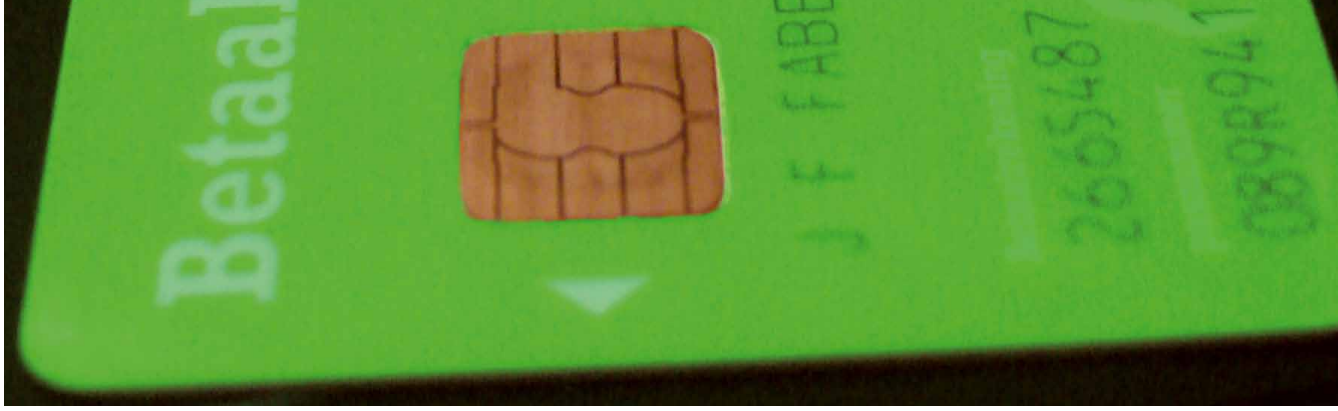

Data security in an era of cybercrime: steering through feeling

Peter Kornelisse

P. Kornelisse
is a director at
KPMG IT Advisory.
kornelisse.peter@kpmg.nl

IT security has always focused on the prevention of threats from hackers and internal fraud. However, something that we ought to have learned from previous incidents of publicized cybercrime, is the fact that one-hundred-per-cent security does not exist and, moreover, actual break-ins frequently remain undetected. Organizations should realize preventive controls as a precondition, and they should also have adequate controls for the detection of, and response to cybercrime.
Security begins with an awareness of the values that deserve to be protected, the recognition of threats, the definition of roles and responsibilities, and the determination of the required maturity of security processes. Then comes the configuration of a secure IT infrastructure. However, how can security be realized without the introduction of a surplus of measures?

Introduction

The world seemed simple prior to the advent of IT; physical security was the only area that potentially could be in danger. Organizations that had to deal with highly sensitive information made (limited) use of data classification and labeling (the marking of data classification on documents).

With the arrival of the first computers, security appeared to have become even simpler, in view of the fact that applications could only approach the data stored in centrally managed mainframes via previously defined functionalities and via strict procedures. *Transactional* data, in particular, was processed in this mainframe environment. The advent of the PC essentially altered the complexity of security. Users now created and processed data themselves in documents (files), and also dealt primarily with *non-transactional* data, which often included the highly sensitive data.

We have advanced quite a distance in the meantime. USB sticks are used for the exchange of data and, unfortunately, also for the transfer of viruses and trojans. Phishing occurs via e-mails, and users are enabled to install software on their own PC. End users store and even process documents in the cloud.

Also, with the advance of social media and a new – young – generation of users, combined with the deployment of private IT resources such as smartphones and tablets within one's own organization, it is becoming increasingly unclear whether or not an adequate level of IT security has been or can be realized.

Therefore, it is time for reflection. Can we apply fewer hard controls and more soft ones? Which criteria have to be imposed on security, where should security be regulated in the technology to ensure transparency, and where should we be able to rely upon the security awareness on the part of end users, developers and managers? Rules for IT management have become increasingly extensive and complex. There are even more rules than the users, managers and developers know about. So, it is time to apply the modern principle of 'steering through feeling' to data security to a greater extent.

More steering through feeling and, with that, greater awareness, are required considering the impact that a positive culture (security consciousness) and governance (organization, roles and responsibilities) can have upon data security, resulting in adequate IT security processes and a secure IT infrastructure (see Figure 1).

It is important for users to think more about the values that they are working with

This article will cover the following themes, analyzing whether or not it is possible to have more 'steering through feeling':

1. security awareness
2. classification and labeling
3. security measures in IT processes and IT infrastructure
4. demonstrability of security.

Security awareness

The regular stimulation of security awareness supports steering through feeling. In terms of security awareness, this means that organizations should pay more time and energy to this development, with the result that users and managers spontaneously deal with data in a better way.

Users themselves appear to be rather naïve: 'Do users think seriously enough about the required IT level of security?' A good example is the introduction of smartphones and tablets in organizations. These devices are usually brought into the organization by board members, and then this habit spreads to other users in the organization. Due to ease of use and trend sensitivity, the idea has arisen that organizations must be able to use such IT resources immediately. Risks are often (temporarily) accepted.

However, with the use of smartphones and tablets, people are not always aware of the value of the data that is stored and processed on these IT resources, or of the external and internal threats that may be involved.

In reflecting on the value of data, people often think of the value of data for the organization itself. However, it is becoming increasingly important to consider data in the ecosystem of collaborating organizations. Think of cybercrime in the public domain for example, where criminals seek data outside the organization under attack:

- Diginotar was attacked in order to create digital certificates.
- RSA was attacked to access SecurID authentication information.

In the past, much attention in security enforcement was devoted to the identification of threats. This tended to result in fear, doubt, and uncertainty. It seems, however, that it is more important for users to think about the values that they are working with, and the values that ought to be protected in that case. This requires training in security awareness – but such training is scarcely available. As a component of security awareness, attention should be paid to the assessment of values, the acknowledgement of generic security facilities, and the corresponding limitations of security facilities for IT resources.

As a part of the data lifecycle, users and managers should reinforce their awareness of how to deal with data security, so that they come to treat data and systems as if these involved their own wallets.

- *Create*. Does a user reflect on the stakeholder to whom the data may be valuable, and on what the magnitude of this value may be? Can people assess, on the basis of the recognized value, who should have right of access to, or be able to process, the data? Is it clear which metadata is being created, or what the document properties are?
- *Store*. Given the value of the data, is a user aware of where the data can be stored, and of whether or not the data ought to be encrypted (think of the use of facilities such as Dropbox, for example)?
- *Transport*. Should a user encrypt his/her data for transport? Can the data be transported via e-mail or a USB stick?
- *Process*. Can the data be processed in the cloud, should the user make specific agreements about this?
- *Sleep*. Is it clear who the owner is of data when it is dormant?
- *Delete*. Are the conditions of data retention known to the users? Is there some kind of guarantee covering the timely or perhaps premature deletion of data?

Figure 1. **Cause and effect.**

Classification and labeling

Highly sensitive data should be recognizable. Data that can be easily and intuitively classified, requires no explicit categorization or labeling to ensure careful treatment. That is self-evident. Accordingly, the formal classification and labeling of most data is unnecessary.

Recognition of classification

Only a few users are requested to classify data on the basis of the value of the data, if an organization classifies data at all. Organizations that actually do so mostly make use of a so-called CIA classification (Confidentiality, Integrity, Availability), directed toward applications rather than the data itself.

The classification of data can take place in many ways, and is generally experienced as being complex and difficult to maintain. That is why, in many cases, data classification simply does not occur, or occurs incorrectly or incompletely. As a consequence, no explicit labeling takes place either. This being the case, it is not always clear to third parties who is entitled to view the data, let alone know where data is stored and when the decision to delete it should be taken.

However, there is often a subconscious awareness of the sensitivity of data, which provides a basis through which the distribution of data can be limited.

It will be evident that public media such as Twitter, LinkedIn and Facebook are only intended for data that is allowed to enter the public domain. For data used within an organization, the allowed distribution is often much more complex. It is advisable to acknowledge as few data classes as possible, and to choose these classes in such a way that they are intuitive to the users and yet still function if the users do not spontaneously remember them. In a simple process we can think of a distinguishing (in-house) style that can be clearly recognized by internal members of staff. On the basis of the acknowledged value (what is important to the organization – think of Intellectual Property, what will be the damage if the data becomes public, etc?), the following classes can be deployed and can be spontaneously applied by users despite a lack of knowledge:

- public (intended for clients and other interested parties)
- internal (intended for all personnel, preferably not for external distribution)
- confidential (intended for a small group of people outside of which the data may not be accessible)
- personal (often intuitive, intended for one specific person, such as HR-specific information).

You should make differences in classification explicit, particularly in situations where the difference in classification is less pronounced. One example is the use of the 'Internal' and 'Confidential'.

Types of data

In the classification of data, it is expected that structured and unstructured data are treated differently:

- *Structured data* is processed by an application and is primarily labeled through classification via the processing application. This means that the application can automatically print a classification on reports. The payslips of the members of staff, upon which the label 'Personal' can be printed, is a good example of this.
An organization should ask itself explicitly if all relevant structured data is adequately shown. In the case of payslips, it is obvious that salary information is personal, and the data is indeed shown. However, data that does not seem to have the 'Personal' classification – but should nevertheless be regarded as private – is often stored in a structured way, via marketing websites for instance. In this context one can think of security incidents where the clients' private information, such as e-mails and other data, was made public by hackers of marketing sites. Suddenly privacy-sensitive data was there for the taking. In this way, it became clear that the data ought to have been classified as 'Personal', and should have been assigned the appropriately strict security status.
Accordingly, it is advisable to first formulate an adequate overview of processed data for each application and to clas-

Choose the classes in such a way that they still function if the users do not spontaneously remember them

First classify the processed data, and only then the application

sify the data, and only then classify the application itself. In view of the fact that structured data is managed for the users, it is advisable to actually classify it.

- *Unstructured data* is less easy to define. For unstructured data, it is important that users have an awareness of the necessary degree of security with regard to the IT resources (laptops, tablets, smartphones) and central IT services (file servers and other shares) they use to store sensitive data. In this process, it must be clear who is allowed to store which data where and for how long.

In view of the fact that unstructured data is managed by the users themselves, the users should be encouraged to steer through feeling; in other words, the issue of classification should be spontaneously assessed at the selection of the IT services, such as e-mail, tablets and file servers.

Measures in IT processes and IT infrastructure

Security services should be realized with the greatest possible transparency, via generic IT services such as e-mail and tablets, which is what a user intuitively expects.

Security services should be directed toward measures for the prevention and detection of, and response to, threats from both outside and in.

In the configuration of security measures, it is advisable to start with the expectations of the end user, and with the value of the data with which the organization normally works. For example, a research department can cover highly sensitive data such as intellectual ownership, while a shop may be dealing with low-sensitive data such as product, price and sales information. Nevertheless, in dealing with data, an organization must be aware of the threats that are directed toward the organization, as well as indirect threats in cases where the organization is a part of a larger chain.

A simple process can consist of limiting necessary measures (not closing off USB ports, for example), and also of the consistent application of measures so that exceptions do not entail an enlargement of complexity (such as the standard configuration of laptops with encryption of harddisks and the use of personal firewalls).

A simple process to realize and maintain data security is shown in Figure 2. First, the necessary security measures are defined in line with an analysis of the risks. Then, on a compliance basis, it is determined whether or not these measures can be maintained. If that turns out not to be the case, any non-compliance is mitigated, explicitly, but in relation to the risk involved.

This security process for the realization of a safe IT service can be run through for both structured data and unstructured data.

With structured data, the sensitivity of the processing application is established, and the security measures are adapted to this.

However, with unstructured data, it is possible that there will be many IT services (IT resources and applications) processing and/or storing the data. In the case of unstructured data, the security process will not be run through for data but for generic IT services (such as the file server, smartphones and tablets, and internet storage services). Unstructured data (such as e-mail) can be read in this framework. Accordingly, with IT services such as these, the possibility to read the highest data classification should be the starting point. On the basis of this classification, the security measures can subsequently be selected. Depending on the sensitivity of the data, more rigorous security measures can be chosen, such as:

- user name and password, or a second form of authentication such as a token
- unencrypted storage on a secure server, or encrypted storage on the same secure server
- standard tablet for the use of e-mail, or e-mail in a so-called 'encrypted sandbox' application.

The selection of security measures is easier said than done. Keep in mind that four regulation sections can be identified for every IT service (see Figure 3).

An example is given of each of these measures. Internal user processes may involve an authorization process for access to the data. Within business applications, a four-eyes principle (i.e., two observers) can be realized and encryption can be introduced. In the IT infrastructure, security can be arranged by the application of stringent configuration of security parameters. Finally, security can be guaranteed via IT management processes by installing

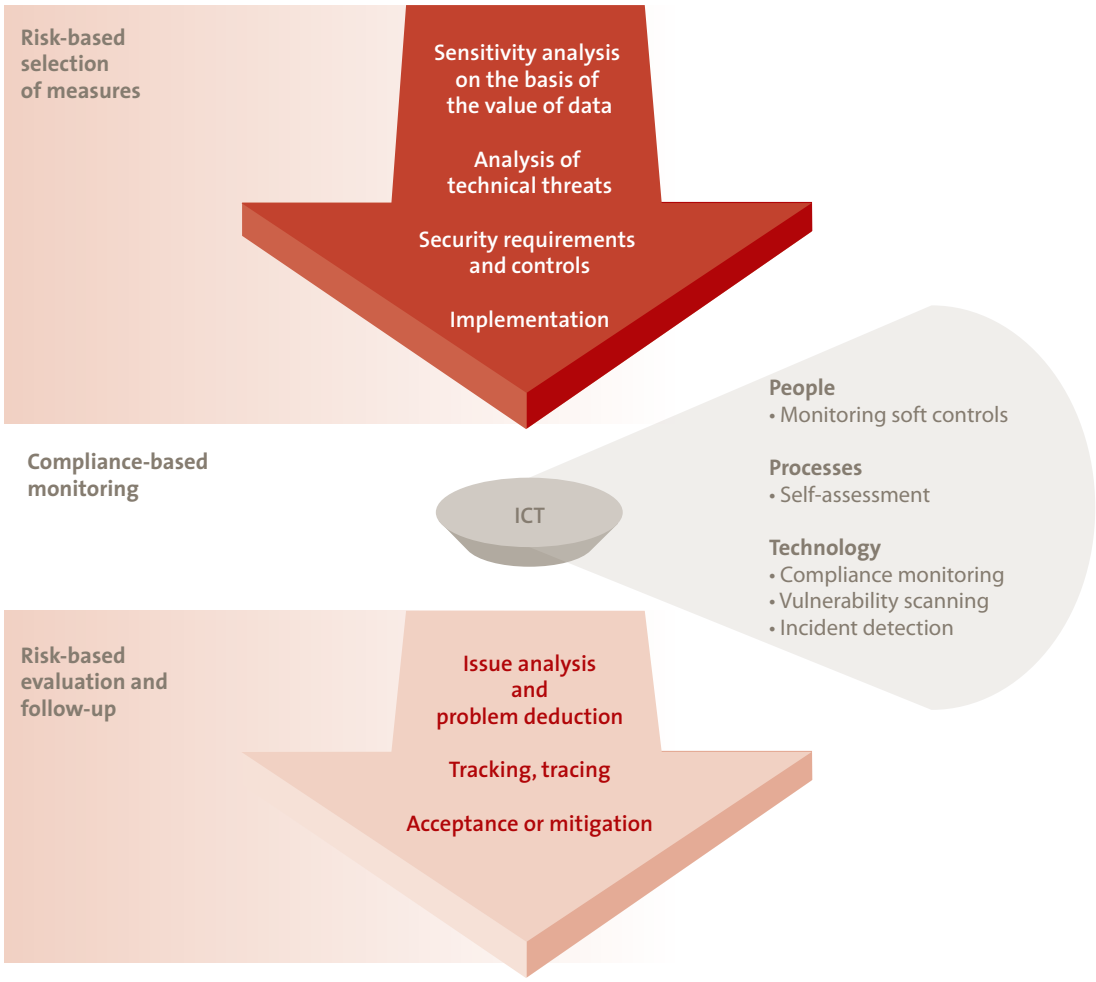

Figure 2. **Security process for data and systems.**

preventative processes for patching and access control, for example, as well as processes for detection and response should the access regulations be breached.

Demonstrability of data security

It is precisely in cases of transparent information security that it is advisable to look under the hood periodically in order to control whether or not confidence in data security is justified.

In this process, the 3-lines-of-defense model stimulates efficiency. Self-control also helps the timely detection of security risks.

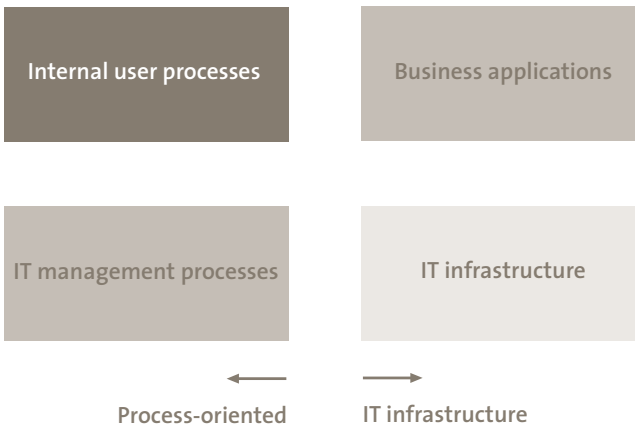

Figure 3. **Regulation sections for data security.**

Especially when it is steered through feeling, an organization should investigate whether or not adequate security measures have been installed, but this should be done in moderation.

The demonstration of adequate security on the basis of the 3-lines-of-defense model guarantees that the co-coordinators themselves assume their responsibility, and subsequently efficiently and effectively demonstrate status to the management of an organization, so that the management can assume its own responsibility for the data it administers, its own and those of his customers. The efficient and effective input of departments such as IT, risk management, security, and internal audit are thus supported.

Prior to the demonstration of data security it is advisable to determine its scope: which data and IT services should be shown to be adequately protected, and for which data and IT services is this not necessary? Do all sensitive data within the organization light up on the radar? By periodically identifying dataflows across the width of the organization, sensitive data remains on the radar. In this context, one can think of project data on file servers, for example, or customer data on an old server where the corresponding application is still active without anyone knowing about it, even if there are no longer any users. And there may be data on old media or in the cloud.

With scoping, it is important to focus on the value of the data to the organization itself, to other stakeholders, and to hackers for example. Consider also the possible effects of WikiLeaks or the publicizing of data after a break-in.

Development of threats in the chain, and demands imposed

Organizations need not always be involved in the development of threats. These threats may also lie beyond the organization. For instance, various organizations in sectors such as security and transport have to admit that if GSM networks fail, their own services to customers will also fail.

Accordingly, it is advisable to examine the chains periodically, and to show that adequate responsibility has been taken within this domain. In the case of dependence upon GSM networks, the question may be asked concerning whether or not back-up measures should be realized.

Current compliance of measures with previously determined demands

Please ensure that, in the monitoring of compliance, both process-oriented and technology-oriented measures are given sufficient attention (see also Figure 3). In the recent past, considerations of efficiency and perhaps even of knowledge have ensured that attention has been increasingly paid to the monitoring of processes. However, this is no guarantee that the correct technology is being maintained. Technology monitoring requires explicit attention!

Risk assessment of the current demands and non-compliances

Monitoring can show whether or not non-compliances are present. A non-compliance can be accepted or mitigated.

There is an increasing need for a dashboard of non-compliances and potential risks, enabling the management to make satisfactory choices with regard to the non-compliances that are to be accepted or mitigated, as well as the speed with which the mitigation of non-compliances should take place. In this risk evaluation, be careful to only take costs into account, and balance the costs of security against the values to be protected.

In conclusion

More ‘steering through feeling’ will be an important managerial feature in the future, because it turns out to become too complex and expensive to document all data security measures in requirements and to have users and managers remember them all. For measures that are genuinely essential – in other words, those covering the sensitive data and systems – it is important to ensure such measures firmly, and to organize the demonstrability of these measures and report on their outcomes.

Balance security costs against the values to be protected

Accordingly, the following priorities apply to the management of organizations:

- *Security awareness*
  - Remember that the landscape is changing, threats are real and here, security measures cannot provide a hundred per cent security; that has always been the case.
  - Security awareness should be constantly stimulated, by periodic campaigns for example.
- *Data classification and labeling*
  - Configure data security specifically for your own organization, on the basis of the acknowledged value of data and systems, and the role of the organization in related business chains.
  - Restrict formal classification and labeling to the essence.
- *Security measures*
  - Lead by example, and be cautious with regard to innovations such as smartphones and tablets. Prevent the management of the organization making unsafe use of these resources and insist, in good time, that only secure use is possible.
  - Do not be penny wise and pound foolish, but invest consciously; do not economize on the avoidance of major risks. Consider monitoring, for example. This makes it possible to control whether or not essential security measures are being adequately applied.
- *Demonstrability*
  - Apply the 3-lines-of-defense model to security. With a higher degree of maturity in control (evident via demonstrability), protection will become more efficient and also a structured and continuous process.

About the author

P. Kornelisse is a director at KPMG IT Advisory, where he is responsible for the ICT Security and Control services. Such services focus on security and control of IT infrastructures. Attention is paid to the prevention and detection of, and response to, various forms of cybercrime. He has executed many assignments, both at home and abroad, such as technical security analyses, including security testing and security compliance in all sectors, supporting organizations in their installation of IT (security) governance, assessing security as a part of the annual report control and SOx, as well as carrying out third-party announcements (including ISAE3402) for various organizations.

Do not be penny wise and pound foolish, but invest consciously