Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Cybersecurity | the way we see it

Insights into Cybersecurity 2015-16

People matter, results count.


ANALYSIS
SEARCH
SCANNING


SCANNING
57%


enter

Preface

The internet is the lifeline of modern society. Our lives increasingly revolve around the digital world of smart phones, social media and the Cloud; whether for work, shopping or establishing and maintaining contacts. Business as usual no longer exists; carrying on as usual is no longer an option. If you choose to participate in the new economy, you will have to change course drastically and set sail towards becoming a digital organization.

This means that you need to develop a lean and flexible organization, which operates and assists customers 24/7 through various channels; an organization that works fast, is easily approachable and delivers consistently.

Unfortunately ease of access is also an invitation to criminals, who have a great interest in your data. This is why every digital transformation should go hand in hand with solid cybersecurity policies, tailored to respond to every risk. In this way you will protect your organization and your customers, who must feel sufficiently secure to shop around and store information within your digital organization. Failure to implement sound cybersecurity measures could result in damage to your organization's image, loss of confidence and serious financial repercussions. The question is not whether you will be attacked but when. This is why it is important to be well prepared. Your customers rely on you.

That is the purpose of this cybersecurity report; to give you new insights and advise you on how to make your digital organization secure. It contains several articles written by our cybersecurity experts, pertaining to various aspects of digital security. We would like to invite you to read these articles and stay one step ahead of the cyber criminals, who are probably reading along…

I wish you successful and safe business!

Erik Hoorweg
Vice President
Capgemini Consulting

Matthijs Ros
Leader Cybersecurity,
Capgemini

** A detailed analysis of the key trends and developments in the field of public order and security can be found in the recently published report Trends in Security. You can download it free of charge from www.trendsinveiligheid.nl or request a copy via trendsinveiligheid.nl@capgemini.com*

Insights into Cybersecurity 2015-16

Contents


SCANNING...
57%

Introduction

The digitization of our society is happening at breakneck speed. Research by Capgemini and MIT shows that many organizations are transforming rapidly by using digital technology. And with good reason. A digital organization can reach many more customers through various new channels, works faster and more efficiently, and can therefore quickly establish an advantage over the competition.

But there is a downside. With the increasing importance of technology in organizations, there comes a corresponding increase in their vulnerability. Cybercrime, digital espionage and hackers pose a serious threat and demand preventive action. And don't forget your own employees, who can leak sensitive data either knowingly or unwittingly. Factors such as these place increased pressure on organizations to make sure their cybersecurity systems are up to date. This pressure is threefold: stemming from within the organization, from customers who want their data to be managed with integrity and from governments.

Numerous companies worldwide are carrying out research on the latest cybersecurity trends. This year, Capgemini has also performed a Dutch study on internet security with TNS NIPO: Trends in Cybersecurity 2015. An overview of these studies reveals a number of important trends. Cybersecurity leads to a competitive advantage and will become a C-level priority. The Internet of Things is regarded by information security leaders as one of the most disruptive technologies of the near future. The critical disconnect between Chief Information Senior Officers (CISOs) and senior leadership remains a major challenge. Another significant trend is the massive shift of new technologies towards big data analytics, forensics and intelligence-based cyber solutions, assisted by Security Operation Centers (SOC).

The question is: what steps should organizations and governments take to prepare themselves for the challenges that accompany digital transformation? This report contains five articles written by our cybersecurity specialists, which offer practical advice on how to improve digital security. With no less than 2,500 cybersecurity professionals and a proven portfolio in the field of cybersecurity solutions, Capgemini assists clients worldwide with their transformation into digital organizations. We advise, protect and monitor. Because of this, our customers are always well prepared and are able to act decisively when needed. Cyber criminals are always sharp and focused but Capgemini is equally sharp and focused. Are you?

The business value of security starts with a common framework

How can security be embedded in the primary process?

Highlights

- Digital security benefits from an enhanced security business case.
- The business case is reinforced if security is connected to the divisions involved in the primary process.
- Connections may be developed through a common framework.
- Security becomes one of the sources of integrated risk management within the framework.
- The business value of real-time security intelligence is still hardly appreciated.

Added value for the primary process

From "business case" to "business value"
Security seems to have many similarities with insurance: as long as incidents fail to occur, all investments in security seem in vain. But if organizations prove insufficiently secure following an attack, the cost of an incident is many times higher than an initial investment in security would have been. The lack of publicly available hard data on direct and indirect damage caused by security incidents reinforces this, because it complicates the quantification of the added value of security. Although it is clear to insiders that it is not a question of whether an organization will be attacked but when, it is often difficult to convince divisions involved in the primary process to take adequate measures. This is especially true of relatively expensive security measures, such as a Security Operations Center (SOC), which must be staffed by employees with scarce and costly expertise. The business case drawn up by security staff should therefore be as strong as possible to protect organizations from future incidents. A well-known weakness of many business cases for security lies in the difficulty to make the "business value" transparent. A major reason for this is the poor connections between security divisions and those involved in the primary process.

What does this imply for your organization?
Organizations place a priority on their primary, critical processes continuing to operate normally. To assess the benefits of a SOC and other security investments, it is essential to describe as clearly as possible the value of security to these primary, critical processes. Especially if there is a specific threat or attack. A security threat or attack only becomes meaningful if it can be reduced to the KPIs of an

organization. Which particular KPIs can vary from organization to organization and may include (sustainable) profits, availability of services and/or protection of data. In the case of an attack, an organization's security department must not only provide insight into what exactly happened and what data was lost but also needs to interpret the potential damage, in terms of the relevant KPIs of the organization.

Building a common framework

This requires a common framework between the security department and the divisions involved in the primary process. This common framework includes speaking the same language, using the same definitions and assuming the same predetermined critical data within the organization. The framework is built up by getting the base of the security in order and under control. Once the base is in order, renewal and innovations can be translated from the primary process to security. The static first step evolves towards a more dynamic environment: once the primary process changes, security changes in tandem. In steps 3 and 4, the synergy and dynamics increase with real-time potential.

1. Make sure the base is in order

In practice, we find that many organizations struggle to get the basics of security in order. Eye-catching security measures, such as physical security, personnel screening, identity and access management, patch management and point solutions for network security are often implemented. Risk-based security, security by design, security management and rule compliance are often less well controlled. In particular, risk analyses are applied only rudimentarily, even though this is the method of choice to ensure effective and cost-efficient security measures. Due to a lack of integration between measures, it is also not clear whether all risks have been adequately covered. In getting the basics of security in order, a connection to the primary process must first be made. A prioritization of the security effort must be established with the divisions involved in the primary process.

Prioritization is based on the organization's most critical business processes. These are the key to the survival of the organization and deserve top priority when it comes to security. The same holds true for critical data held by an organization, such as personal data or intellectual property. These deserve priority over other processes and data. The divisions involved in the primary process determine the appropriate level of security in terms of confidentiality, integrity and availability. Only these divisions can decide whether it is acceptable for a process to be down for a minute, an hour or a day.

2. Renewal and innovation

The basic protection must evolve alongside the ever-changing business processes. It cannot be limited to a one-off analysis and implementation of measures. Today's business processes change rapidly through digitization; on the one hand this increases dependence on IT but on the other hand, customers and the public often receive more direct access to business processes. Both aspects of digitization therefore make security

indispensable. But especially a change to a business process increases the need to re-evaluate security. Change does not necessarily mean that security should be increased. If a (part of a) process is placed with a third party, this could mean the reduction of certain measures.

The process from step 1 must therefore be repeated periodically to bring security in line with changes in business processes. Guaranteeing security as a part of the existing planning and control cycle of the organization ensures continued attention. At the same time, it is important that the security connects with those organizational units that are often at the forefront of renewals and innovations, such as purchasing,programs and projects and, of course, the primary process itself. Security thus becomes an advisor to the divisions involved in the primary process.

3. Integrated risk management

When the connection to the primary process has evolved into a dynamic collaboration, new opportunities present themselves. Digital security should be part of the organization's integrated risk management strategy. Given the potential impact of digital security (both positive as a business enabler, and negative as business risk) on attaining the organization's KPIs, this is more than justified. Moreover, it is a primary concern: the CXO of the organization must be constantly informed and must be cooperative. The CXO may not be responsible if things go well but is certainly responsible if things go wrong. Digital security must go hand in hand with known risk management specialties like financial, reputational and contractual risk management, so that digital risks become transparent for the whole organization. The translation of technical vulnerabilities or 'Indicators of Compromise' into business value related to the organization's KPIs is crucial. The question: "What does that mean for our organization?" must be answered in order to quantify the correct added value for the primary process. For the translation of technology to the primary process, security can deploy unexpected alliances. Insight into reputational risks following a digital leak or an attack can be gained from collaboration with reputation experts in organizations' communications and marketing teams. The same applies to financial risks and so on.

4. Real-time monitoring: SOC as Big Data Source

The way to strengthen the connection between security and the primary process on a daily basis is for the most operational department, the Security Operations Center (SOC), to lay the foundations for real-time integrated risk management in an organization (for successfully setting up a SOC, see the article by Michail Theuns and Roger Wannee in this edition of Trends in Security). The 'intelligence' that SOCs generate for the information security of organizations has not yet been developed to strengthen the divisions involved in the primary process. But the value for the primary process is potentially available. The difference to step 3 is that a SOC can act much more accurately and dynamically. Risks can be made transparent in real time, enabling the primary process to respond. A SOC (in-house or managed) is in fact a precondition for any IT-dependent, digital organization. By supplying the divisions involved in the primary process with actionable intelligence from the security organization, the business case and visibility of security are also improved. Also in actual incidents, fixed-risk scenarios do not need to be interpreted. Incidents can be analyzed in real time, making it possible to precisely estimate the risks and damages involved. In the area of security intelligence, it seems that much business value can be gained.

Business value of security measures

In general, it is difficult to quantify the business value of a particular security measure. In this respect, the security specialist resembles a lawyer who constantly says: "it depends". For security, it is essential to take the specific threats and risks to a process as a starting point in relation to the organization's KPIs. Looking at trends in digital transformations, such as social, mobile and the Internet of Things, security must evolve to operate in real time and take on ever broader and deeper digitization of processes. Security Operations Centers and security intelligence respond to the need for resilience and real-time monitoring, and attribute identity-based management to control access to data, which is both more effective and safer.

Conclusion

It is no longer a question of whether organizations will experience digital attacks but when. Despite significant threats and risks, it often remains difficult to convince divisions involved in an organization's primary process to introduce adequate measures. To improve this situation, the business case for security must be strengthened by making the business value of security increasingly clear. This will improve as the connections between security and primary process divisions are strengthened. Because when its relevance can be related to the organization's KPIs, security will gain its rightful voice in the boardroom.

About the author

Drs. Laurens van Nes is a managing consultant at Capgemini, active in the field of law and order and security. Specifically, he focuses on issues in the field of intelligence and cybersecurity.

For more information,
please contact the author
laurens.van.nes@capgemini.com

Open data and privacy

How can data be made available in a responsible way within the security domain?

As governments open up data to the public, up to now the security domain has been a blind spot. This article underlines the importance of making data available properly and securely.

Highlights

- Open data provides opportunities for value enhancement and risk reduction.
- Open data provides the opportunity to increase the involvement of citizens worldwide.
- The security domain significantly lags behind other sectors in this respect.
- Privacy risks must be central from the start.

The opening up of access to large amounts of data by governments offers many opportunities to citizens and businesses. Many governments worldwide are, therefore, making relevant information available to citizens digitally. This ties in with many governments' efforts to deploy the supply and usage of open data for the improvement of public administration and public services. Governments store many details about their citizens and should therefore implement security measures at an early stage. These measures should ensure that information made available through an open-data initiative is shared without risk to the privacy of citizens.

Open data offers unprecedented (and unknown) opportunities

Governments hold huge amounts of data in the most diverse fields. The potential of open data seems endless: useful travel applications have been developed by opening up traffic data, weather applications have been developed using data from meteorological institutes, and open geo-data have contributed towards solutions to energy issues. Increasing investments are also being made in the unlocking and linking of data sets.

Governments can benefit in many ways from the unlocking of open data. For example, by generating revenue in new ways (encouraging entrepreneurship and/or selling data to commercial suppliers), by saving costs (reducing transaction costs and increasing efficiency) and indirectly, by encouraging new industries and skill sets in the workforce.[1]

Open data in the public context are generally defined as data that are:

1. Publicly funded and generated by or for the execution of a public duty;
2. Public;
3. Free from copyright or other third-party rights;
4. Computer-readable (machine-readable) and compliant with open standards (XML or CSV);
5. Available for re-use without restrictions, such as costs or mandatory registration.

Source: Algemene Rekenkamer (2012) Trendrapport Open data

Besides the development of useful new applications, it is also possible to increase governmental transparency based on open data, to improve the accountability of governments and to involve the public in government.[2] Schools can be compared based on data from education inspections, for example, and government spending can be verified and checked based on financial data. This also makes it easier for authorities to compare their finances with those of other authorities.

Open data in the justice & security domain

In many countries, open data have been used in the security domain for years. The police in the UK, for example, make datasets available through police.uk: examples include crime maps based on geo-data, information on local neighborhoods, and insight into performance figures, such as the response time to emergency calls.

The use of open data in the security domain from other countries has so far been limited. For example, in the Netherlands (data.overheid.nl, a specific web page through which the Dutch government releases data in the security domain) only access to data from the police in the city of Rotterdam is mentioned, for which no reference is given. Admittedly, in the Netherlands examples of incidents, burglaries and emergency calls are mentioned that could be unlocked and this could be a good start in unlocking further government data. However, many more applications are possible, especially in terms of providing insight into the way the security and justice chain operates. These could include:

- Information on legal proceedings (turnaround time of cases, results by jurisdiction and/or region);
- Response times of police emergency rooms;
- Reports and prosecutions;
- Dimensions of cells and costs per detainee.

Privacy risks of open data

In any disclosure of government data, at the very least the following privacy risks should be taken into account:

- Anonymity is often no guarantee that the data cannot be traced back to people. Even when data are analyzed at a more abstract level, it is still possible to identify particular groups or individuals. This can be achieved by combining

different data sets, for example. Anonymous data can often be traceable to individuals.

- Data that, in principle, contain no personal details can be traced to those of one or just a few persons by linking them to other data. An example of where this occurred took place in England. A few years ago a 'crime map' was developed based on open data, allowing viewers to see where burglaries and crimes had taken place per postal code. By zooming in on the map, individual addresses where certain offenses had taken place could be identified.
- By analyzing and aggregating large data sets on individu als, profiles can be created (profiling) and conclusions attached, which can sometimes have profound consequences for individuals. When this is done sloppily, without protecting the rights of individuals, it is in breach of privacy laws. Notably, in the proposal for a European data protection regulation (General Data Protection Regulation, GDPR) much more stringent requirements are set for profiling.

Privacy by design

It is therefore important that all authorities (particularly those in the security domain) intending to make datasets available in the near future should think carefully about how they will do so. Making data accessible requires coordination between organizations, a new design of technical and non-technical processes within organizations, open data standards to which everyone adheres and a culture of openness, cooperation and trust.[3] Authorities sometimes use the privacy argument as a pretext for delaying making data available but making open data available can be easily embedded in regular processes under the right conditions. The management and storage of data must meet the stringent technical security requirements in Europe (and the US). The correct anonymity techniques should also be applied. However, experience shows that this is only a first (technical) condition to unlocking data.

Organizations that unlock open data should immediately devote attention to privacy in the following ways:

- Properly identify internal roles and responsibilities with respect to privacy (governance): who is in charge, who monitors, and in what way accountability is applied;
- Properly describe the processes for handling personal data;
- Develop a framework within which the processing and exchange of personal data takes place. This should not only cover the legal framework but especially the governance aspect and policies. It should describe how organizations should deal with personal data, both internally and externally;
- Employees must have a sufficient level of privacy awareness to recognize privacy-sensitive situations. They can be trained in how to deal with specific situations. Good communication, both internally and towards the public, is essential.

The unlocking of data is an important part of the services provided by governments. At this time, the level of access to government data is still insufficient in many countries. Open data initiatives can only succeed when knowledge on privacy within certain governments improves greatly. Major opportunities exist when privacy legislation is respected and government organizations make privacy part of their daily methods of operation.

[1] Capgemini Consulting (2013) The Open Data Economy: Unlocking Economic Value by Opening Government and Public Data.

[2] McKinsey (2014) How Government Can Promote Open Data And Help Unleash Over $3 Trillion in Economic Value.

[3] NSBO, 'Open data, open gevolgen', 2012. OR [NBSO, 'Open Data, Open Consequences', 2012].

About the authors

Drs. Melle van den Berg and Christian Le Clercq MSc LLM are managing consultant and consultant, respectively, at Capgemini Consulting. Melle van den Berg specializes in cybersecurity and crisis management, while Christian Le Clercq specializes in privacy issues and policy implementation.

For more information,
please contact the authors:
melle.vanden.berg@capgemini.com,
@mellevdberg en
christian.le.clercq@capgemini.com, @cleclercq

Prevent digital intrusion with a Security Operations Center

How to set up an effective Security Operations Center

The correct design of the organization, processes, information and technology of a Security Operations Center (SOC) ensures the security of digital services.

Highlights

- As well as potential financial losses, security incidents can often result in reputational damage to organizations, customers and partners. A SOC ensures the early detection and prevention of digital attacks.
- The SOC combines technology with processes and procedures in order to deal with incidents while keeping the organization “in business”.
- A hybrid SOC combines external expertise with the in-depth knowledge from within the organization.
- A well-designed SOC answers the current needs of the organization while utilizing the knowledge of its employees, but also ensures that it can expand in the future.

Introduction

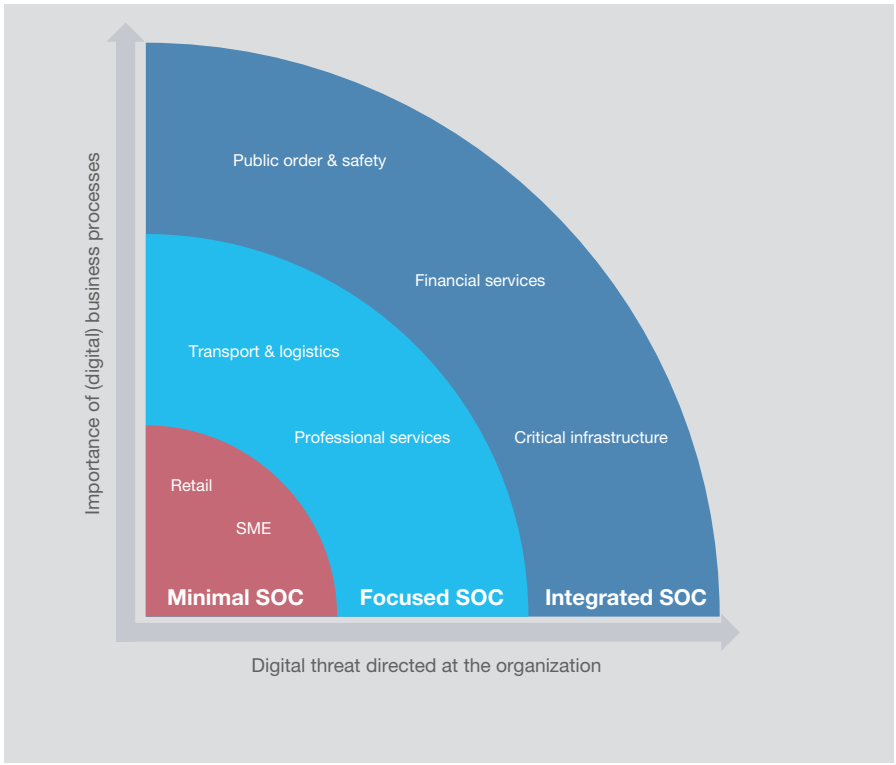
Organizations increasingly communicate with their customers through digital means, as well as with their partners and other companies. This leads to an efficient and customer-oriented organization but, at the same time, introduces risks concerning the reliability and continuity of the information technology within the organization. These risks can lead to high-impact problems, such as a government’s digital portal becoming (temporarily) unavailable, an online retailer being unable to sell its goods due to its website being hacked, or customers being unable to book airline tickets online because the company website is under cyber attack. It is no longer sufficient simply to create a large ‘digital fence’ around the organization. Above all, securing information requires the early detection and timely mitigation of digital threats. A so-called Security Operations Center (SOC) can play a key role in this.

The added value of a Security Operations Center

A SOC is the part of an organization that focuses specifically on the early detection and prevention of cybersecurity-related incidents. A SOC combines the technology to monitor, detect and prevent digital intrusion with procedures that deal with these incidents effectively and keep the organization “in business”. In this way, the SOC supports the organization in maintaining secure digital business operations.

A SOC focuses not only on securing digital communication within the company but also enables the company to provide secure digital services to its customers, other companies and partners. To enable the company to provide secure digital services, the SOC employs systems that collect real-time information from the information flows within the organization and from its customers and partners. This information is analyzed using advanced techniques so that cyber attacks can be prevented before they cause any actual damage.

Figure 1: The need for and added value of a Security Operations Center.



The importance of digital business operations to the organization and the cyber threat level determine the necessity and added value of the SOC (see figure 1). For example, a bank or a Department of Defense organization requires more extensive SOC services to protect its information assets than a retail company. The design and structure of a SOC therefore depends on the desired breadth and quality of the service provided. The ensure that the SOC attributes to the company's objectives, its mission and its services catalogue should be based on the needs and risks to information security of the primary business processes.

When setting up an SOC, it is necessary to take into account the essential design principles combined with the axes of the operating model: *people and organizations, processes, technology and information.*

Setting up a Security Operations Center

Due to the large initial investment required, few organizations have taken the step of setting up a complete SOC independently. Instead, many organizations choose a hybrid SOC model, in which parts of the SOC are implemented internally and other parts are outsourced to a specialized service provider.

Figure 2: Design principles dictate how the SOC should be set up.

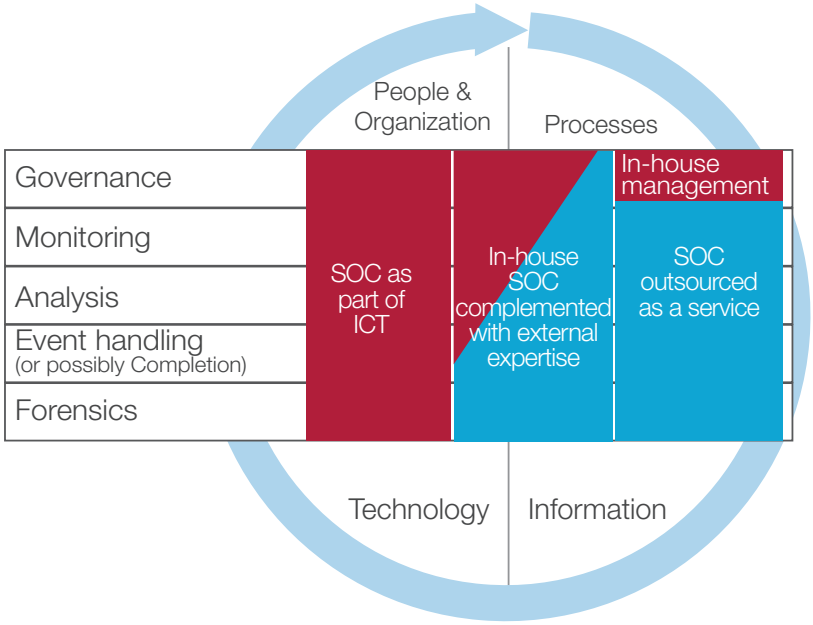


Figure 2 presents a number of alternatives for setting up a SOC. All SOCs incorporate a number of fixed areas of responsibility. The governance function ensures the embedding of the SOC within the organization as well as the management of the SOC. The core of the SOC consists of operational processes, such as (real-time) monitoring of the information flows within the organization. SOC employees analyze suspicious data traffic and irregular transactions. In the event of an actual incident, such as a digital intrusion or network disturbance, they are also responsible for handling and resolving the incident. A forensic investigation may be conducted to help identify the perpetrators.

A SOC is an integrated assembly of people & organization, processes, information and technology. The aforementioned task areas should be arranged along these axes in the operating model. People & organization concerns the organizational structure of the SOC and its placement within the organization. The SOC's scope must therefore be derived from the corporate objective. The administrative, operational and technological processes within the SOC should be arranged to match this objective. The most critical flow of information within the organization (the 'crown jewels') is determined based on risk analyses and is monitored, analyzed and protected with high priority by the SOC. For integrated risk management in relation to information security, please refer to the article 'The business value of security starts with a common framework' by Laurens van Nes. The choices made here also determine which technological support is required.

Some organizations, particularly those in the law and order and public security sectors, opt to set up a SOC entirely in-house, given the sensitivity and importance of their information assets. Other organizations benefit from outsourcing certain tasks, by bringing in the appropriate knowledge and experience required for an effective and efficient SOC, thus enabling them to focus on their core business.

The hybrid SOC model

In a hybrid model of a SOC (or hybrid SOC) certain tasks are performed in-house (for example, because specific knowledge from within the organization is required or because certain information must remain within the organization by law), while other tasks are outsourced because the organization does not have the staff or knowledge available to perform them.

The table on the next page illustrates the design of a hybrid SOC. The most important design choices are shown along the axes of the operating model. In the column to the far right, these are translated into the hybrid model. By setting up the SOC along these axes, it will fit optimally within the existing organization while allowing it to expand to meet changing needs.

Element	Design choices	Hybrid SOC
People & Organization	1. Where to assign the responsibility of the SOC? 2. Do we want a centralized or decentralized set-up? 3. Do everything in-house or outsource certain tasks? 4. Allocate staff internally or attract external staff?	A SOC should contribute to the organization's corporate objectives. Therefore, it is essential that the SOC is assigned to a representative of the primary process, preferably to someone from C-level management. A hybrid SOC combines external expertise with in-depth knowledge from within the organization. For most organizations a centralized SOC is preferred, with possible decentralized operations centers when office locations are far apart geographically.
Processes	1. Which SOC processes should be performed internally and which should be outsourced? 2. How are guidance and quality control ensured?	To enable the hybrid SOC to function effectively, the internal processes and outsourced processes must be aligned. The SOC's management should be embedded within the organization itself. To ensure that the organization's mission and vision are reflected in the SOC's objective, the governance processes should be established internally. Specialized tasks, such as in-depth analyses and forensic research, can be outsourced to a specialized party to maximize efficiency and performance.
Information	1. Which business processes and what business information should be protected first? 2. What information is collected by the SOC, in what detail and how frequently? 3. Which analysis methods should be used for the early detection of digital intrusions?	In order to add value swiftly, it is important to start by protecting data with the highest value (the so called 'crown jewels'). Hence, start by determining which data streams should be monitored, in what way events are filtered, in what detail data is analyzed and how the results are dealt with in terms of handling and reporting. Some data could be business-sensitive or privacy-sensitive, or subject to laws and regulations. A risk analysis will help to determine which data are most vulnerable and what measures are needed to protect the integrity and confidentiality of the data.
Technology	1. How can the new SOC technology be connected to the existing infrastructure as efficiently as possible? 2. What technical support is required - for operational processes and for management purposes?	The hybrid model employs the technology of an outsourcing partner to collect and analyze data. At the same time, the SOC's staff should have sufficient access to allow them to perform their duties. It is important that the new technology is aligned with the existing technical facilities within the organization. Choosing the required technological support will largely be based on economic considerations. It is therefore important to select software and hardware that match the current needs of the organization and employees' knowledge, but which also have the potential for future growth. The aforementioned design choices will help to set up a mature SOC. One trend that will be increasingly prevalent over the next few years is the Security Intelligence Center (SIC), in which advanced post-incident analysis and forensic research are performed on large amounts of data. Because of its improved analysis capacity the SIC will have a better defense against prolonged and targeted cyber attacks (so-called advanced persistent threats). We will also see SOC services in the Cloud more often, such as SIEM-on-top-of-Cloud.

Conclusion

In the next few years, organizations will increasingly transform into modern, digital, customer-oriented service providers. This requires digitization of the channels through which they communicate with customers, corporations and partners. But it also requires innovation of processes and ICT aimed at working digitally. An essential condition of this is that the reliability, security and privacy of digital services provided by governments and businesses are properly safeguarded. This condition can only be met if cybersecurity is addressed proactively through the deployment of a Security Operations Center.

About the authors

Michail Theuns MSc is a cyber-security consultant and Roger Wannee is a principal consultant at Capgemini. Both are active in the field of public order and safety. They help clients in solving issues related to cyber-security, crisis management, policy implementation and business management.

For more information,
please contact the authors
michail.theuns@capgemini.com
roger.wannee@capgemini.com

The new privacy regulation requires a risk-based approach

Is a Privacy Impact Assessment (PIA) sufficient for the legitimate processing of personal data?

The new European privacy regulation is mandatory in relation to the protection of personal data. Performing a Privacy Impact Assessment alone is insufficient.

Highlights

- Increasing globalization and digitization call for a reform of the EU privacy directive in 2015.
- More and more personal data is being recorded and shared (e.g. the biometric passport).
- The introduction of the obligation to report data breaches and mandatory Privacy Impact Assessments.
- The scope of the Privacy Impact Assessment as a risk-assessment tool.

Privacy Legislation

In an increasingly digital world, in which organizations often process data using information systems, organizations are being forced to deal with privacy legislation. Organizations that process personal data must conform to privacy guidelines. To protect individuals against improper or careless handling of personal data, the European Union created a privacy directive in 1995. However, this European privacy directive was interpreted differently by each member state. To transform this patchwork of privacy legislation into a uniform package, a European directive was drafted, which is expected to be implemented in 2016. Once this directive has been implemented, the same interpretation of privacy laws will apply in each member state. One of the consequences of this is the mandatory Privacy Impact Assessment for all organizations that process personal data.

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a tool that helps in the early recognition of privacy risks that occur when processing personal data. A PIA consists of a focused questionnaire that adopts a structured approach towards exposing the (negative) consequences of processing personal data. Its

questions are linked to privacy principles, namely: data minimization, data quality, purpose limitation, limitation of data usage, compatibility of further processing, data security, transparency, the rights of those concerned and accountability. The PIA provides insight into the impact of processing personal data, both to individuals and the organization, and where this impact is localized. In this way, privacy risks are identified as early as possible. Moreover, an image is formed of the type of data that may be legitimately processed by the organization..

A properly executed PIA contributes towards improved data quality and improved services based on the data. An additional benefit is that the privacy awareness of the individuals involved increases. A PIA is organization-independent and can be implemented in all types of organization. Preferably, this instrument should be applied as early as possible; in the design phase of a process and information system (Privacy by Design). This avoids the need for costly changes, such as redesigning the process or information system at a later stage.

PIA coverage

Based on the results of the PIA, a risk-based approach should be followed to determine the proper design of the process and the supporting information. The PIA offers an insight into the vulnerability of the personal data being processed. The measures required to protect these personal data result from the risk analysis mentioned below.

Figure 1 shows the place of the PIA in the analysis carried out during the design of a new process and/or information system, or during a relevant change to an existing situation. The PIA is of particular importance in establishing a baseline for possible existing measures and the information security of a risk analysis. Carrying out a PIA as a sole measure is usually insufficient to meet statutory demands; a PIA is certainly not a risk analysis. To meet requirements and thereby improve the protection of personal data, a risk analysis must also be performed.

Figure 1: Place of the PIA in the Capgemini Risk Framework

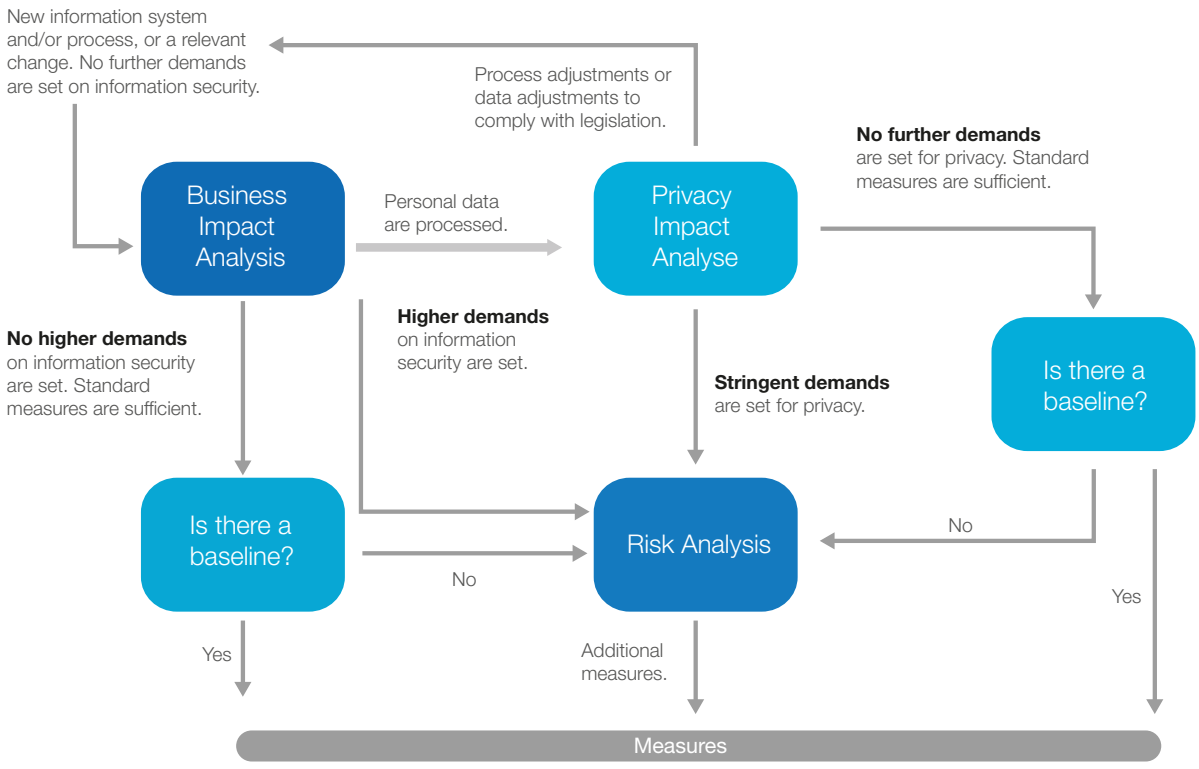


Figure 1 shows the place of the PIA in the analysis carried out during the design of a new process and/or information system, resulting from a relevant change to an existing situation. The PIA is of particular importance in establishing a baseline for possibly existing measures and the information security of a risk analysis.

A risk analysis provides an insight into the demands placed on a process and its information supply, in terms of availability, integrity and confidentiality. Because these risks are mapped from a privacy perspective, the point of view of the person involved, whose personal data is at stake, is always taken. Based on a risk assessment, the risk analysis describes the security measures that need to be introduced. Whether this information comes from one person or several people is unimportant. As the required confidence level becomes higher, further and tougher security measures must be implemented. The implementation of appropriate security measures remains a management decision.

The PIA and the duty to report data leaks

Once an incident concerning the protection of personal data has occurred, the supervisor and those concerned (data subjects) must be notified immediately – depending on the severity of the incident. Organizations that do not report a data breach will be penalized with an administrative fine, the amount of which depends on the extent of the data breach. To demonstrate that appropriate security measures have been taken, organizations must prove that at the very least privacy risks have been considered and demonstrate this by producing a completed and documented PIA and risk analysis.

Measures to ensure privacy

The necessary security measures are determined based on the results of the PIA and the risk analysis. To ensure good coverage of the risks, certain measures (based on the ISO 27002 standard) are required at minimum:

Information security and privacy policies

Information security & privacy policies should be established at the administrative level of the organization. Moreover, the organization should clearly convey how it deals with the issue of privacy. The legal requirements and the ambition of the organization in terms of privacy are expressed through an established privacy policy.

Assigning responsibilities

The management process relating to information security and privacy must be established by assigning responsibilities. From a legal perspective, the organization's management (directors) has the final responsibility. For the processing of (personal) data, monitoring may be delegated to an officer for data protection. Where information security is concerned, this may be delegated to the Information Security Officer (CISO in large organizations).

Security and privacy awareness

TInsufficient awareness of the privacy and security responsibilities of staff in an organization can lead to an increase in the risk of errors in the processing of (personal) data. A training program on security and privacy policy, with attention paid to dealing with (personal) data, should help to raise awareness levels among employees.

Implementing security measures

The measures recommended in the risk assessment should be implemented within the organization. These should take into consideration, for instance, physical security measures, access to equipment and logical security access to information systems and security. In this context, it is important to prevent unauthorized access to information systems and information, to manage access and to observe foolproof procedures. In addition, an important role is assigned to logging and review, which are important for detecting a data breach and complying with the right to carry out inspections.

Incident Management Process

The efficient handling of security incidents is necessary to respond quickly and appropriately to a data breach, for example. Specific attention should be paid to roles and responsibilities, to ensure that the right people ultimately report to the supervisor.

Tips for implementing a PIA

- Take into account that the PIA and analysis are not a cookbook. Their implementation requires expertise and experience.
- The PIA provides an insight into process and privacy risks, enabling the process to be carried out or the required collection of data to be adjusted. In addition, it is necessary to perform a risk assessment, because the privacy-sensitive data used must be suitably protected.
- The scope of the privacy analysis should be precisely determined at the outset, to ensure that the right people, in terms of roles and responsibilities, are part of the PIA.

Conclusion

The new European privacy regulation is expected to take effect in 2016 and ensures a mandatory standard for the protection of personal data. Adjustments include, among others, a mandatory Privacy Impact Assessment (PIA) and the “duty to report data leaks”. Hefty administrative fines can be avoided by organizing the handling of personal data within processes and information systems to conform to the new directive. Simply performing a PIA is insufficient, however. A risk-based approach to the processing of personal data in the design of new (or amendments to existing) processes and information (relating to personal data) will result in a complete picture of risks in terms of availability, integrity and confidentiality. Based on this combined/additional strategy, appropriate mitigating measures can be determined by those responsible.

About the authors

Lieke Schepers MSc, Jule Hintzbergen and Roger Wannee are, respectively, consultant, managing consultant and principal consultant in the field of public order and safety. Specifically, they focus on issues in the field of cybersecurity and the transformation of government processes and ICT.



For more information,
please contact the authors:
lieke.schepers@capgemini.com
jule.hintzbergen@capgemini.com
roger.wannee@capgemini.com

Strengthening resilience against digital service disruptions through preventative cyber stress testing

Is your organization prepared for a digital services disruption?

Highlights

- The question is not if digital services are affected by outages, but to what extent and how adequately an organization is able to recover from failures and outages.
- The emphasis of security measures shifts from defensibility to resilient intervention. This is measured by a "cyber stress test".

On December 16, 2014 nu.nl, a dutch news website reported: "In the past 12 months, the Dutch bank ING had the most outage days of all banks worldwide. This is the conclusion of Dutch website 'Allestoringen.nl', which relies on information collected in 27 countries."
Disruptions and outages of digital services are increasingly often in the news. 'Allesstoringen.nl, like downdetector.com, document the failure of digital services. These websites record everything from major malfunctions to isolated or small incidents. Both commercial services and government services are measured 24/7. Remarkably, all forms of digital service are more or less equally affected by disruptions. So the question is not if digital services are affected by outages, but to what extent and how adequately an organization is able to recover from these outages. The 'resilience' of organizations is even more important when it pertains to digital services that are critical to us or to society as a whole.

Dependence on digital services

Digital services have become an integral part of our daily lives. Just think of online banking or shopping, or the use of a smartcard for public transport, which is common practice in many countries. Filing a tax return is an online process in many countries nowadays. Our personal mailboxes are online and often in the Cloud too, when supplied by Google, Microsoft or Apple, for example.

Organizations are digitizing rapidly and increasingly developing critical services online. When disaster strikes or in

times of crisis, phones are used as an emergency communication system. If the website of a major supermarket chain is down on Christmas Day, we would encounter some problems preparing our Christmas Dinner. Society can no longer function smoothly without effective and secure digital services. Disruptions have an enormous impact on our society. Both organizations and individual users rely on the safety and efficacy of digital systems. Or, to quote the European Commission: "The more we depend on the internet - the more we depend on its security".

Increasing disruption to digital services

Disruptions to digital services take various forms, ranging from system errors or directly disruptive activities, such as DDoS attacks and indirect disruptions, which are caused by activities aimed at stealing sensitive and valuable data and information.

In the past year, a large number of disruptions were seen globally, having a significant impact on the digital services of organizations such as Amazon, Google, Apple and the RBS Group. The main question is whether these organizations were prepared for the disruptions and the impact they had on their customers, employees and, ultimately, the organization's business result.

Digital disruptions introduce a relatively new dimension to the wide range of problems that can affect an organization. They are therefore an addition to the set of existing security risks of an organization. Because of this, digital security is a necessary prerequisite for the continuity of an organization and must be part of an integrated security approach. The ongoing digitization of our society requires organizations to not underestimate digital disturbances and for them to take the necessary actions to avoid or recover from them.

Reaction to digital disruptions

Disruptions to digital services occur daily. Often there is an identifiable cause which can be resolved easily. Small organizations have their own network administrators, while large organizations have a professional Security Operations Center (SOC). These entities are expected to respond quickly and adequately to disruptions and to make sure a disruption does not escalate into an incident. Within the national crisis system, an 'incident' is seen as a relatively small event which disturbs public order to some extent and which is resolved reasonably easily and with the allocation of limited resources. An incident can be mitigated at an operational level but requires specific attention from a specialist. In some cases, a team of specialists is needed; this involves so-called "internal scaling".

An IT crisis is an event which has a great impact; such as an IT threat, a possible vulnerability or incident that threatens to damage the reliability, integrity or availability of vital parts of an organization. The severity is such that it cannot be dealt with in terms of decision making at an operational level. In the case of a crisis - as opposed to an incident - tactical and strategic dimensions are involved.

This system of defining the operational, tactical and strategic level of response is useful for both public and private parties. Each organization must identify the impact of a digital service disruption. The impact may be beyond IT and it is therefore critical to assess the business impact a digital services disruption causes. Is the disruption of a short-term nature? Does the disruption have an impact on primary services? Is there a risk to the continuity of the organization? Organizations in vital sectors in the Netherlands have the possibility to submit a request for help to the National Cyber Security Center. Other organizations have to resolve problems they encounter themselves.

Are we well prepared for the loss of digital services?

Suppose ING is indeed the bank with the world's most outage days or, in other words, has the lowest digital availability worldwide. As an ING customer, I would say that the level of digital services provided by banks isn't that bad. Apart from a few hiccups, my experience with internet and mobile banking has been very satisfactory. Of course, there will be customers who have had a different experience. But generally speaking, there haven't been many hugely disruptive situations. However, based on the increasing number of disruptions to digital services - not only in the financial sector - it must be concluded that there should be more focus on preparation for the failure of digital services.

When planning, organizations should assume that one day they will have to deal with a disruption to their digital services. This implies that the security focus should shift from building higher digital walls (defensibility) to being able to respond in a resilient way. Detection of - and response to - disruption ('recovery') should be well organized. To minimize inconvenience to customers and the organization's own business processes, attention must be paid to restorative capacity and the management of continuity.

Especially in private organizations, a digital revolution is currently taking place. But the attention paid to loss of digital services is falling behind. Of course, the classic information security department will monitor systems and be prepared for failure. IT management monitors the availability, integrity and confidentiality of IT systems. Often, however, the organi zation relies completely on the notion that CISCO "has everything under control". It is very rare that the primary process is involved in the possibility of a system failure and therefore

the loss of service within the primary process. The emphasis in private organizations is placed mainly on the preparation and/or adoption of baselines, standards and frameworks for information security. Certification by an independent third party must then ensure that these measures are actually taken.

In a substantive examination, the high dynamics of cyber threats requires a dynamic approach, which takes into account the development of threats and the specific risk profile of the organization. The system has to be tested in realistic, actual scenarios. The surge of Distributed Denial of Service (DDoS) attacks in the Netherlands in 2013 showed that those organizations which were prepared through exercise attacks were more capable of absorbing the real attacks and quickly restoring their services. Unfortunately, for most affected organizations the 'practicing' started during the attack itself. How does an organization know if it really is defendable and resilient enough to withstand the cyber threats of today? Only through an exercise that approximates current reality: the 'cyber stress test'. The cyber stress test is a preventive measure which prepares employees for any emergency and also provides insight into the resilience of an organization. An added benefit of the test is increased awareness concerning knowledge, attitude and behavior. The best test is, of course, reality. But who wants to wait for that?

About the authors

Drs. Roeland de Koning and Maaike Willemsen MA are principal consultant and consultant, respectively, at Capgemini Consulting and are active in the field of public order and security. Their specific focus is on issues in the field of resilience, crisis management and testing.

For more information, please contact the authors:
roeland.de.koning@capgemini.com
maaike.willemsen@capgemini.com
@MFWillemsen

Publications

Are you interested in our other cybersecurity thought leadership reports and point of views? View our publications below.

The complete list of our cybersecurity solutions can be found at: http://www.capgemini.com/cybersecurity

Capgemini's FastTrack approach

In a world in which everyone is connected to everyone, through any device or the cloud, traditional security measures are no longer up to the task. Moreover companies that are entering through the Digital Transformation are facing new security challenges. That is why it is important to put focus on the one thing you can control - access. But how to take control?

View the video via: www.nl.capgemini.com/cybersecurity

Cybersecurity Strategic Consulting

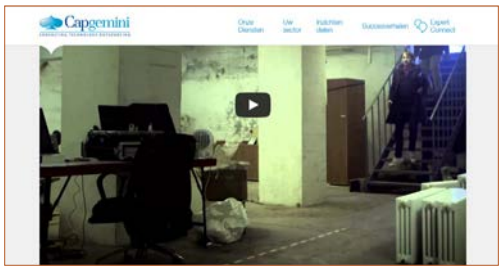
Is your cybersecurity in order? An important question because despite media attention, cyber incidents and awareness of cyber risks, organization are still facing cyber attacks every day. Capgemini's Cybersecurity strategic roadmap offer, helps clients develops a robust plan of action to remain safe from cyber attacks.

View the video via: www.nl.capgemini.com/cybersecurity

Testing the security of your applications

With 84% of security breaches occurring at the application layer, identifying vulnerabilities has become a priority for organizations worldwide. Many organizations now depend on the rapid release of critical applications to remain competitive. Our offering gives them a valuable layer of security by identifying vulnerabilities in the applications.

Download via: www.capgemini.com/cybersecurity

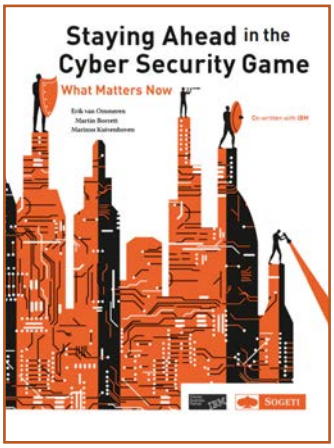


Cybercrime: Don't Fall into the Hands of Hackers

It is 9 am and two hackers are up to their tricks to glean vital information from Smit-Golders Capital.

Two scenarios. One safe option. Which one are you in?

Download via: www.capgemini.com/cybersecurity



Staying Ahead in the Cybersecurity Game

This essential book gives you the most recent and relevant topics on cybersecurity. It focuses on the organization, management and governance dimensions of security, whilst staying away from over-technical discussions. Each chapter highlights one of the most recent developments, what it means and why you should consider doing things differently as a result.

Download via: www.capgemini.com/cybersecurity

Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT

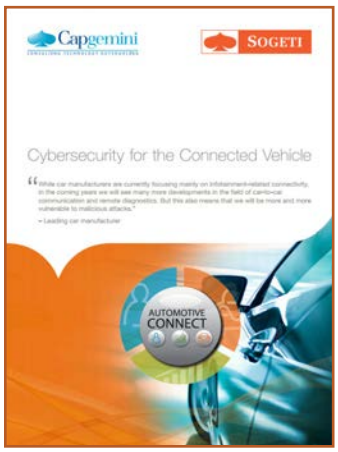
Why are organizations lagging behind in securing their IoT products and systems? Key reasons for this include an expanded attack surface, inefficiencies in the IoT product development process, and the lack of specialized security skill-sets. Building a secure IoT system begins with the recognition that security needs to be as much of a priority as the features and functionality of an IoT product. The report highlights the key measures that organizations must take in order to put security at the core of their IoT value proposition.

Download via: www.capgemini.com/cybersecurity

Security Operations Center: 24/7 IT Systems Monitoring

Watch how Energy City is able to track and stop security breaches around the clock thanks to a security operations center.

Download via: www.capgemini.com/cybersecurity



Cybersecurity for the Connected Vehicle

Security is not something that can be delegated to suppliers. OEMs need to take overall responsibility for security and make it central to their business. They must view the vehicle as part of a wider system and, in that context, take steps to secure both the existing fleet and new vehicles. OEMs that gain and fulfill the trust of their customers will also win a competitive advantage, and will be able to grow securely and confidently as digital enterprises

Download via: www.capgemini.com/cybersecurity

Trends in Security 2015

Trends in Security is an annual vision report from Capgemini where the most relevant developments in the field of public order and safety are showcased.
In this fifth edition, “Digital services in the security domain” is the central theme.

Download via: www.nl.capgemini.com/cybersecurity


Login

Colophon

Capgemini Nederland B.V.
Reykjavikplen 1
P.O. Box 2575 - 3500 GN Utrecht
Tel. + 31 30 689 00 00
www.nl.capgemini.com/cybersecurity

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

About Capgemini

With 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 2014 global revenues of EUR 10.573 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.nl.capgemini.com

Rightshore® is a trademark belonging to Capgemini.

Capgemini Nederland B.V.
Reykjavikplein 1
P.O. Box 2575 - 3500 GN Utrecht
Tel. + 31 30 689 00 00
www.nl.capgemini.com/cybersecurity

People matter, results count.