Security in IT projects properly planned, used cost-effectively.

Despite many recognized IT security standards, many IT projects fail on the subject of security. What needs to be considered and what mistakes should be avoided is explained in this paper project.

The Author Bernhard Bowitz (Diploma Engineer, CISSP, AISP, CISA, CISM, MCP, ITIL, Prince2, ISO27001, BSI Primary Protection, EGDPR, GDPR, Blockchain, Cloud, PhD) is a licensed security officer with more than 25 years experience on all platforms, technically and theoretically, understand and map processes, use hardware correctly. Understand VM, use cloud technology.

IT security applied correctly, technically and advisory, project management done right.
ISMS, SIEM, SOC, IAM, PAM, GRC, Cloud, and latest blockchain technology, etc. professional, understand applications, not just as keywords. Serve all platforms, even historically grown systems.

IT security in projects and products

By definition, IT projects involve building an information technology system. This can be the pure installation of existing solutions or the complete redevelopment of your own components. A combination is also possible, for example if standard or open-source software is further developed with its own extensions. No matter whether a product is created in the end or an IT system that is otherwise used commercially, IT security plays a key role in the success of the project today.

This also applies to systems where IT seems to play only a minor role in the overall product, such as the central heating control interface. Projects such as the construction and hosting of a standard web shop also address IT security to the same extent. The topic IT security employs companies of all sizes. In most cases, large corporations implement certain security standards that enable them to meet the highest security requirements in IT projects in a standardized manner. Smaller and medium-sized companies experience it harder. Mostly because scarce budgets leave little room for security issues or lack the appropriate know-how and can not always be easily procured.

Enforce IT security in the project - project management for example with MS-Project

Most IT projects have a tight budget. In the rarest cases, a project manager can make the most of financially. This is true for projects of both large and small companies alike, and usually harder the smaller the company is. If security can not be used as a selling point for a product or to build a system, the project leader often has difficulty earmarking a reasonable budget for security issues.
Because:

- You do not see security (superficially).
- Security does not make the system faster.
- Security does not make the system easier to use.
- Security complicates the processes around the operation.

Provocatively, you can ask the question: why spend money on something that degrades the end product? To make matters worse, in most cases**, very few project participants have a technical understanding of the subject of safety or worse, the so-called "dangerous half-knowledge".**

That's understandable. **IT security is one of the most complicated topics ever.**

A suitable specialist in this area not only **requires appropriate training but also years of practical experience in order to be able to sensibly and appropriately implement safety topics.** The added value of IT security can not be viewed in the short term.
A micro site for a week-long advertising campaign, for example, can be completely ignored by hackers. Nevertheless, it would be negligent to deliberately exclude IT security in such a project. Conversely, one has to look at what happens when projects lack security. For example, a successfully launched web service that will inevitably attract hackers after some time of success can quickly lose reputation when vulnerabilities are exposed. If security has been given too little attention in the project, it can be very difficult to close gaps in the long term. As a result, the service could not come out of the negative headlines for some time and even a new development will be necessary because a security concept in the existing system is not meaningful to implement. In the medium and long term, products that take the security of their benefits and their data seriously are gaining ground. Gaps are inevitable - how to deal with them is crucial. Furthermore, various laws can be used to derive minimum requirements for systems and products in order to avoid negligence as a management and to be liable for attacks by third parties. This should also be reason enough for every project manager to deal with the subject of IT security. The respective management must provide the basics and ensure - also in their own interest.

IT security in the project: from the beginning

The critical factor for security in IT projects is the time. Too often, projects are viewed from a commercial or functional point of view and implemented as proof-of-concept without even considering security issues. Prospects of success and financial forecasts are created. Then it comes to the implementation phase in which security requirements and data protection requirements in whatever way come to light.

These can destroy the entire business, case at worst. Usually at least adjustments are needed that will affect the project plan and can be a source of confusion for project participants. Depending on the extent to which the proof-of-concept is to serve as the technical basis for the actual realization, a complete new development may be necessary due to the security requirement. If you want to postpone security requirements to the next release after the go-live, the problems increase massively. Of course, this also makes itself felt in the budget accordingly. A departing project manager can thus "inherit" a corresponding burden to his successor. Any compromises in realization will prove long-term unsustainable and ultimately expensive, as practice shows. If contracts have already been concluded with suppliers and other partners - for example for development or hosting services - before safety requirements have been considered, massive problems also arise for the overall project.

All suppliers must be contractually obligated to the safety requirements, standard contracts must be substantively checked. If these are not customizable anyway, for example because you make contracts with a larger company and you have a certain amount of dependency, you have to make your own provision, at worst through your own risk management. For example, many web agencies that make tight price calculations in order to be competitive will need to separately calculate requirements from security catalogs. Here, too, it is important to incorporate appropriate planning into the project at an early stage.

A typical example

In an IT project, a web shop is to be built using standard software. This includes, among other things, installation and hosting. Changes to the shop software are not agreed. Hosting must provide hardening of the system as well as patch management. This must be provided for the entire operating time of the web shop and be carried out promptly in case of critical security updates of the shop software. If this is not contractually agreed, additional costs will be incurred. Alternatively, the owner of the shop must operate their own process for it and turn off staff accordingly. As experience from the practice can be observed that even in companies with its own security organization, this is often used too late.

For example, meetings of potential project teams should be accompanied by a security adviser - and by the way also a privacy adviser.
In this way, it is possible to point out appropriate security and data protection requirements at an early stage and avoid no-go's. **Also, security consultants are usually able to suggest simpler technical alternatives because of their project experience.** Accompaniment by a security consultant may also be advisable for pure idea development meetings without technical character. Projects fail on the subject of IT security, but usually on long-existing but unknown or ignored requirements of the project team.

Safety is always to be understood as a process

IT security causes running costs. IT security requires permanent staff. The latter does not necessarily have to be full-time. Why is that so? - Security is a process! This applies to all types of IT projects. Here are some examples.

a.) A specially developed web application is put into operation. Vulnerabilities are reported during operation. There must be a process to receive, review and correct these messages. If the software is self-developed, this process must be established in the company itself. If the software is an external order service, an agreement must be reached with the supplier. The interface between the internal and external processes must be defined, as well as appropriate service level agreements, such as the maximum processing time and general cost coverage.

b.) A standard application is hosted on the Internet. The systems were initially cured. Due to the emergence of newly discovered security vulnerabilities in standard software, a patch management process must be established. This includes, among other things, the viewing and recording of patches. Safety-critical patches must be able to be viewed and made in a timely manner. Depending on the complexity of the application, this requires a separate test system in addition to the actual production system in order to ensure the perfect functioning of the system

c.) A system not only allows system administrators but also certain applicative roles access to customer data (which may even be punishable under the latest data protection projects). For this an adequate logging of access actions was implemented. Even if an automatism has been established that includes misuse detection, a corresponding detection must be reported to and checked by a person. This requires a process. Irrespective of this, regular audits are to be carried out solely from the point of view of privacy.

d.) Intrusion Detection (APT) is set up for hosting systems. This allows monitoring of unusual events and potential attacks. Apart from certain automatisms, it is necessary that suitable personnel supervise this monitoring and if necessary initiate countermeasures. In addition to these practical examples, the same applies to the subject of IT security as in all other areas: with each new project, you learn about it and adjust your own processes accordingly.

Safety Standards

If you want to set up an IT security process for a project or an entire company, you do not have to start from scratch. There are many recognized safety standards to build on. This also applies to smaller projects and smaller companies. Large companies usually already have a certified IT security process and provide project managers with specific technical and non-technical requirements for IT security as well as data protection. You should also be aware of any industry-specific standards that need to be applied.

However, if you do not want to go the "big step" of a security process and build your own security organization, a so-called "Information Security Management System" **(ISMS),** which is a comprehensible problem especially for smaller companies, security standards still help: Either for your own software - Development or dealing with suppliers and partners. An advantage of the relevant safety standards is that they can be used in contracts as a reference. This guarantees at least a certain minimum level of security. If the companies involved in the project are certified according to established safety standards **(minimum recommendation: CISSP, ISO, BSI, CISO, Splunk, Agile ...)** and if these are also used for the project, this should also be contractually secured. A small overview of some selected safety standards, of course without claiming to be exhaustive:

• **ISO / IEC 27001:** Probably the most widely used, international standard for corporate information security organizations. The specific expression is company and industry specific.
• **BSI IT-Grundschutz:** A concrete implementation catalog for ISO / IEC 27001 issued by the German Federal Office for Information Security (BSI). IT-Grundschutz also includes a publicly available catalog of specific technical security requirements at the specification level for a variety of software and hardware components.

• **Certifications of TÜV:** Different Sub-organizations of the TÜV carry out various technical and non-technical tests of IT systems. Depending on the type of exam selected, general or TÜV-specific certifications are issued.

• **Common Criteria for Information Technology Security Evaluation (CCITSE):** An international standard that enables testing and certification of security requirements in specific products. Such a test is usually very extensive and costly.

• **PCI-DSS and PCI-PA-DSS:** These are standards of the credit card industry that businesses that have credit card information must meet. These are publicly available and due to their high requirements can also be meaningfully related to other data and thus used in their own projects. The safety catalogs contain concrete technical and organizational implementation measures. Specifically, the PADSS standard is about in-house development that processes credit card information.

• **OWASP** Top Ten Project: As a non-profit organization, the Open Web Application Security Project (OWASP) releases security policies (and more) for free use. In particular, the so-called "Top Ten Project" can be used as a reference for minimum requirements for secure web applications.

For Privacy it is the same

This article primarily refers to IT security. However, most of the issues presented are equally applicable to privacy requirements. Data protection requirements for IT projects derived from laws and other regulations must also be borne and implemented in IT projects as early as possible. Due to non-negotiable legal regulations, for example, missing contractual agreements can become real, self-inflicted "project killers". Just as a specialist is required for IT security, a suitable specialist is also required for data protection **- in the ideal case also with experience on the technical side**. For the technical implementation of data protection requirements, an IT security specialist can be consulted in the further course of the project. Preferably, **a project manager should become a leader with experience in all areas.**

Checklist for project managers

The following checklist should serve as an orientation for IT project managers to implement the often underestimated topics of IT security in the project. The list is not exhaustive. IT projects differ significantly in their requirements. If company-wide requirements apply, these must of course be considered first. For international projects, country-specific requirements, in particular data protection, may need to be examined.

Levels of IT security

Safety requirements are defined at various technical levels of a project. Since IT projects differ widely, the following list should only serve as an aid to early on specific security issues in a project. Depending on the project, it may only partially or not at all. However, a complete security concept (governance) should cover at least all these levels.

Technical levels

Similar to the **OSI layer model**, it is necessary to examine the various technical levels that may be appropriate for a project.

• **Network layer:** This includes the network concept (for example, the appropriate segmentation) and all network components such as switches, routers, network firewalls, VLAN settings and WLAN access points. Advanced components could be intrusion detection or intrusion prevention systems (IDS / IPS).

• **Virtualization level:** If virtualized components are used, the virtualization management software must be properly configured and hardened. It also needs to be verified that virtualization can provide a level of security appropriate to the project.

• **Operating system level & application level:** In addition to the actual applications, this also includes libraries used, extensions, runtime environments, server components (for example web server) and middleware components. Here, the operation of current and secure software must be ensured as well as the secure configuration of all components (for example, web server configuration), in general, it is called the system-hardening. Also included in this category are advanced security components such as application-level firewalls. Other topics that the project must cover for all technical levels are

• **Roles and permissions**

• **Monitoring and logging** (such as system behavior, login and access patterns) (SOC.NOC)

• Login methods for a reasonable security level (eg password authentication, two-factor authentication), IAM, PAM, AD, MFA .....

• **Encryption concept:** It must be clarified whether an adequate security level requires an encryption concept, for example through the use of database, file, hard disk or email encryption solutions.

• **Operational safety and reliability**

• **Access protection:** in the case of physical access to IT systems in-house developments (Secure Programming)

• **Encryption**

• **For in-house developments,** regardless of whether these are held in-house or commissioned, additional measures must be taken to ensure secure programming. For this purpose, one should fall back on the aforementioned safety standards. The requirements that arise here are highly dependent on the respective development context and the chosen programming environment. For example, the security requirements for Windows programs, mobile apps, web applications, or ABAP applications for SAP differ significantly from one another. Even with mobile apps alone you have to depend on the different mobile operating system (for example iOS, Android oder Windows).

• There may also be industry-specific security requirements, such as **PCI-PA DSS** for credit card applications. For web-based applications, the general standards of the aforementioned **OWASP** can be used.

Project ideas and Project development

• After the development of the project or product idea, first drafts with IT security specialists and data protection specialists are discussed.

• Requirements and comments of the specialists are included and presented in the project team. If necessary, questions arising from this and modified realization ideas will be discussed again with the specialists.

Project Kick-Off

• For the project kick-off all project participants are invited including the security and data protection specialists. Ideally, the specialists serve the project team as direct or at least as indirect contact persons throughout the entire project period.

Defining the security concept

• If you are part of a large company with an established IT security process, you will already know the security requirements for IT projects. As a rule, a suitable catalog of requirements has to be put together for each IT project, as IT projects differ greatly in their nature and content and therefore not all

requirements apply to all projects. Also, projects can make new requirements necessary due to their topic, for example, to meet legal requirements.

• If you do not have any given security requirements, you must create a requirement catalog yourself or have it created by external help. It is advisable to separate the role of the security specialist from the executive role. For example, it makes no sense to let a web agency control its self-defined security requirements. Of course, this makes sense for the agency internally, but not for you as a customer of a service. Note that usually an external security specialist will have the smallest share of your overall project budget. If you define the catalog of security requirements yourself, you can refer to or refer to one of the previously mentioned established security standards. Depending on the scope of the project, a specific subset may make sense. Alternatively, you can search for other security standards established in your industry.

• As a smaller company, for example, that a web agency can realize a web shop, the aforementioned "OWASP Top Ten" should be included as a minimum requirement in the contract. In addition, there are questions about the security of web hosting: Does the agency host itself or is an established service provider used for this purpose? Who implements patch management (operating system level, application level)?

External Serviceproviders

• If external service providers are involved in the project, for example for hosting, installation, installation, software development or delivery of standard software, these are also contractually bound to IT security. In the design of the contracts, certain minimum requirements should be specifically specified. Should any security vulnerabilities occur after commissioning, a corresponding bug fix must be provided, if necessary, taking into account additional costs. If delivered software violates the agreed security criteria already at the time of acceptance, a repair of the vulnerabilities free of charge for the customer should be provided for.

Technical acceptance

• Whether self-developed or delivered by external service providers, every project must be approved. In addition to the functional acceptance, technical safety acceptance is a must in every IT project. This includes at least the random checking of version statuses in order, for example, to identify outdated software and, if necessary, even to estimate the basic quality of the delivered service. Ideally, a true penetration test is used for acceptance. Incidentally, this can not only be done with web-based applications, but in adapted form there are also security tests for desktop applications, mobile apps and server services such as mail servers.

• The acceptance always refers to the previously agreed safety requirements. What has not been agreed, can not be demanded or causes additional costs.

Ongoing Security Processes The following list should serve as a rough overview of the common security processes in the operative area of IT systems:

• Patch management: Patch statuses must be monitored and updated for all components of the entire system if this is relevant to safety. These include, for example: firewalls, operating systems, middleware components, web servers, application servers, runtime,

Applications in general

• Regular Penetration Tests: Due to changing threat situations and new attacks, a regular penetration test should be part of the operation. The frequency depends on the project, but is recommended once a year. It is advisable to change the exporting penetration tester at certain intervals in order to avoid monotonous test behavior. Of course, it is time- and cost-efficient for post-tests to commission the same penetration tester.
• Monitoring of security-relevant accesses: Operational accesses such as administrator actions as well as logs of security components such as intrusion detection systems, application-level firewalls or the like must be regularly inspected. Safety critical events must be directed to and handled by appropriate personnel.
• Monitoring of application-based access against misuse: Data access, for example to customer data, by employees must be auditable, but also be detected promptly in the case of concrete suspicious cases. Therefore, established access controls at the application level must be made verifiable in a process that makes sense for the project.

Operational Safety

• If you need resilience and high availability measures, you will usually need another specialist in the field of administration. At least the project should define what the maximum tolerable downtime is for the IT systems used. If contracting parties are provided for these cases, they must be contractually bound to the corresponding recovery processes and service level agreements.
• Another central issue of operational security is backup & recovery. In particular, this includes all changing (user) data from databases, NAS and other storage locations. Although it is costly, the only way to test the correct functioning of a backup is to try a restore on a non-installed system. That's the only way to make sure to be prepared for the emergency. Although you do not want to do this process regularly, it should be done at least once before go-live.

Conclusion

IT security is a complex undertaking. Even the most experienced project managers can not tackle this issue alone and need professional support. In small businesses, the shortage of budgets may make it necessary to tackle the issue of safety itself. Here, safety standards can help to control suppliers and partners accordingly. In doing so, the mentioned central topics have to be considered. In general, however, suitable requirements must be defined for the respective project. IT projects of all sizes must adhere to the principle of integrating IT security and data protection requirements in the early stages of development. Failures in this area can make projects fail or at least lead to high follow-up costs.