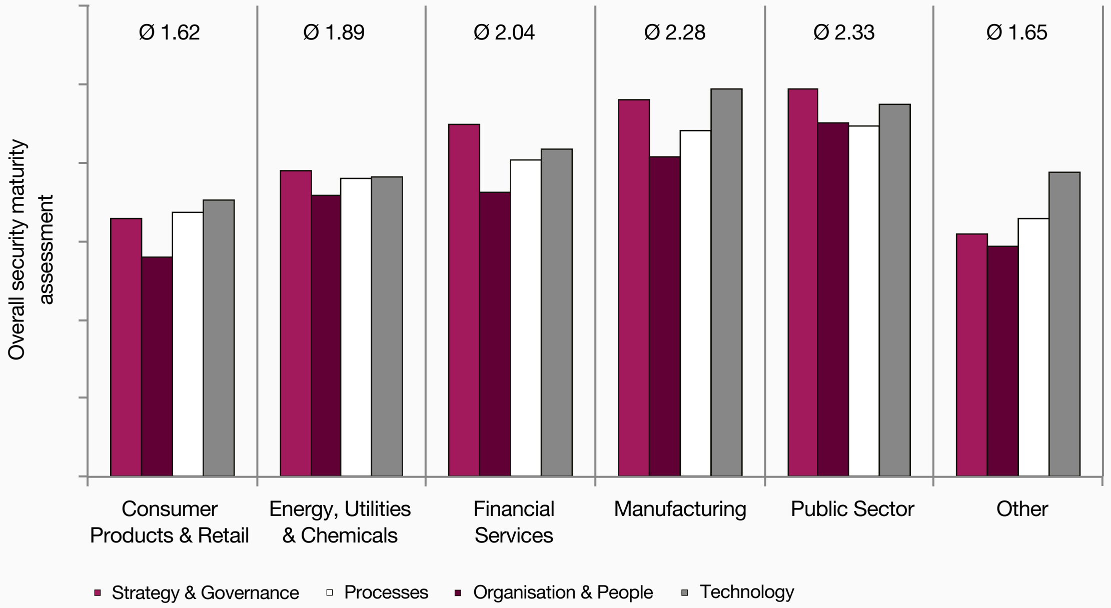
How organizations assess their security maturity compared to peers is demonstrated in Figure 21. Nearly half of participants think that their maturity level is on average with peers. 23% of participants classify their maturity level at below average, whereas 30% think that their Information Security maturity is above average.

Figure 21: Self assessment - comparison to peers



© Capgemini Consulting 2016

Figure 20: Overall security maturity assessment



© Capgemini Consulting 2016

MATURITY LEVEL VS. BUDGET

Taking into account the maturity level and the percentage of participant IT budgets spent on Information Security, the peer group can be clustered into four groups (Fig. 22):

- Security masters
- The innocent
- Costintensive security showpieces
- Security pretenders

Participants are called “security masters”, when they spend a relatively low percentage of their IT budget on Information Security (below 3%), but achieve a maturity level higher than 1.97, while “the innocent” participants have a relatively low Information Security budget and therefore achieve a maturity level below the average.

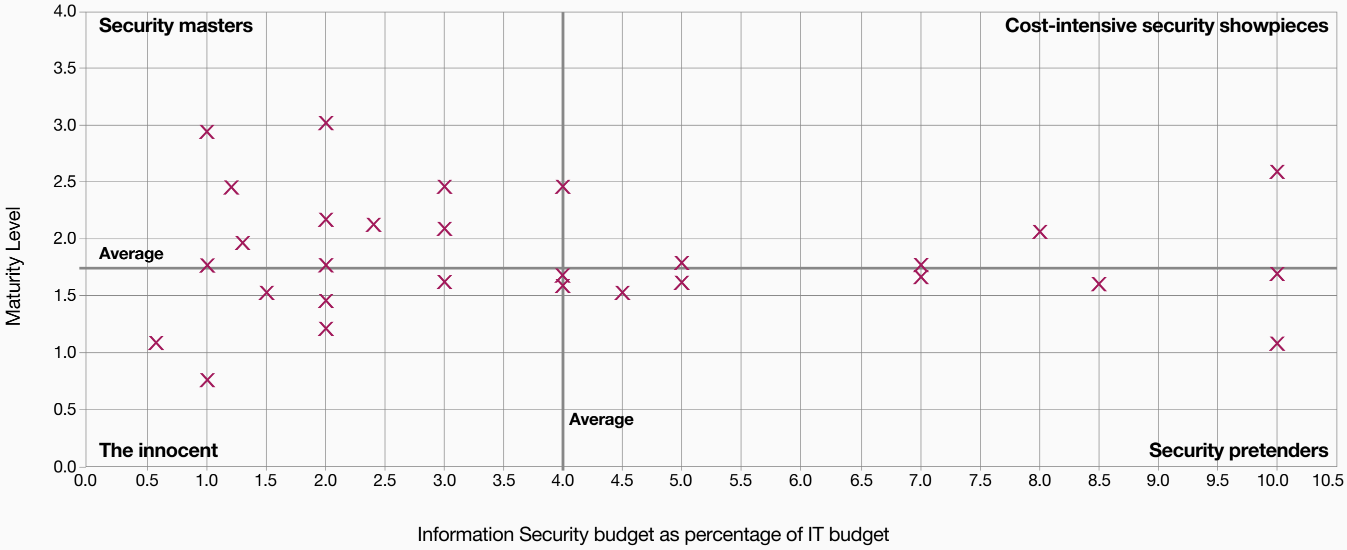
In regards to the right side of Figure 22, security pretenders are participants with higher budgets spent on Information Security than others, but who achieve a maturity level below the average, whereas a few participants achieved an above-average maturity level with cost-intensive investments.

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 portion of the budget on Information Security does not directly translate to greater Information Security maturity.

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

- Security governance
- IT risk management
- Audits
- Awareness & expert training
- Threat management & network intrusion detection

Figure 22: Maturity level vs. budget



× = Participants overall security maturity level in relation to its Information Security budget as percentage of IT budget

© Capgemini Consulting 2016

CONCLUSION

Organizations in all industries and regions are benefitting from Digital Transformation. However, new technologies introduce further risks to sensitive assets and business activities. As a result, organizations are looking, today more than ever, for answers to omnipresent security questions.

Capgemini's 2016 Information Security study shows that participants face a high number of critical security breaches, leading to substantial costs for their organizations. The actual number of security breaches might be even higher, as many incidents remain undetected due to the low maturity level of implemented monitoring capabilities.

Although the level of attention top management pays to Information Security is high, and has even increased by 10% compared to the results from the previous year, the study highlights an insufficient awareness level among employees, which is considered as one of the top risks. Hence, there is a strong need for holistic awareness programs.

Another key result from the study is that high Information Security investments do not directly translate into a high security maturity. However, some participants achieve high maturity with a below-average budget. Our analysis shows that these security masters are characterized by a high maturity level in the areas of security governance, IT risk management, audits, awareness and training, threat management and network intrusion.

The insights of Capgemini's study should help organizations to shape an effective Information Security strategy and prepare for the growing challenges of ongoing Digital Transformation.

MALWARE
HACKER
NETWORK
PASSWORD
CRIME
TROJAN
https://
INFORMATION
RISK
VIRUS
PRIVACY
DATA
SPAM
EMAIL
WEB
PROTECTION
ACCESS
WARNING

CAPGEMINI CYBERSECURITY PORTFOLIO

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

MATURITY ASSESSMENT & STRATEGY

“gain a profound understanding of your **current Cybersecurity situation** and support you in a **strategic realignment**.”

DIGITAL RISK & DATA PRIVACY

“identify your **critical assets**, manage **business-oriented risks** and protect the **privacy of your data.**”

“foster a **people-centric security culture** and a **holistic security by design** based on awareness and training programs.”

AWARENESS & TRAINING

“establish an effective Cybersecurity **organization, governance, policies** and **processes** for a digital resilience.”

SECURITY TARGET OPERATING MODEL (ISMS)

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 Hanschke
Senior Consultant
Cybersecurity Expert

Capgemini Consulting
Phone: +49 221 3799 2172
E-Mail: sebastian.hanschke@capgemini.com

Capgemini Consulting

Alexander Klier
Consultant
Cybersecurity Expert

Capgemini Consulting
Phone: +49 699 515 1197
E-Mail: alexander.klier@capgemini.com

Strategic Cybersecurity Consulting

www.de.capgemini-consulting.com/capabilities/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.de.capgemini-consulting.com

About Capgemini

With more than 180,000 people in over 40 countries, Capgemini is one of the world‘s foremost providers of consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at

www.de.capgemini.com