# 9 STEPS TO CYBERSECURITY

## THE MANAGER'S INFORMATION SECURITY STRATEGY MANUAL


DEJAN KOSUTIC

# 9 Steps to Cybersecurity

## The Manager's Information Security Strategy Manual

**By Dejan Kosutic**

# Copyright Page

Title: 9 Steps to Cybersecurity
Subtitle: The Manager's Information Security Strategy Manual
Author: Dejan Kosutic
Published by: EPPS Services Ltd, Zagreb
http://www.iso27001standard.com/



ISBN: 978-953-57452-0-4


First Edition, 2012

# Disclaimer

This book is designed to provide information on cybersecurity only. This information is provided and sold with the knowledge that the publisher and author do not offer any legal or other professional advice. In the case of a need for any such expertise, please consult with the appropriate professional. This book does not contain all information available on the subject. This book has not been created to be specific to any individual's or organization's situation or needs. Every effort has been made to make this book as accurate as possible. However, there may be typographical and/or content errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. This book contains information that might be dated and is intended only to educate and entertain. The author and publisher shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book. You hereby agree to be bound by this disclaimer or you may return this book within the guarantee time period for a full refund.

# Foreword

Businesses have become more vulnerable than ever before to a wide range of causes that can damage their data, systems, and overall operations. As Dejan Kosutic shows us, the risks are many, very real, and the stakes are high. He exposes the popular myths regarding cybersecurity. He then eloquently and simply explains the basics of cybersecurity and defines the benefits with convincing facts that will help you bring top management on board with implementation.

You will discover the cybersecurity framework options and the knowledge to choose what is appropriate for your business and situation. Dejan Kosutic explains risk management and what training and awareness your management and employees will need.

After this enjoyable read, you will have a clear concept of cybersecurity and the benefits and direction on planning implementation that will lead to protecting your business, as well as how to use cybersecurity to make your business more successful.

# Table of Contents

# Introduction

What is cybersecurity? How is cybersecurity related to information security? How do I protect my company from hackers? How about from a fire or natural disaster?

If you were an executive in an organization ten years ago, you probably would not be so concerned with these questions. Today, you are in the second decade of the third millennium and you cannot ignore such threats anymore. What's more, in the future you will need even more protection. Why? Because the majority of organizations are now in the business of processing information.

Most of us imagine that a bank handles large amounts of cash every day. While the banks still conduct many cash transactions, the fact is electronic money transactions far outweigh cash transactions – in some cases by more than a million to one. So, this means that a typical bank is in the business of processing information – it is one large factory of information. And guess what; for some time now robbing a bank by hacking is far more profitable than walking in

with a mask over your face and robbing the tellers. And hacking is far less risky, too.

Think about your business; are you an information factory, too? Chances are, your business is, if not completely, then in most part about processing information. This means your business is more vulnerable. Your information, your knowledge, your know-how, and your intellectual property are all at risk. And now the one-million-dollar question, or if you are in a larger business this might be a one-billion-dollar question: What do you need to do to protect the information in your company, and where do you start?

The problem nowadays is there is an abundance of information about cybersecurity; you are probably bombarded with information about new firewalls, anti-virus software, frameworks, methodologies, legislation, and so on. Many companies offer services touted to be the solution to all of your cybersecurity problems. Yet, these individual solutions aren't going to protect you completely. For instance, you cannot solve the problem of a disgruntled employee with

a firewall, the same way you cannot solve the problem of a hacker just by complying with a law.

So, it's obvious you need something more, something comprehensive. But, the challenge is where to even begin, what steps to take that will best protect your business.

This book will take you through the basics of cybersecurity, explain why safeguarding your information is of strategic importance for your organization, tell how to set the foundations of cybersecurity in an organization, which preparations are needed, and finally, how to plan your cybersecurity and have measurable results.

The text within will avoid the technical jargon and details of cybersecurity implementation, because that is not what you need to know to make decisions. The purpose of this book is to give you necessary guidance so that you'll be able to understand the essential building blocks of cybersecurity – this way, you'll be able to control your cybersecurity specialists better when they start with the implementation.

# Chapter 1: The Need for Cybersecurity

## The Four Types of Security Incidents

1. Natural Disaster
2. Malicious Attack (External Source)
3. Internal Attack
4. Malfunction and Unintentional Human Error

### Natural Disasters

In the last few years the world has experienced several natural disasters that have gained worldwide attention. Hurricanes such as Katrina and Sandy, the Fukushima disaster, tsunamis, and earthquakes such as the one in Haiti have all been devastating and destroyed entire businesses and banks of data. In addition, disasters such as tornados, floods, and storms can be enough to wipe out a business most anywhere. Even a localized fire can destroy all

your data if you didn't relocate your backup to a remote location.

## Malicious Attacks

Cyber attacks and security breaches are happening every minute and are too widespread to track. Some are small, others are large, some succeed in their purpose and others do not.

Here are some of the leading incidents in recent history[1].

**In May of 2006** the names, Social Security numbers, dates of birth, and some disability ratings for 26.5 million veterans and active-duty military personnel and spouses were taken from the U.S. Department of Veterans Affairs.

The information had been on a laptop and external hard drive stolen in a burglary. While the items were recovered later, the VA predicted

[1] http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century

estimated losses and prevention costs could top half a billion dollars.

**Date: August 6, 2006** AOL attacked; data on more than 650,000 users, including shopping and banking information, were posted publicly on a website.

**In March of 2008,** a Heartland Payment Systems database was attacked, exposing 134 million debit and credit cards. Albert Gonzalez was later convicted of the crime and sentenced to 20 years in federal prison.

**In 2009** the Chinese government launched a massive and unprecedented attack on Google, Yahoo, and dozens of other Silicon Valley companies. Google confessed that some of its intellectual property had been stolen.

**In 2011** RSA Security reported as many as 40 million employee records were stolen. This incident is attributed to subsequent attacks on Lockheed-Martin, L3, and others. The breach has been described as utterly massive from a potential tactical damage perspective, and from a psychological perspective.

**In 2011** ESTsoft lost the personal information of 35 million South Koreans due to hackers.

*"Nearly everyone will be hacked eventually,"* states Jon Callas, CTO for Entrust in a post on Help Net Security.

## Internal Attacks

**In July of 2007** an employee of Fidelity National Information Services stole 3.2 million customer records, including credit card, banking and personal information. A database administrator named William Sullivan was later sentenced to four years and nine months in prison and ordered to pay a $3.2 million fine.

The famous Wikileaks website was spawned from access to inside information. The jury is still out on the damage and effects of this monumental case.

## Malfunction and Unintentional Human Error

Equipment and infrastructure malfunction is something we meet almost daily – power loss, failure of Internet links and phone lines, breakdown of hard disk drives, and so on.

And how about when your colleague overwrites your data by mistake? And when you spill a cup of coffee over your laptop?

All of these situations have two things in common: first, the consequence is that you will lose your data or you will be unable to access it; second, these kinds of incidents happen rather often.

Hopefully, I didn't terrify you with these examples too much. But, one of the starting steps in building your cybersecurity is being aware of the environment we are living in.

I guess in this respect cybersecurity is not too different from managing other parts of your company.

# Chapter 2: The Cybersecurity Myths

Before we discuss more about cybersecurity, let me explain what cybersecurity is not; there are many well-established myths that can hamper your consideration of this subject.

## Myth #1 – It's all about IT

Imagine this scenario: a disgruntled system administrator intentionally disables your core application and deletes your most important databases.

Is this an IT issue? No, this is hardly an IT issue; more like an HR issue. Could this have been prevented by IT safeguards? No. The person in this position is required to have direct access to all of your systems.

So, the way to prevent this type of scenario falls outside the technology area and comes down to how to select your employees, how to supervise them, which kind of legal documents have been

signed, how this person is treated within the company, and so on.

Don't get me wrong – information technology and IT safeguards are extremely important in cybersecurity, but they alone are not enough. These measures must be combined with other types of safeguards to be effective. And this is something I'll explain later.

## Myth #2 – Top Management has Nothing to do with Cybersecurity

You are probably aware that safeguards cannot be implemented without money and employee work time. But, if the executives in your company are not convinced this protection is worth the investment, they are not going to provide the required resources. Hence, the project will fail.

Further, if top executives do not comply with security rules and, for instance, leave the laptop (with its list of top clients together with details about sales and related correspondence)

unprotected at the airport, all other security efforts will be in vain.

So, your top managers are a very important part of cybersecurity.

## Myth #3 – Most of the Investment will be in Technology

False. Most of the companies I have worked with already had most of the technology in place. What they did *not* have were rules on how to use that technology in a secure fashion. This is like purchasing a fancy new BMW and only using such a luxury car for delivering pizzas.

The information will be protected if everyone with access knows what is allowed and what is not, and who is responsible for every piece of information or for every piece of equipment. This is achieved by defining clear rules, usually in the form of policies and procedures.

As a rule of the thumb, I would say investment in technology is usually less than half of the required investment. In some cases, it may even

be less than 10%. The majority of the investment is usually in developing the policies and procedures, training and awareness, etc.

## Myth #4 – There is no ROI in Security

Yes, security costs money, and usually this protection will not bring you additional revenues.

The whole idea of cybersecurity is to decrease the costs related to security problems (i.e., incidents). If you manage to decrease the number and/or extent of security incidents, you will save money. In most cases the savings achieved are far greater than the cost of the safeguards; so, you will "profit" with cybersecurity.

We will talk more about Return on Security Investment in a bit.

## Myth #5 – Cybersecurity is a One-time Project

False. Cybersecurity is an ongoing process. For instance, if you develop an Incident Response

procedure which requires your employees to notify the Chief Information Security Officer on his or her cell phone about each incident, but then this person leaves your company, you obviously no longer want these calls to go to him or her if you want your system to be functional. You have to update your procedures and policies, but also software, equipment, agreements, etc. And this is the job that never ends.

## Myth #6 – The Documentation Myth

Writing a pile of policies and procedures does not mean your employees will automatically start complying with them.

Security is normally quite a big change and, frankly speaking, no one likes to change established practices. For example, instead of your good old “1234” password, you suddenly have to change your password every 90 days to something with eight characters, out of which at least one must be a number and one a special character.

What this means is that your employees will resist change, and will try to find ways in which to avoid these new rules. I will tell you later what you can do to help overcome this resistance.

Now that you know what is wrong, let's see what is right.

# Chapter 3: Basics of Cybersecurity

So, what exactly is cybersecurity and how does this fit in with all the other technology buzzwords we hear so often?

Let's first go through some basic definitions:

**Information security** (commonly referred to as **infosec**) definition – the "preservation of confidentiality, integrity and availability of information" (ISO/IEC 27001:2005); where **confidentiality** is "the property that information is not made available or disclosed to unauthorized individuals, entities, or processes," **integrity** is "the property of safeguarding the accuracy and completeness of assets," and **availability** is "the property of being accessible and usable upon demand by an authorized entity."

Just a small warning here – when you hear your security guys speak about the CIA, they are probably not referring to the government organization with international fame; they are probably referring to the three concepts mentioned above.

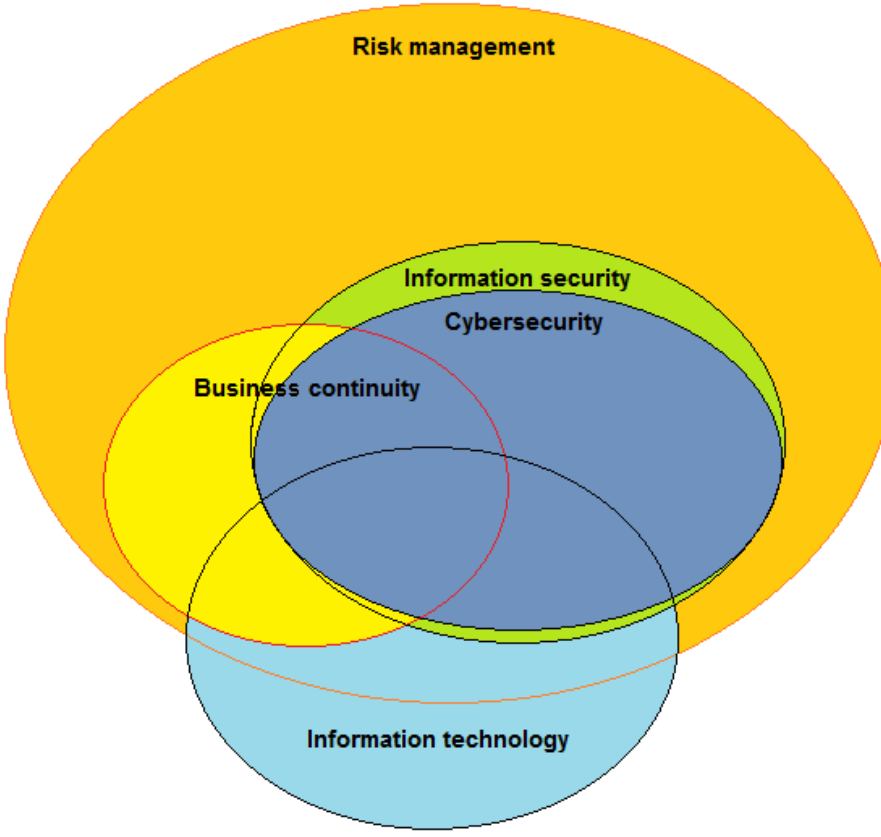
Using plain language, information security would be the following: if I come to a bank and deposit $10,000, first of all I do not want anyone else to know about this money except for the bank and myself. (This is **confidentiality**.)

In a few months time when I come to withdraw my deposit, I want the amount to be $10,000 plus any interest; I do not want the amount to be $1000 because someone has played around with my account. (This is **integrity**.)

Lastly, when I want to withdraw my money I do not want the bank clerk to tell me that the bank's systems are down and that I have to come back tomorrow. (This is **availability**.)

The definition of **Cybersecurity** is not far from information security; "Cybersecurity is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information." (The National Cyber Security Strategy 2011, Dutch Ministry of Security and Justice)

As you have probably noticed, these two terms are quite similar. See how they are related in the image below:




## Information Security vs. Cybersecurity

Although there is no official position about the differences between information security and

cybersecurity, I like to interpret them as follows: cybersecurity is 95% of information security; the only difference between them is that information security includes security of information on non-digital media (e.g., paper), while cybersecurity focuses on information in digital form only. Today, non-digital media is a small portion of total information available, often much less than 5% of all information.

In many cases, *information security* and *cybersecurity* are used interchangeably, as synonyms; *cybersecurity* seems to be a more preferred term in government circles in the United States, while *information security* is generally used in banks and healthcare organizations.

The point here is – the use of “information security” and “cybersecurity” are usually interchangeable. You can use both of these terms and you won't miss the point. You will notice I use the terms interchangeably.

## Business Continuity and Risk Management

**Business continuity** is "strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in

order to continue business operations at an acceptable predefined level" (BS 25999-2:2007). I mention this here as a distinct concept because this is usually where most of the investment into technology is required, and business continuity is also indispensable in the case of natural disasters.

As you may have noticed from the above image, Cybersecurity has a big overlapping area with business continuity, because one of the key characteristics of cybersecurity is keeping the information available; this is where business continuity plays a key role.

The purpose of them all: cybersecurity, information security, and business continuity, is basically to decrease the risks of doing business, or risk management. In the banking world, this is called the operational risk management. While you might not use this term, or have an organizational unit for managing risks, when you are trying to protect your information from being stolen or compromised, you are basically decreasing your business risks.

You might be surprised to learn that information technology is such a small part of cybersecurity. As mentioned earlier, technology is not the solution for all the risks because IT safeguards are normally 50% of cybersecurity.

What you do to decrease risks is, of course, the main effort of your cybersecurity. From a terminology point of view it is important to know that **countermeasures**, **safeguards**, **security controls**, or simply **controls** all have the same meaning: "means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature" (ISO/IEC 27000:2009).

Simply speaking, controls are what you do to protect the information in your company.

Now that you know the basics of cybersecurity, let's move on to the 9 steps of implementation.

# Chapter 4: 9 Basic Steps for Setting Up the Cybersecurity in Your Company

What are the necessary steps to achieve this famous CIA triangle – the protection of confidentiality, integrity, and availability of the information in the company?

As already noted in the introduction, we are not going to focus on the details of each of the steps. Instead, I am going to give you an overview of which steps are needed, and the purpose of each step so that you will be able to start this project in your company, and you will also be able to understand what you need to be successful. All this is in easy-to-understand terms without all the technical details so that you can plan and then give the implementation to the right specialists.

## Step #1 – Explore the Legislation and Other Requirements

This might feel like a strange way to start your cybersecurity implementation plan, but this is also the most effective one; if you are a financial institution, government body, or health organization, most probably there are laws or regulations in your country that force you to implement information security safeguards. For a list of laws and regulations related to information security in the United States, please see the Appendix.

In some cases, even the suppliers and partners of financial institutions and government agencies are regulated; for instance, in some countries the providers of IT services to banks are under the supervision of the government body that supervises banks. The point here is that the regulator has understood that the IT system of a bank is as secure as a company that is developing its applications or is providing maintenance services of the bank's system; if someone breaks into that IT company's servers, most likely they will have access to the bank's IT systems as well.

In most cases your company will be required to comply with at least the personal data protection

laws; even if you don't handle any of the personal data of your customers, chances are you probably do maintain the records containing personal data of your employees.

In any case, you will probably be surprised at how many laws and regulations there are. Start by making a list, and make sure you know the exact deadlines; disobeying these laws and regulations are very often accompanied with high fines.

You also need to review your contractual obligations. If you're an IT company providing some critical services to a government agency, for example, you will most likely have an agreement with them that requires strict confidentiality rules, service-level definitions, intellectual property rights clauses, rules for access control, and so on. Other contracts with customers and vendors also have requirements to be met in a structured way, and you do not want to risk losing your clients or incurring fines.

## Step #2 – Define the Benefits & Get the Top Management Support

In my experience, this is the number one reason why cybersecurity initiatives and/or projects fail.

Why is this step so crucial?

The answer is rather simple, but even so, top management support is all too often overlooked; there is no project or initiative (cybersecurity or otherwise) that can succeed if the money or manpower necessary for the implementation is lacking. And the only people who can provide those resources are within your top management; even if you are the CEO of a company you still need the commitment, or at least understanding, of other members of your top management team. Without their support, they can slow down or even stop your project even though you are 100% behind it.

Now, the question is – how do you get the support and understanding and commitment from top management? As with everything else in business (and private life), you have to find some common ground, meaning you have to find some benefits not only for the company, but also for the people working in the company.

So, let's go through the four potential benefits that your company can gain from the cybersecurity project. Not every one of these potential benefits might apply to your situation; what is important is that you find at least one that will make a difference for your business.

## Compliance

If during Step #1 you have identified any kind of law or regulation, or a contractual requirement related to information security, you can tout your cybersecurity project as meeting compliance with all the identified requirements. So, the main benefit would be that this kind of a project will give you peace of mind that you didn't omit any piece of the puzzle, so that you will avoid paying any penalties. Furthermore, if you choose the framework for the cybersecurity implementation wisely (see Step #4), you will spend far less time implementing all the safeguards as opposed to if you didn't have such a systematic approach.

## Marketing edge

Unless you are selling some kind of information security tools or consulting services, at first

glance cybersecurity and marketing do not seem to have much in common. However, you need to show third parties – such as clients – that you can handle their information safely. This can be done through the certification process – most widespread certificates for organizations are ISO 27001 and PCI DSS. (I'll explain what they are in Step #4.) In some situations you don't need a certificate – if you have larger clients you can simply ask them to send an audit team to check if your level of security is satisfactory.

This can be a sales tool to help your company gain new clients because you can prove to your potential customers that you will protect their information better than your competitors. This also means that your chances of retaining existing customers will be higher because you can prove to them you are a more secure option than the other companies that are trying to earn their business. And the investment in the cybersecurity is usually far less than the potential profit from these customers.

## Decreasing the costs

The underlying philosophy of cybersecurity is the prevention; you invest now in order to save money later. You can also consider cybersecurity

to be your insurance policy; you pay now in order to avoid the consequences of some damaging incident later.

The main catch here is how to make sure that the investments in safeguards do not exceed the costs of the potential incidents that you prevent. In other words, the question is how to make sure you have a return on investment in cyber-security. This is where the concept of risk management is utilized. I'll speak more about risk management in Step #6, though here are the basics: let's imagine that you want to calculate the ROI on mitigating the risk of fire in your data center; for instance, if your data center gets destroyed in a fire and the cost to become operational again is estimated to be $2 million including all related costs and the damage, and the odds of this kind of occurrence are rated at once in 100 years; your annualized risk is $20,000 ($2 million multiplied by 1%). This means that as long as your investment in fire suppression systems is less than $20,000 annually, you should make a profit.

Now, you might be thinking that predicting the likelihood and total cost of damage is impossible, and you are right. Unless you have precise statistical data, calculating this type of risk can be difficult, but the point is that you can show how an investment in cybersecurity is profitable

when done wisely and with a good measure. (You can use this Return on Security Investment Calculator to help you estimate your risks, damage, and mitigation costs.)

## Optimizing the business processes

Finding an organization where everything is running smoothly is rare, and even then the situation is usually temporary. In fact, chances are that the companies who didn't set their internal organization clearly will have higher cybersecurity risks. For example, in fast-growing IT companies the main problem is that they did not have time to sit back and think how to optimize their internal processes. As a result, who needs to do what, who is authorized to make certain decisions, who is responsible for what, and so on are not very well defined. Commonly, the effect of such a situation is that employees are wasting their time filling in loopholes in the organization, robbing them of focusing on their own work.

As mentioned before, cybersecurity is very often nothing else but clearly defining working procedures, so as a byproduct of cybersecurity implementation you will have a much more organized company. Security is primarily the

product of well-defined processes, and since security is present in all areas of your organization, this sorting out of your business will cover a much wider area than the security processes only.

## How to determine the benefits?

The best option would be to fit one or more of these benefits into your company strategy – if you could find a link between the cybersecurity benefits and your strategic objectives, then you would hit the target dead center. This might seem like a longshot at first glance, but with careful thinking this is not such an impossible task. Frequently, a brainstorming session will produce this kind of a link.

On a personal side, defining benefits that would fit certain key players in a company is vital. For example, your sales manager might initially oppose the idea of information security because of a possible slowdown of sales operations. However, if you explain to him or her that an increased level of information security will mean that the competition will not be able to access confidential information (such as details of your proposals) while in the phase of negotiating with

a new client, you will probably get an enthusiastic commitment.

But, let me also mention here that you will not be able to figure out the benefits to everyone on your own. Finding out the benefits will most probably have to include other members of your top management, as well as employees from various parts of your organization and from various levels in the hierarchy. This is an ongoing process, not a decision that is made at one point in time.

This is even truer when it comes to "diplomatic" activity in your company; you simply cannot expect all the members of your top management to share your enthusiasm just because you had a 30-minute briefing with them. Discovering the benefits and persuading everyone can be quite a bit of work.

## Step # 3 – Setting the Cybersecurity Objectives

*"What gets measured gets managed."* – a classic quote from Peter Drucker.

Until now you probably have realized that you should treat cybersecurity as a business case: you want to invest certain resources and achieve some positive outcomes for your company. If you achieve what you aim for, you will know your investment in cybersecurity made sense; the opposite is also true – if you failed to reach your objectives, there is something wrong with your cybersecurity.

And this is where things can become tricky. How will you know if you achieved a "marketing edge" or "compliance"? The answer to this question is that you have to set clear and measurable objectives. For instance, an objective that states: "We want to be secure" does not give you anything to hold onto; however, think about objectives along the line of: "Retain all the existing customers," or: "Get 2% new customers who are sensitive about cybersecurity in the following 12 months," or how about: "Comply fully with all laws and regulations within the next four months," or even better: "Decrease the

costs of security incidents by 50% in the following two years."

If you set these types of objectives for your cybersecurity, you will be able to determine if all the planned steps in cybersecurity implementation make sense. Not only this, after a year or two you will be able to look back and conclude with high precision if this whole effort made sense – just compare where you are now to what you have written in your objectives.

Setting clear objectives is also important for others in your organization. All the other members of your top management team will know exactly why you are pushing this project; mid-level managers and all of your employees will also have a much clearer picture of why this effort is important. And if they understand why this is important and useful, you have a much better chance that the project will succeed. If they do not accept your vision for cybersecurity, they will most likely try to avoid anything related to it.

When trying to think about the cybersecurity objectives, always start with the benefits you have defined in the previous steps; once you're clear with these, setting the objectives will be much easier. If you already have some kind of system for establishing the objectives and

measuring if they are achieved, for example a Balanced Scorecard, you should definitely incorporate cybersecurity objectives into this system. The more your cybersecurity activities are incorporated into your everyday business activities, the better.

## Step #4 – Choose the Framework for Cybersecurity Implementation

Once you are clear about what you want to achieve, the next step is to define how you are going to execute. Cybersecurity certainly is not something you would be able to do in a week or two. The project will include numerous people from your company, your suppliers, partners and clients; and changes in your existing working procedures and responsibilities, in technology, in human resources practices, and so on. This is a lot of work.

And this is why it is best to use experiences of other organizations who have already implemented cybersecurity with success – such frameworks are publicly available and here is a list of the ones that are the most widespread:

### ISO 27001

ISO/IEC 27001 is an international standard published by ISO (International Organization for Standardization) that defines how to implement and operate the Information Security Management System – it gives a good ground for building cybersecurity because it offers a

catalogue of 133 security controls, and offers flexibility to apply only those controls that are really needed (based on risk assessment). But, its best feature is that it defines a management framework for controlling and directing the security issues; therefore, achieving that security management becomes a part of the overall management in an organization. It is a leading information security standard, and at the time of writing this book, there were approximately 20,000 companies certified against this standard worldwide. (Certification is performed by accredited certification bodies.) To see how to comply with this standard, download this free implementation diagram.

## COBIT

COBIT is a framework issued by ISACA (Information Systems Audit and Control Association) that focuses on governance of enterprise IT – it is distinct because it reflects the central role that information technology has in modern organizations. As well as other frameworks, it is also based on the concept of risk management and keeping the IT-related risks at an acceptable level; but, perhaps its best feature is that it provides a direct link between a company's strategic goals and the use of IT.

Many information security/IT auditors prefer this framework as a basis for doing their audit work.

## NIST SP 800 Series

NIST SP 800 series is a series of over a hundred IT security publications published by the National Institute of Standards and Technology. It is probably the most comprehensive library of best practices publicly available, and similarly to PCI DSS, it is mostly oriented to technical issues of security. Since SP 800 is not a single document, but a series of rather unrelated documents, it would not be suitable as a single framework for implementation – however, NIST SP 800 publications are indispensable when it comes to implementation of single controls or particular areas of information security.

## PCI DSS

PCI DSS is a series of standards issued by PCI Security Standards Council, focused on enhancing payment card data security. This framework consists of very specific and detailed specifications, tools, measurements and other resources for data security and technical

protection of payment systems. Compliance with these standards is practically a must for any company dealing with credit card payments and other types of online transactions, and some U.S. states directly support the implementation of these standards. Regarding certification, only certain types of organizations that participate in payment card transactions must be assessed by qualified assessors.

## ITIL© & ISO 20000

ITIL, formerly known as IT Infrastructure Library, was published by the UK Office of Government Commerce (OGC). It is a framework for identifying, planning, delivering and supporting IT services to the business side of the organization and it is without a doubt the most widely adopted approach for IT service management worldwide. Although it does have elements of information security and service continuity (i.e., business continuity) management, the main focus of ITIL is not on these areas. ITIL certification of individuals is very popular; however, the companies cannot be certified against this framework. Organizations can certify against an international standard ISO/IEC 20000-1, which is based on ITIL.

## ISO 22301 and BS 25999-2

ISO 22301 is an international standard also published by ISO, focused on developing the Business Continuity Management System – it was published very recently; however, it is a new and enhanced version of British Standard BS 25999-2, which had already become a leading business continuity standard worldwide. ISO 22301 is fully compatible with ISO 27001, and these two standards can be implemented very easily together, providing a very good framework for integrated information security and business continuity protection. As with other ISO standards, companies can also get certified against this business continuity standard. To see how to comply with this standard, download this free implementation diagram.

## NFPA 1600

NFPA 1600 is a standard published by the U.S. National Fire Protection Association, and is focused on disaster and emergency management, and business continuity. It is highly popular in the United States, and it is also recognized as the National Preparedness Standard by the National Commission on Terrorist Attacks Upon

the United States. Compared to ISO 22301, it is more detailed in the area of crisis management; however, being a local U.S. standard, it is not as popular outside the United States. It remains to be seen which of these two standards will prevail in the U.S.

## ISO 27032

ISO/IEC 27032 comprises the guidelines for cybersecurity implementation – a completely new international standard published by ISO that covers the baseline security practices for all stakeholders in cyberspace. It still remains to be seen how this standard will turn out in practice and how widely it will be accepted, but at first glance it seems it will function much better as a supporting standard for ISO 27001 implementation than as an independent framework. It is not possible to certify an organization against ISO 27032, because this is not a standard that describes a management system.

## How to choose an appropriate framework?

When thinking about all these frameworks, you need to keep the following questions in mind:

- What are the requirements of the legislation?
- What are the contractual requirements?
- What are the benefits you'd like to achieve?
- What are the objectives you would like to achieve?

For instance, if you have signed an SLA with some of your clients where you are required to guarantee a certain minimum level of service availability, ISO 22301 (or perhaps NFPA 1600 if you are based in the United States) will probably be the best choice. This is because you will need to focus on business continuity aspects, while security aspects will not be the main focus.

On the other hand, if your objectives are to clearly define processes and procedures in your IT department, then ITIL would probably be the best solution because this is the main focus of this standard.

However, if, for instance, the legislation requires you to implement comprehensive organizational and technical safeguards, then you will probably look toward ISO 27001, NIST SP 800 series and COBIT. My personal preference would be ISO 27001 because I think it is the easiest to implement; then again, I'm probably too biased here.

Whatever your choice is, it will still be far better than nothing. Implementing cybersecurity without any know-how will most probably end up in failure.

# Step #5 – Organizing the Implementation

No matter which framework you decide to use, your cybersecurity implementation will probably be quite a complex job. Therefore, you cannot just give this to your system administrator to do as part of regular work, because (1) this is too complex for one person to handle without some clear plan, (2) because this is not primarily an IT job, and (3) because anyone who is too low in the organizational structure and without experience in managing people probably will be ill-suited for this job.

So, how do you start the implementation from an organizational point of view?

## Setting up project management

This kind of complex implementation will never be finished without a project structure. This does not mean you have to apply some fancy project management methodology, but it does mean that you have to establish at least the following: (1) what you want to achieve with this project, (2) who is responsible for the project, for example, a project manager who will coordinate all the

efforts and be responsible for the project timing and outcomes, (3) who will be the sponsor of the project, a person from top management who will intervene when the project comes to a halt (and believe me – that will happen very often), and (4) what are the steps in the project, deliverables, deadlines and milestones. Unless you are a small organization, you can also (5) form a project team that will help coordinate the project across different organizational units. The best practice is for members of the project team to be selected from both the business and the IT sides of the organization.

## Obtaining know-how

The framework or a standard you have selected in the previous step will provide you with an excellent foundation upon which you will build your cybersecurity; however, this will not give you all the knowledge and know-how needed for implementation.

Therefore, you will have to decide which of these options you will choose:

a) Implement cybersecurity with your employees only

b) Implement cybersecurity with your employees utilizing guidance from an outside expert
c) Implement cybersecurity primarily using outside help (i.e., consultants)

Option a) will initially be the cheapest; however, it will also require the most time because you will have to train your employees or find someone knowledgeable in the market to hire. However, during an implementation you might find that you took some wrong steps that ultimately cost you more than you would have paid for outside help. This option is probably the best if you have high confidentiality issues, because you do not want to let anyone from the outside get to know your company from the inside.

Option b) will certainly be quicker than option a); however, not as quick as option c). But, what I like about this option is there is a good balance between not making too many mistakes while enabling the largest possible knowledge transfer to your own employees. This happens not only through trainings, which will still be necessary, but also through learning from an expert you hire, and also learning through your own experience during the implementation.

Option c) is the quickest option, and probably the best if you have very short deadlines. However, you must be aware that consultants are not cheap (at least good ones are not cheap, and hiring bad ones is going to cost you even more), but also if someone else writes all of your procedures and policies, no matter how good this consultant is, you could face two problems: first, your employees might not feel that these policies and procedures are something that they have produced and might resist implementation, and second, the knowledge transfer will not be as extensive as in option b), so you might face a situation where you will lack knowledgeable employees to maintain your cybersecurity after the consultant is gone.

## Determine required resources

Simply creating a project plan does not mean that your project will succeed. You also need money and employee time to finish the project successfully.

Normally, this is what you have to plan for in your budget and other business plans:

1) **Time & cost of your employees:** The time they will have to invest in new training, developing documentation, coordinating the

project, adapting to new rules, etc. At the same time, they will not be able to do their regular job. This will most probably be your largest expense.

2) **Cost of technology:** You will probably need to invest some money in new technology as you become aware of the largest risks. However, as noted before, it is highly likely that you already have most of the technology in place. Typically, the largest investment needed is in "disaster recovery." Disaster recovery is a technical solution where your data and technology are available not only at your regular location (so-called "primary site"), but also at an alternative location (so-called "secondary site"), which is used in case of disaster. Nowadays, with the advance of cloud computing and other alternatives, your secondary site does not have to be too expensive (unless you have highly confidential data you cannot store in a cloud, for instance, if you are a bank).

3) **Cost of external assistance:** This includes consultants (if you hire them), training, various tools you might be using, documentation templates, and so on. Make

sure each one will actually decrease your total cost and/or duration of the implementation, instead of increasing it.

4) **Certification costs:** If you decide to go for the certification, there will be a cost. However, these costs are going to be the smallest of all those mentioned above; of course, first you have to decide whether you see any benefit in certification.

You will be able to calculate your costs much more precisely after you finish your risk assessment and treatment process.

## Step #6 – Risk Assessment & Mitigation

The details of your cybersecurity implementation will depend on your objectives and the framework you choose. No matter which approach you take, it will have to be based on managing your information security risks.

### The purpose of risk management

Why are risk assessment and treatment important? Let me give you an example.

Let's say you frequently leave your laptop on the back seat of your car. Chances are, sooner or later this laptop will be stolen. What can you do to decrease the risk of compromising confidentiality, integrity and availability of the information stored on that laptop?

First of all, you can make a rule (by writing a procedure or a policy) that laptops cannot be left in a car unattended, or that you have to park a car where some kind of physical protection exists. Second, you can protect your information by setting a strong password and encrypting your data. Further, you can require employees to sign a statement by which they are legally responsible for the damage that may occur. But, all these measures might remain ineffective if you do not explain the rules to your employees through training.

So, what can you conclude from this example? Information security is never a single security control. This is always a combination of safeguards, and the safeguards must not be only IT-related, they must also involve organizational issues, human resources management, physical security and legal protection.

The problem is that this example was a single laptop, with no insider threat. Now, consider how complex protecting the information in your company is, where the information is archived not only on your PCs, but also on various servers, in desk drawers, on your mobile phones, on USB memory sticks, and in the heads of all employees. And what if you have a very disgruntled employee?

Securing all this information can seems like an impossible task. Difficult? Yes, but not impossible. The answer is systematic risk assessment and risk treatment (i.e., mitigation).

## Elements of risk management

The methodologies for risk management vary, but in essence risk assessment is finding out which kind of bad things can happen to every important piece of information in your company. Risk treatment is finding the best ways (and the

most cost-effective ones as explained in Step #2) to mitigate the largest risks.

Therefore, risk assessment and treatment should be the centerpiece of your cybersecurity, and all the safeguards (or at least most of them) should be implemented based on risk management. Otherwise, you may find yourself investing huge amounts of money in some safeguards that are actually not needed (i.e., there are no risks or they are too low), while some bigger risks are left unaddressed.

Do not rely on someone's instincts to be aware of all the risks. From my experience, IT people are usually aware of only 40% of the risks that are present in their departments, while people from the business side of the organization score even worse at somewhere around 25%. To get a better feeling about which risks can happen in your company, see this List of threats and vulnerabilities.

## Step #7 – Implementation of Safeguards

Once you are finished with your risk assessment and treatment, make sure you write a very precise action plan. In this action plan you should specify exactly what should be implemented, the deadlines, who is responsible, the budget, and who has to be notified about the implementation. This action plan must be incorporated with your project plan.

The implementation of cybersecurity is usually performed through these means:

1) **Defining new rules:** Rules are documented through policies, procedures, instructions, etc., although you will not have to document some less complex processes. Scaling your documentation for your real needs is extremely important. Example: if you are a smaller company with 50 employees, you certainly don't want 150 new policies and procedures, each of them 20 pages or more. Also, observing the existing rules that work well in your company is advisable – you do not have to change everything in your company just because you are implementing ISO 27001. Just remember the documentation myth I mentioned in Section 2: writing the

documents is not enough; what is much more important is to live those rules in everyday life.

2) **Implementing new technology:** As said before, think hard before you purchase some expensive new system. Sometimes alternatives will exist that will be as effective, but with lower cost. Also, be aware that most of the risks exist because of human behavior, not because of machines. Therefore, it is a question of whether a machine is a solution to such a problem.
3) **Changing the organizational structure:** In some cases you will need to introduce a new job title, or change the responsibilities of an existing position. A typical example is to introduce a position of Chief Information Security Officer (CISO) who is responsible directly to the Board. Usually, such a person comes from the IT department, but to avoid a conflict of interest, this position has to be brought out of that department. Cybersecurity implementation might also mean you will need to hire someone full time. In smaller companies try to avoid such an increase in costs by adding additional tasks and responsibilities to existing personnel.

From a management perspective, it is important that you will be able to track not only if the safeguards were implemented as planned, but even more importantly, if they have fulfilled their purpose.

In order to be able to follow the track record of your safeguards you need to ask your project team three things:

(1) To define measurable objectives for each implemented safeguard.

(2) To define a method by which your company will measure periodically if the objectives have been achieved.

(3) To establish responsibilities for measuring and reporting the results.

Do not confuse these objectives and metrics with objectives from Step #3. In Step #3 I was talking about the objectives for your whole cybersecurity that should enable judging whether your whole cybersecurity effort makes sense. As opposed to that, here I'm talking about lower level objectives, for each element of your cybersecurity, the purpose of which is fine-tuning every nut and bolt of your system.

This is the only way to create a basis for (always necessary) improvements.

## Step #8 – Training & Awareness

Lack of training and awareness is the number two reason of failure of cybersecurity projects. Why?

**Security is usually a drag.** As mentioned before, no one likes changing passwords more frequently than before and having to remember complex ones. And such an attitude is present with all other security rules. So, if you do not explain to your employees why this is necessary, they will likely look for ways to avoid such rules. The way to address this issue is to explain which kind of benefits your company will get through these safeguards, but equally important is to explain what benefits the employees will personally get from these changes. For example, if high-quality passwords are used, the chances are much lower that someone will abuse their accounts; otherwise, it would be the very same employees who might have to pay for any damage if such an incident happens.

**Security usually requires new skills.** If you implemented a new kind of (complicated) software, you cannot expect all the employees to start using the program just by reading the manual. They need training if you want to avoid mistakes.

When planning your training and awareness programs, there are three things you have to bear in mind:

1) Since cybersecurity is not only the job of the IT people, you will have to **implement such programs company-wide**. What's more, you will have to focus on employees from the business side of your organization, because they usually perceive information security as someone else's job, not theirs.
2) When implementing new safeguards you have to plan trainings and awareness sessions **in parallel to the implementation**. You cannot expect everyone to accept a new rule with enthusiasm if the procedure was published six months ago and you are just now raising awareness.
3) It is not enough to do training and awareness sessions only once. There will be new people in the company, existing people will forget about what they have heard, safeguards will change, and so on. Therefore, **training and awareness is a continuous business**, so your CISO and/or human resources department will have to act accordingly.

## (Step #9) – Cybersecurity is a Never-ending story

This is not actually a step, but a series of activities you should perform continuously if you want your cybersecurity to be effective.

Unfortunately, many times I have seen companies invest a lot of effort and resources, and after the implementation is finished, they push aside all the policies, procedures and technology because they became out of date and useless. Did I already mention this is reason number three of the most common cybersecurity failures?

If you want to avoid this you will have to focus on the following activities in order to maintain and improve your system:

**Monitoring:** Employees who are responsible for particular safeguards will have to track how they are performing. This is normally done on a regular basis. For example, a system administrator might check every day whether the backup has been performed as expected. Logging all incidents is vital when monitoring to learn why they have happened, and how to prevent them from reoccurring.

**Measurement:** As opposed to monitoring, measurement is done periodically (e.g., quarterly or annually), and the purpose is to determine if objectives are being met. There are at least two levels of objectives: general objectives that are set for your whole cybersecurity (see Step #3) and objectives set for each individual control (see Step #7).

**Listening to suggestions:** All the interested parties (employees, partners, clients, government bodies, etc.) probably have certain knowledge on where your security is lacking. You need to make sure the communication channels remain open, and that all the information reaches the right people within your company.

**Internal audit:** Although most companies perceive such an audit as a waste of money, this can be quite useful if done properly. The reality is that many employees will bend the rules in order to spend as little time as possible on tasks they consider irrelevant. In some cases, the employees are convinced they are doing things correctly, only to be discovered later that quite the opposite is true. It is very difficult to discover such deviations unless someone (objective and thorough) checks if everyone is complying with the rules.

You should also perform audits of your suppliers and partners who have access to your critical information and systems. Ultimately, an internal audit could be the biggest contributor to enhancing the security of your information.

**Top management review:** Every so often (for example, quarterly) members of your top management should dedicate some time for cybersecurity. Normally, this is done at your regular management meetings, where one topic is cybersecurity. For such a meeting, the person in charge of cybersecurity should prepare materials such as: measurement results, internal audit results, list of incidents, newly identified threats, required investments, proposals for changes in policies, etc. Based on this knowledge, top executives should reach some important decisions such as: changing the objectives of cybersecurity, providing resources, making organizational changes, removing obstacles to implementation, etc.

**Certification audits:** Such audits might not be mandatory, but could be useful for marketing purposes. They can also be helpful for improving the level of security, because if everyone in the company knows there will be a certification audit coming at a particular date, greater effort will be made to make everything right.

**Continuous improvement:** All the mentioned activities will create a kind of To-Do list that has to be implemented. ISO standards have a practical way of approaching these lists in a systematic way – this concept is called *corrective and preventive actions*. They have to be listed in a transparent way with clear deadlines and responsibilities, and once implemented every one of them has to be checked to make sure the problem was really eliminated.

And there are the 9 steps you need to do. While this might sound time consuming and challenging, let me ask you one question: if you omit any of these steps, do you think your cybersecurity will work?

The answer is probably not.

This is why I think it is extremely important that you know what the elements of cybersecurity are, so that when you let your specialists do the implementation, none of the important steps are forgotten.

# Chapter 5: Conclusion

While working with many companies and helping them implement information security/ cybersecurity projects, I have realized one basic fact: the management of most of the companies had misconceptions of what cybersecurity actually is.

And what's more, too few of them had a real idea of how cybersecurity could actually help their core business.

So, I hope this book has helped you to understand all these issues and explained how to use cybersecurity as a tool to make your business more successful.

# Appendix

## Legislation Related to Information Security and Business Continuity

To see an unofficial list of laws and regulations worldwide, click here.

Laws and regulations in the United States that have requirements related to information security and business continuity are as follows:

- 6 CFR Part 29 Procedures for Handling Critical Infrastructure Information - Department of Homeland Security
- ACH Rules Book of 2001 (National Automated Clearing House Association - NACHA)
- Adam Walsh Child Protection and Safety Act of 2006
- Cable Communications Policy Act (Cable Act) of 1984
- California SB 1386 Security of Non-encrypted Customer Information of 2003 (State of California) and progeny
- The Californian Online Privacy Protection Act of 2004
- Children's Internet Protection Act (CIPA) of 2001

- Children's Online Privacy Protection Act (COPPA) of 1998
- Communications Assistance for Law Enforcement Act (CALEA) of 1994
- Computer Fraud and Abuse Act (CFAA) of 1986 (FTC - Federal Trade Commission)
- Computer Security Act of 1987 – [Superseded by the Federal Information Security Management Act (FISMA)]
- Consumer Credit Protection Act (CCPA) of 1992 Section 2001 Title IX – Electronic Funds Transfer
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003
- Deleting Online Predators Act of 2006
- The Digital Millennium Copyright Act of 1998
- Driver's Privacy Protection Act of 1994
- Electronic Communications Privacy Act (ECPA) of 1986
- Electronic Freedom of Information Act (E-FOIA) of 1996
- Electronic Fund Transfer Act (EFTA) (OCC)
- Fair and Accurate Credit Transactions Act (FACTA) of 2003
- Family Education Rights and Privacy Act (FERPA; also known as the Buckley Amendment) of 1974

- Federal Acquisition Regulation: Electronic Funds Transfer Final Rule (Securities and Exchange Commission)
- Federal Information Security management Act (FISMA) of 2002 (FTC)
- Federal Trade Commission Act (FTCA) of 1999
- FERC COOP 2007: FERC RM01-12-00 (FERC - Federal Energy Regulatory Commission)
- FFIEC FIL 67-97/82-96 (FFIEC - Federal Financial Institutions Examination Council)
- FFIEC Policy SP-5 (FFIEC - Federal Financial Institutions Examination Council)
- Foreign Corrupt Practices Act 1977 (P.L 95-213)
- Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) of 1999
- Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule #7. Contingency Plan 164.308 (a)(7)(i)
- Inter-Agency Policy of 1997 from Federal Financial Institutions Examination Council (FFIEC)
- Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System of 2003 - Federal Reserve System; OCC (Office of the Comptroller of

the Currency); SEC (Securities and Exchange Commission)
- Internet Gambling Prohibition and Enforcement Act
- IRS Procedure 91-59 (superseded IRS Procedure 86-19) (IRS - Internal Revenue Service)
- Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth of 2010
- Minnesota Plastic Card Security Act (PCSA) of 2007
- NASD Rule 108 (Sept 9, 02) and SR-NASD 2002-112 (March 10 2003)(Release No. 34-48503: File NO SR-NASD-2002-108)(NASD (North American Securities Dealers Association) / SEC)
- NASD Rule 3500: Emergency Preparedness Part 3510: Business Continuity Plans (NASD)
- NASD Rule 3500: Emergency Preparedness Parts 3520: Emergency Contact information (NASD)
- Nevada Security of Personal Information Law of 2005
- NFA Compliance Rule 2-38: Business Continuity and Disaster Recovery Plan (CFTC - Commodity Futures Trading Commission)

- NYSE Rule 446: Business Continuity and Contingency Planning (NYSE - New York Stock Exchange)
- OCC 2001-47. Third Party Relationships of 2001 (OCC - Office of the Comptroller of the Currency)
- Privacy Act of 1974 (SUSC552a)
- Privacy Protection Act (PPA) of 1980
- Public Law 110-53 Title IX (PS Prep)
- Right to Financial Privacy Act (RFPA) of 1978
- Sarbanes-Oxley Act of 2002 (PL 107-204 2002 HR 3763) – Section 404 (PCAOB (Public Company Accounting Oversight Board))
- Sarbanes-Oxley Act of 2002 : Section 409 (PCAOB)
- Securities and Exchange Act, Sections 32(a) and (b) (SEC)
- Telecommunications Act of 1996
- Telephone Consumer Protection Act (TCPA) of 1991
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001
- Video Privacy Protection Act of 1988 discussion and overview

- Washington State HB 1149: Protecting consumers from breaches of security of 2009

Grateful thanks to Lisa Sotto of Hunton & Williams for help with making this list.

# Bibliography

BS 25999-2:2007, *Business continuity management. Specification*

COBIT 5, *A Business Framework for the Governance and Management of Enterprise IT*

ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements*

ISO 22301: 2012, *Societal security – Business continuity management systems – Requirements*

ISO/IEC 27000:2009, *Information technology -- Security techniques – Information security management systems – Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 27032:2012, *Information technology – Security techniques – Guidelines for cybersecurity*

ITIL©, *IT Infrastructure Library*

NFPA 1600, *Standard On Disaster/Emergency Management And Business Continuity Programs*

NIST Special Publications (800 Series)

PCI DSS, *Payment Card Industry Data Security Standard*

http://blog.iso27001standard.com/ ISO 27001 & ISO 22301 Blog

# Index

# About the Author

Dejan Kosutic is the author of numerous articles, video tutorials, documentation templates, webinars and courses about information security and business continuity management.

He is the author of the leading blog on ISO 27001 – the ISO 27001 & ISO 22301 Blog, and has helped various organizations including financial institutions, government agencies, and IT companies implement information security and business continuity management according to these standards.

He has an MBA from Henley Management College (now Henley Business School).

Click here to see his LinkedIn profile.

# Contact Information

Company Name: EPPS Services Ltd.
Author: Dejan Kosutic
Address: Nazorova 59, 10000 Zagreb, Croatia
Website: http://www.iso27001standard.com/
Email: info@iso27001standard.com
Phone: +385 98 304 566
Fax: +385 1 556 0711
Twitter: https://twitter.com/Dejan_Kosutic
Facebook:
http://www.facebook.com/pages/Information-Security-Business-Continuity-Academy/119822218040795