# The Chief Information Security Officer

## Insights, tools and survival skills

Barry L. Kounds
Jake Kounds

IT Governance Publishing

# The Chief Information Security Officer

## Insights, tools and survival skills

# The Chief Information Security Officer

## Insights, tools and survival skills

BARRY L. KOUNS
&
JAKE KOUNS

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely
Cambridgeshire
CB7 4EH
United Kingdom

www.itgovernance.co.uk



First published in the United Kingdom in 2011 by IT Governance Publishing.

ISBN 978-1-84928-183-6

# FOREWORD

Welcome to *The Chief Information Security Officer: Insights, tools and survival skills*. This book challenges security professionals to recognize that the serious and ever-changing nature of today's security threats demands a strategic-minded response and not just an operational reaction to the latest headlines. It poses the premise that it's time for CISOs to transition from being a security coordinator, to being an evangelist for risk management who is also a technology innovator and a trusted adviser to senior management.

The goal of this book is to challenge and guide information security professionals to think about information security and risk management from the enterprise level and not just from the IT perspective. The practical information presented will help CISOs understand how an enterprise view of information security, business continuity, compliance, safety and physical security impacts risk and is crucial for the success of tomorrow's CISO.

## WHO SHOULD READ THIS BOOK

This book is recommended for current and newly appointed CISOs, CIOs and senior managers involved in, or interested in, the management of information security and technology risk management. Anyone thinking about a career in information security would gain from the insights provided and the skills discussed. The topics discussed are applicable to all industries and geographic locations worldwide. All organizations can benefit from the material covered, but the guidance offered would be most applicable to medium to large organizations with the complexity to warrant the CISO position. In addition, this book can be a how-to guide for the Information Security practitioner as it would help them understand the goals of a CISO and an Information Security department. CEOs, CIOs, CFOs and anyone else who has responsibility for managing a CISO could use this book to better understand the role and the best way to fully support the function.

## ABOUT THE AUTHORS

Barry Kouns is a security and risk management expert with over 25 years of experience in information security consulting, risk assessment and quality management. He formed and operates SQM-Advisors, an information security, risk assessment and IT service management firm that has led eight organizations to ISO/IEC 27001:2005 certification. Mr Kouns is frequently quoted in magazines and news articles on information security and has held the position as Trainer for the British Standards Institute (BSI). He holds a BS in Statistics and a MS in Industrial Engineering Management. Mr Kouns has earned the CISSP designation and is a trained ISO/IEC/27001 Lead Auditor and ISMS Implementer, and is ITIL Foundation Certified.

Jake Kouns holds a Master of Business Administration with a concentration in Information Security from James Madison University. He holds a number of certifications including CISSP, CISM, CISA and CGEIT. Mr Kouns is currently Director of Cyber Security and Technology Risks Underwriting for Markel Corporation, a specialty insurance company. He has presented at many well-known security conferences including RSA, CISO Executive Summit, EntNet IEEE GlobeCom, CanSecWest and SyScan. He is the co-author of *Information Technology Risk Management in Enterprise Environments* and has also been interviewed numerous times as an expert in the security industry. Mr Kouns is the co-founder, CEO and

CFO of the Open Security Foundation (OSF), a non-profit organization that oversees the operations of the Open Source Vulnerability Database (OSVDB.org) and DataLossDB.

## ACKNOWLEDGEMENTS

The authors would like to express gratitude to our wives, Roxanne and Jill, for their wisdom and support during the writing of this book. A special thanks to Elora Nicole, Devin Jacob and Savannah Rose for their continuous optimism.

## CONTENTS

# INTRODUCTION

This book is divided into eight chapters designed to introduce you to the CISO position by discussing the tools used by the most effective CISOs and how current CISOs can grow with the challenges of the position. A brief description of each chapter follows:

**Chapter 1 The nature of the CISO role**: The CISO is bombarded with new issues on a daily basis, making it one of the most challenging positions in organizations today. CISOs find themselves held responsible for the protection of the organization's information, but often reporting to the CIO who is rewarded for making the organization's information more readily available to all.

**Chapter 2 The traditional CISO job description**: The CISO is responsible for overseeing the overall corporate security strategy, security architecture and security function. The scope of the role traditionally covers all implemented security technologies and services, including security applications, perimeter defenses, physical and logical access control, and access management for all employees, contractors and visitors.

**Chapter 3 The changing CISO role**: The experience and skills that made yesterday's CISO successful will no longer meet today's organizational needs. While still very much a technologist, today's CISO must have excellent communication and presentation skills, be able to

understand everything as a process and demonstrate keen business acumen.

**Chapter 4 The new CISO's toolbox**: Today's CISO cannot remain just a master technician, but needs to develop the skills of a leader, facilitator, communicator and an agent of change. Today's CISO needs to prepare to be a trusted adviser to senior management who can translate information security threats and business risk into terms that stakeholders can relate to and understand the impacts.

**Chapter 5 Risk management**: The heart of any Information Security Management System (ISMS), is the risk management methodology. The methodology used to identify, analyze, evaluate and treat risks is foundational to any ISMS and sets the stage for identifying and appropriately protecting the organization's assets. A proper risk assessment foundation must be in place to ensure a CISO's success.

**Chapter 6 The Information Security Management System**: This chapter discusses the elements of a living, breathing Information Security Management System (ISMS) as defined in ISO/IEC 27001:2005, and the benefits of ISMS implementation and third party certification. Third party certification of an organization's security program can provide the CISO with professional credibility and be a competitive differentiator in today's environment.

**Chapter 7 CISO survival**: Forty-four percent of global companies employed a CISO in 2009

compared to just 29% in 2008.[1] How many of these CISOs will remain employed will for the most part be determined by how well they prepare and position themselves for survival. This chapter discusses the techniques and strategies needed to better your chances for remaining in the role.

**Chapter 8 Summary – you become what you think about**: With the challenges facing a CISO on a daily basis, focus on and proper thinking about your role in risk and security is essential. Making a conscious effort to think about what you want to become can have a powerful impact on your job effectiveness and your success in life, if you think about the right things. This chapter offers guidance on how to properly align your thinking with the needs and challenges of today's organizations.

[1] The Global State of Information Security Survey, 2010 conducted by PricewaterhouseCoopers.

## CHAPTER 1: THE NATURE OF THE CISO ROLE

Technology presumes there's just one right way to do things and there never is.

*Robert M. Pirsig*
*American Writer and Philosopher*

Chief Information Security Officers (CISOs) are bombarded with new challenges every day. In fact, the challenges that demand the CISO's daily focus change so fast it makes little sense to list them here since they will be replaced with others tomorrow. Instead, let's take a look at the very nature of the role and why it may well be one of the most unique and challenging in organizations today.

Information security and the role of the CISO has for far too long been about implementing the latest security technology. Yes, technology plays a large role in businesses today, but identifying and implementing technology is only part of the information security challenge an organization faces. In fact, in today's successful organization, implementing technology is only a small part of the CISO's role.

Today's CISO quickly discovers that they are in a dilemma of sorts; they are held responsible for the protection of the organization's information, but often reporting to the CIO who is rewarded for making the organization's information more readily available to all. CISOs are in the business of managing information, not just securing it.

Information that was once a static entity that stayed where you stored it, is now on the move, constantly flowing in and out of the organization. Traveling via laptops, thumb drives, PDAs, smart phones and all means of Internet connectivity, information can no longer be protected by simple perimeter-based security.

**The beginning**

The title of Chief Information Security Officer, CISO, burst onto the national scene soon after the attacks on September 11, 2001. Creating a dedicated office of the CISO became the go-to answer for many companies anxious to demonstrate a serious commitment to information security, disaster recover planning and business continuity. A CISO was appointed/hired because company executives believed a dedicated office and an appointed executive would be viewed by clients and regulators as the best way to address the security "issue."

Many of the first CISOs came from the ranks of current employees that were simply re-cast into the new role. Most CISO offices were set up with the belief that responsibility for the organization's information security is a task like any other that could be assigned to a single individual in the company. With few to no staff and limited budgets, minimal formal security education and a reporting structure through the CFO, CIO or lower, the first CISOs were simply tolerated and only appreciated during an audit or the recovery from a crisis.

**Forever increasing threats**

Law enforcement investigations over the past several years have discovered that cybercrime is an organized global business that hires, equips and directs hackers in their attacks on financial institutions and personal accounts. The creation of new malware programs in 2009 far exceeded any forecasts and today averages well over 55,000 new programs per day.[2] The number of financial service companies indicating that they had suffered a data loss within the past 12 months rose to 42%, nearly a 50% increase from the previous 12-month period.[3]

According to Symantec,[4] 75% of enterprises surveyed experienced some form of cyberattack in 2009, showing that the risk is not limited to a few large organizations. Attackers are increasingly looking to exploit new Web 2.0 technologies and social networks for criminal purposes. Drive-by-downloads (infecting or taking over a legitimate website with the purpose of infecting visitors), social network infections, "vishing" (voice phishing), "smishing" (SMS or text phishing) and variations of spear phishing are all used by fraudsters around the world to attack banks, credit unions and credit card companies in order to attempt account takeovers.

Exploits against the ever-increasing sophistication of smart phones, like MITMO (Man in the Mobile), or building a botnet using the iPhone or

[2] *Annual Report PandaLabs 2009*.
[3] *Global Fraud Report*, Annual Edition 2010/11, Kroll/EIU.
[4] *2010 State of Enterprise Security Report*, Symantec.

Android phones, have become a greater threat as smart phones become more ubiquitous. Multi-factor authentication, once thought to be the pinnacle of layered security, has been defeated by Trojans subjecting users to "man-in-the-browser" attacks targeting online banking accounts.

And last but not least, the trusted insider remains the most dangerous adversary for any CISO. The frequency of insider-committed or assisted crime can be blamed on several factors, but the threat is predicted to increase in part because of the poor economy and the constant move toward ease of access to the organization's data. A forever-changing and growing threat landscape is a fundamental element of the nature of the CISO's role.

**Challenges**

As if the constantly evolving threat landscape is not challenge enough, most CISOs find themselves with limited resources and not reporting directly to top management. The role is large and complex, and the CISO often needs to make risk trade-offs when deciding how to spend their limited dollars or task their scarce human resources. Without a seat at the table with senior management, the CISO often makes risk trade-off decisions well above their pay grade. Risk decisions that should be made by senior management after understanding the potential impact on the business, are often forced upon the CISO.

Another substantial challenge for the CISO, is the human element. Whether it's the lack of information security awareness or the innovation

people display when trying to work around security controls to do their jobs, the human element remains a top CISO challenge. As tough as implementing new technology can be, nothing is as demanding as managing people during the implementation of change. Add to this an intensifying regulatory environment and limited available metrics and you begin to understand the challenges faced by the CISO.

**The satisfaction**

The CISO is meant to drive all information security functions within an organization and effect change across the entire enterprise. The role provides the opportunity to have significant impact and influence on the security posture of the organization. As cybercrime has emerged as a major national security concern, and compliance with new regulations pose greater threats to organizations, the CISO is expected to lead the company's response.

If you love a challenge, enjoy learning, relish something new every day and want to make a real difference in the safety and soundness of your organization, the CISO role has it all.

## CHAPTER 2: THE TRADITIONAL CISO JOB DESCRIPTION

Tradition becomes our security and when the mind is secure, it is in decay.

*Jiddu Krishnamurti*
*Indian Philosopher*

The position and title Chief Information Security Officer (CISO) refers to the individual in an organization with an exclusive information security focus. The CISO is the individual responsible for overseeing the overall corporate security strategy, security architecture and security function. The scope of the role traditionally covers all implemented security technologies and services, including security applications, perimeter defenses, physical and logical access control, and access management for all employees, contractors and visitors. As the company's dedicated information security officer, this role also has enterprise-level responsibility for all data/information security policies, standards, evaluations, audits and corporate security awareness programs.

The CISO works with user and technical groups as well as internal auditors in the development and implementation of a security strategy designed to provide a high level of security over information and information processing systems while preserving and enhancing system access and usability.

A typical CISO is responsible for directing the overall activities of the security function along with the following roles and functions:

- Develop and implement policies, standards and guidelines related to information security.
- Develop, implement and manage the overall enterprise process for security strategy and associated architecture using security standards and best practice.
- Work with corporate executives, business managers, internal audit and legal counsel to understand security and regulatory compliance requirements and to map those requirements to current projects.
- Oversee the continuous monitoring and protection of information and information systems.
- Serve as the enterprise focal point for security incident response planning and execution.
- Investigate and analyze suspected security breaches and recommend corrective actions.
- Define and implement an ongoing Information Security Risk Assessment program, which will define, identify and classify critical assets, assess threats and vulnerabilities regarding those assets and recommend safeguards.
- Assist internal audit with developing appropriate criteria to assess the compliance of new/existing applications and technology with enterprise security standards and best practice.
- Establish and monitor the analysis of the planned procurement of new applications, services and technologies.

- Oversee the development and implementation of a corporate information security awareness and training program.
- Evaluate changes to the corporate environment for security impact and present findings to management.

Generally reporting to the CIO, Legal Counsel or Chief Financial Officer, the CISO is often viewed as a technician and policy enforcer who ensures that the organization's networks, information and information systems are secure. Often this places the CISO in a negative light when perceived by business units as saying no to the implementation of new products and services.

Qualifications for the early established CISO positions often read more like that of a subject matter expert then a senior manager:

- Awareness of and experience in:
  - vulnerability testing and penetration testing
  - standards-based architecture
  - network-based security
  - compliance monitoring and policy enforcement
  - developing security practices.
- A college degree (BA/BS), or equivalent work experience.
- Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and/or Certified Information Systems Auditor (CISA).
- Results-oriented and commitment focused.
- Excellent project management skills.

- Business continuity planning, auditing and vendor management experience.
- Knowledge of pertinent regulations and laws.

Although technical expertise remains a foundation requirement for the CISO role, to be truly effective today, the CISO must be an articulate and persuasive leader with real business experience who can communicate security-related concepts to the senior management team in order to guide risk management decisions. Chapter 3 will continue the discussion about the changing role of the CISO.

## CHAPTER 3: THE CHANGING CISO ROLE

Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting others to current facts.

*William O. Douglas*
*US Supreme Court Justice*

The experience and skills that made yesterday's Chief Information Security Officer successful will no longer meet today's organizational needs. While still very much a technologist, today's CISO must have excellent communication and presentation skills, be able to understand everything as a process and demonstrate keen business acumen. Today's successful CISO will be able to relate the adoption of new technology with the legal, regulatory and business objectives in a way management can use when making decisions about resource allocations and risk management.

While today's CISO must stay abreast of the latest in security technology, the position requirements go far beyond this alone. Managing information security today has evolved into being more about the management of risk, business priorities, compliance requirements and the latest threats to the business. Today's CISO needs to be integrated into all aspects of the business and have a full understanding of the business requirements, strategy and objectives in order to do the job effectively.

**Today's CISO – enlightened leader**

Today's threat environment requires more than a security function coordinator. The successful CISO will not only fulfill the role of security leader, but will also act as a connecting agent between functions to assist executives in seeing their common challenges. The CISO will accept the role of helping to build these connections between departments to specifically address the challenges impacting security and operational risk. By virtue of their position, CISOs have the ability to not only add value and lead a business-enabling function, but also to provide the means for a competitive advantage for the organization.

The CISO as an enlightened leader realizes that organizations succeed by taking risks and the ones that fail do so because they didn't take the right risks or they didn't oversee the risk management process very well. CISOs need to consider risk from a business perspective and view each business function owner as a customer that requires help to innovate or deliver his/her product/service. The days of automatically saying no to any new idea that involved access to sensitive data, penetration of the security perimeter or allowing mobile computing or remote access to data, must be left behind for the new CISO. Today's new solutions are opportunities for the enlightened CISO to provide creative direction and influence to directly contribute to the overall revenue growth while ensuring information security for the organization.

A large part of a CISO's job is to clearly articulate to everyone in the organization how security

relates to business objectives. To be effective as the organizational communicator, the CISO must assume a variety of roles to reach all employees from the shop floor to the board room. To deliver the message about the importance of information security effectively, the CISO must be prepared to play an enabling role during system development, by introducing security early, and by being accessible, approachable, responsive and willing to be accountable throughout the product lifecycle.

**Holistic security**[5]

Even though CISOs frequently participate in related areas such as business continuity/disaster recovery planning, loss and fraud prevention, physical security and employee safety in addition to information security and privacy, it is rare today for the CISO to have full responsibility for these areas. In organizations taking an enlightened view of the total responsibilities placed on the security officer, the title Chief Security Officer (CSO) has emerged as the executive responsible for the organization's entire corporate security posture including human resources, physical and electronic assets.

There are a number of factors at work, not the least of which is the growing motivation of CEOs and corporate boards to take a strategic and enterprise-wide view of business risk. Driven in part by regulations such as the Sarbanes–Oxley Act, Gramm–Leach–Bliley Act and Health Insurance Portability and Accountability Act, organizations

[5] The holistic security momentum theory: Why resistance is futile, Derek Slater, 15 April 2005, CSO.

realize the importance of coordinating compliance activities in order to positively impact business objectives, internal operations, external partner relationships and, most importantly, satisfying customers. In addition, the following business forces are taking place that require a consolidated and efficient response from a CISO.

**Technology convergence**: Physical security controls such as video surveillance, access control and fraud detection are increasingly database driven and network delivered. The CISO, like it or not, will be ever more involved in these areas.

**Security provider convergence**: More and more, the traditional physical security service provider is packaging electronic services, such as managed network security, supply chain security consulting and data recovery, to offer cross-functional services.

**Threat convergence**: As technology plays a larger role in physical security, the threat of a blended attack, one that combines both a physical and logical element, is likely. An example would be a Distributed Denial-of-Service (DDoS) attack aimed at a website and/or telecommunications concurrent with a physical assault against the premises.

In summary, at the tactical level, technology is increasingly being infused into physical security tools, and at the strategic level, CEOs and corporate boards are looking for one person to go to for both advisory services and guidance during times of crisis. The new CISO needs to prepare for this role.

## CHAPTER 4: THE NEW CISO'S TOOLBOX

Tomorrow comes at us with ever-increasing speed. We need to engage it – today. Seize its opportunities – now. Start shaping its possibilities – in this very moment. And our approach must be very different from the behaviors we've relied on in the past.

*Dr. Price Pritchett*
*Author and Management Consultant*

According to Cisco's CSO, John Stewart, "the number and quality of security professionals being educated in the nation's universities (USA) increased in recent years, but there's still a shortage."[6] Yet in spite of this somewhat encouraging news, there appears to be a chasm between C-level managers' expectations and reality with regard to the security professional's ability to not only understand and align with business objectives but to actively participate in achieving those objectives.

To narrow the chasm between expectations and reality, today's CISO cannot remain just a master technician, but needs to develop the skills of a leader, facilitator, communicator and an agent of change. Today's CISO needs to prepare to be a trusted adviser to senior management who can translate information security threats and business

[6] CISOs have growing clout in agencies, but still face challenges, William Jackson, 30 April 2009, Government Computer News.

risk into terms that stakeholders can understand and relate to.

This chapter discusses the skills required of the new CISO in order to be this trusted adviser.

Let's begin by contrasting the labels used to describe the CISO of yesterday to the adjectives defining the new CISO (Table 1).

| Yesterday's CISO | New CISO |
|---|---|
| Subject Matter Expert | Trusted Adviser |
| Analyst | Facilitator and Leader |
| Technical Risk Expert | Risk Manager |
| Individual Contributor | Integrative Business Thinker |
| Chief Security Officer | Chief Risk Officer |
| Administrator | Strategist |
| Manager | Visionary |

**Table 1: Labels used to describe CISOs**

The most obvious contrast identified above is that yesterday's CISO is singularly focused on individual expertise and all things technical while the new CISO's focus is on leadership, risk management and business objectives.

**How do we start the shift?**

In short, CISOs need to break the stereotypes. The first, and possibly the most, ingrained stereotype is that security professionals don't understand business. Or at least they don't demonstrate any signs that they do. It appears to most senior managers that the only risk a CISO focuses upon is the risk of loss, and never do they hear CISOs speak of the business benefits of taking risks to meet objectives.

The CISO's focus on the negative and the potential loss expressed in terms few understand, like cyberforensics, intrusion prevention and security patches, all cause most managers to believe CISOs have little interest in or understanding of business. The truth is there are few people in the organization in a better position to understand the business processes than the security professional. How else would a CISO know what needs protection, where to place the controls and how to implement those security measures?

The issue then, is that CISOs need to shift at least part of their attention to how to add increased value for clients and stakeholders without increasing the risk to the organization's assets. CISOs need not always be focused on decreasing risk. Sometimes increasing the potential of positive outcome without increasing risk is what the business needs. Today's security professional, the new CISO, is in a great position to offer insight into how the business can do just that.

**What actions can you take today?**

1 **Learn what keeps senior management up at night**: In the past, security professionals could allow themselves to be primarily focused on regulatory compliance and corporate governance issues; however, today's CISO needs to be a trusted adviser as management seeks to balance risk aversion and value-creating behavior. Senior managers must focus on creating and sustaining business value. The CISO's job is to understand what this means to the business and to proactively support their efforts. According to IBM's 2010 Global CEO Study,[7] CEOs are focused on adopting new channels to engage and stay in tune with customers, capturing and analyzing the data that is flowing from social networking sites and to take full advantage of emerging advanced technologies. As a security professional, you are in a unique position to assist in these areas.

2 **Learn what your business competitors are doing**: One of the best ways to demonstrate your value to senior management is to discover and report on what technologies and initiatives your competitors have implemented or are considering. Some of the best places to find information on the competitive landscape in your business sector include the Internet, competitors' locations, the competition's customers, competitors' ads, trade shows, marketing and advertising publications, local newspapers and business journals, industry

[7] *2010 IBM Global CEO Study*.

and trade association publications, and industry research and business surveys.

3 **Look for ways new technology can benefit your business**: Technology is constantly changing and at any given time a new product or upgrade to an existing product could drastically alter the competitive landscape. Whether the new technology will improve customer service or allow you to be more price competitive, not being aware could place your business's survival at risk. The actions required to discover the innovations are simple and straightforward. The discipline to persevere is the challenge. There are entire sections in most e-papers devoted to technology news. Make it a habit to scan over the articles looking for news about computers, telephones, wireless networking, software and consumer-focused technology news. Google™ and other search engines allow you to sign up for news alerts using specific keywords. The Internet houses a wealth of information about the latest in technology and product and service enhancements. Take note of your surroundings and especially notice the technology used by the 20-year-olds.

4 **Learn how to speak business**: The days of the security guru hanging out in the data center without face-to-face contact with management are over. Not only do CISOs need to come out from the dark, they need to be able to speak a language management can understand about the topics that they care most about. Remember senior managers are interested in broad business issues like long-term corporate strategy and how to increase revenue,

profitability and market share. Being able to relate your goals and objectives to a business-focused value proposition is critical to any C-level executive listening to you. Although polishing your group presentation skills will always come in handy, you need to be able to explain easily how your security-based initiatives align to the business goals. Define the way your initiatives support their objectives and be ready to interject when appropriate. Listen to how non-technical managers talk to one another and avoid using security jargon whenever possible.

5 **Dress for your audience**: This means dress to fit in with the people you are addressing and not necessarily the way you usually dress every day or according to what may be acceptable at your company. This could mean a business suit, business casual, weekend casual or something in between. Depending on the audience you are addressing, a business suit won't help when you are trying to make a point with the 20-something attendees. Wearing your jeans and T-shirt or even a business suit that looks like it belonged to a family member, when asked to present to the board, will detract from your message. Always inquire about the appropriate and proper dress and don't take a flimsy answer from the organizer. Know how you need to dress. There are numerous reasons for the poor communication between security professionals and management; don't let your appearance be one of them. It doesn't take much to look around and determine how to dress like the C-level managers you want to influence. Don't

jump from torn jeans and a T-shirt to a business suit; everyone will think you have a job interview. Start off slowly by going to the next level of dress over a period of weeks. Dockers and a golf shirt with a collar, followed by dress slacks and a short-sleeve dress shirt and then to a business suit. You are looking to fit in with the level you want to influence.

6 **Write for your audience**: Just like you need to dress for your audience, you need to write appropriately for your intended audience as well. It may be perfectly acceptable to come right-to-the-point using the appropriate technical jargon and abbreviations when writing to your security colleagues, but, when communicating with management you need to know how they think and how they prefer to be briefed. When writing to a C-level executive, think business journal. Articles in the world's best business newspapers say it all in the very first lines of each article. If you want more details you read on if not, you can stop and still know the key points. You need to learn how to write as if your article would be published in the *Wall Street Journal*, *The Times* of London or *The Globe and Mail*. Think of it as starting with the conclusion and then providing the details to back it up. Don't think management will read through your entire thought process to reach the conclusion with you. It's not how they think.

7 **Make yourself known outside your organization**: No matter how little your senior management team seems to know what you do all day, the moment your name or your

company's name is mentioned positively in print or at a management gathering they will care and care a lot. Consider setting yourself up on LinkedIn and Twitter and freely share in your areas of expertise. Contact organizations that set up conferences and volunteer to speak. Start a blog about one of your passions and update it regularly. Look for opportunities to volunteer your time and talents in your field of expertise. Jump at every chance you get to meet new people because the more people you meet, the more people will know you, and the more they know you the better your chances are of finding an opportunity to bring favorable press to you and your company.

8 **Think holistically about your job**: In organizations taking an enlightened view of the Chief Information Security Officer's role, the CISO is the executive responsible for the organization's entire corporate security posture including both physical and electronic. At the tactical level, technology is increasingly being infused into physical security tools, and at the strategic level CEOs and corporate boards are looking for one person to go to for both advisory services and guidance during times of crisis. The new CISO needs to prepare for this role.

## CHAPTER 5: RISK MANAGEMENT

Good risk management fosters vigilance in times of calm and instills discipline in times of crisis.

*Dr Michael Ong*
*Executive Director, Center for Financial Markets*

This chapter is about the heart of any Information Security Management System; the risk management methodology. The methodology used to identify, analyze, evaluate and treat risks is foundational to any ISMS, and sets the stage for identifying and appropriately protecting the organization's assets.

Before we begin, what would you say is the definition of risk? Most security professionals would quote something like this:

1 Risk is the impact to an asset considering the probability that a particular threat will exploit a particular information system vulnerability.
2 Risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset.
3 Risk is the combination of the consequence of an event and the probability of the event happening.

The preferable definition that can be used to teach information security risk management concepts to senior management is an extension to point 3 above.

Risk is defined as the consequence of an event *multiplied* by the probability of the event occurring.

Consequence is further defined as the impact to the organization from a breach of confidentiality, integrity or availability. Probability is defined by two parts: the probability of the threat occurring and the probability of exposure to the threat.

In other words, consequence is defined as the Asset Value (AV), the probability of the threat occurring as the Threat Likelihood (TL), and the probability of exposure to the threat as the Vulnerability Exposure (VE).

The definition of risk then becomes: Risk = AV × (TL × VE), where AV is the consequence and (TL × VE) is the probability.

*Note: Asset Value (AV) has little to do with an asset's cost or financial calculations. An asset's value to the organization is a relative measure of the impact to the organization that could be caused if that asset was breached.*

Breaking the risk equation into these three distinct elements helps both security practitioners and business owners understand the risk assessment process and to do a better job of estimating the relative ratings[8] for each element. Helping the business owners understand the risk assessment process provides accuracy, credibility and repeatability to the process. Remember, the objective of calculating risk scores is to identify

[8] A qualitative scale of 1–5 is commonly used to rate each element using definitions relevant to the organization for each number on the scale.

the appropriate allocation of your organization's limited resources to mitigate the highest risk to your most "valued" assets.

One of the best descriptions of an organizationally appropriate risk assessment approach can be found in the International Standard, ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.[9]

**What does ISO/IEC 27001:2005 have to say about risk management?**

ISO/IEC 27001:2005 (referred to as "27001" going forward) comprises two major sections: the management system requirements defined in paragraphs 4 through 8, and the security controls defined in Annex A of the standard. While organizations have the right to select only the controls applicable to their operations from Annex A, excluding any of the requirements defined in paragraphs 4 through 8 of the standard is unacceptable if an organization claims compliance with the international standard.

To be compliant with 27001, an organization must demonstrate the establishment and use of a risk assessment methodology that is suited to the business considering information security as well as legal and regulatory requirements. Paragraph 4.2 of the management system section defines the

[9] International Standard ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.

necessary and critical elements of a risk assessment methodology.

The risk assessment approach must also define the criteria for accepting risks and identifying acceptable levels of risk. The standard also provides the framework for conducting risk assessments, risk analysis and risk treatment leading to the selection of the proper security controls from Annex A.

Steps defined within the risk assessment framework include:

1 Identifying the organization's **assets and the owners** of the assets. This is all about knowing what you need to protect and who is responsible.
2 Identifying the **threats** to the assets along with the **vulnerabilities** that may be exploited. This is an analysis of how the assets may be compromised.
3 Identifying the **impacts** that losses of confidentiality, integrity and availability of the assets may have on the business. In this step, the organization determines what would be the impact or lost value to the organization if the asset was compromised.
4 Assessing the **realistic likelihood** of a security failure leading to the compromise of the asset. With the completion of this step, the organization can calculate the risks it faces, make a conscious decision to accept individual risks, or set priorities on the implementation of security controls to mitigate the risks.

The risk methodology selected does not have to be complex, expensive or over-reaching; it must

however, ensure the risk assessments produce comparable and reproducible results.

**Risk treatment plans**

With the risks to the organization more fully understood, a CISO is now ready to evaluate the various options for the treatment of risks. Possible actions could include:

- knowingly accepting risks
- avoiding risks, by not performing the activity that creates the risk
- transferring the associated risks to other parties like suppliers or insurers
- applying appropriate security controls.

If applying a security control is the preferred action in the treatment of a risk, Annex A – Control Objectives and Controls of 27001 – provides a comprehensive list of security controls that have been found to be commonly relevant in most organizations. Of course, the list claims not to be exhaustive and organizations are encouraged to add controls as needed.

As you can see, implementing a security control is just one of four potential risk treatments. It is the established and operating risk assessment methodology that allows an organization to make informed decisions about the uncertainty involved in accomplishing its objectives. The concept of risk assessment defined in 27001 has been expanded to risk management in the recently

released international standard, ISO31000:2009.[10] The next section will discuss the major concepts found within ISO31000:2009.

**ISO31000:2009: Risk management – principles and guidelines**

The recently released international standard, ISO31000:2009 (referred to as "31000" going forward), provides principles and generic guidelines on risk management and can be used by any public, private or community enterprise, association, group or individual and can be applied to any type of risk.

31000 defines risk as the "effect of uncertainty on objectives." Notice that the definition's focus is on the "effect" of "uncertainty" on the achievement of an organization's objectives and not on a single event.

The "effect" is parallel to the asset value or impact to the organization in the definition above and "uncertainty" can be thought of in terms of threat likelihood and vulnerability exposure. The real insight offered in 31000 comes with the notion that the consequence of uncertainty can not *only* involve loss, noncompliance and harm but *also* benefit and advantage to the organization.

[10] International Standard ISO31000:2009 Risk management – principles and guidelines.

**Risk management principles according to ISO31000:2009**

According to 31000 for risk management to be effective, an organization should at all levels comply with the following eleven principles:

1 Risk management creates and protects value [contributes to achievement of objectives and improvement of performance].
2 Risk management is an integral part of all organizational processes [not a stand-alone activity, but part of management's responsibilities].
3 Risk management is a part of decision making [supports fact-based decisions and helps prioritize actions].
4 Risk management explicitly addresses uncertainty [and how uncertainty can be addressed].
5 Risk management is systematic, structured and timely [provides consistent, comparable and reliable results].
6 Risk management is based on the best available information [historical data, experience, stakeholder feedback, observation, forecasts and expert judgment].
7 Risk management is tailored [aligned with the organization's external and internal context and risk profile].
8 Risk management takes human and cultural factors into account [recognizes capabilities, perceptions and intentions of both internal and external people important to the process].
9 Risk management is transparent and inclusive [open involvement at all levels assures all

views are taken into account when determining risk criteria].

10 Risk management is dynamic, iterative and responsive to change [continually sensitive to and responding to change].

11 Risk management facilitates continual improvement of the organization [implement strategies to improve risk management maturity].

Although 31000 can be applied throughout an organization, the design and implementation of your organization's risk management framework will need to take into account its particular objectives, context, structure, operations, processes, functions, projects, products, services, assets and specific practices employed.

**Risk management – the heart of information security**

The right-sized, organization-appropriate risk management process will assist you in maximizing the potential benefits and in selecting the controls necessary to protect your business while producing repeatable and comparable results to measure the effectiveness of your risk management process.

Taking the perspective that security professionals need to think and behave like "business owners," a CISO needs to not only implement a certified, living, breathing risk management methodology, but also must encourage the organization to only do business with other companies that do the same to ensure the appropriate security controls are in place.

Information security has never really been just about IT security controls. IT is only a part of the information security challenge, just as information security is only a part of the larger issue of risk management – protecting and ensuring the life and health of the business. The business of risk management is far too important to be left to any single department. Failure to manage information security risks has serious and far-reaching effects, including:

- threatening the continuity of operations
- eroding the "bottom line"
- depressing the value of the business
- compromising future earnings
- destroying an organization's reputation and image
- substantial financial penalties and even jail time.

What differentiates successful CISOs and their information security strategies from the not-so-successful appears to be a strategic and comprehensive risk management focus, rather than just reacting to security incidents one by one. Successful CISOs assure that their organizations have a defined risk management methodology that systematically identifies and evaluates uncertainty before security controls are selected and implemented. Identification and valuation of the organization's most valued assets and understanding the uncertainty surrounding those assets, along with the consequences of a security failure, is the best way to guide the appropriation of limited resources.

In order to encourage, no, in order to lead organizations to establish this framework, CISOs need to accelerate a change in focus away from technical security controls to a greater focus on an overall risk management methodology.

## CHAPTER 6: THE INFORMATION SECURITY MANAGEMENT SYSTEM

The problem is never how to get new, innovative ideas into your mind, but how to get the old ones out.

*Dee Hock, Creator of VISA*

In spite of the views of many CISOs, securing an organization's information assets has never really been *just* about implementing technical security controls. The role of the traditional CISO within the typical IT department can play only a small part in solving the information security challenge. Implementing technical security controls defined by the CISO is only a part of the larger issue of risk management. Today's CISO needs to adopt, promote and lead the implementation of an Information Security Management System designed to protect the organization's information assets and ensure the life and health of the business. The International Standard, ISO/IEC 27001:2005, defines the management system required for today's threat environment.

This chapter is not another general tutorial describing the background, history and security objectives defined in 27001. Nor is it focused on the 133 best practice security controls listed in Appendix A of the standard. Instead, this chapter discusses the elements of a living, breathing Information Security Management System defined in 27001 and the benefits of implementation and third party certification.

**Elements of an Information Security Management System**

27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) that should be scaled in accordance with the needs of the organization. The design and implementation of the ISMS follows a process approach and should address the organization's needs and objectives, security requirements, the processes employed, and the size and structure of the organization.

The Standard requires the use of the "Plan-Do-Check-Act" (PDCA) model (also known as the Shewhart Cycle or the Deming Wheel) to guide the development and implementation of the ISMS processes.

- **Plan (establish the ISMS)**: Understanding the organization's information assets and security requirements in order to establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with the organization's overall business strategy objectives.
- **Do (implement and operate the ISMS)**: Implement and operate the ISMS policy, procedures, processes and controls developed during the Plan phase in order to manage the organization's information security risks within the context of the organization's overall business risk.
- **Check (monitor and review the ISMS)**: Monitor and, where applicable, assess process

performance against ISMS policy, objectives and practical experience and report the results to management for review to measure the performance and effectiveness of the ISMS.

- **Act (maintain and improve the ISMS)**: Take corrective and preventive actions, based on the results of the internal ISMS audit program and management review or other relevant information to achieve continual improvement of the ISMS processes and implemented security controls.

**Key processes within an Information Security Management System**

The processes defined within 27001 describe a methodology to properly identify an organization's information assets, the threats to those assets, the necessary controls to assure the security of those assets and to make sure the implemented controls are effective. But, most of all, 27001 defines a management system to establish processes, policy and procedures relevant to managing risk and improving information security in accordance with the organization's overall business strategy. A management system is much more than a list of security controls, even if they are "best practice."

Key management system processes include:

***Plan phase***

- Document management's commitment to provide resources to establish, implement, operate, monitor, review, maintain and improve the ISMS.

- Establish a framework for setting security objectives and the overall direction and principles for action.
- Define the risk assessment approach and methodology of the organization.
- Select control objectives and controls for the treatment of risks.
- Obtain management approval of the proposed residual risks to implement and operate the ISMS.
- Establish document and record control procedures.

***Do phase***

- Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks.
- Implement the risk treatment plan in order to achieve the identified control objectives.
- Define how to measure the effectiveness of the selected controls or groups of controls.
- Implement training and awareness programs.
- Manage the operation of the ISMS.
- Manage resources for the ISMS.
- Ensure all personnel assigned responsibilities defined in the ISMS are competent to perform the required tasks.
- Implement procedures and other controls capable of enabling prompt detection of and response to security events.

***Check phase***

- Execute monitoring and reviewing procedures and other controls.
- Undertake regular reviews of the effectiveness of the ISMS.
- Measure the effectiveness of controls to verify that security requirements have been met.
- Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks.
- Conduct internal ISMS audits at planned intervals.
- Undertake a management review of the ISMS on a regular basis.
- Update security plans to take into account the findings of monitoring and reviewing activities.
- Record actions and events that could have an impact on the effectiveness or performance of the ISMS.

***Act phase***

- Take appropriate corrective and preventive actions.
- Implement the identified improvements in the ISMS.
- Communicate the actions and improvements to all interested parties.
- Ensure that the improvements achieve their intended objectives.

The real power of 27001 comes from embracing the elements of the management system and not just implementing a list of security controls. When

an organization implements the 27001 management system, not only do they safeguard assets through best practice security controls, they more importantly empower the organization with a management framework and risk assessment methodology that assures the proper treatment of all risks to the business.

Whether the risk comes in the form of data privacy legislation, legal or regulatory actions, theft, IT failures, natural disasters, terrorism, hacking or malicious employees, the risk assessment methodology and management system will guide the organization to the proper risk treatment. The management system allows the organization to be ever responsive to new risks and to address each risk in a manner most suitable to the organization at the time. This means that when you have a well-structured risk assessment framework you can not only minimize negative impact from threats but also maximize positive impact from opportunities.

A well-implemented control may provide security for a time, but a well-established management system and risk assessment methodology will provide the means for an organization to protect the business at all times.

**The case for ISO/IEC 27001:2005 certification**

Seeking third-party certification against the 27001 standard is a powerful step for an organization toward effecting and demonstrating compliance with internationally recognized best practices in information security. The standard provides an organization with a continuous protection methodology allowing a flexible, effective and

defensible approach to security and privacy compliance.

The most powerful aspect of certification is the demonstration to customers, employees, suppliers and business partners the validated existence of a fully operational risk assessment methodology and management system.

The international mutual recognition certification scheme for 27001 makes it the touchstone for effective, comprehensive and verifiable information security management practices. There are many benefits derived from certification, but a few of the most noteworthy include:

- demonstrated credibility and trust with stakeholders, partners, citizens and customers
- documented operational, productivity and quality improvements
- certified once … accepted globally
- holistic, risked-based approach to compliance
- reduced business disruption from ongoing customer assessments
- demonstrated security status according to internationally accepted criteria
- demonstrated due diligence in complying with SOX, HIPAA, GLBA and 21 CFR Part 11.

Certification in 27001 assures clients, employees, suppliers, business partners and future customers that your organization has a continuous protection methodology allowing a flexible, effective and defensible approach to security and privacy compliance. This is far more effective than a list of implemented security controls that may or may not be needed or appropriate.

To summarize the importance of risk assessment in information security, it's all about the risk assessment framework and management system that guides an organization through the process of identifying and protecting the organization's most valuable assets. It's not about the technology and it's not about aimlessly implementing security controls, even if they are "best practice." As an organization's CISO you need to not only understand this but live this every day.

## CHAPTER 7: CISO SURVIVAL

Learning is not compulsory … neither is survival.

*W. Edwards Deming*

Chief Information Security Officers (CISOs) are bombarded with new challenges every day. In a single week, a CISO can be called upon to recommend security applications, build security awareness, be a risk manager, be a consultant to management, lead incident response, be an advocate for business innovation, be a strategic thinker, and establish and support top management security champions.

The role of CISO includes developing, articulating and delivering an IT security and risk management strategy that is aligned with business objectives. The scope of the role is wide and includes technology deployment, strategy and communications, risk management, security operations, investigations/incident response, security awareness training and business continuity planning/disaster recovery.

There are a number of skills and competencies that a CISO must possess and demonstrate on a daily basis to initially earn and then maintain organizational credibility in order to meet the latest business challenges.

**A solid foundation**

To truly execute the role at a high and sustained level, the CISO must maintain a combination of both hard and soft skills. The CISO role requires not only understanding information security, but also mastering competence in three foundational areas: education and certifications; relevant experience; and soft skills including personal qualities, habits, attitudes and social graces.

**Education and certifications**: With a large majority of information assets being electronic, a technical education and/or an in-depth understanding of how the organization's information is created, processed and stored is essential. Ideally the CISO would have a degree in Information Technology or Information Security combined with a business degree. Short of the ideal formal education, a law or business degree combined with a deep understanding of security industry frameworks, approaches and standards such as ISO/IEC 27001:2005, COBIT, NIST 800-53 or Information Technology Infrastructure Library (ITIL) would be valuable.

Continuous education is a hallmark of today's successful CISO. Vendor-neutral certifications, including Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA) demonstrate knowledge, refresh previous training, invoke innovative thinking and increase internal and external credibility. An Information Systems Audit and Control Association (ISACA) Information Security Career Progression Survey found that

92% of respondents indicated that their professional certifications proved to be important in demonstrating competency in their job, 89% felt certifications are important for gaining professional recognition and 83% pointed to their certifications as important in gaining recognition from peers. Additionally, 77% felt industry certifications proved important in qualifying for a new position.[11] In addition, to maintain your certification as a CISSP, CISA and/or CISM, you are required to complete annual Continuing Professional Education credits, another way to demonstrate your currency and commitment to the field.

**Relevant experience**: Having a documented track record in successfully developing a security program, implementing security controls and responding to a security incident goes a long way toward preparing the security professional for the CISO role. The CISO with an understanding of the management side of business and what it takes to support business objectives will find him/herself in great demand. Business management experience ensures the CISO has a firm understanding of the potential impact decisions and recommendations may have on the organization's security/risk posture, operational cost, efficiency and ability to respond to customer demands. If the CISO understands the business, its functions and processes, they have a higher success rate in predicting the security weaknesses that may be in play or introduced when deploying new products or services.

[11] 2008 ISACA Information Security Career Progression Survey Results.

Involvement in industry events, associations and security forums is also an important aspect of a CISO's experience. Active participation outside the organization provides a vehicle for sharing experiences with other CISOs to explore how they have tackled common problems, deployed technology and addressed the latest security threats. Although the CISO needs to spend time "in the office" to protect its assets, it helps to "get out" in order to remain up to speed with the continually changing threat landscape and the developments in the world of technology.

**Soft skills**: There is an axiom in the business world that suggests that hard skills (education, certifications and years of experience) can get you an interview, but it's your soft skills that get you the job offer. So what are "soft skills" and which ones are important for today's CISO? Soft skills refer to your personal qualities, habits, attitudes and social graces that make you an employee that is compatible with the organization's values. Although all organizations may not value the same set of soft skills, it is the combination of both hard and soft skills that will enable you to perform well on the job.

When looking for a CISO position, or to further your advancement in the role, the soft skills you possess and demonstrate are every bit as vital to your success as education and experience. Some of the most important soft skills[12] for today's CISO include:

[12] Top 10 Soft Skills for Job Hunters, Kate Lorenz, 26 January 2009, CareerBuilder.com.

- **Strong work ethic**:[13] A strong work ethic is a set of values based on commitment and diligence. The characteristics of a strong work ethic can be described in four words:
  - Desire: How important is it to accomplish goals?
  - Dedication: Turning desire into action and lasting commitment to goals.
  - Determination: Represents the intensity with which a person is dedicated to the accomplishment of goals.
  - Discipline: Staying with the strategy to achieve goals.
- **Positive attitude**: A positive attitude means to keep a set of ideas, values and thoughts that tend to look for the good, to overcome problems, and to find the opportunities in every situation. A positive attitude helps you cope more easily with the daily challenges of both work and life. Adopted as a way of life, a positive attitude brings optimism and constructive change, and makes it easier to avoid negative thinking. A positive attitude is a state of mind that is well worth developing.
- **Communication skills**: Good communication skills mean that you are verbally articulate and a good listener. You are able to make your case and express your thoughts in a way that builds bridges with colleagues, customers and vendors. The maturity of your communication skills has a direct bearing on your professional image and potential to influence. Organizations place a high value on employees

[13] Building a Strong Work Ethic, F. Scott Addis, January 2010, Moneywatch.com.

with polished communication skills. The art of effective communication does not depend on the use of impressive words or flashy e-mails. Rather, it is reflected in your ability to get a point across as concisely, politely and clearly as possible.

- **Time management abilities**: Time management skills boil down to awareness, organization and commitment. Awareness comes from knowing and recording everything you are committed to doing. Organization is the ability to translate those goals into actionable tasks, and commitment is the follow-through to get the tasks complete. Time management skills are learnable abilities that recognize and solve personal and business problems.
- **Problem-solving skills**: Problem solving occurs when solutions are identified and implemented to resolve a gap or remove obstacles between our present situation and a desired goal. Problem solving generally includes the following steps: problem recognition, investigation and analysis, solution brainstorming, option analysis and decision selection.
- **Team player**: Successful CISOs will be comfortable working as part of a team. It is important to fit in with and get along with other employees in order for the organization to run smoothly. Being a team player is not about being liked by everyone, nor does it mean you like everyone on the team. A true team player is an employee that can be counted on to do his or her part of the work, be

relied on to complete tasks, and work cooperatively with others.

- **Self-confidence**: Self-confidence is essentially an attitude that allows us to have a positive and realistic perception of ourselves and our abilities. It is characterized by personal attributes such as optimism, enthusiasm, affection, pride, independence, trust, assertiveness, the ability to handle criticism and emotional maturity. Self-confidence is a deserved belief in your abilities without cockiness. Self-confidence projects a sense of calm, and inspires confidence and courage in others to ask questions and to freely contribute ideas.
- **Teachable**: For anyone to progress in business or in life he/she needs information. Information is acquired through the process of learning which involves a teacher–student relationship. A successful learning relationship requires a student with a teachable spirit that is open to learning as a person and as a professional.
- **Flexibility/adaptability**:[14] Successful CISOs live in the moment. Gallup Consulting defines those having adaptability as a strength as those who don't see the future as a fixed destination. Instead, they see the future as a place created out of the choices that are made today. Adaptability enables them to respond willingly to the demands of the moment even if they pull them away from their plans. At heart, CISOs must be very flexible people who can

[14] *GALLUP Management Journal*, Adaptability, 12 September 2002.

stay productive when the demands of work are pulling in many different directions at once.

- **Calm under pressure**: Staying calm under pressure leads to clear thinking, better decisions and an overall healthier work and personal life. Being able to handle the stress that accompanies conflicts, deadlines and emergencies is a great asset to any CISO.

**Your strategy to survive and prosper**

To survive as a CISO, you need to have a daily plan that reminds you of the "right" things to be thinking about (*see Chapter 8*), and a strategy that demonstrates your capability to be a trusted adviser to management while you deliver measurable results and maintain security at your organization.

There are six key principles[15] that a CISO should focus on:

1 **Build relationships within the business**: CISOs need to develop relationships with key stakeholders long before contacting them to perform an assessment or to ask for money. A demonstrated understanding of the organization's processes, politics, expectations, concerns and goals is essential.
2 **Focus initiatives on business goals**: Produce security strategies that support the business strategy and objectives to produce products and services. This will better ensure business

[15] What makes a CISO employable? Avtar Sehmbi, 20 July 2010, Infosecurity (UK).

owner and management buy-in and receiving of sponsorship.

3 **Link initiatives and plan**: Connect the business objectives with the requirements and challenges facing information security – threat environment, regulatory compliance, resource constraints and technology deployment. Using these connections, map out the next 12–18 month period displaying how the security initiatives support what the business is trying to achieve strategically and tactically.

4 **Deliver service**: Staff managers often forget who their customers really are. They don't realize they need to sell themselves continuously by focusing on quality service, presentation, punctuality, physical appearance and credibility. Adding value to the business is the goal of every engagement you have with management. Articulate cost reductions, return on investment and risk reduction whenever possible.

5 **Professional credibility**: To be a trusted adviser to top management you need to build your professional capabilities and accomplishments. Stay connected to and seek recognition from the larger security community. Distribute informative industry white papers, relevant case studies, information security alerts, regulation overviews and best practice summaries. Deliver top management and board level information security and risk management training whenever possible.

6 **Surround yourself with excellence**: If you want to be excellent, you need to surround yourself with excellence. The role of the CISO

> is no different. Great CISOs have surrounded themselves with great people that force them to be on their toes and to strive to be better. Don't fall into the trap of only hiring people that won't challenge you. If you do, your challenge may well be just keeping your job.

Historically, the typical CISO had a background in technical security/consulting or IT operations management. As regulatory compliance and new laws became a larger part of the CISO landscape, people from the legal profession and senior business managers started joining the specialty. Regardless of his/her background, a CISO's longevity is not just about having the right qualifications (hard skills), but complementing them with both the soft skills discussed above and a well-executed survival strategy.

## CHAPTER 8: SUMMARY – YOU BECOME WHAT YOU THINK ABOUT

A man is but the product of his thoughts, what he thinks, he becomes.

*Mohandas Gandhi*

The concept is far from new; its truth is self-evident and it has never been more relevant. A more recent rendition of the concept is from a renowned author and speaker, Mr Earl Nightingale who says, "You Become What You Think About." If this is the first time you have heard this phrase, let it sink in a little while. It may not change your life in some lightening-strike way, but if you give it a chance you will begin to recognize that you are surely becoming what you find yourself thinking about. Making a conscious effort to think about what you want to become can have a powerful impact on your job effectiveness and your success in life, if you think about the right things.

### What do great CISOs think about today?

For starters, don't even think about looking at a traditional CISO job description. There, all you will find is overly technical requirements and the occasional high-level responsibility clause for the organization's security program. Neither is well suited to establishing you as a trusted adviser to senior management.

To define what great CISOs should be thinking about, let's remember the challenges facing today's CEO. In a recent report from the 2010

CEO Challenge Survey, it is no surprise that what CEOs view as their greatest challenges do not specifically focus on information security. The Conference Board *CEO Challenge 2010*[16] reflects the following challenges that, when you think about it, align well with what a great CISO should be thinking about.

- Excellence in execution
- Sustained and steady top-line growth
- Customer loyalty/retention
- Profit growth
- Corporate reputation for quality products/services
- Stimulating innovation and creativity
- Enabling entrepreneurship
- Government regulations.

In support of business objectives, the great CISO would focus on the following:

- Business projects require security to manage the company's risk.
- Support everyone who builds products, delivers services or sells either one.
- Technology's role is to support business objectives.
- Business is the art of managing risk and I am the master of risk.
- Work on a daily basis to make C-level executives risk management disciples.
- Technology enables innovation and creativity.
- Explain everything in terms of risk levels so that people can understand.

[16] *CEO Challenge 2010: Top 10 Challenges*, The Conference Board, February 2010.

- Security is every employee's job. Teach them what they need to know.

**Protecting our greatest assets**

In the past, technology has been the IT department's stronghold on the rest of the organization. The IT department used to be the first adopter of new technology and the first to explore the value of the latest hardware and software upgrades. Today, and likely even more so in the future, the IT department finds itself trying to catch up with and even slow down employees already using the latest in smartphones, social networking, instant messaging and wireless applications. It seems the "users" are not waiting for the IT department to introduce the new technology. They are not waiting for the CISO to bless the technology as "safe" for use within the organization. The fact is, employees have become increasingly more tech-savvy and with that comfort with technology they are willing to remain connected to their jobs at all hours of the day. Employees want to merge their work and personal technology. The expression, "Employees are an organization's greatest asset," is as true today as ever before. The great CISO will take steps to both recognize and support this fact.

**What will great CISOs think about tomorrow?**

Great CISOs recognize that the serious and ever-changing nature of today's security threats demand a strategic-minded response and not just an operational reaction to the latest headlines. This is a drastic change from being a working security

coordinator to that of an evangelist of risk management, innovation through technology and information security within the organization. Identifying threats, defining security controls, developing security architecture, overseeing planned mitigations and monitoring the organization's security posture will always remain a CISO's responsibility, but the great CISO will also be thinking about how to attain business objectives through enabling technology while properly managing risk.

Future CISOs will need to develop the ability to think about information security and risk at the enterprise level and not just from the IT perspective. An enterprise view of information security, business continuity, compliance, safety and physical security, and the ability to understand how it all impacts risk is crucial for tomorrow's CISO.

Every great CISO will ask themselves the following questions:

- How do I create a risk aware culture?
- How do I advance information security and risk management into the business strategy?
- How do I communicate risk to stakeholders and become a trusted adviser to the executive team?
- How do I educate and collaborate on security and compliance issues?
- What information security strategy will keep us ahead of the bad guys?

**How do you start thinking about the right things?**

The secret to help you free your thinking is to take a sideways step and look at your position in the organization from the purview of senior management. Stop trying to desperately think of new technology projects that might inspire you and start considering what you can do to meet the organization's business challenges.

Especially in a challenging economic climate, management is looking for more ways to achieve business objectives and are not as interested in focusing solely on information security and regulatory compliance. The challenge for you is to break out of the mindset that taking on risk only has a negative component.

The CISO of yesterday rarely, if ever, deviates from his or her "risk avoidance at all cost" mentality. If you want to be perceived as a valuable member of the team, it may be time to rethink your message. We will be living in a much different financial world for the next five to ten years. The CISO as-usual method of thinking and operating used to influence senior management in the past must now undergo a radical shift to reflect the realities of the current economic environment. More than ever before, you must know how to communicate effectively with senior management to compete for the organization's limited resources.

Mr Nightingale encourages us to complete a 30-day challenge[17] where you would intentionally manage what you think about. His suggestion is to carry a card in your pocket that contains the key thoughts that you want to take hold and look at it throughout the day.

**On one side of the card you write:**

| |
|---|
| You Become What You Think About |
| Ask; and it shall be given to you |
| Seek; and you shall find |
| Knock; and it shall be opened unto you |

**On the other side of the card you could write:**

| |
|---|
| I am a trusted adviser to senior management. |
| I will focus on helping people build products, deliver services and increase sales. |
| I will manage risk while maximizing positive outcomes. |
| I will use technology to enable innovation and creativity. |
| I will look for ways to build collaboration on security and compliance issues. |

Create your own card today and carry it with you. Look at it several times a day and especially when you feel yourself slipping back into your old way of thinking. Try it for 30 days and watch how "You Become What You Think About," a great CISO.

[17] The Strangest Secret, Earl Nightingale, 12 September 2006.

## ITG RESOURCES

IT Governance Ltd. sources, creates and delivers products and services to meet the real-world, evolving IT governance needs of today's organizations, directors, managers and practitioners.

The ITG website (*www.itgovernance.co.uk*) is the international one-stop-shop for corporate and IT governance information, advice, guidance, books, tools, training and consultancy.

*http://www.itgovernance.co.uk/iso27001.aspx* is the information page on our website for our ISO27001 information security resources.

### Other Websites

Books and tools published by IT Governance Publishing (ITGP) are available from all business booksellers and are also immediately available from the following websites:

*www.itgovernance.co.uk/catalog/355* provides information and online purchasing facilities for every currently available book published by ITGP.

*www.itgovernance.eu* is our euro-denominated website which ships from Benelux and has a growing range of books in European languages other than English.

*www.itgovernanceusa.com* is a US$-based website that delivers the full range of IT Governance products to North America, and ships from within the continental US.

*www.itgovernanceasia.com* provides a selected range of ITGP products specifically for customers in South Asia.

www.27001.com is the IT Governance Ltd. website that deals specifically with information security management, and ships from within the continental US.

**Pocket Guides**

For full details of the entire range of pocket guides, simply follow the links at www.itgovernance.co.uk/publishing.aspx.

**Toolkits**

ITG's unique range of toolkits includes the IT Governance Framework Toolkit, which contains all the tools and guidance that you will need in order to develop and implement an appropriate IT governance framework for your organization. Full details can be found at www.itgovernance.co.uk/ products/519.

For a free paper on how to use the proprietary Calder-Moir IT Governance Framework, and for a free trial version of the toolkit, see www.itgovernance.co.uk/calder_moir.aspx.

There is also a wide range of toolkits to simplify implementation of management systems, such as an ISO/IEC 27001 ISMS or a BS25999 BCMS, and these can all be viewed and purchased online at: http://www.itgovernance.co.uk/catalog/1.

**Best Practice Reports**

ITG's range of Best Practice Reports is now at www.itgovernance.co.uk/best-practice-reports.aspx. These offer you essential, pertinent, expertly researched information on a number of key issues including Web 2.0 and Green IT.

**Training and Consultancy**

IT Governance also offers training and consultancy services across the entire spectrum of disciplines in the information governance arena. Details of training courses can be accessed at *www.itgovernance.co.uk/training.aspx* and descriptions of our consultancy services can be found at *http://www.itgovernance.co.uk/consulting.aspx*. Why not contact us to see how we could help you and your organization?

**Newsletter**

IT governance is one of the hottest topics in business today, not least because it is also the fastest moving, so what better way to keep up than by subscribing to ITG's free monthly newsletter Sentinel? It provides monthly updates and resources across the whole spectrum of IT governance subject matter, including risk management, information security, ITIL and IT service management, project governance, compliance and so much more. Subscribe for your free copy at: *www.itgovernance.co.uk/newsletter.aspx*.