Chapter 2
Foundations of Cybersecurity

2.1 History

The use of **information systems** and the capabilities of the cyberspace became an integrated part of almost all companies and nearly every individual. Especially remarkable is the fact that the most important part of the cyberspace—the Internet—fundamentally transformed from an exclusive equipment of the government and academic institutions to an essential part of our whole society in less than three decades.

The beginning of the **Internet** is was primarily caused by the Advanced Research Project Agency (ARPA), which is an agency of the U.S. Department of Defense and today called Defense Advanced Research Projects Agency (DARPA). Its intention is to develop emerging technologies for military use. In the year 1969, it created the Advanced Research Projects Agency Network (ARPANET). The goal was to provide a computer network infrastructure that enables various universities to connect to each other and facilitate communication within research activities. It succeeded and the network was joined by more and more nodes over the following years. In 1973, European countries started to join the network, at first United Kingdom and Norway.

In 1981, the basic **protocols**, e.g. IPv4, for the connection and data transmission via the Internet were defined. They are still in use today. Due to the development of the Domain Name System (DNS) in 1984, the usage of human recognizable names for addressing computers within the Internet became possible.

In 1990, ARPANET was dissolved and remaining nodes were connected to the National Science Foundation Network (NSFNET). The NSFNET was created by the National Science Foundation (NSF) in 1979 and was formerly known as Computer Science Network (CSNET). The **commercialization** of the Internet began in 1991 when the NSF modified its acceptable use policy to allow commercial use, which was forbidden before.

S. Beissel, *Cybersecurity Investments*, Progress in IS,
DOI 10.1007/978-3-319-30460-1_2

The Internet had been shaped strongly by the possibilities of content representation to the users. Tim Berners-Lee started in 1989 to develop the Hypertext Markup Language (HTML) that helps to create **webpages** and to make them readable by web browsers. HTML was publically available since 1991. The popularity of the Internet increased highly when the first graphics-capable browser, which was named Mosaic, had been released in 1993.

The intensive integration of interactive content beyond static webpages became widespread in 2004 when the term **Web 2.0** was popularized at the O'Reilly Media Web 2.0 conference. Web 2.0 enhanced the interaction and collaboration between users and made user-generated content popular. The understanding of roles changed, because the internet users were no longer just content viewers, but furthermore, they were creators of their own content.

Currently, one of the biggest trends within the Internet is commonly known as **cloud computing**. Infrastructure, platform and application usage is offered and provided via the Internet to cover exactly the need of the users. They benefit from high flexibility in IT usage, and reduced complexity and costs of IT resources. They do not need to invest in hardware and software anymore. They just have to pay for services. The beginning of cloud computing is difficult to isolate, because even at the beginning of the Internet in 1969, the vision to be interconnected and access resources from everywhere was generally present. Surely, Microsoft, Google and Apple have a big influence by providing reliable and easy consumable services for the public.

Cybersecurity is as old as the cyberspace. Therefore, it is quite as old as the computer. However, real importance of cybersecurity has not been raised until the Internet became open to public access.

The first **cyber threat** was developed in 1989—just before the Internet provided new broad access possibilities beyond universities. The creator of the first cyber threat was Robert Morris, who understood to integrate self-propagating mechanism into the first computer worm. By this threat, highly malicious software vulnerabilities in UNIX systems had been exploited so that these systems became unusable. In result, the first widespread attack had been performed, which impaired the availability of many computers. In the following years, a vast number of viruses and other cyber threats had been developed. The number of threats strongly increased over time. Although the numbers move up and down from year to year, a trend of a general increase in vulnerabilities (Symantec 2015, p. 36) and security breaches (Identity Theft Resource Center 2015) can be seen clearly, as shown in Fig. 2.1.

The **threat landscape**, and the Internet security as a whole, is characterized by constant change. In the recent past, far-reaching vulnerabilities, faster attacks, files held for ransom, and far more malicious code than in previous years have been seen (Symantec 2015, p. 5).

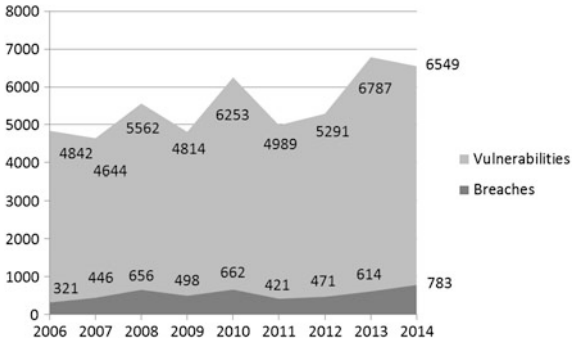

Fig. 2.1 Trend of vulnerabilities and breaches

2.2 Cybersecurity Principles

The **cyberspace** has been formed by the interconnection of information systems to computer networks, like the Internet. It enhances the capabilities of information systems broadly. These networks, especially the Internet, lead to a variety of benefits for company and personal use. Companies can reach an enormous number of potential customers. They can exchange time sensitive information around the globe in seconds. In addition, they can build an own cluster of knowledge, which can be accessed independent from the users' location. They can also participate from existing online communities. Individuals are enjoying the conveniences of the timeliness, transparency and comprehensiveness of information from the cyberspace. They are able to use constantly available shopping opportunities, communication possibilities from everywhere and an extensive knowledgebase.

However, the huge capabilities of the cyberspace are combined with serious **risks** for all connected information systems. Thereby, all information-related values could be at risk and potentially endanger the viability of whole companies, and the financial and personal safety of individuals. These risks are the consequences of countless threats mainly accompanied by the openness of the Internet. Sensitive or classified information could be stolen and misused. For example, competitors could gain advantage from strategic business information or criminals could misuse personal information for the purpose of identity theft or financial fraud. Important and valuable information could be manipulated or damaged. For example, criminals could manipulate the amount of financial transactions or damage files that are essential for business conduction, like customer records. Information systems and, thereby, all stored information could be unavailable because of attacks over the Internet, like a flooding with requests or a harmful infiltration of crucial information systems.

Cybersecurity includes all activities and measures intended to prevent and cover any threats regarding information systems connected to the cyberspace. The prevention of stealing and misusing sensitive or classified information is covered by the principle of confidentiality. The prevention of manipulating or damaging information is covered by the principle of integrity. The prevention of attacks

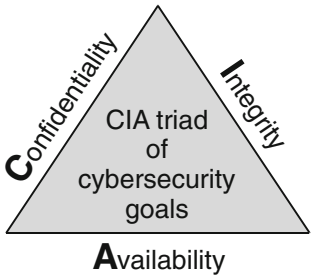

Fig. 2.2 CIA triad

against the availability of information systems is covered by the principle of availability. These are the three **basic principles** of cybersecurity (see Sect. 2.2.1 for details), which are often described as the CIA triad (see Fig. 2.2), relating to the first letters of these principles.

Furthermore, **extended principles** can be defined that correspond more or less with the above-mentioned basic cybersecurity principles. The extended principles are access control, regularity, legal certainty, authenticity, non-contestability, traceability, non-repudiation, accountability and reliability (see Sect. 2.2.2 for details). It strongly depends on the company which of the extended principles are desirable and sought. For some companies, accountability is very important while, for others, it is of less importance, e.g. because they might have such strict technical controls that performance deviations are prevented or quickly noticed. Some companies could seek obscurity to enhance the protection of their information assets while others could value transparency and pursue security by design.

2.2.1 Basic Cybersecurity Principles

2.2.1.1 Confidentiality

Confidentiality means that only authorized individuals or information systems should be able to **access information** that is not intended for the public. This can be achieved by preventing or disturbing activities of unauthorized individuals and systems that aim at the secrecy of private or business information. Attackers try to bypass technical or organizational safeguards in order to unveil information that can be used e.g. for their financial benefit or for harming their competitors. If this bypassing was successful and secret information could be read, the affected information would have been compromised.

Compromise of information and the subsequent misuse can lead to serious damages for the life, health and privacy of individuals as well as the existence of companies. Examples for information influencing the life and health are current medical data, and control data for critical systems. Not only can the data itself be worth to be protected, but also information about the communication process.

Information about which individual transferred or received data from specific sources or sinks can be very sensitive. After compromise, the concerned information could be misused to harm individuals or to disturb life-sustaining systems. Information about the informational self-determination and private interests, e.g. politics and religion, impair the privacy of individuals when compromised. The disclosure of such information could be uncomfortable or even defamatory. A company will be seriously affected, if e.g. secret research results and strategic plans are compromised. This can affect the competitive advantage as well as the financial or reputational situation of the company, possibly leading to bankruptcy.

Common **safeguards** for ensuring confidentiality are access control and encryption. Access control ensures that only authorized persons are allowed to access sensitive data within the company environment. For example, this can be implemented by Microsoft's active directory. However, if data leaves the company, access control will often be more difficult to operate than encryption. Encryption protects data on the hard drive or on the transmission path. The data can only be read by authorized persons that have the decryption key.

2.2.1.2 Integrity

Integrity is a condition, where information and information systems are fully protected against any kind of **manipulation or damage**. Thereby, it can be assured that the information is hundred percent correct. If facts of the real world are reflected by the information, it will have to include the truth without missing essential parts. The information must not be altered in any unintentional or undesirable way, neither by an individual nor by any kind of information system. If alteration of information cannot be excluded, at least, the alteration will have to be discovered and traced reliably. In addition, particular conditions can be essential for the integrity of information. For example, sequences or maximum delay times of transferred data over a network can be important. If the data transfer is not in correct order or if it is delayed too long, the receiver will no longer assume that the integrity of the related information has been met.

In order to ensure the integrity of information fully, both the unintentional and the malicious **type** of data modification must be taken into account. The unintentional part can be the result from technical defects or human errors. The malicious part can be the result from illegal or, at least, unethical attempts of individuals to gain any kind of benefits or to harm their opponents.

Common **safeguards** for protecting data integrity are hashing, and change management. Hashing includes the creation of check sums that can be used to detect if data has been changed. Changes can always be detected because even a small change within a file leads to a different check sum. With hashing, data can be regularly checked regarding intentional or unintentional changes within the company or on the transmission path. Change management is an administrative safeguard that requires all employees to change important data systematically and in a traceable way.

2.2.1.3 Availability

Availability is present if all systems and infrastructure components that are necessary to access and process information are ready for use and if they have sufficient capacity to process all requests quickly enough. The availability is importance because **time** is a valuable resource that can lead to serious benefits or drawbacks in conducting business tasks. Some business processes are time-critical, e.g. because of contractual agreements with customers, or dependencies to other processes. The delay of processes could result in high revenue-losses. External conditions can also lead to time-critical tasks, e.g. the transportation of perishable foodstuffs. The unavailability of crucial information usually delays the affected business processes. For example, a truck driver cannot look into the routing information of his GPS navigation system and has to make a long stop in order to read paper-based maps, and to plan his route manually.

The **capacity** of information systems can also have a serious impact on the availability. An example is a file server that cannot process any write commands because the hard disk storage capacity is completely occupied. Another example is a business application system that cannot be used by more than ten persons at the same time due to license restrictions. In order to protect the availability against capacity problems, all resources required to deliver the needed services must be controlled. In addition, all plans for short, medium and long-term business requirements must be taken into account. For example, a dramatically increase of costumer requests could lead to a high utilization of front-end systems.

Common **indicators** for rating the availability are the downtime und uptime. The downtime indicates how long a system or service was not available, and the uptime indicates how long a system or service has been run without problems or disruptions. Therefore, the availability can be expressed by the ratio of uptime to the sum of uptime and downtime:

$$Availability = \frac{Uptime}{Uptime + Downtime}$$

Another way to calculate the availability is the consideration of time to repair. It is assumed that every failure of a system or service needs to be repaired, and that during the time to repair, the system or service is not usable. The mean time between the occurrences of two sequential failures is called Mean Time Between Failures (MTBF) and the mean time needed to repair a failure is called Mean Time To Repair (MTTR). The availability can be expressed by the ratio of MTBF to the sum of MTBF and MTTR:

$$Availability = \frac{MTBF}{MTBF + MTTR}$$

The scheduled unavailability that is caused by maintenance events is not taken into the account by this formula.

Technical redundancy helps to increase availability rates further. By parallel processing capabilities, the overall availability will only be disrupted if all parallel nodes, e.g. similar servers, are down. The more nodes are present, the higher is the availability:

$$Availability_{overall} = 1 - (1 - Availability_{node})^{number\ of\ nodes}$$

Low availability rates can have a high negative impact on the efficiency of the company's supply chain or on the customer opinion. Availability rates will be of particular importance if the company must meet a service level agreement. If the actual availability rates are below the agreed ones, the company can be obligated to pay penalties.

Common **safeguards** that serve the protection of availability are backups and resilience: Backups ensure that data that has been lost or damaged can be recovered. The more often backups are made, the less data can get lost. Due to the required recovery time, the affected systems are temporarily unavailable. Unavailability can be prevented largely by raising the resilience of a system. Resilience means that a system becomes robust against negative influences. For example, an uninterrupted power supply raises the resilience of a system against power outages. Redundant hardware components, e.g. power supply units and hard drives, raise the resilience of a system against hardware failures.

2.2.2 Extended Cybersecurity Principles

2.2.2.1 Access Control

Access control is necessary to control the access to resources, including sensitive information and information systems. The idea is to **restrict access** as much as possible so that unauthorized individuals and potential criminals are not able to misuse access rights that actually would not have been necessary for business operations. The area of access control can be very challenging if a large number of users must be matched to a large number of resources, which also can be affected by continuous changes of the company's environment.

The **stages** of access control mechanisms in sequential order are identification authentication and authorization:

1. The **identification** is used to obtain the identity of a subject, particularly an individual or information system. The identity can be represented by a username or any other kind of unique characteristic.
2. The **authentication** is the process to verify that the given identity is truth. Thereby, the theft and misuse of identity shall be hampered. Common authentication measures are something a person knows, e.g. passwords, and

something a person has, e.g. tokens. Besides of these, something a person is, e.g. fingerprints, is a more secure and sophisticated way of authentication.
3. The **authorization** starts only after the authentication was successful. It matches the subject to the assigned access rights and checks if the desired operation is allowed, and if it does not contradict with the assigned access rights. Only after the successful authorization, the intended operation can be conducted.

The principle of access control itself also has subsequent **principles** that are called least privilege, separation of duties and need to know:

- The principle of **least privilege** means that, per default, nobody should have any access rights. The access rights must be assigned to a user or a user group explicitly.
- The principle of **separation of duties** forbids that a workflow can be fully performed by a single person. By splitting the workflow among multiple users, the risk of fraud and errors can be strongly mitigated.
- The principle of **need to know** requires that all access rights must only be assigned to someone who definitely needs them to perform his or her job.

2.2.2.2 Regularity

The regularity implies **conformity** of IT objects and processes to all required rules, e.g. as stated within laws or contracts. These rules are not only be made by external parties, but also by the company itself. Most companies require their staff to comply with internal guidelines. To fully comply with these rules, the staff has not only "to do the right things", but also "to do the things right". The first means that they have to follow certain processes or to develop certain objects, while the second means that they have to fulfill necessary tasks in the required or approved way.

Which **rules** from external parties have to be taken into account by a company, strongly depends on the location and industry sector of the company and the applicable laws, standards and best practices. For example, the US law includes:

- The **Health Insurance Portability and Accountability Act** (HIPAA) is mandatory for healthcare organizations. It was enacted in 1996, and it is focused on the protection of confidential patient records.
- The **Gramm-Leach-Bliley Act** is mandatory for financial institutions. It was enacted in 1999, and it requires the protection of customer data in the financial sector. Financial institutions must comply with security standards and develop enterprise-wide security policies.
- The **Homeland Security Act** (HSA) contains requirements around security, including information security, and it was enacted in 2002. Among others, it includes the Federal Information Security Management Act (FISMA), which binds federal agencies to secure the information and information systems that support their operations and assets.

Some important **standards** that are related to cybersecurity are:

- The **ISO 27000** series includes several standards relating to IT security. The most important standards in this series are ISO 27001, which contains a process model for an information security management system, and ISO 27002, which was derived in 2005 from the former ISO 17799, and which describes specific control measures for IT security.
- The **Payment Card Industry Data Security Standard** (PCI DSS) is an industry-specific standard for the Payment Card Industry. It aims to improve the security of cardholder data. It includes requirements for data security, and information about related test methods. The PCI DSS will be binding if a company stores, processes or transmits cardholder and authentication data.
- The **National Institute of Standards and Technology** (NIST) provides a resource for various information security standards and guidelines. Among other things, it developed a cybersecurity framework, which utilizes risk management principles and best practices to protect critical infrastructure, and cryptographic standards, which give guidance regarding the usage of algorithms and keys.

Some authors of **best practices** that support cybersecurity are:

- The membership organization **ISACA** has published the framework Control Objectives for Information and Related Technology (COBIT). It is a comprehensive framework to assist companies in achieving sufficient control by the governance and management of IT, including information security.
- The **Center for Internet Security** (CIS) is a non-profit organization that is specialized in IT security recommendations for private and public companies. Very popular are the security benchmarks that are focused on hardening of information systems, e.g. by disabling services, uninstalling software and setting important system parameters.
- In the European area, the **European Network and Information Security Agency** (ENISA) provides best practices around information security, e.g. guidance in cloud computing, incident response and building trust.

2.2.2.3 Legal Certainty

A company will achieve legal certainty if the **rights and obligations** resulting from applicable legal requirements are sufficiently clear, predictable and controllable. Thereby, the legal situation helps to provide an orientation for business actions and a safety in case of legal infringements by others.

For a company, legal certainty is necessary because the **infringement** of binding laws could cause financial and reputational damage. The financial damage can result from compensations for business partners and from penalties from legislative institutions. In addition, fraud by business partners can cause financial damages, especially if they are not held fully accountable. The reputational damage corresponds with a negative impact on the public opinion about the company. The public could

avoid businesses with the company, on the one hand, because of ethical reasons, and, on the other hand, because people could assume unreliable work performance.

In order to achieve a sufficient legal certainty, a company should ensure to employ skilled **professionals**, who have solid knowledge in all relevant legal requirements. One option could be to hire a specialized law office. Contracts should be proofed very well regarding any rights and obligations. The work of the employees should be compliant to all relevant legal requirements, and it should be transparent so that this compliance can be proven in case of any dispute. This can be supported by well-trained employees who are supervised or audited sufficiently. Internal policies are an opportunity to restrict the work of the employees in order to ensure that no legal requirements are infringed. A log of all actions by business partners and costumers supports the preservation of evidence in case of fraud or any kind of disputes.

Furthermore, it should be considered that **internationally** operating companies are often faced to new legal situations that are caused by differences in legal requirements from country to country. Besides, to claim the own legal rights could be more or less difficult in other countries.

2.2.2.4 Authenticity

Authenticity means that someone or something has the characteristics of being **genuine and verifiable**. The reason behind authenticity is to get reliable indicators on how much trust should be granted to someone or something.

Authenticity is an important part of access control systems. Only a person or a system with an **identity** that was sufficiently proven should be able to get access to sensitive information and systems. Otherwise, attackers could be able to compromise, manipulate or disturb information and systems.

To prove a person's identity, three **factors** of authentication can generally be used. When two or three factors are combined, it is called two-factor or three-factor authentication. In particular, the three factors of authentication are:

- Something that the user **knows** is a secret information in the user's mind, e.g. a password. The longer and more complicated the information is, the more difficult it is to guess by an attacker. However, long and complicated information is quickly forgotten or written down by the user as a reminder.
- Something that the user **has** is an object owned by the user, e.g. a token. This object cannot be guessed, but there is a risk that it is stolen or lost.
- Something that the user **is** includes any biometric data about a user. Everything that makes a user unique can be used, e.g. a fingerprint, the tone of voice, the handwriting or the inner structure of the eye. This type of authentication can be very reliable, but the user acceptance could be difficult. Some controls like eye scanning can be uncomfortable for the users. Besides, if an attacker seeks to get biometric information by any means, the health and life of the users can be in danger.

In addition to identities, the **truthfulness** of documents, web pages and other kind of data need to be trusted often. Only the processing of trusted data can lead to reliable and sustainable results. For example, a fraudulent payment transaction should not be accepted. Otherwise, it should be challenged after processing so that the received payment can be refunded if possible. By sufficiently ensuring the authenticity of the cardholder, this situation can be avoided. Besides, web pages of companies are sensitive because they often have serious impacts on the costumer opinion and even provide purchasing and payment opportunities. By ensuring the authenticity of web pages, e.g. by digital certificates, the customers can be sure that a web page can be trusted and that it has not been spoofed.

Improper decisions made by authentication mechanisms are called false positives and false negatives:

- **False positives** are positive decisions about something that is actually false; therefore, these decisions should be negative. They are performed e.g. before granting access to a system. The authenticated person or object has not been sufficiently checked by the system. For example, access is achieved with a fake identity or a manipulated object.
- **False negatives** are negative decisions about something that is actually true; therefore, these decisions should be positive. The authenticated person or object is genuine and e.g. it has the right to access a particular system. However, by mistake the authentication was not proven genuine.

Furthermore, false negatives are also known as type one errors, and false positives as type two errors. False positives are generally much more **dangerous** than false negatives. False positives could lead to the situation that an attacker has access to sensitive information, while false negatives cause "only" inconveniences for rightful users.

2.2.2.5 Non-contestability

The term contestability refers to a situation when under legal conditions, particular rights and obligations can be declared **void or voidable**. Void rights and obligations are not valid from the beginning, and voidable ones are valid until they are repudiated or annulated. For example, a declaration of will could be void, if the person was under the influence of alcohol. A contract will be voidable if it is contested in court by one of the parties involved, but stays valid before.

Contestability can lead to the repudiation or annulation of **contracts**, which would be not enforceable anymore. If in consequence, previously legal transactions have to be rolled back, a huge administrative effort for a company can occur. Payments must be refunded and goods must be returned. Especially in case of huge and crucial business transactions, the contestability can cause big uncertainty and even financial damage. The company could already have initiated depending business transactions that are now built on an annulated contract. For example, after a contract with an important supplier has been concluded, multiple contracts with

customers could have been followed. After it becomes known that the first contract is voidable and will be annulated, the company could suffer from price calculations that cannot be retained with alternative suppliers. Also resulting from missing supplies, time restrictions from customers could be infringed, which could cause contractually agreed penalties.

Therefore, companies generally try to avoid contestability. Essentially, this can be achieved by supporting the knowledge generation by employees and raising the awareness regarding doubtful situations. Among others, the following **situations** should be particularly taken into account:

- Contracts could be voidable due to a **mistake of fact**. If the performance of a contract is significantly affected by a mistake regarding a fact, the contractual partner will be allowed to repudiate it.
- If the contractual partner is **not physically or mentally able** to fulfill the contract, e.g. due to intoxication, he will have a lack of capacity. That makes a contract voidable.
- **Threat, coercion, undue influence and false statements** also make a contract voidable by the contractual partner, who has been negatively affected by a dubious behavior.
- A contract that has been conducted by a **minor** is voidable and can be repudiated by the minor or a guardian of the minor. The age of majority is reached at the age of 18 years in most states.
- Contracts that involve the contractual partner in **illegal** activities, like prostitution and gambling, are void directly.
- If certain activities are **restrained**, e.g. the right to marry or to work, the contract will also be void.
- A contract that contains clauses against **public policy**—the common sense of the community regarding social and legal situations—is void, too. Among others, the stipulation of unfair disadvantages to other companies, and the custody of a child cannot be contractually defined.

2.2.2.6 Traceability

Generally, traceability can be sought for various reasons. From outside the cybersecurity domain, it is often understood as the possibility to follow someone's conclusions and to **understand** his decision. In addition, traceability can mean that every single step within a chain of activities can be repeated after they have already been performed. In cybersecurity, traceability is focused on logging and monitoring all relevant activities, e.g. administrative activities on sensitive information systems.

In cybersecurity, it is crucial to trace the action of users and administrators. Otherwise, persons cannot be held **accountable** after a breach. This could lead to an unconcerned and possibly fraudulent behavior of employees. In addition, external parties could gain rightful or wrongful access to company owned systems. For example, the technical support of a vendor could use remote access. Without a full

trace, nobody could know what exactly has been done by the remote user. Besides, a trace is very useful to support the monitoring of events. Particular events could be connected to user activities that facilitate the early detection and prevention of security breaches.

The **level of detail** that is used to generate traces depends on the preferences and capabilities of the systems' owners. At a less detailed level, only specific events could be logged, especially the ones that could possibly correspond to a security breach. At a more detailed level, all available information about user activities could be logged. Even a full video recording of his desktop can be possible. However, the more information has been logged, the more resources are used for tracing and the more difficult is the processing and monitoring of this information. The company should find the right balance between effort and security.

Although traceability is a security principle, in another context, it can also affect the security level of a company **negatively**. A company normally has a legitimate interest in logging all activities that could affect the security of sensitive information. However, traces that can be accessed by unauthorized persons could be a serious risk. Attackers would be able to analyze the user behavior and violate the privacy of users or the secrecy of sensitive information properties, e.g. the storage location. They could misuse this Meta information and discover additional vulnerabilities. Therefore, every company that generates traces must ensure a secure storage of these traces and enforce a strict policy of need-to-know. Besides, any kind of information regarding user behavior should be obscure because attackers often use this information to prepare a targeted attack.

2.2.2.7 Non-repudiation

Repudiation relates to sending and receiving data. If a person **denies** sending or receiving data and no one can prove otherwise, he will repudiate. The sender could repudiate sending data and the receiver could repudiate receiving data. The reason behind repudiation is mostly that a person does not want to be bound by the consequences of a data transmission, e.g. the approval of a payment transaction.

All measures a company implements to prevent repudiation have the purpose to achieve non-repudiation. Mostly, sufficient **evidence** is collected so that all sending and receiving are completely provable.

Within the private network of a company, non-repudiation is mostly achieved by requiring all users to enter unique **credentials** before using a company owned computer or accessing sensitive information. Thus, strong authentication systems can improve a strong non-repudiation.

One common possibility to achieve non-repudiation via the Internet is the usage of **digital signatures**. The evidence that a certain sender sent the data is generated by verifying his identity. Therefore, the data to be sent is encapsulated within a message that is signed. The signing is done by encrypting the hash value, or digital fingerprint, of the message with the private cryptographic key, which is only known by the sender. The receiver can verify the sender's identity by using the sender's

public key for the decryption of the hash value. If the public key fits to the previously used private key, the identity of the sender will be verified. This type of cryptography is called asymmetric. It utilizes two different keys for encryption and decryption. In contrast, both operations are performed with the same key when symmetric cryptography is used.

The evidence that the **receiver** received the data is generated e.g. by a registered e-mail. Registered e-mails require the receiver to confirm his identity before accessing the e-mail, e.g. by entering a secret key.

2.2.2.8 Accountability

Accountability is a similar, but slightly weaker principle than non-repudiation. Since non-repudiation is focused on preventing the repudiation by a sender or receiver of data, it also has to be clear who sent or received the data. The clear **identification** of someone who sent or received data is called accountability.

Accountability can be achieved by the same measures as non-repudiation. The **difference** is primarily that, for accountability, only the identification is needed while, for non-repudiation, also the material evidence is needed that the identification has not been spoofed.

For example, activities executed via a **shared user account** can only be assigned to a particular person if further information is available, e.g. a staffing schedule. If these activities can be assigned to a particular person, this person will be accountable. However, this person can repudiate the activities if the evidence is not material. In contrast, a unique user account that needs biometric authentication would be sufficient to prevent a repudiation by the person.

2.2.2.9 Reliability

Reliability is an attribute of a system, a person, or a process. It defines in which extend pre-defined **rules or requirements** are fulfilled so that the residual risk of violating these rules or requirements can be tolerated by all stakeholders. The pre-defined rules or requirements include mainly cybersecurity requirements, like confidentiality, integrity and availability.

There is a strong connection between **regularity and reliability**. The regularity defines and demands compliance to pre-defined rules. The reliability demands that a violation of these rules has to be so improbable that there is only a small residual risk.

Besides rules, there are requirements, especially of information systems, that affect the **quality**. Software or hardware errors, which lead to outages or damages, must also be minimal. Only after the risk of errors has been mitigated sufficiently, the systems can be called reliable. An indicator for reliable systems regarding errors is e.g. the MTBF, known from the area of availability.

2.3 Protection Level

The **protection level** indicates how well the information and information systems of a company are protected from attacks or disturbances. A protection level that provides a protection of hundred percent can hardly be reached. If it were reached, it would only be of short time due to the fast moving IT environment. Instead of seeking full protection, an appropriate protection level should be seen as sufficient. Costs and benefits of the safeguards should be put in an appropriate **balance**. How a company evaluates the appropriateness of safeguards for themselves depends on the individual preferences of the company. In practice, the company should find a protection level that, on the one hand, excludes unreasonably high risks and, on the other hand, does not require costly safeguards that strongly affect the profit expectations of the company.

The **appropriateness** of safeguards can be defined as their effectivity, suitability, practicality, acceptability and efficiency (Federal Office for Information Security 2008, p. 65):

- **Effectivity**: The safeguards must provide effective protection against the possible threats, i.e. they must fulfil the identified security requirements.
- **Suitability**: It must be actually possible to implement the safeguards in practice, which means they must not impair the organizational procedures or bypass other security safeguards.
- **Practicality**: The safeguards should be easy to understand, easy to apply, and not prone to errors.
- **Acceptance**: All users must be able to use the safeguards (barrier-free), and the safeguards must not discriminate or adversely affect anyone.
- **Efficiency**: With the resources used, the best possible results should be achieved. On the one hand, the safeguards should minimize the risks as much as possible. On the other hand, the cost of implementation should remain in proper proportion to the value of the protected objects.

2.4 Protection Scope

The **protection scope** is determined by identifying the assets that have a specific protection need and all components that are related to these assets. From the **technical** view of cybersecurity, primarily all technical components that store, process, or transmit sensitive information are within the scope:

- While **storing** information, in other words interpretable data, data is technically recorded on a disk. This is done in the form of binary data, which can be converted by systems into program or text data. While program data need to be interpreted by a compatible system, text data can be directly interpreted by humans. Media that store these data can be used either stationary or mobile.

Stationary media are integral parts of systems, like servers, workstations, or network storage. Mobile media, for example CDs, DVDs, tapes and SD cards, can be read by using drives. Other mobile media, for example USB hard drives, USB sticks and FireWire hard drives, can be connected directly to system interfaces. In order to use media storage more efficiently, data are often compressed. Before using compressed data, a performance-intensive decompression must be performed. Therefore, compression is only useful for data that does not have to be directly available.

- The **transfer** of information is performed when data are transferred from one system to another system. For transmission, local area networks (LAN), for example, within a company building, and wide area networks (WAN), such as the Internet, can be used. The infrastructure of local networks can be wired or wireless (WLAN). The protection of confidentiality and integrity of transmitted data plays an important role, in particular for transmissions over the public Internet.
- The **processing** of information includes the transformation of interpreted data into different formats or structures. For example, they can be merged, distributed, enriched, abstracted or otherwise transformed. Processing is often part of a business process or supports it. For example, a merchant, who is active in e-commerce, can process customer data after receiving orders. Among other processing steps, invoicing and shipping are based on these data. The processing can be triggered by a user, who uses an application, or by a time or an event, which triggers a system that begins processing automatically. An example for a time trigger is the start of a certain weekday. An example for an event trigger is the creation of an order by an e-commerce customer.

The technical **components** that should be included in the scope are not only servers and workstations, but also many infrastructure components that are could be overlooked quickly. Examples for these components are:

- Servers that provide network services, like authentication, name resolution or web redirection
- Network segmentation and connection components, like firewalls, routers, switches, hubs and wireless access points
- All applications that are available internally and externally, even if they are hosted by an external service provider
- Other devices that are connected to systems that handle sensitive data, e.g. printers and scanners

In addition, the **organizational** view must be considered. In particular, people that handle sensitive data and processes that use sensitive data must be taken into account while determining the scope.

The correct **determination** of the scope can be very challenging. On the one hand, it should be avoided that relevant components are seen as out-of-scope, although they should not be. These components will probably be not secured sufficiently so that a hacker could easily attack them. On the other hand, it should be

avoided that the scope is larger than it has to be. Sophisticated safeguards can be very costly so that components that should be out-of-scope can cause unreasonable costs if they are protected for no purpose. In order to determine the scope as accurate as possible, the following **tasks** should be performed:

1. Sensitive data should be defined so that sensitive data can be clearly distinguished from insensitive data.
2. The existence of sensitive data within the components in the scope should be verified.
3. The nonexistence of sensitive data within the components outside of the scope should be verified. If sensitive data are found outside of the scope, these data will have to be mitigated into the scope or securely deleted.
4. All locations of sensitive data and the related components should be documented, e.g. with a network diagram or an inventory list.

In order to reduce security requirements and testing needs for systems that process data, sensitive environments can be confined. Thereby, they can be isolated from systems with lower security requirements. Consequently, the scope of the sensitive environment has been **reduced**.

The limitation of scope is mainly useful under cost-benefit aspects. To assess the **cost-effectiveness** of the limitation, the investment costs and the operation costs must be compared to the potential savings. The investment costs include the cost of new hardware, software, and installation. In addition, organizational activities, e.g. developing work instructions and guidelines, must be considered. The operation costs include the costs of maintenance and administration of the new infrastructure. Potential savings from the limitation are caused by the fact that, in security design, development, administration and auditing, only systems within the limited scope must be considered. Thus, the effort regarding security can be reduced. In addition, the risk of compromise, manipulation or corruption of sensitive data and the subsequent damages can be reduced by a scope limitation. The administrative effort outside of the secure environment is also reduced because fewer requirements, e.g. regarding hardening, encryption, and logging, need to be implemented on the systems.

While limiting the scope, the potential need for future adjustments, in other words the **scalability**, should also be considered. If business changes and the data to be processed is affected, the company will have to scale the technology that is used to limit the scope. It can be necessary to scale the technology, if an outsourcing of data processing is planned and less sensitive data are processed internally.

Common **techniques** to limit the security scope within environments are tokenization, point-to-point encryption, network segmentation and outsourcing. While the first three techniques are based on technical means to isolate sensitive data, the last one is an organizational matter. In contrast to theses technical means, outsourcing does not reduce the security requirements in general, but rather shifts the duties to another party that has to protect the outsourced environment.

2.4.1 Network Segmentation

Network segmentation is used to **separate** the part of the network, where sensitive data are processed, from the remaining part in order to perform a targeted raise of the protection level. With the network segmentation, the access from insecure network segments to the secure network segment can be limited. Thus, many attack attempts can be blocked. The network segmentation serves to protect the confidentiality, integrity and availability because attack attempts of any kind can be blocked.

The technical **implementation** of the network separation (see Fig. 2.3) can be done with firewalls, routers, or switches with access control lists (ACL). Often, the connected systems are assigned logically to a virtual local area network (VLAN). ACLs can be used here so that the systems in the first segment—an isolated VLAN—cannot communicate with the systems in the second segment.

If network segmentation is implemented with **firewalls**, a standalone firewall will need to be positioned between the secure and the unsecure network environment. Firewalls can filter traffic. Thus, they provide the greatest possible protection in network segmentation. Firewalls and routers can connect network environments with different address ranges or architectures. This will be important if a network environment with a different architecture is present, which is supposed to exchange data with the secure network environment, e.g. for the remote maintenance of systems. **Routers** should be used for network segmentation if the traffic is not required to be filtered, but only to be passed between network environments. **Switches** do not have security features or filter options. If the switch model supports ACLs, it can only be configured with which network environment a system is allowed to communicate. Switches should be used for network segmentation if the network environments use both the same architecture and the same address range.

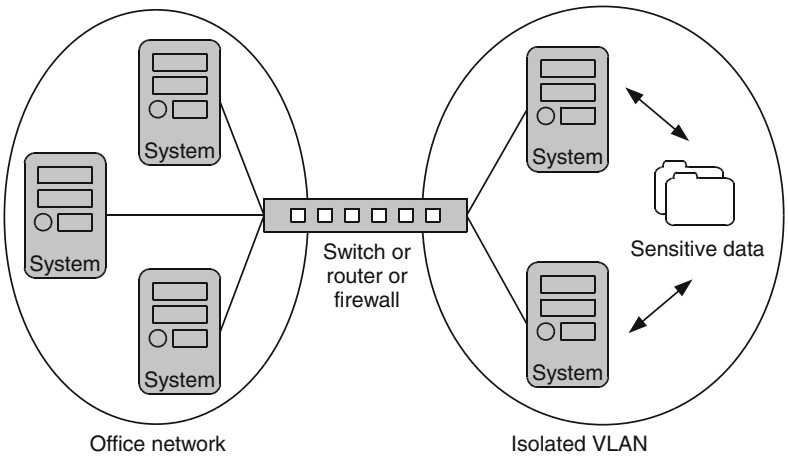

Fig. 2.3 Scope limitation with network segmentation

2.4.2 Point-to-Point Encryption

Point-to-point encryption allows **transmitting encrypted data** by encrypting the data at the starting point by the transmitter and decrypting the data at the end by the recipient. Therefore, all intermediate communication points no longer need to be in a secure environment. The point-to-point encryption prevents that tapped data can be read. If an attacker eavesdrops the network traffic, he will not be able to read the collected data. Consequently, it serves to protect the confidentiality.

On the side of the **transmitter**, an encryption component is used and, on the side of the **receiver**, a decryption component is used. These components can be a hardware module or software. Hardware modules are used e.g. in interaction points for card payments. For example, a transaction can be encrypted with this module on a payment terminal and decrypted with software in the secure environment of a payment service provider.

A distinction is made between the **symmetric and asymmetric** encryption technique: In the symmetric technique, the same key is used for encryption and decryption. In the asymmetric technique, data are encrypted with the public key and decrypted with the private key. The symmetric technique is much faster, but the asymmetric technique facilitates greater security because only the recipient is in possession of the decryption key. In practice, the symmetric and the asymmetric encryption technique are often combined (see Fig. 2.4). First, the transmitter sends its symmetric key to the recipient. To prevent that this key is intercepted by an attacker, it is encrypted using the public key of the recipient. Only the recipient is in possession of his private key and therefore only he can decrypt the symmetric key.

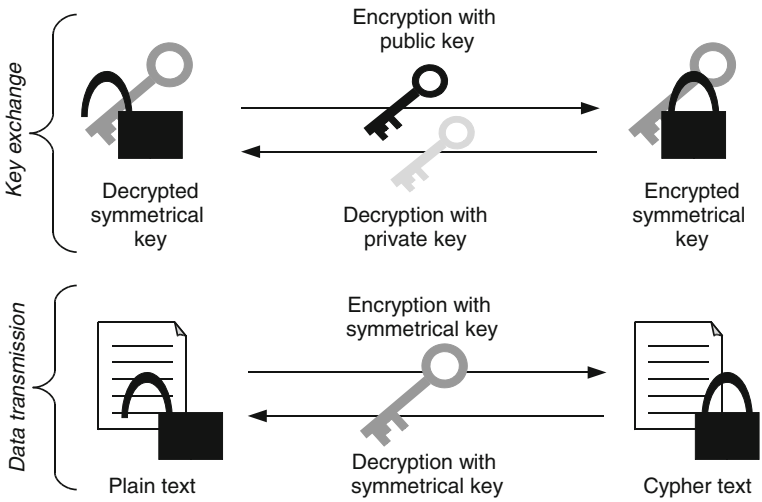

Fig. 2.4 Combined encryption

After both parties are in possession of the symmetric key, the transfer of the data, which is encrypted with the symmetric technique, can be performed.

When using point-to-point encryption, a **key management** must be operated. Thereby, it can be ensured that cryptographic keys are exchanged in case of a compromise or after a defined lifetime. Best Practices for key management have been published by the National Institute of Standards and Technology (NIST) in the Special Publication 800-57 (Barker et al. 2012, p 49 ff.). Each type of key has a certain recommended service lifetime. Private keys that are used to negotiate symmetric keys have a recommended lifetime of one to two years. Symmetric keys should be used for one month to encrypt data and can be used for several years to decrypt data.

2.4.3 Tokenization

Tokenization can be used if no special data contents are required within certain processing steps, but merely the unique **identification** of the data. Tokenization replaces sensitive data with tokens. It transforms sensitive data into anonymous strings—the tokens—that cannot be reconverted into the original data by an algorithm.

By using tokenization, systems that operate with tokens instead of sensitive data can be removed from the **secure network environment**. Tokenization prevents that sensitive data can be found and compromised in areas where only the uniqueness of the data is important. It serves to protect the confidentiality.

Tokens can be designed for single or multiple usage. In the **single usage**, a new token is created for each data value, e.g. a new consecutive number. In the **multiple usage**, always the same token is created for the same data. This usage facilitates cumulative evaluations.

The type of usage must be taken into account when choosing the **generation technique**: Encryption and hashing techniques automatically create the same token for the same data. If numbers are generated as tokens, an additional procedure should be integrated in order to reuse the same token for the same data value. The above-mentioned generation techniques are characterized as follows:

- If **encryption** technologies are used when generating tokens, the sensitive data will be encrypted and the resulting cipher text is used as a token. The possibility that tokens are transferred back to their original form is actually not needed or wanted in tokenization. The encryption key or algorithm could be hacked and, in result, the sensitive data could be compromised by hackers.
- **Hashing** is used to calculate small checksums from large data strings with an algorithm. Hashing is better suited for the generation of the tokens because the tokens cannot be transformed back into sensitive data. Although hashing was originally designed for integrity checks of data, the generated checksums are very suitable to be used as a token. However, the uniqueness of the token might

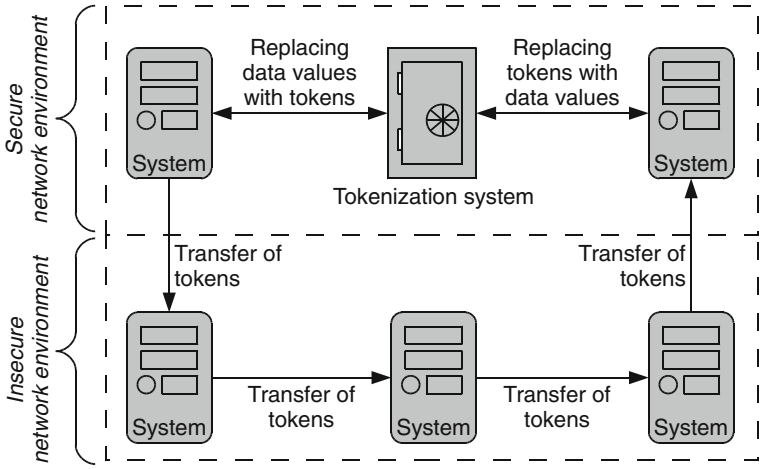

Fig. 2.5 Tokenization system and network environments

not be ensured if a hashing algorithm that is affected by collisions was used. Collisions occur if the same checksum is assigned to different data.

- Tokens can also be generated with **numbers**. Often, a serial number or a random number is used. In principle, any string can be used as a token. It just have to be ensured that it allows a unique identification, includes almost no collisions and cannot be easily converted back to its underlying original data.

Tokens cannot only be generated for individual data values, but also for a **combination** of two or more data values. Optionally, an additional data value (Salt) can be appended to the primary data before generating the token. This makes it more difficult for attackers to guess the original data.

Normally, the original data that is transformed into tokens is retained in its original form, too. The original data are stored in a highly secure environment. If a company wants to know which token represents which original data, an assignment of token to its original data will have to be performed. This is done with a **tokenization system** (see Fig. 2.5). Since the assignment is not possible by using mathematical algorithms alone, the tokenization system must provide association data. Besides the tokenization system, all systems that still process the original sensitive data should be positioned in a secure network environment and should be particularly protected.

2.4.4 Outsourcing

With outsourcing, certain business-related activities can be **transferred** to an external company. This company is contractually bound to perform these activities.

Outsourcing is a safeguard that can be also used to serve other security objectives (see Sect. 3.2.8).

However, in the context of scope limitation, especially those activities are transferred to external parties that include the processing of sensitive data. By transferring these activities and the according data out of the company, the necessary protection level can be reduced strongly. Thereby, activities that are affected by **high security requirements** are outsourced. In this case, it is important to specify the security requirements in the contract and to ensure that the contract is met by the external party. The security requirements should not only be specified in the outsourcing contract, but also related to claims for damages or contractual penalties in case of deviations. If the external party is specialized in high security activities, it can possibly provide a higher protection level than the outsourcing company itself. If several clients of the external party are interested in the protection, independent auditors will be hired to perform an objective audit and to certify compliance.

The outsourcing of activities will not keep the outsourcing company from taking **responsibility** if something goes wrong. The damages might be claimed against the external party, but in the public view, the outsourcing company is the one to blame. In conclusion, the outsourcing company should monitor the outsourced activities continuously. Therefore, the outsourcing company should have a current overview about which activities are outsourced and which are performed in-house. In consequence, the company has always an overview of in-house activities that can be used for planning audits. Auditors that are going to analyze in-house activities can save much effort if they use this overview as a starting point.

With outsourcing, the outsourcing company can optionally **transfer** assets, staff, buildings and existing contractual relationships to the service provider. Thereby, the outsourcing company can benefit from a high flexibility. No costly assets and buildings need to be unused and no staff need to be dismissed. Another advantage in transferring staff is that knowledge remains within the company. Staff can be transferred back to its employer, and, at the end of the outsourcing contract, important specialists will not be lost.

A similar approach to outsourcing is **out-tasking**. Here, specific IT activities are transferred to external parties under the requirement that all the resources and conditions are provided by the service provider. This approach causes high costs. On the one hand, the service provider might need to invest in additional resources. On the other hand, the outsourcing company often has to dismiss employees, which might lead to a loss of specialists and possibly to the payment of compensations.

Another approach is the use of **shared services**. Here, the outsourcing company buys shares from the service provider. The companies share a property and work together. In result, the outsourcing company has comprehensive control options due to its ownership. Shared services are not the ideal option for limiting the scope, because the activities that have been transferred are still performed by a part of the company.

2.5 Stakeholders of Cybersecurity

From the company perspective, stakeholders of cybersecurity are all persons and groups that have an eligible **interest** in the cybersecurity of the company. The term stakeholder can be defined very broadly. It can also include the interest holders that are connected to the company only in an indirect or temporary way, e.g. customers or political interest groups.

The interests of stakeholders can strongly influence the cybersecurity of a company. While some stakeholders, e.g. the members of senior management, have a **direct** impact on cybersecurity decisions, others, e.g. customers, have an influence that is more **indirect**. Customers can affect the sales of a company. Thereby, they can uphold interests in an indirect way.

As shown in Fig. 2.6, the stakeholders with interests in the cybersecurity of a company are mostly:

- **Company owners**, also called shareholders, have a strong interest in the influence of cybersecurity to the company's success. Depending on the company type, the success can be assessed from an economic, idealistic, social or cultural point of view. The economic success of the company can be measured, e.g. with earnings before interest and taxes (EBIT). For economic success, especially the effective management of resources is essential. Therefore, the owners are interested in an appropriate balance of costs and benefits from the cybersecurity safeguards.
- **Executive management** is interested in an optimal implementation of all objectives that have been defined by the company owners. They lead the employees to comply with requirements and to achieve work related targets. Regarding cybersecurity, the executive management gives rough instructions and monitors their detailing and fulfillment.
- **Department management** is responsible for the work of employees within their department. It puts the rough instructions by executive management into concrete terms and incentivizes the employees to meet or implement derived

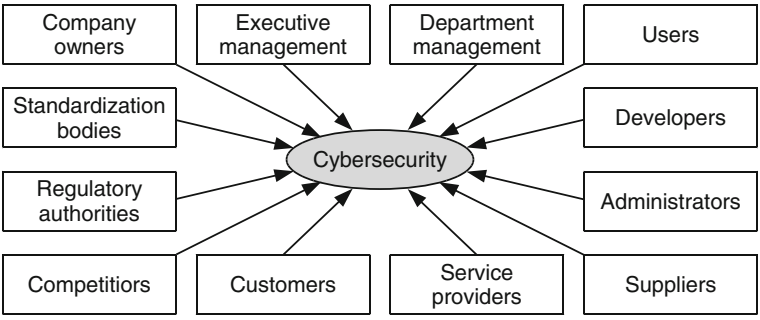

Fig. 2.6 Stakeholders of cybersecurity

objectives for their work. Cybersecurity objectives include e.g. the participation in trainings, the creation of handling instructions for electronic devices, or the secure storage of sensitive files.

- **Users** are interested in the best possible use of their work performance. They can profit from cybersecurity because a secure work environment helps them to concentrate on the work without being distracted, e.g. by outages of systems, or manipulation or comprise of data.
- **Developers** are supposed to consider actual knowledge about vulnerabilities during their coding. The best way to achieve a high protection level is to integrate cybersecurity by design. Already during the early planning phases, cybersecurity should generally be taken into account. Secure software leads to less rework and a tendency to more satisfied users.
- **Administrators** ensure that all systems are reliable and function as supposed. By hardening the systems, administrators make the systems more resilient against external attacks. Cybersecurity is an important way to raise the reliability.
- **Suppliers** deliver goods that are needed by the company to run through the supply chain. Cybersecurity is important to secure any communication between the supplier and the company. Furthermore, a breach could affect the business of the company severely so that the supplier might lose a valuable customer.
- **Service providers** provide various services to the company. Especially if the services are related to data processing, the information systems of the service provider and the company will often be meshed with each other. Therefore, a security breach will probably not only disrupt the processing, but also affect the service provider directly.
- **Customers** are in a business relationship with a company in order to receive a product, which can be a service or good. They are primarily interested in the product, especially in low prices and high quality. If the customers are in a long-term business relationship with a company, e.g. for regular purchases, not only product attributes, but also company attributes, like the cybersecurity protection level, will be of great importance.
- **Competitors** do often have a low interest in the cybersecurity of the company. A low protection level of the company could even lead to a migration of customers to competitors. However, the competitors could also be interested in a mutual improvement of cybersecurity. Because of partially similar processes and systems, a cooperation regarding cybersecurity could be beneficial for both.
- **Regulatory authorities** are mostly government institutions that require companies to adhere certain requirements or specifications. Their primary interest is to protect the public. They give special requirements that protect consumer data and raise the protection levels of companies in general. A well-known example is the Health Insurance Portability and Accountability Act (HIPAA) for the protection of confidential patient records.
- **Standardization bodies** include all companies or organizations that give mandatory or facultative rules for companies in general or for particular sectors. Mandatory rules must be fulfilled by companies and are found e.g. in laws.

Facultative rules can be fulfilled by companies optionally. Companies comply with mandatory rules to prevent the negative consequences, e.g. fines. They comply with facultative rules because they hope for further benefits. A common goal related to facultative rules is the standardization of processes and products. This can lead to a higher efficiency of internal operations, an improved use of resources and a positive public perception. Standardization can also lead to competitive advantage over companies that do not comply with these rules. Various certifications are available in the market. They allow certifying the compliance of facultative rules by an independent third party. A certification is often used as an advertising measure by the marketing department.

Prior to a cybersecurity investment project, there is sometimes uncertainty about the stakeholders, their relationship and their influence. A technique that helps to make this information transparent is the **stakeholder analysis**. It facilitates to distinguish cooperating from competing stakeholders. A targeted addressing of stakeholder interests can stimulate cooperation and prevent resistance. Thereby, key stakeholders can be convinced and—in the best case—encouraged to support the project at senior management level. This often leads to advantages regarding budgeting and prioritization.

The analyst should remind that the stakeholder analysis is characterized by a high **subjectivity**, since both the analyst and the stakeholders are making individual subjective evaluations:

- In order to reduce the subjectivity of the **analyst**, a committee should be set up. In contrast to a single analyst, a committee can find more objective and reasonable evaluations. The committee should consist of a heterogeneous group of people. Only with different perspectives, the widest possible identification and evaluation of stakeholders and their interests can be achieved. In addition, the analysis process should be unified within the committee and should be logged. As a result, the transparency of the evaluation is strongly increased not only within the committee, but also to external parties.
- The **stakeholders** find their own interests mostly in a subjective way. A reduction of this subjectivity cannot be achieved within the stakeholder analysis because the interests are already predefined. However, by using a survey, the interests of stakeholders can be made more transparent so that the understanding will be increased. Thus, at least inter-subjectivity can be achieved.

In order to perform a complete stakeholder analysis the following **six steps** must be completed (Resch 2012, pp. 128 ff.):

1. **Definition of Goal, Scope and Granularity**:
   After the general decision regarding a cybersecurity investment project had been made, further conditions for the stakeholder analysis must be established:

   - The **goal** clarifies why the stakeholder analysis should be performed. For example, it must be determined which addressees shall be identified and

consulted for assistance. Alternatively, the intention of the analysis can be to prevent that any stakeholders block the project.
- The **scope** indicates which perspective will be used for the identification of stakeholders. For example, internal or external stakeholders, managers or employees, and local or international stakeholders could be in focus.
- The **granularity** refers to how much the stakeholders will be abstracted by the analyst. A high level of abstraction summarizes stakeholders to groups, such as companies. A low level of abstraction means that single individuals are considered as stakeholders. In between, there are further levels of abstraction, e.g. departments.

2. **Identification and Selection of Stakeholders**:
The stakeholder role is generally attractive because a company mostly tries to meet stakeholder interests. Therefore, potential stakeholders will endeavor to be included in the group of selected stakeholders. The analyst is affected by a huge amount of work that is caused by not only the analysis itself, but also by the communication with stakeholders. Therefore, only those stakeholders should be selected that have a significant impact on the success of the project. Similar stakeholders can be combined to stakeholder groups.
3. **Prioritization of Stakeholders**:
This step is used to create a ranking regarding the strength of stakeholders' influences. At first, the influence of each stakeholder on the success of the project must be measured. Therefore, attributes can be considered whose values can be arranged on a nominal, ordinal or cardinal scale. Power, authority and involvement are examples for a usage of the ordinal scale. Using weights, the single attribute values can be aggregated to an overall assessment of the stakeholders' influences. It is possible that a stakeholder generally keeps a very important position in the company, e.g. a director, but he has only minor influence on the project.
4. **Identification of Stakeholder Interests**:
The stakeholder interests should be considered in such detail that it is clear if the stakeholders have a positive or negative opinion regarding the project. In some cases, this might overlap with demand management because requirements are also handled there. In contrast to demand management, the level of detail of the stakeholder analysis is rather abstract.
5. **Stakeholder Map**:
The stakeholder map (see Fig. 2.7) visualizes previous findings and provides an overview of priorities, convergences and conflicts of stakeholder interests.
6. **Consideration of Stakeholders' Interests**:
The stakeholders' interests can be considered by adjusting the project or by performing additional measures. Generally, a distinction can be made between three different types of consideration:

    - **Complete satisfaction**: The interests of all selected stakeholders are fully taken into account.

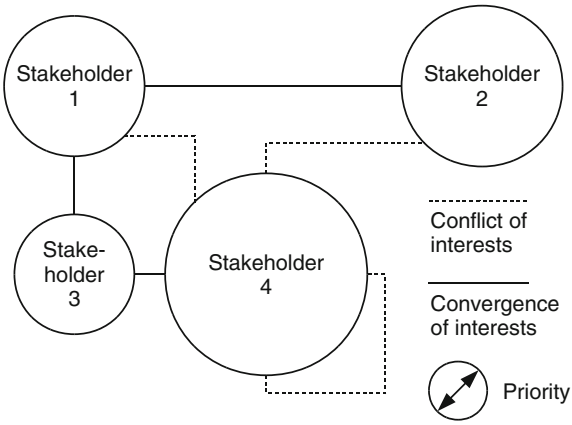

Fig. 2.7 Stakeholder map

- **Orientation**: The interests of a subset of the selected stakeholders are taken into account. The interests of the other stakeholders will be adjusted accordingly. This can be achieved e.g. by directives that are made by superior stakeholders.
- **Balancing**: Hereby, a compromise between the interests is created. The objective is finding a balance that is accepted by all stakeholders.

The **types of involvement** of stakeholders affect their interests. The identification and understanding of these types help the analyst to improve the quality of the stakeholder analysis and to select the best way of considering the stakeholders' interests. As shown in Fig. 2.8, the types of involvement can be distinguished in six categories, which are known as the **ladder of involvement** (Roper et al. 2006, pp. 75 f.):

- **Ownership**: Stakeholders on this rung of the ladder have assumed responsibility for cybersecurity or a specific security program. They personally identify with it and concentrate in making cybersecurity work. They are willing to devote as much time, attention and resources as needed. Cybersecurity is an integral part of their responsibilities and they are willing to invest in it.
- **Participation**: Stakeholders on this rung believe that cybersecurity and the specific security program make sense. They contribute something worthwhile to

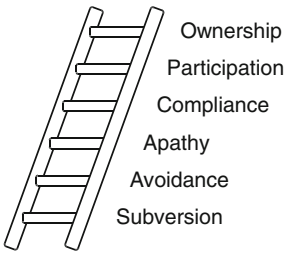

Fig. 2.8 Ladder of involvement

the company. They are willing to cooperate, follow the rules, and even advice in improving cybersecurity.

- **Compliance**: Stakeholders with this attitude will do exactly what they are told to do regarding cybersecurity. They will carefully comply with the rules. If something is not specifically covered by the rules, they will not care in finding a solution or performing any action. If they are criticized, they will get defensive.
- **Apathy**: These stakeholders just do not care about cybersecurity. They might not believe in the existence of the threat or in the appropriateness of the safeguard. They will follow the rules only if they think they will get in trouble if they do not. If they do not think they will get in trouble for wrongdoing, they will not bother with cybersecurity at all.
- **Avoidance**: Stakeholders on this rung view cybersecurity as inherently dangerous. In their eyes, cybersecurity only gets people in trouble. In result, they do everything they can do for not getting involved. If they detect a situation that puts an asset at risk, they will ignore it. They also avoid any contact to the cybersecurity staff.
- **Subversion**: Stakeholders on this rung deliberately and willfully try to make the cybersecurity program break. On the one hand, these stakeholders could just ignore the program, but this would have a negative impact only if the stakeholders participated in cybersecurity tasks directly, e.g. as an administrator. On the other hand, they could also try to influence the program actively. There is even a risk that they act illegally, e.g. by stealing necessary hardware components.

The stakeholders' interests must not necessarily be seen as unchangeable. By moving stakeholders **up the rungs** of the ladder of involvement, the interests could be changed positively. Probably, the strongest influence is firsthand experience. By getting stakeholders involved, they can build new experiences and compare them to their interests repeatedly. In consequence, their interests are likely to change.

http://www.springer.com/978-3-319-30458-8

Cybersecurity Investments
Decision Support Under Economic Aspects
Beissel, S.
2016, IX, 281 p. 58 illus. in color., Hardcover
ISBN: 978-3-319-30458-8