Threats, Risks and the Derived Information Security Strategy

Lenka Fibikova[1] · Roland Mueller[2]

[1]Daimler Northeast Asia Ltd.
[2]Daimler Financial Services AG
{lenka.fibikova | roland.g.mueller}@daimler.com

Abstract

This article concentrates on the development of an information security strategy.

An information security strategy needs to focus on an overall objective, usually the objectives laid out in an organization's business strategy and its derived information technology strategy, where it takes the status quo and reflects the main objectives derived and postulates how and when to close the identified gaps. This strategy approach for improving information security is intended for an organization which supports an automotive and captive finance enterprise but is not restricted to this. The approach is aligned to the scope of ISO 270002 "Code of Practice for an Information Security Management System" [ISO05]. However, compliance is left out of the scope.

The strategy concentrates on four areas considered the relevant areas for information security: people, business processses, applications and infrastructure and has therefore a clear focus on processes, stability, resilience and efficiency which are the pillars of a successful enterprise.

1 Introduction

There are two main streams related to a security strategy nowadays – either it is considered an information security strategy and its main focus is on the three common objectives of information security which are confidentiality, integrity and availability (CIA) or it is considered a cyber security strategy and there are various discussions why cyber security has a broader view in addressing also objectives which go beyond the CIA objectives such as reputation and legal consequences.

Although a strategy should consider the latter objectives as well, we will make use of the more common term "information security" throughout this article. Therefore, we concentrate on an information security strategy and the main objective is the establishment of a "process driven organization with stable and efficient operations."

Today's information technology is in a flux where well-known techniques are now used in a way offering new opportunities for security and stability as well as for cost savings. Areas like virtualization, cloud computing, and big data are based on technologies which were examined and discussed for decades but can now be handled by the underlying technical equipment and the technical development. Also, the Internet is on a threshold which is not only triggered by higher speed but also by technical standards such as Internet Protocol version 6 (IPv6) and the Domain

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2012), 11-20

H. Reimer et al. (eds.), *ISSE 2012 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-00333-3_2,

Name Service Security Extensions (DNSSEC)[DNSS11]. Finally, the work life is changing and the limits between work and leisure are also in a move; the trend of BYOD or "bring your own device", social computing and social networks and tools like smart phones and tablet PC have played a major role in bringing work to the people.

2 Scope

The goal of implementing information security in an organization is to protect the organization's information by ensuring its confidentiality, integrity and availability.

Information is created and processed by employees, contractors and third party users (also known as information users) within business processes using applications and tools which are hosted in the IT infrastructure (see also Figure 1).

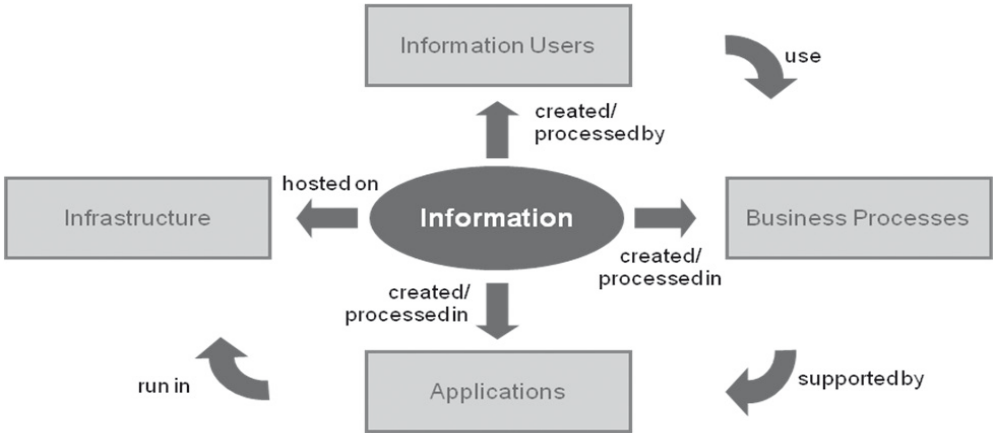

Fig. 1: Aspects of the information processing

Consequently, four areas need to be taken into account when implementing information security:

- **Information users,** or how people handle information and use tools and applications properly to protect information
- **Business processes**, or how information security is embedded within working practices
- **Applications,** or how well they are developed to ensure the protection of information stored and processed
- **Infrastructure**, or how well it provides sufficient capacities and adequate protection of information and applications against unauthorized access and modification

Information security is ensured via implementation of various measures. These measures need to

- cover all aspects of the four areas—information users, business processes, applications and infrastructure (**completeness**)
- provide adequate protection for information (**effectiveness**)
- be seamlessly integrated into the processes (**integration**)
- be supported by efficient tools and simple templates (**support**)
- avoid putting an unacceptable burden on the employees (**simplicity**)

Each of these properties is crucial for achieving effective protection of information.

- If any of these areas is not completely or not sufficiently covered (completeness and adequacy) then the existing weaknesses may be deliberately exploited or lead to failures.
- If a measure is not sufficiently supported or simple to use (support and simplicity) then users may try to circumvent the measure.
- If a measure is not integrated within the existing processes (integration) then its use cannot be guaranteed.

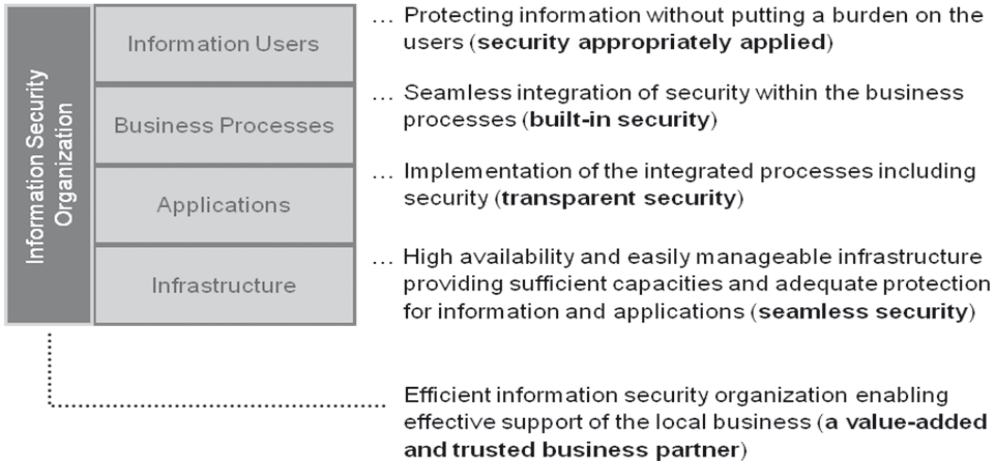

Fig. 2: Information security areas and high-level objectives

In addition to the named four areas, there must be an organization that initiates, coordinates and supports all activities with respect to information security. Therefore, the organization of information security is another area that needs to be taken into account in order to achieve an effective implementation of information security, i.e. adding a fifth area:

- **Information security organization**, or how efficiently the information security organization enables effective support of the local business in protecting their information

Figure 2 provides an overview of the defined information security areas and summarizes the high-level objectives.

3 Threat Landscape

The following section will first address common threats as reported in Verizon's 2012 Data Breach Report [Veri12] as well as introduced in Symantec's Internet Security Threat Report 2011 [Syma12] and will then focus on the threats directed to the four areas which the information security strategy is addressing. Additionally, it will point out where new technologies may influence the situation.

3.1 Common Threats

During the last years the threat landscape has changed dramatically. In former years, the main threats were caused by viruses, phishing and unintended data losses. Nowadays the number of targeted attacks has increased to a level beyond expectations. And these attacks are not only

caused by "hacktivism" which is politically motivated but even more by data thieves who "are professional criminals deliberately trying to steal information they can turn into cash" [Veri12].

Despite the decline of new disclosed vulnerabilities in commercial applications – the peak of disclosed vulnerabilities reported was reached in 2006 and is slowly decreasing – the severity of the vulnerabilities has increased. As lined out in the HP 2011 Top Cyber Security Risk Report [TCSR12], in 2011 almost a quarter of disclosed vulnerabilities is rated as high-severity vulnerabilities.

Finally, it has to be mentioned that vulnerabilities are rising in non-traditional enterprise infrastructures such as industrial control systems (e.g., supervisory control and data acquisition (SCADA)), IP telephony (Voice over IP (VoIP)) and new infrastructure such as mobile phones and cloud infrastructure [TCSR12]. Stuxnet, Duqu and Flame are examples of targeted malware against SCADA infrastructures.

All these aspects need to be considered in order to protect the areas an organization relies upon.

3.2 Information Users

The primary problems caused by information users include the incorrect handling of information due to missing awareness and knowledge about its value and insufficient training and awareness in using applicable tools. Additionally, problems arise through external attacks targeting information users (so-called advanced targeted attacks, phishing, social engineering, etc.), especially considering the increased use of social networks.

The number of occurrences of intentional misuse is decreasing, since users are becoming more aware of internal security measures and compliance issues; however, the extent of misuse, if it occurs, increases heavily and causes greater damage [Veri12]. Therefore, in order to ensure that no further risks arise from information users, awareness activities have to be kept on a high level and some of these activities have to address common weaknesses in processes administering employees.

3.3 Business Processes and Applications

The main threats for business processes are interruptions to critical processes which endangers the availability of these processes and the inability of the processes to guarantee confidentiality, integrity and correctness of the information.

Applications supporting the respective business processes are confronted with analogous threats.

3.4 Infrastructure

The IT infrastructure provides the medium for communication between information users, applications, and business processes, and builds the border between an enterprise's internal environment and the external world. Consequently, it is facing threats from the outside as well as from within of the organization.

Threats targeting the infrastructure (internal as well as external) are either passed to the information user (e.g., Trojans and viruses) and applications (e.g., hacking), or addressing the infrastructure components (e.g., denial of service attack, hacking the components). Therefore, the

protection of the infrastructure builds the basis for protecting the other three areas, the users, processes and applications.

Specific threats arise of technologies where common security techniques need to be modified. As an example, virtualization may counter a certain kind of threat but impose new risks because common security mechanisms do not work as used before.

4 Risk Considerations

In this section, the four areas are examined from the perspective how an organization usually applies measures. All measures are validated on their completeness, effectiveness, integration support and simplicity as far as applicable taking into account an average enterprise, its security posture and its setup. This will build the basis for later prioritization of measures.

4.1 Information Users

Information security for information users is based on three pillars:

1. *User awareness* targets on training the behavior focusing on compliance with applicable legislation and the organization's policies and using applicable tools.
2. *HR processes* which ensure that appropriate employees are selected, their skills are kept up-to-date and starter/leaver/position change procedures enforce the need-to-know principle.
3. *Procurement* is usually responsible for implementing measures that contractors and third party users follow the same regulations as employees and do not increase the risks.

Completeness: 1) An induction training/orientation days usually cover information security topics. Further user awareness programs are rarely established at an organization. 2) An end-to-end employee lifecycle management does rarely exist. Starter processes usually work well for employees. During employment, many organizations pay attention that their workforce is sufficiently trained and kept up to date with new technological developments. Deficiencies exist in the leaver process with the exception of dismissal. Position change is frequently implemented only rudimentarily. 3) Contractors and third parties are usually not considered at all because they are frequently not administered by HR and its processes. Procurement departments are not aware about their responsibility and the requirements for proper termination of contracts with third parties.

Effectiveness: 1) Since induction training is a one-time activity at the start of employment, it does not have any long-term effects. 2) and 3) The implementation of the need-to-know principle relies on the respective line managers and the people who manage and direct third party users in an organization.

Integration: With the exception of an induction training or orientation days, there is almost no integration in the internal HR and procurement processes.

Support: 1) A sample induction training as well as on-going awareness programs are usually centrally provided. However, these do not cover all aspects of information security, especially information handling is dealt with rudimentarily. There exist also several tools enabling appro-

priate handling of information within an organization (e.g., tools for information classification [LFRM10] or for the encryption of files, MS Office document templates for labeling). However, these do not cover all aspects and users are neither sufficiently aware of the tools available nor do they know how to handle them properly. 2) and 3) There are only few tools on the market and seldomly in use which support the user provisioning in the HR and procurement processes.

Simplicity: Varies, depending on the tools in use.

A simple conclusion follows out of this evaluation: the processes for securing information by the respective owners are usually not sufficient to reduce risks with respect to confidentiality, integrity and availability.

4.2 Business Processes

When it comes to business processes, two aspects are of relevance with respect to information security: 1) the information flows, and 2) the importance of the respective process for the enterprise. Information flows need to be evaluated to ensure proper handling of information in protecting its confidentiality and integrity. Importance of the business process indicates how important its information is for conducting business; this determines the priorities for continuity activities and recovery.

Completeness: is usually not given. Handling of information within the business processes relies on the attentiveness of the employees (see also Section 4.1) and individual business owners dealing with the information. As a consequence, segregation of duties violations and missing business continuity are the most frequent deficits in many organizations. Business continuity management has currently played an important role only in the Asian market due to the past experiences (SARS, bird flue, and tsunami); usually, no central activities exist to establish a proper business continuity management process.

Effectivenes for the respective measures cannot be validated since only limited activities have been initiated in most organizations. However, if business continuity is properly set up and tested regularly then an appropriate level of effectiveness can be achieved.

Integration, support and *simplicity* have to be considered when other areas are reviewed.

Here the verdict is almost identical to the one related to information users: business processes do not sufficiently implement information security requirements but focus on topics triggered by compliance (e.g., segregation of duties and dual control).

4.3 Applications

Business applications need to be developed in such a way that they enforce proper protection of information by implementing the need-to-know principle. This includes input and output controls (especially for web applications), correct data processing, authentication and authorization of users and processes, protection of information during transfer and storage and appropriate deletion of information. The development and the change of applications need to follow a stringent approval process. Furthermore, application recovery activities ensure that the business processes can return to normal work after a disruption of the application operations as fast as possible.

Note: Applications currently include the respective server operating systems and middleware (e.g., databases); with the rise of cloud computing and its approach of software as a service (SaaS) this will change.

Completeness: All major organizations have set up an approach which is similar to Microsoft's Secure Development Lifecycle (SDL) where information security is an integral part of software development. However, most organizations usually rely on a majority of legacy applications and only some modules have been modified or expanded in order to better use the Internet. The improvement of existing applications is a crucial issue, especially when it comes to applications that are used by business entities, but not developed and hosted within the IT organization which usually is the driver for the SDL. This way, applications are brought into operations whose information security features are not sufficiently used respectively known.

Effectiveness: The SDL methodology and similar approaches effectively enforce the implementation of information security within applications for an organization

Integration: For the in-house development of major applications, the use of an SDL is enforced. However, there is no integration of information security for other development projects or for approaches like SaaS due to non-existent formal requirements.

Support: Usually, project management tools support the project management process for developing major applications. This encompasses the enforcement of the quality gates, including information security. They cover all phases of the application development lifecycle; however, additional information security tools and guidelines (e.g., information classification tools and tools for ensuring compliance with existing policies) are not integrated (separate tools and guidelines need to be used to fulfill individual requirements). Also, some aspects of information security within common quality gates are often not supported by tools (e.g., code inspection).

Simplicity: Currently, SDL processes are quite complex and need to be simplified in order to improve acceptance.

The verdict is now more complex: there are areas where information security is integrated and there are areas where there is a gap. The risks rely heavily on the implementation and integration of a secure development lifecycle for applications and its support by tools..

4.4 Infrastructure

The infrastructure covers networks, network components, file, print and authentication services, work station and server operating systems, the respective hardware, and the facilities in which the infrastructure components are located (server rooms, data centers). The infrastructure needs to provide sufficient capacities and adequate protection of information and applications against unauthorized access (physical as well as logical) and modification. Protection of the infrastructure focuses on proper network architecture, hardening of components (operating systems, routers and switches), vulnerability management identifying and remediating potential weaknesses, malware protection, intrusion detection and prevention, logging, authentication and access control (including use of administrative privileges), backup, capacity management, and IT service continuity management.

Completeness: Guidelines for setup and operations of the infrastructure elements exist for all areas, but sometimes without information security in scope (e.g., LAN standard).

Effectiveness: The majority of the measures are implemented correctly. Problems arise with local network architecture, operating system hardening, vulnerability management (especially proper patching) and inadequate provisioning of local administrative privileges. Shared service centers specializing in specific infrastructure services show an increase in effectiveness and efficiency in the implementation of information security when provided centrally by specialized experts.

Integration: Some information security measures are commonly included in the operating procedures (e.g., backup, capacity management); some measures are rarely integrated (e.g., vulnerability management). Procedures are rarely documented within an organization.

Support: Some areas are covered by tools, however not continuously throughout the processes, i.e., some tools support only a part of a process (e.g., vulnerability management tools like Qualys support the vulnerability identification phase within vulnerability management but not the remediation). Tools are often wrongly configured.

Simplicity: Varies, depending on the respective tool.

4.5 Information security organization

An information security organization for a global enterprise has to be set up in a way that it covers global aspects as well as local ones. Ideally, the global aspects are the methodologies, policies and tools for all entities and the local aspects concentrate on the different markets and their specialties. Global aspects are then managed by a department providing methodologies, policies and tools globally. Local aspects are dealt with people in the markets. Depending on the portfolio of an organization, there might be as well a regional or a divisional intermediate level between the global and the local areas; we will describe them as divisional coordinators. Commonly, information security is part of an IT organization.

Positive aspects:

- Direct responsibility for information security at the local entities is assigned locally. In case of divisional coordination it can be ensured that subject matter expertise is available for supporting the local entities, which do not necessarily have this expertise locally.
- The divisional coordinator serves as a validation/distribution platform for problems in escalating general problems to the global department, in developing divisional solutions for division-internal problems and in providing solutions gained from local entities to the other entities within the division
- A self-assessment and the regular on-site assessments conducted at the local entities by the divisional coordinator enable measuring of the quality of information security, and help identifying common problems as well as enforcing ongoing improvement of the information security status at the local entities.
- On-site assessments serve also to provide consultation for the local entities in their specific problems and for creating awareness about the importance of information security among the local management.

Negative aspects:

- An information security organization which is integrated within an IT organization is usually not sufficiently involved in the business processes, which is crucial for the success of all initiatives. Therefore, its possibilities are limited at all levels (local, regional as well as central level).

- Global information security departments tend to concentrate on information security problems related to those entities which are considered the heavy weights of an enterprise's portfolio and other portfolio items are left without support.

5 Strategic goals

By mapping the high-level objectives defined in Section 2 and the deficiencies identified in the in Section 4 on risk considerations, the following strategic goals should be set up in order to generate an integrated information security strategy within an organization:

1. Set up a role concept for all business processes (target areas: information users, business processes).
2. Integrate information security procedures in all business processes (target areas: information users, business processes).
3. Set up business continuity management at all entities (target areas: information users, business processes, applications, infrastructure).
4. Provide and embed information security in the software development lifecycle seamlessly, including the change process (target area: applications).
5. Establish an ongoing improvement process for existing applications (target area: applications).
6. Integrate information security into the IT operating procedures and services (target area: infrastructure).
7. Optimize resources by establishing an exchange platform within the information security community (target area: information security organization).

Some of these goals sound simple, some of them are quite complex. If we map the new technology trends which have been touched in the very beginning, then one can see that some goals can be achieved by simple directives of the management and executive management support and some need further elaboration.

For example, the role concept is a task which requires an organization to document its business processes and the roles that are required in executing the business processes. Also, if an enterprise defines which of the business processes are the most critical ones from a global perspective then business continuity activities can also be streamlined. Finally, if a mapping between business processes and applications is achieved by the first two goals then standardization on the application level could be an outcome as well.

However, there are areas which need special attention: if we look at a common infrastructure concept today then we must be aware that a switch to IPv6 will on the one hand solve old problems like the seamless integration of virtual private network into the infrastructure but will bring up new ones which were solved by techniques that cannot be used any more. For example, IPv6 does not allow hiding a network layout via network address translation and private IP addressing but requires more stringent methods.

In addition, some upcoming or newly introduced technologies have not sufficiently been evaluated: if we look at virtualization then we can simplify backup for many virtual servers at once but are confronted with the risk that a recovery of data for a specific virtual server is substantially

more complex. And similar problems arise with virus protection; it needs to be understood that if different operating systems are hosted as guest operating systems within a virtual server then virus protection cannot be established on the hosting virtual machine.

And there are technologies waiting whose potential is not yet sufficiently examined. If we look at the Domain Name Service Security Extensions (DNSSEC) then we easily notice that this approach helps fighting hackers who misuse the DNS for attacking networks but it also allows prohibiting phishing attacks which might damage the reputation of an organization. And there are more ways how this DNSSEC infrastructure can be used in establishing trust for an organization and within an organization.

6 Conclusion

We have outlined in this article which pillars of an organization should be looked at when developing an information security strategy. We have also touched areas of new technologies which may influence such a strategy.

However, we have not sufficiently discussed which are the critical success factor whenever developing and implementing an information security strategy. We strongly believe that a well-accepted information security strategy is tightly aligned with the business strategy and has full support by executive management.

We have noticed that information security can play an important role in modernizing IT if the influence of information security and potential drawbacks are clearly pointed out and discussed in depth. There is a common understanding among many information security expert who say that "with an up-to-date information security strategy we can do business which was either impossible or prohibited in the past."

References

[DNSS11] eurID insights: DNS SECurity Extensions Technical Overview, 2011, http://www.eurid.eu/files/Insights_DNSSEC2.pdf

[ISO05] International Organization for Standardization – ISO 27002: Code of Practice for Information Security Management, 2005

[LFRM10] Lenka Fibikova, Roland Mueller: "A Simplified Approach for Classifying Applications" at ISSE 2010, Berlin, Germany, October 2010.

[Syma12] Symantec: Internet Security Threat Report 2011 – Trends, Volume 17, April 2012, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

[TCSR11] Hewlett-Packard: 2011 Top Cyber Security Risk Report, September 2011, http://www.hpenterprisesecurity.com/collateral/report/2011FullYearCyberSecurityRisksReport.pdf

[Veri12] Verizon: 2012 Data Breach Investigations Report, March 2012, http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf