



CIO Platform Nederland

Het CIO Netwerk van Nederland voor CIO's en ICT eindverantwoordelijken in grote organisaties

Information Security



CIO Platform Nederland

**“Empower Employees -
...surrender control?”**

Whitepaper publication by the CIO Interest Group

Recommendations for CIO's

CIO Platform Nederland
June 2010

On behalf of the steering committee

Giving your employees the freedom to decide how, where and when they achieve the committed results is known as “Employee Empowerment”.

The primary responses to the subject of Employee Empowerment were “isn’t it inherently dangerous? Doesn’t this imply serious risks?” Since that time, most organizations have realized that it is almost inevitable and even imperative to adopt this new principle. A principle that offers organizations lots of new opportunities.

Employee Empowerment is imperative because the new generation of employees requires this new principle and organizations cannot miss out on this new generation. The new generation is the driving force that helps organizations to develop and to grow. To enable Employee Empowerment even helps to boost productivity of current employees.

Although we cannot afford to risk losing this new generation when we do not start with Employee Empowerment, the risks previously mentioned have to be taken in consideration when it comes to Information Security. Therefore a number of assessments and choices are required with respect to Information Security and data protection. These choices will have to be secured in the existing Information Security policies.

Experts within the Interest Group Information Security of the CIO Platform Nederland researched this subject. This publication provides a summary of their interesting and usable observations.

For members of the CIO Platform Nederland this publication provides a prototype tool to quickly and easily obtain an indicative understanding of the risks and controls associated with IT components.

On behalf of the board and the steering committee Information Security I would like to thank all those involved for their input and I hope you enjoy reading this publication.

Kees Jans

Chairman Steering Committee Information Security
CIO Schiphol Group

Publications by the CIO Platform Interest Groups are:

- Functieprofielen en toepassingsgebieden (juni 2007)
- Informatie beveiliging in Control, Awareness, Identity en Access Management. (juni 2007)
- Functies in de Informatievoorzieningsketen, een handreiking (juni 2008)
- Software Asset Management, handvatten voor goed licentiemanagement (juni 2010)
- Human Resource Management, de “nieuwe” medewerker (juni 2010)
- Information Security, Empowered Employees - Surrender Control? (juni 2010)
- Informatiebeveiliging, Checklist Informatiebeveiliging (juni 2010)

For up-to-date information on the CIO Platform and the Interest Groups, visit:
www.cio-platform.nl

Contents

1	Introduction.....	5
2	Background and research questions	7
2.1	Background	7
2.2	Research questions	10
3	Employee Empowerment associated risks	11
3.1	Which risks do we face?.....	11
3.2	Which risks do we focus on?.....	12
4	Adressing the risks	13
4.1	The traditional security principles won't help much.....	13
4.2	Identifying & controlling security risks	14
4.3	Addressing the risk	16
5	General findings.....	18
5.1	Empowered Employee Information Technology demand	19
5.2	Empowered Employee IT Security consequences	19
5.3	Delicate balance between organizational control & employee trust	20
5.4	Establish and ascertain employee trust.	21
5.5	Miscellaneous issues.	22
6	Conclusions & Recommendations.....	23
6.1	Conclusions & overview of CIO recommendations	23
7	Open issues	25
	Appendix 1: BSI based risk assessment tool	26
	Appendix 2: Participants CIG-IB Empowered Employees.....	28

1 Introduction

Considering all recent technological developments Information security is a relatively mature discipline, focusing on assuring information confidentiality, integrity and availability, based on a risk/threats-model.

Depending on a company's 'risk appetite' and 'threat profile' all kinds of technical security measures are taken to reduce risks to an acceptable level.

Think of security measures like anti virus software, firewalls, intrusion prevention systems, strong authentication, authorization management, etc., all turned to a commodity in the traditional world of information technology (IT). In this traditional world information security is an inherent part of a controlled environment that guarantees compliancy.

However times are changing, there are new developments that extend beyond the well established world of traditional IT, traditional organizations and even traditional employees.

We see the emergence of a new generation of employees Generation Y1, also known as the Millennial Generation, Generation Next, Net Generation or Einstein Generation).

A generation of empowered employees, familiar with and using state of the art information technology, i.e. tools & technologies like social networks (a.o. Twitter, LinkedIn, Wikis, Blogs), personal computing and communications devices (a.o. portable devices, smart phones using UMTS/HSDPA), cloud computing (a.o. Google Apps), etc.

These new, always-online-employees feel restricted by the traditional controlled environments and they feel the need to use their own toolkit consisting of hardware and applications in order to grow.

The newest trend anytime, anyplace, anyhow access to any-info and to any-who isn't fictitious anymore: for empowered employees it has become the new reality and they require these facilities even working within traditional organizations.

¹ http://en.wikipedia.org/wiki/Generation_Y

In current knowledge-based economy² enterprises don't hold off but embrace these developments in their pursuit to improve productivity and gain market share, but also to be acceptable as an employer for the empowered employee.

Organizations still focused on information security of traditional IT (using traditional techniques) however, are insufficiently equipped to effectively control the risks stemming from this unavoidable development, i.e. empowered employees demanding the state of the art information technology which they grow up with.



*Empower employees,
... surrender control?*

But even for the current generation of employees these new ways of working are becoming a necessity (businesses requiring their employees to work anytime and anyplace), so we have to be prepared for even more connectivity and for even more, still unknown, challenges.

What are the consequences of this unstoppable development? What are the consequences for information security; do we maintain or surrender control?

Our goal is to start a discussion, illustrate perspectives (threats, opportunities and strategic issues), raise awareness and enhance CIO's and IT director's insight in information security risks related to employee empowerment and "new world of working" issues.

This white paper is the output of several CIG-IB3 Empowered Employee working group meetings. The white paper consists of contributions from CIG-IB participants listed in section "Appendix 2: Participants CIG-IB Empowered Employees".

² http://en.wikipedia.org/wiki/Knowledge_economy

³ CIO-Platform Interest Group 'Informatiebeveiliging' (en: "Information Security")

<http://www.cio-platform.nl/over-het-platform/cio-interest-groups>

2 Background and research questions

Employee empowerment is the process of enabling or authorizing an individual to think, behave, take action, and control work and decision-making in autonomous ways.

2.1 Background

People are changing

Whereas in the past years an employer-supplied PDA was seen as a gadget and received by employees with enthusiasm, nowadays the situation is different. The new generation of employees has made its own choices where it comes to a mobile phone, PDA, laptop, home computer, etc.. They are a lot less enthusiastic when receiving yet another device from their employer. Instead, they prefer to use the equipment (including software and services!) of their own choice. They are willing and mostly able to maintain their own equipment, but want to use it in their own way, at the place and time they choose themselves. They expect their employer to accept that choice.

Companies are changing

In the world of the employers, the amount of information that is available and necessary to do the work has rapidly increased. Very few companies can do without electronic information nowadays. As a consequence the value of information has increased, but on the other hand more employees need the information to do their work.

In the economy of today, employers are more than ever seeking efficiency. This requires them to engage the new generation of employees and to look for cost reductions.

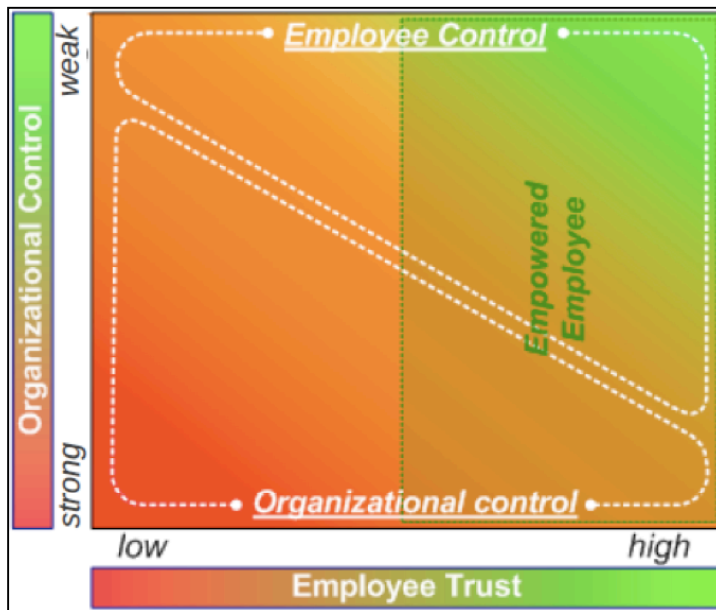
Empowered Employee - Definition

These two developments create the desire and need to empower employees. In the setting of current knowledge-based economy this results in the following definition of 'Empowered Employees':

Empowered Employees are knowledge workers⁴ who, when processing information within their scope of responsibility / work and organizational boundaries have the resources and authorization to control information, work and decision making in an autonomous way.

⁴ http://en.wikipedia.org/wiki/Knowledge_worker

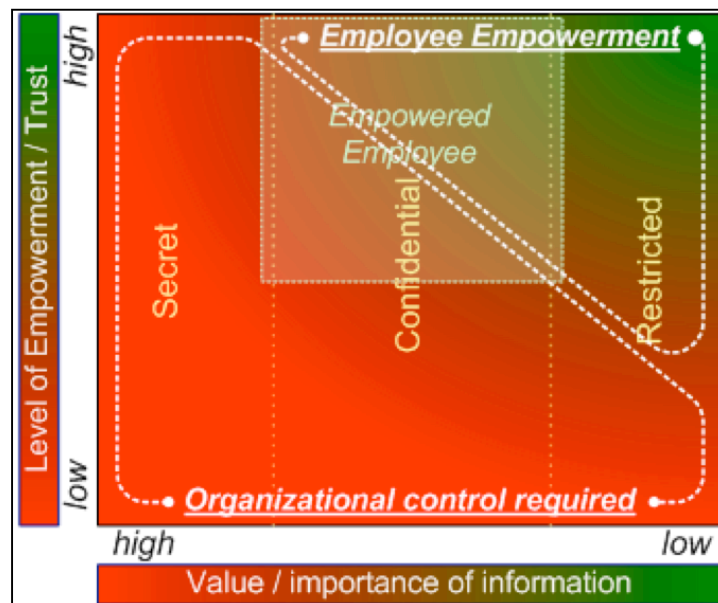
Extent of Empowerment



In principle all employees can be(come) 'Empowered Employees'. However, taking into account the value of information and level of employee trust, we have to note that not all employees are expected to be(come) equally empowered.

Trust as a limiting factor

In principle a wide variety of minimally low (e.g. 'production' workers) and high empowered (e.g. knowledge workers) employees can be distinguished. For this white paper (taking into account the business case for empowered employees) we focus on the category of high empowered employees.



Risk as a second dimension

Business case for the Employee

As mentioned above, the new employee wants to make his own choices. Nowadays Young professionals grow up with information technology. They have used it heavily in their education and are dependent on IT in their personal life for access to information, communication, social networking, etc. They are used to state-of-the-art IT being available on a 24*7 basis and to multitasking in IT. As a consequence, boundaries (e.g. between personal life and education) have become less distinct. When it comes to employment, this is their starting point.

Business case for the Employer

Enterprises can benefit from this new generation of employees:

- The current knowledge and information based economy requires employees who are used to using knowledge and information as a productive asset.
- Enterprises can benefit from the new, smart, fast communication skills of this new generation of employees, as communication needs are increasing everywhere: between businesses, with partners, and with (potential) customers, which are going through a similar transformation ('empowered customers').
- Enterprises can benefit from the willingness of this new generation of employees to do their work in the 24*7 economy in a flexible manner (if only to avoid peak-hour traffic jams).
- Enterprises can benefit from the willingness of this new generation of employees to create (or at least contribute to) their own working environment and to be self-supportive in that respect. It can reduce their investments in e.g. office space and IT equipment for their employees.

All these are drivers that solicit for "The New World of Work"⁵, a vision of an optimal and flexible way of employee empowerment. Anytime, anyplace, anyhow access to anyinfo & anywho, which fits in the 21st century (incl. enterprise 2.0). It aims to increase productivity and employee satisfaction so that organizations improve productivity and gain market share.

In conclusion: enterprises should welcome these new employees, but should also be willing to empower them to do their work in the most productive way, for both employer and employee. And that is where the challenges arise.

⁵

<http://www.youtube.com/watch?v=uH8tW1lihtA>

Towards a new balance

IT and information security is always a question of finding the balance between security (i.e. confidentiality, integrity and availability of data and systems), cost and ease of use.

The empowerment of employees can provide cost reduction for the employer and increase in ease of use and flexibility for the employees. It implies transferring (some) control to the empowered employee. This transfer of control provides extra risks for the IT security. The challenge is to find a new balance by identifying those risks and subsequently...

- ...selecting and executing counter measures (either technical or procedural) to adequately reduce those risks, and/or
- ...accepting that some increased risks are balanced by increased productivity or revenue, and/or
- ...defining the limits of empowerment if the resulting risks cannot be dealt with in one of the above ways.

2.2 Research questions

Given this background the working group has tried to grasp the challenge of empowering employees while ensuring the security of information and infrastructure technology in the following main research questions to be answered:

Which changes to current, traditional information-technology-related security practices⁶ are necessary to enable employee empowerment (The New World of Work)?

To what extent can these changes be made without compromising the security level of traditional information technology related security practices?

⁶ i.e. the combination of organizational (i.e. policies, processes & procedures) and infrastructural, (i.e. network, system & application) security measures

3 Employee Empowerment associated risks

Now that we shared some views on the changes in information technology required to empower employees, we want to identify risks associated with these changes.

3.1 Which risks do we face?

We focus on the main risks associated with most significant changes in the state-of-the-art information technology required to accommodate empowered employees.

These main risks, as selected by our working group, are clustered in two categories:

Category I. Risks associated with the transfer of control from the organization to the employee

Employee managed and/or owned tools (such as laptops and PDA's) do not necessarily comprise larger risks than company owned and managed devices. But such tools will not always be configured specifically for use within company-policy-secured environments. Risks that may be introduced in this way are:

- Incompatibility risks
The company cannot control what hard- and software is used. The employee owned software (version) could make conversions necessary and may produce incompatible or even unusable files.
- Legal and compliancy risks
Law may require special protection measures such as encryption when handling data.
- Software license risks
The company can not assure used software is legal, but may be liable for the use of it.
- Data-security risks:
The company can not control who has access to the device. Relatives of the employee may also use the family laptop and could have access to the company's confidential information. He or she could read, alter or even destroy company data.
- Availability risk
It is not likely that the employee has equal support and backup contracts for his or her private tools as the company. When a privately owned laptop breaks down, it may take more time to be repaired or replaced.

Category II. Risks associated with the use of state of the art information technology

Many of the confidentiality risks involved are not introduced by the empowered employee or by using state of the art technology.

Ever since the existence of Xerox machines employees could easily copy and distribute information. With USB memory sticks, internet, social media, etcetera, this distribution has become easier, but the measures preventing "leaking of information" are fairly the same. One should, however, realize that it is almost impossible to remove (leaked) information from the internet. The risks are the same, but they have become larger.

When publishing data on the internet it is not always clear where and under which legislation the actual data resides. This is almost always the case for cloud computing services.

3.2 Which risks do we focus on?

For this white paper we focus on category I. We consider the risks associated with the transfer of control to employees to be the most differentiating type of risks. Risks associated with the use of state of the art information technologies like social media aren't of less importance, but the first category is more related to our research question(s) and topic of exploration.

4 Addressing the risks

Now we have seen that employee empowerment conducted risks are mostly associated with the transfer of control from the organization to the empowered employee, we turn our focus to possible ways to address these risks.

A regular risk analysis method is applicable if explicit attention is paid to a number of points in the risk assessment for controlling empowerment. In this chapter an ICT resource-chain-model-based risk assessment approach is introduced.

4.1 *The traditional security principles won't help much...*

Empowerment implies that the organization transfers (part of) the control of IT facilities to the employee. Risk managers of organizations applying (or planning for) empowerment are often applying known and trusted security principles instinctively:

- Security is the competence of security professionals: the risks are translated into (mostly technical) measures by the security professionals;
- Security is based on perimeterization: security is achieved by means of "trusted zones" and "defense in depth" principles;
- The human factor is seen as a residual risk: "awareness" is an important measure addressing what can not be enforced technically.
- Security is enforced: "comply or explain" is the starting point.

Various levels of empowerment can be applied. The requirements associated with empowerment are often in conflict with the familiar security principles.

The "anyhow" requirement conflicts with the principle that security is exclusively conducted by security professionals. The "anyplace" requirement is not easily combined with security based on for example "perimeterization".

The often instinctively deployed security principles are not useful in empowerment situations because they mostly hinder empowerment.

A different approach to empowerment from security perspective and in risk assessments is necessary.

4.2 Identifying & controlling security risks

Levels of empowerment can be derived from combinations of the empowerment requirements:

- Anytime
- Anyplace
- Anyhow
- Any-info (Access to information)
- Any-who (Access to persons)

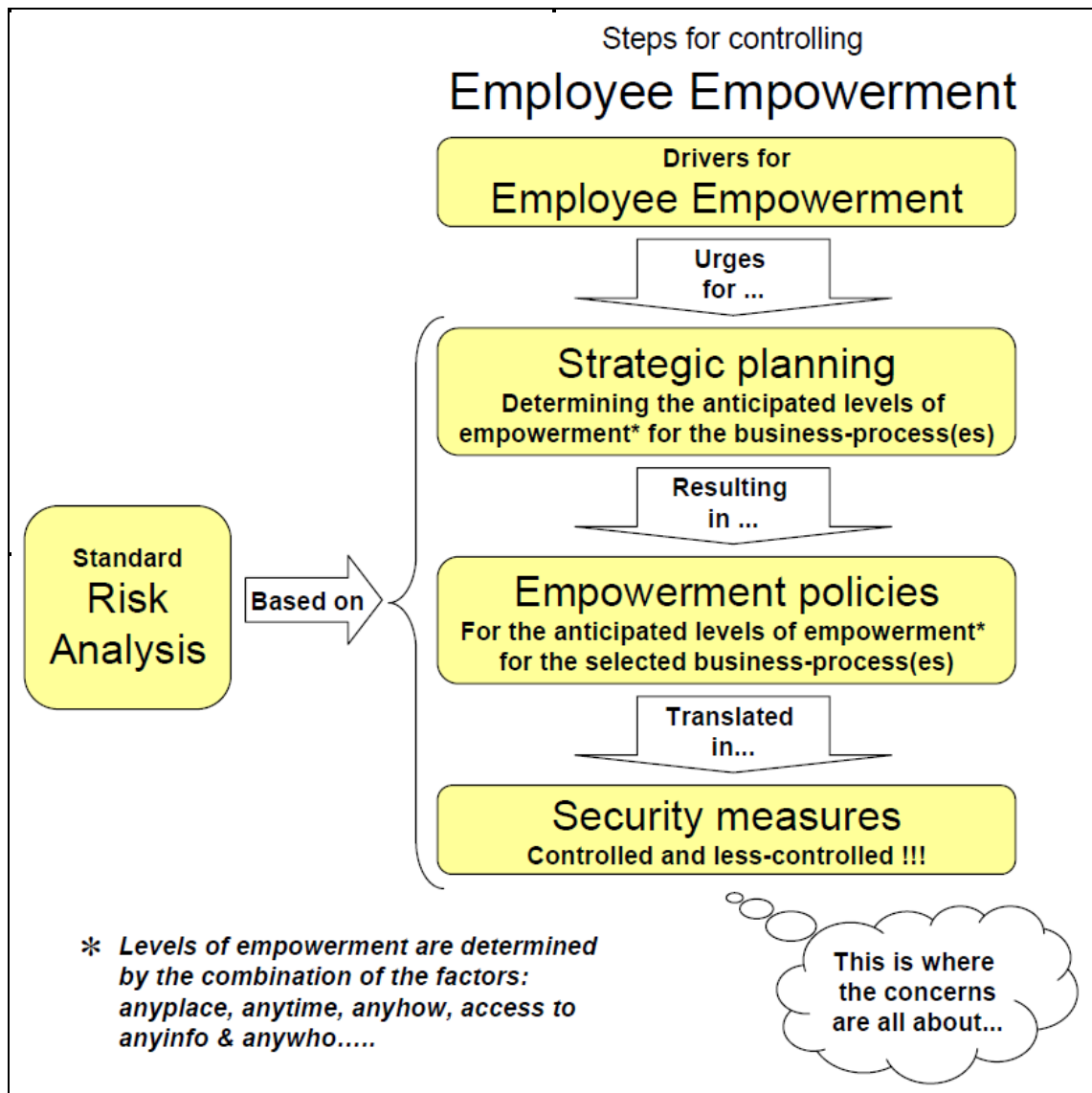
Based on a comprehensive risk analysis it is possible to determine what level of empowerment may be justified and should be adopted. This risk assessment focuses on business, process and security issues. From a security point of view a more principle-based approach is necessary to examine what level of empowerment is justified and feasible. In what way the risk assessment aimed at mastering empowerment risks can be done is shown in the flow diagram on the next page.

Important steps in the risk analysis for a level of empowerment are:

- Identifying the risks and controls for the IT-facilities;
- Assessing which controls are and aren't completed / covered by the empowered employee;
- Considering the residual risk, a choice can be made to enable, or not to enable, the empowered employee.

From a security perspective there are a number of important points in the risk assessment for a level of empowerment:

- The traditional security principles are not applicable;
- Confidentiality, integrity and availability of information must be controlled in proportion to the importance of the data;
- Trust relationships with entities and / or technology play an important (and sometimes decisive) role;
- Risk assessments should be repeated as new possibilities and technological developments (technology and applications) emerge.



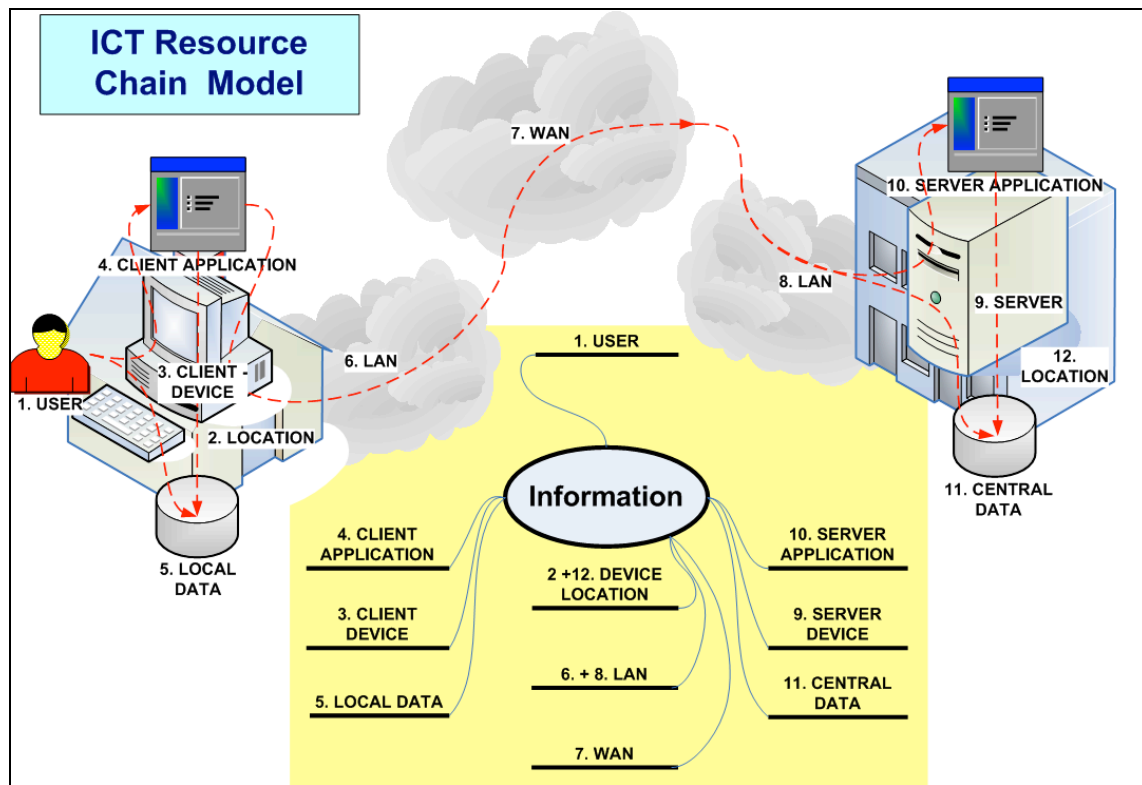
Flow diagram: Steps for controlling employee empowerment

4.3 Addressing the risk

As a method for a quick-scan ‘risk analysis for empowerment situations’ (i.e. ‘anytime, anyplace, anyhow access to any-info & any-who’), we developed and evaluated an ICT resource-chain-model-based risk assessment approach.

Within this model (see picture below) we distinguish the following ICT resource elements:

Client Side	Server Side
1. User (Employee)	7. Wide Area Network
2. Client Location	8. Local Area Network
3. Client Device	9. Server Device
4. Client Application	10. Server Application
5. Local Data	11. Central Data
6. Local Area Network	12. Server Location



Picture: ICT Resource chain model for empowerment risk analysis

This model provides the option to simplify a huge, tedious and complex overall-risk-assessment by breaking it up into smaller manageable elements. In this way it is possible to identify the risks associated with empowered employees.

Based on this approach the working group developed a practical method for risk-analysis based on the BSI: IT-Security Grundschutz⁷ and a simple Excel-tool.

The following steps in conducting the risk analysis are supported by the tool:

- Identification of IT chain elements concerned in the IT scenario which you want to empower employees for;
- Risk factor analysis by chain element (using the BSI-tool):
 - Identification of chain elements associated with used IT modules;
 - Identification / selection of relevant risks;
 - Identification / selection of effective / applicable measures that can be executed in the empowered situation;
 - Generation of residual risk and ineffective / applicable measures;
- On the basis of residual risk from ineffective / applicable measures an organization can then take a reasoned position to empower employees for the IT scenario.

The Excel-tool was primarily developed for exploring the empowerment research task, but can also be used by CIO Platform members for risk analysis purposes based on the BSI: IT-Security Grundschutz.

For CIO Platform members the tool (BSI-tool.xls) can be downloaded from the CIO platform website⁸. Appendix 1 provides a short explanation on the use of this tool (BSI-tool.xls).

⁷

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_no_de.html

⁸ <http://preview.tinyurl.com/35zqdr4>

5 General findings

This chapter provides a summarized overview of the findings of the working group regarding the IT-security aspects of empowered employees.

The principal changes to current, traditional IT-related security practices necessary to enable employee empowerment are:

- IT departments within organizations will be confronted with the delegation of the 'client / office' IT environment and associated information security control to the employees to be empowered, and will be deprived from the management/control themselves.
- Organizations having delegated the control of the 'client / office' IT environment to their employees will have to find ways (similar to outsourcing) to obtain sufficient assurance on compliance to their information security policies. Ways to obtain sufficient assurance are a.o. organizational policy awareness, contractual agreements, and compliance monitoring.

To what extent these changes can be made without compromising the security level of traditional IT-related security practices depends on the level of assurance on empowered employee information security policy compliance that can be obtained. In addition organizations may be faced with the consequences linked to employee use of consumer-grade instead of enterprise-grade technologies.

The working group's findings are grouped in the following categories:

- Empowered Employee Information Technology demand
- Empowered Employee IT security consequences
- The delicate balance between organizational control and employee trust
- Establish and ascertain employee trust
- Miscellaneous issues

5.1 Empowered Employee Information Technology demand

Empowered employee's pursuit of 'state-of-the-art' technology.

1. IT enables employee empowerment.

Information Technology will not enable employee empowerment⁹ by itself. But without appropriate Information Technology, empowered employees cannot hope to reach their potential.

2. Empowered employees demand the right to use of state of the art information technology (IT).

Not the use of 'traditional' but state-of-the-art information technologies enabling anytime, anyplace, anyhow access to anyinfo and anywho is what the new generation of employees grew up with, are familiar with, depend upon and expect (future) employers' consent.

5.2 Empowered Employee IT Security consequences

Empowered employees require control over their IT (client) environment.

1. Empowered employees demand both the right to use, and control of state-of-the-art information technology (IT), hence control of associated security measures.

For an organization enabling employee empowerment it implies transferring control of information technology and associated organizational and technological security measures to employees demanding to be empowered.

2. Traditional IT security often relies mainly on protective measures applied not to the information itself, but to the various objects around it (e.g. the device on which it is stored); just these objects are now controlled by empowered employees.

Security practices for traditional information technology rely mainly on the company control by combination of organizational (i.e. policies, processes & procedures) and technological, (i.e. network, system & application) security measures.

This implies that security practices for traditional IT mainly rely on security measures to objects surrounding information assets, but in general don't rely on security measures to information assets, i.e. the data itself.

⁹ Other matters like organizational structures and other resources that let employees make decisions are also key to enable employee empowerment.

3. **Security measures to company information assets (i.e. the data itself) (though currently considered immature) are anticipated to provide control of company information outside organizational boundaries in the (near) future¹⁰.**

Control of company information outside organizational boundaries can be achieved by means of security measures to information assets, i.e. the data itself. Current technology is however considered to be immature and certainly not mainstream.

5.3 *The delicate balance between organizational control & employee trust*

The decline of organizational control is to be compensated by empowered employee trust.

1. **The loss of organizational control as a consequence of enabling employee empowerment has to be compensated by employee trust.**
As part of enabling employee empowerment the control of state-of-the-art information technology (IT) and associated security controls is transferred to the employees themselves. As a consequence the associated loss of control of organizational and infrastructural security measures needs to be compensated by employee trust, i.e. confidence in employee integrity and their capabilities regarding the security controls transferred¹¹.

2. **Empowered employees, having different levels of trust are not all equally credible to perform business processes or handle information.**

The 4 cores of credibility (i.e. Integrity: Are you congruent? Intent: What's your agenda? Capabilities: Are you relevant? and Results: What's your track record?)¹² determine a person's level of trust, and influence the level of empowerment. In general employee credibility (level of trust) won't be equal for all employees.

As employee trust levels differ, their scope of enablement (i.e. delegation of organizational control) should differ and match the employee's level of trust.

¹⁰ Reference: Jericho Forum commandment 9 - "Access to data should be controlled by security attributes of the data itself".

¹¹ Reference: Jericho Forum commandment 6 - "All people, processes, and technology must have declared and transparent levels of trust for any transaction to take place"

¹² From Stephen M.R. Covey, "The speed of Trust" (ISBN-10: 074329730X)

- 3. The value and importance of a specific business process or information determines which empowered employees may or may not be credible, i.e. have sufficient level of trust to perform / handle that business process / information.**

The levels of risk and control associated with company business processes & information differ based on value and importance of these business processes & information. As a consequence, depending on their level of trust some empowered employees will be allowed to perform specific business processes or handle information while others won't. The level of trust must match the degree of control required.

- 4. Information exchange between company and empowered employee controlled environments should be regulated.**

When compared, company and empowered employee controlled environments are considered having different levels of trust; consequently (similar to e-mail based information exchange with other parties) information exchange between these environments should be regulated.

5.4 Establish and ascertain employee trust.

Organizations could (but shouldn't) simply assume trust; organizations must establish and ascertain employee trust.

- 1. Contractual agreements and company policy dissemination are some of the key elements in establishing employee trust.**

Similar to the law for citizens, proper organizational policies in combination with contractual arrangements need to provide direction on empowered employee do's & don'ts.

To be effective, policies need to be comprehensive and employees have to be aware of them and accept them. When considering contractual arrangements (e.g. a post-contractual non-competition clause) the organization's HR & legal departments should be consulted.

- 2. Monitoring and auditing are some of the key elements to ascertain employee trust.**

Similar to law enforcement, the monitoring of company policy & contract compliance provides additional assurance on the level of employee trust.

5.5 *Miscellaneous issues.*

There are more issues to be taken into consideration depending on the characteristic of each company. Some of the more general ones are:

1. Compliance to regulations (e.g. Sox)

In the empowered employee scenario compliance to regulations like Sox and others may be more than just a challenge.

2. Software licensing

It should not be taken for granted that software licenses purchased by employees include the right to process company information; legal issues are to be expected.

3. Information ownership

Organization's ownership of company information on employee devices should not be taken for granted; the law is not always conclusive in this respect. Consider consultation of the legal department and/or contractual agreements.

6 Conclusions & Recommendations

6.1 Conclusions & overview of CIO recommendations

'Anytime anyplace' has been a feasible option for a long time. Using thin client and server-based computing facilities; employees have already been empowered partially. But only in such a way that the traditional environment has been made accessible from outside the traditional and physical boundaries.

But empowering employees means accepting other new paradigms too. Empowered employees use more than just the traditional environments. Accepting those working methods means more than just offering Citrix clients.

It also means accepting a cultural change within the organization. Organizations have to adjust their policies in order to allow the empowerment of employees in accordance with the new virtual world order.

Transfer of organizational control over IT implies transfer of organizational control over associated security controls to the empowered employee himself.

The loss of organizational control over IT & security is to be compensated by employee trust. Employee trust is based on credibility. The 4 cores of credibility are:

- Integrity - Are you congruent?
- Intent - What's your agenda?
- Capabilities - Are you relevant?
- Results - What's your track record?

These questions should be answered in order to be able to allow employees to be empowered. These questions are, of course, not new, but answering these questions explicitly is needed to define a new security policy.

We expect that, no matter what the policy and culture is within an organization, employee empowerment will develop sooner than we think. In order to achieve and manage employee empowerment by itself, organizations have to take the following steps:

- Define a security policy that is broad enough to accept empowered employees. The Jericho 2.0¹³ principles (securing data, not channels) should be the leading principles.

¹³ http://en.wikipedia.org/wiki/Jericho_Forum

- Define new HR procedures: employees are no longer under control; they require freedom and their own control. That means for instance that employee performance has to be measured based on output instead of on working hours. New KPI's have to be developed in order to facilitate this transition.
- Allowing employees to manage their own IT might be more efficient than providing standardized IT, which could lead to new budgeting paradigms: pay the employee to manage his/her IT.
- Train the manager according to manager 2.0 principles: the managers who trust their employees and new result based performance indicators: trust, but verify.
- Analyze your business processes to understand the process risks that apply to empowerment. Define up front what processes cannot be executed by empowered employees, because of the inherent risks.
- Analyze your business risks using the techniques described in this white paper.
- Define security measures to mitigate the specific risks surrounding empowered employees, use the tools described in this white paper.
- Use state-of-the-art information technology for the new forms of authentication. Single-use passwords using GSM's and tokens are effective.
- Investigate the possibilities to migrate from fat client (client-server) applications to web based applications or even SAAS solutions, thereby removing the need for specific hardware and operating systems. It is far more convenient to manage and secure service oriented and web service based information systems.
- Don't rely on traditional role-based access control measures for cloud tourists. Move towards claims-based access control, using digital passports. Define the boundaries of employee control over the new technology.

Most of the companies need to be prepared for the New World of Work; this future world for knowledge workers is happening right now. The old world of work is doomed.

7 Open issues

- The current version of the tool (BSI-tool.xls) developed to assist in a swift BSI based risks & control assessment for a certain set of IT resource chain elements has the status of “proof of concept”. Depending on the demand the creation of a (more) professional version could be considered.
- Next to controls related to employee trust, compliance/audit and legal controls have to be considered as well. Within the scope of this paper these have not been addressed and should be considered in a future assessment.
- Application level risks associated with the use of state-of-the-art applications, e.g. social media, cloud sourcing, etc. have not been addressed and should be considered in a future assessment.

Appendix 1: BSI based risk assessment tool

To reduce the work associated with a manual assessment an Excel-based tool was developed. The following is a short explanation on the use of this tool (BSI-tool.xls)

Introduction and disclaimer

The tool is neither fool-proof, nor fully tested. (for example: macro's may crash in case no choice is made where a selection had to be made). Wherever an English text is unavailable, the German text is used. This is showed by the addition: "(Uit Duits)". The tool is created with Excel 97 and not tested with Excel 2007 (but we assume that the macros are upward compatible).

Instruction:

Step 0 - Preparation:

Make your own separate copy of BSI-tool.xls. CIO-platform members can download a copy of this tool using the following link: [BSI-tool.xls14](#)
Open your own copy of the BSI-tool.xls.

Step 1 - Relevant modules selection:

On tab 'Analysis', in column C select the modules that are relevant to your case (Note: everything in column C <> "empty" has the effect of having ticked, spaces included).

Collect the risks to the modules by using "Ctrl-t" to perform macro "voor_stap2". On the tab "Analysis", in the columns E through F you will find the risks list.

Step 2 - Relevant risks selection:

In column G tick the risks that are relevant.

Collect the actions to the risks by using "Ctrl-m" to perform macro "voor_stap3". On the tab "Analysis", in columns I through J, a list of measures will be displayed.

14

[https://www.surfgroepen.nl/sites/cio-platform/ib/Shared%20Documents%20\(Empowrd\)/Diversen/BSI.xlsx](https://www.surfgroepen.nl/sites/cio-platform/ib/Shared%20Documents%20(Empowrd)/Diversen/BSI.xlsx)

Step 3 - Feasible measures selection:

In column K tick the achievable measures.

Create the residual risk report (only useful if not all feasible measures have been selected) by using "Ctrl-r" to perform macro "voor_stap4". On the tab "Analysis", in the columns M through P, the list of residual risks will be displayed.

You can always repeat steps by returning to a previous step in the instruction. This can cause some loss of entered data; if necessary you must manually secure the work done (e.g. if you made the residual risk report and you still want to add a module, collecting the risks again using "Ctrl-t" erases the existing selections on feasible measures and residual risks).

Explanation on the residual risks report.

The residual risk report is only useful if not all feasible measures are selected! The list contains only the relevant risks that are not or only partially covered by actions. This list also contains further measures to enforce the coverage of the risk. The list of residual risks does not include the irrelevant risks (i.e. not selected in step 2).

Appendix 2: Participants CIG-IB Empowered Employees

The participants of the CIG-IB interest group contributed to this 'White Paper':

Organization	First name	Surname
Ahold / Albert Heijn	Nico	de Groot
Belastingdienst	Max	van Staveren
CBS	Roel	Rot
CJIB	Henk	Gomis
De Nederlandsche Bank	Guus	Grijpink
De Tweede Kamer	Marcus	Bremer
Delta	Hans	de Moor
Draka	Aad	Oudeman
DSM	Luc	Dupuits
Eneco	Anne	Spoelstra
Enexis	Hans	Baars
Espria	Erik	Pieters
Facilicom	Anton	Harder
Fortis Bank Nederland	Wim	Lagendijk
Gemeente Haarlemmermeer	Michael	Pols
Havenbedrijf Rotterdam	Chris	van den Hooven
Heineken International	Vic	Teunissen
ING	Niels	van Brecht
Koninklijke BAM Groep	René	Colsen
Marel Food Systems	Rob	Jansen
Martinair	Jan	Vegt
Ministerie VenW	Cees	Vaes
Nederlandse Spoorwegen	Jaap	de Bie
NXP Semiconductors Netherlands	Kay	Behnke
Océ	Eric	Piepers
PGGM	Piet	Kalverda
PGGM	Rob	van Otterdijk
Rabobank Nederland	Paul	Samwel
Rabobank Nederland	Adrie	Janssen Steenberg
Schiphol Group	Hans	Aldenkamp
Socile Verzekerings Bank	Pamela	Mercera
TNT Post	Dick	Brandt
TNT Post	Michel	Tinga
Transavia.com	Ronald	Verstraeten
UMC Groningen	Ron	van den Bosch
UMC Groningen	Leon	van der Krogt
UMC Leiden	Erik	Flikkenschild
UMC Utrecht	Evert Jan	Evers
Univé-VGZ-IZA-Trias	Hendrikus	Beck
Univé-VGZ-IZA-Trias	André	Koot
Van Gansewinkel Groep	Arjan	Arendse
SNS REAAL	Rolf	Heggie
CIO Platform	Rik	van Embden
CIO Platform	Foppe	Vogd