Assessing Information Security

Strategies, tactics, logic and framework

A Vladimirov

K Gavrilenko

A Michajlowski

Assessing Information Security

Strategies, tactics, logic and framework

Assessing Information Security

Strategies, tactics, logic and framework

A VLADIMIROV
K GAVRILENKO
A MICHAJLOWSKI

itgp™

IT Governance Publishing

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

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 2010
by IT Governance Publishing.

ISBN 978-1-84928-036-5

‘He who is willing and able to take the initiative to exploit variety, rapidity, and harmony – as the basis to create as well as adapt to the more indistinct – more irregular – quicker changes of rhythm and pattern, yet shape the focus and direction of effort – survives and dominates.’

Colonel John Boyd

PREFACE

Assessing Information Security is a book about the philosophy, strategy and tactics of soliciting, managing and conducting information security audits of all flavours. It is often controversial and is written to be so. When we throw criticism at others, we expect to be criticised ourselves. It contains a lot of what you can rightfully label as ‘common sense’. However, this ‘common sense’ is frequently ignored or overlooked, leading to disastrous consequences. Thus, it must be reiterated and reinforced, sometimes from an unexpected angle or viewpoint. On the other hand, there is hope that some of the statements and issues presented in this book, will at least be challenging and thought-provoking. When compiling various references and assembling the content, the general feeling was ‘How did we miss it before?’ or ‘How could anyone fail to mention or formulate that?’. Such impressions can be contagious.

We don’t aim to provide an A to Z, step-by-step guide, on how to perform information security assessments. It would contradict the whole spirit of this work and fail the test of time. This is not a technical manual, compliance guideline, or security policies and procedures checklist. If you are looking for one, you should search elsewhere, preferably online or in the specialised periodic press. Nowadays, the tempo is exceedingly fast. For instance, if someone wants to write a tome on hands-on hacking and counter-hacking (as we did in the past with *Wi-Foo* and *Hacking Exposed Cisco Networks*), the chances are that when the book hits the shelves, many issues, methods and techniques it describes, will already be obsolete. Today we tend to view such approach as arguably counterproductive. What we are trying to accomplish instead, is to provide a fluid framework for developing an astute ‘information security mind’, capable of rapid adaptation to evolving technologies, markets, regulations, laws, etc. To do so, we appeal to our observations and experience as an information security auditing team and the infinitely larger volume of applicable wisdom produced and accumulated by others. There is a fable about the evolution of a musician who said ‘Me’ at the age of 20, ‘Me and Mozart’ when turning 30, ‘Mozart and Me’ when approaching their 40s and, eventually, ‘Mozart’ at 50.[1] It appears that we have reached the ‘Mozart and Me’ stage and will inevitably proceed to the final conclusion of this cycle. The reflections of relevant great minds of past and present clearly point at the necessity of a synthetic interdisciplinary approach. Transcending the boundaries of the specialised IT security auditing field becomes inevitable. A solid understanding of the overall information security paradigms is called for. Therefore, we sincerely hope that this book might become an entertaining read for all information security adepts, whether coming from a corporate, managerial, governmental, technical or academic background.

[1] Apparently, it is based on a real historical quote attributed to Gounod: ‘*When I was very young, I used to say ‘I’; later on, I said ‘I and Mozart’; then ‘Mozart and I’. Now I say ‘Mozart*’.

ABOUT THE AUTHORS

Dr. Andrew A. Vladimirov, CCNP, CCDP, CISSP, CWNA, TIA Linux+, is a security researcher with a wide scope of expertise, ranging from network security and applied cryptography, to the relevant aspects of bioinformatics and neural networking. He published his first scientific paper at the age of 13 and is one of the co-founders of Arhont Ltd, one of the leading information security consultancies in the UK. Andrew has an extensive background in performing information security assessments, ranging from external and internal penetration tests, to configuration, security policies, processes and procedures reviews. He has also participated in creating and implementing ISMS and secure architecture designs for large companies, assisted corporations with meeting ISO27001, FSA Annex 2 and other compliance demands, and took part in numerous forensic investigations. Andrew has published a variety of security advisories and papers, authored a chapter on wireless security in *Network Security: The Complete Reference,* McGraw-Hill/Osborne, and is a co-author of *Wi-Foo: The Secrets of Wireless Hacking*, Addison Wesley (2004) and *Hacking Exposed: Cisco Networks,* McGraw-Hill/Osborne (2006). On the basis of these publications and his relevant practical experience, he has composed and read tailored public and private training courses on the subjects of internal security audits, information security strategies, and wireless offence and defence. Andrew is supportive of both open source and full disclosure movements. He is a graduate of King's College London and the University of Bristol.

About the Authors

Konstantin V. Gavrilenko (London, UK) has more than 15 years' experience in IT and security, and together with his co-authors, is a co-founder of Arhont Ltd. Konstantin's writing draws primarily from his real-world knowledge and experience in security consultancy and infrastructure hardening, for a vast range of clients. He is open-minded and enthusiastic about research, where his main areas of interest lie in information security in general and, more specifically, in networking and wireless. He is proud to say that he is an active supporter of open source solutions and ideology, public disclosure included. Konstantin has published a variety of advisories uncovering new software vulnerabilities, alongside essays on assessment types and methodologies, articles on other information security-related topics, and is a co-author of the bestselling *Wi-Foo: The Secrets of Wireless Hacking*, Addison Wesley (2004) and *Hacking Exposed: Cisco Networks*, McGraw-Hill/Osborne (2006). He holds a first class BSc Honours degree in Management Science from DeMontfort University and an MSc in Management from Lancaster University.

Andriej A. Michajlowski (London, UK) first became enticed by UNIX flavours back in high school times. He cultivated and expanded his knowledge into the networking aspects of information technology, while obtaining his bachelor's degree from the University of Kent at Canterbury. Soon he was engrossed in network security and penetration testing of various wireless and wired devices and systems. On accomplishing his MBA, he co-founded information security company, Arhont Ltd, participated in security research, published articles and advisories, and greatly contributed to the overall success of the Arhont team. Andriej's technical particularities include user and device authentication mechanisms, database and directory services, wireless networking and application security, and systems integration. He has participated in compliance consulting at many financial and legal sector organisations, and has extensive experience in performing internal and external information security assessments. Andriej has also co-authored *Wi-Foo: The Secrets of Wireless Hacking*, Addison Wesley (2004) and *Hacking Exposed: Cisco Networks*, McGraw-Hill/Osborne (2006).

CONTENTS

INTRODUCTION

'We can't just look at our own personal experiences or use the same mental recipes over and over again; we've got to look at other disciplines and activities and relate or connect them to what we know from our experiences and the strategic world we live in. If we can do this we will be able to surface new repertoires and (hopefully) develop a Fingerspitzengefühl[1] *for folding our adversaries back inside themselves, morally-mentally-physically – so that they can neither appreciate nor cope with what's happening – without suffering the same fate ourselves.'*

Colonel John Boyd

A thorough treatise dedicated to various aspects of information security auditing must cover why and what kind of assessments have to be performed, subject to a particular situation. It is expected to elaborate by whom, when, how, and in which specific sequence, they should be executed. It ought to address how to present the audit results in the most palatable manner and which corrective actions these findings might trigger. However, all we have just listed are mere technicalities. If you concentrate on them too much, without applying a sufficient level of abstraction, you are risking missing something of a much greater importance: their logical, and even philosophical, backbone.

[1] This German term literally means 'fingertip feeling', and is synonymous with the English expression of 'keeping your finger on the pulse', while emphasising intuition.

You will fall into a trap of adhering to rigid ‘if-then-else’ mechanical instructions. These can easily become outdated and flawed, even by a subtle change in the operating environment. A smart opponent can outwit them by utilising non-conventional ways. Until the new appropriate schemes are generated, usually by someone else and late, you are lost.

In contrast, if you have a firm holistic grasp of the whole picture and understand what we may rightfully call ‘the philosophy of information security’, you can easily adjust to any change ‘on the fly’. Even more, you can shape the change yourself, and become its primary engine and source. This means that you will be able to dictate the rules of the game, and it is others that would have to adapt. Or, to put it plainly, ‘submit’. The ‘bird’s eye view’ idiom is misleading: an eagle hovering high in the clouds can spot a tiny mouse lurking in thick grass and nosedive in no time. This is a good analogy of what we have alluded to as a ‘sufficient level of abstraction’, coupled with a rapid and precise act.

Unfortunately, when we scoured for what others have said about ‘the philosophy of information security’ and its implications towards security assessments in specialised texts, we got strongly disenchanted. We stumbled across multiple security management sources presenting solely managerial, technical displaying purely technological, and legal offering exclusively legal perspectives. The existing information security standards are presented as an infallible verity that contains everything a security specialist might need. There are multiple occasions of transient, specific or narrowly technical statements passed as grand philosophical truths. Tactical discourses are presented as strategic paradigms. Endless arguments about information security being a process, approach, system, a state of mind or even a lifestyle are rampant. Generalisations like ‘be paranoid’ or ‘everything is vulnerable’ are omnipresent. We are not implying that these are somehow incorrect. They have their time, place, value and significance. However, they do not form a coherent integral framework that can be easily adapted to a variety of relevant situations, in both theory and practice.

We have also turned to other disciplines for guidance. For instance, we have looked at modern mathematical chaos and game theories. Both are fine examples of applicable ‘coherent integral frameworks’ that offer useful insights. However, it was the philosophy of war and its core principles that truly hit the ‘nail on the head’. This is hardly surprising. When writing *Wi-Foo*, we employed numerous quotes from ancient Chinese military masterminds, as epigraphs for the majority of chapters. Being highly reusable and appropriate, some of these epigraphs are repeated in this book. At that time, we found a high suitability of statements written more than 2,000 years ago, to what is still considered a cutting edge technology of today, at the very least amusing. They also provided a needed symbolic martial arts link. In this work, the assertions, opinions, estimations and judgements of master strategists of all times are not just some fancy spice up citations and epigraphs, they form its *fluid backbone*. They are the ‘Mozart’ part of ‘Mozart and I’.

Apart from the noted completeness, coherence, all-around applicability, systematic nature and apt abstraction, we are fond of taking advantage of the philosophy of war, for the following reasons:

- Focus on conflict and its polarity.

- Realism and utilitarianism.
- Simplicity and clarity of statements.
- Clear distinction between strategy and tactics.
- Taking into account a wide selection of variables.
- Reusable terminology.
- Multidisciplinary approach.

As a matter of fact, the contextual replacement of ‘war’ or its synonyms by ‘information security’ or ‘information security assessment’, in many excerpts of military classics, naturally produces shrewd observations. Practise this technique on the infamous ‘*Everything is very simple in war, but the simplest thing is difficult’* saying, of Carl von Clausewitz and see where it might lead your thoughts. Then, perform this simple exercise every time you encounter a martial classic citation in this book.

Of course, applying philosophy and the strategy of war to other disciplines is not news. In particular, this was extensively (and, perhaps, excessively) done in business management. We have encountered a linguistic opinion stating that ‘Sūn Zǐ Bīng Fǎ’, traditionally translated as ‘Sun Tzu Art of War’, actually means ‘Sun Tzu Competitive Strategies’. The Boston Consulting Group *Clausewitz on Strategy* book affirms: ‘*As perplexing as this may appear at first for a work on warfare, Clausewitz speaks loudly and clearly to the modern business executive who is inclined to listen. He does not, of course, speak the language of today’s audience. He does better: He speaks the executive’s mind*’. This is one of the reasons why we make a sustained heavy use of his thoughts throughout this work. Note, that Clausewitz himself did compare business and military conflict: ‘*It would be better, instead of comparing it with any art, to liken it to business, which is* *also a conflict of human interests and activities; and it is still more like state policy, which again, on its part, may be looked upon as a kind of business on a great scale*'.

Nonetheless, this approach has met with sharp and objective criticism. The spearhead of critics is that business, after all, is not war. It is more akin to politics and diplomacy. A company is not an army detachment. Its chief executive officer is not a general. But perhaps the mightiest blow comes from the modern game theory. From its point of view, the majority of situations in business and commerce can be described as 'non-zero-sum games'. That is, they are co-operative. They involve complex relationships between different sides, with net gain or loss. There is a mutual benefit, even from some forms of intercourse with direct competitors, and we are not at other information security companies' throats. We have met their professionals during various industry conferences and informal gatherings and have exchanged ideas and shared research. We have also had many beers together! This is good for the industry, thus it eventually benefits us all.

However, consider the following suppositions:

- *Information security is a form of warfare.*
- *In essence, it has plentiful similarities with counter-intelligence and counter-insurgency efforts.*

The latter is one of the cornerstone ideas actively elucidated in this book. Note, that more than a decade ago, RAND researchers, John Arquilla and David Ronfeldt, coined a term 'netwar', to distinguish 'an emergent form of low intensity conflict, crime, and activism' waged, employing 'decentralised and flexible network structures'. They also proposed the somewhat ill-fated term 'cyberwar', which is

Returning to the game theory:

- *Applied information security is a zero-sum or strictly competitive game.*

Co-operating with a cybercriminal does not make any more sense than collaborating with a burglar who broke into your house. One can, and should learn a lot from security incidents, but this is not co-operation. Collaboration with criminals is a crime *per se*. Co-operation with the enemy is treason. According to Clausewitz, '*the principle of polarity is only valid when it can be conceived in one and the same thing, where the positive and its opposite the negative, completely destroy each other. In a battle both sides strive to conquer; that is true polarity, for the victory of the one side destroys that of the other*'. Thus, we conclude that the philosophy and strategy of war is fully applicable to the field of information security in theory and practice.

Where does this bring us? Let's formulate some basic founding principles.

- *Information security is the science and art of protecting data.*

It is not merely a system, process, approach, service, and set of methods, mindset and so forth. It is much more. We will discuss the perceived 'science versus art' dichotomy at the end of the very last chapter of this book.

- *IT security is the science and art of protecting data in electronic format.*

IT security is a sub-discipline of general information security. Protecting data in electronic format inevitably includes defending all systems, media and communication includes defending all systems, media and communication channels that carry it. It will also affect all people that have, or can potentially have, access to this data and resources.

- *Information security assessments are a practical way of improving the information security state.*

They can and should be more than only evaluating the risks, or verifying compliance to security policies, or finding and consequently eliminating tangible security gaps. This is the main subject of our study.

Further interesting clarifications can be gathered from the so-called teleology of conflict. Anatol Rapoport was a renowned mathematician with major contributions to game theory and cybernetics. In his foreword to a (much criticised) Penguin edition of Carl von Clausewitz's opus magnum *On War*, Prof. Rapoport has suggested three main teleological concepts of warfare:

- *Eschatological*
- *Political*
- *Cataclysmic.*

In Rapoport's own words, '*metaphorically, in political philosophy war is compared to a game of strategy (like chess); in eschatological philosophy, to a mission or the dénouement of a drama; in cataclysmic philosophy, to a fire or an epidemic*'.

From the information security specialist's standpoint, we find the eschatological approach as nearly irrelevant. It has played a grand role in the history of mankind, primarily due to its immense propaganda value and power. Examples of classical 'eschatological conflicts' include crusades, jihads, Communist 'final worldwide revolution', Nazi 'domination of the master race' and American 'Manifest Destiny'. The instances which are more close to this particular discourse are the so-called ‘war on drugs’, ‘war on guns’ or ‘war on knife crime’, sometimes declared by law enforcement bodies. Being realists, we understand that in the foreseeable future there will be junkies, dealers, shootings and stabbings, unless some unthinkable miracle happens. In a similar manner, you may announce and promote the epic ‘war on cybercrime’, ‘war on SPAM’, or ‘war on Web applications insecurities’. It may motivate some people to do something about these issues, but that is the best you can hope to achieve by such an act.

The political concept of warfare is the one we find to be the most pragmatic, fruitful and efficient. In relation to applied information security, it is advocated throughout this entire work. As such, it can be rightfully dubbed as ‘Neo-Clausewitzian’. This is particularly evident in Chapter 2 of this book, dedicated to directing and shaping effects that policies, governance and compliance have on information security assessments. Note, that the political approach is always heavily at play when security budget considerations are discussed.

Unfortunately, many security professionals consciously or instinctively adhere to what can amount to a cataclysmic concept of information security. This outlook seems to be common among both management and ‘techs’. It is reflected in viewing security as a mere part of business continuity, disaster recovery and prevention, or even service availability. It is often expressed by the defeatist ‘c’est la vie statements’, such as ‘everything can and would be hacked anyway’ or ‘we can do our best, but sensitive data will still leak out’. It appeals on the grounds of realism, along the line that ‘the pessimist is a well-informed optimist'. *However, we scorn this way of thinking as fundamentally, strategically flawed.*

The cataclysmic approach to information security reduces initiative, decreases morale, and promotes a passive defensive response, if not paralysis of action. By succumbing to it, one may even start accepting security incidents as something close to a divine wrath that can only be (partially) softened by countermeasures and insured against. *Experienced security auditors should be able to determine whether the cataclysmic doctrine dominates the company's or organisation's information security paradigm, and deliver appropriate warnings and explanations.*

Comparing a natural disaster or unfortunate accident to a premeditated malice is senseless. Even if the end effects are the same, both preventive and reactive responses will have to differ. Assessing the related risks and predicting their impact will be distinct. To summarise:

- *There are passive and active security incidents.*

Accidentally losing a memory stick or portable computer with sensitive data is a common instance of the former. Deliberate unauthorised access is an example of the latter. This can be compared to non-combat and combat-related losses in the military.

- *Passive security incidents happen due to error.*
- *Active security incidents happen due to the combination of error and a hostile act.*

Nearly all successful attacks involve some mistake on the defender's side. Infectious disease happens when virulence of the microbe and lack of immunity of the infected host are superimposed.

- *Passive security incidents can pave a way for their active counterparts.*

An accidental access control flaw or sensitive information leak are likely to be deliberately abused later. It is better to be prepared for the worst.

- *Security assessments must evaluate probabilities and the potential impacts of passive and active security incidents.*

While different in nature, both present significant risks that should be reduced. Besides, see the previous point.

- *To assess the likelihood of passive security incidents it is usually sufficient to analyse controls, their implementations and enforcement.*

In the example of accidental loss of data on a portable carrier, it is generally enough to verify that:

1 Correct security policies that prohibit the use of portable storage media in the company or organisation are present.
2 All users are aware of them and have agreed in a written form.
3 The policies are reinforced by appropriate technical means, such as specialised software blocking use of all USB ports.
4 The enforcing software is present on all corporate systems that contain, or may contain, sensitive data. It is correctly installed, configured, maintained and documented.

Alternatively, the prohibition of use can be substituted by employing strong cryptography.

However,

- *To assess the probability and impact of active security incidents, a more aggressive and all-encompassing path must be taken.*

In the specific example above, we will have to add the fifth point: verify that the USB port blocking software cannot be circumvented. If this is possible, than it becomes necessary to discover how much effort and skill such a hack would require from a potential attacker. And then the sixth point – check whether other mobile storage media that does not rely on USB ports can be, and is used, to carry information. If encryption is employed, strength of ciphers, keys and its actual implementation must be analysed. Again, how much skill, effort and time the attacker has to expend to break it, needs to be estimated. In a nutshell, all these additional security auditing means are a form of penetration testing which is always active and intrusive intervention.

Thus, we have finally arrived at a crucial statement of unequalled, unsurpassed gravity:

- *Prevention and mitigation of any hostile information security act always involves the clash of human wills.*

Which is, essentially, a specially adapted version of:

- '*All war supposes human weakness, and against that it is directed*' (Clausewitz).

While this is common sense ('guns don't kill people, people kill people'), in information security it is strongly obscured and obfuscated by technology, bureaucracy and lack of abstraction. Even when you are dealing with a 'purely technical' threat, such as viruses and worms, you are not battling an inanimate piece of code. It is nothing else than yours and your allies will, against the will of malicious software creators and deliberate users. If you are a technical specialist, just add skill to will. If you are an IT manager or a CISO, that skill is managing or directing the technical team. For some, this may sound unsettling. Still, disgruntled employees, cybercriminals, vandals, industrial spies or political activists are all flesh and bone. Unless your name is John Connor and the year is 2027, you are not engaged in some chimeric stand-off against swarms of hostile machines.

There are information security consultants that would assume a discussion of 'social engineering' any time 'the human factor' is mentioned. The implications we are looking at in this book are of a much broader scope. In this context, social engineering is one of the highly important technicalities. If Clausewitz meant anything like it when he wrote about war being aimed at human weakness, he would have written about the penetration of enemy ranks by spies. It was the closest equivalent of social engineering at his times. What the master strategist did have in mind is that:

- '*The activity in war is never directed solely against matter, it is always at the same time directed against the intelligent force which gives life to this matter, and to separate the two from each other is impossible.*'
- '*If we desire to defeat the enemy, we must proportion our efforts to his powers of resistance. This is expressed by the product of two factors which cannot be separated, namely, the sum of available means, and the strength of the will.*'

Note, that the energy in the excerpt is directed at 'matter' and 'intelligent force' 'at the same time', as they are fully indivisible. The significance of the 'material side' (resources, documentation, technology) is by no means denigrated. Instead, the balance between 'human' and 'material' factors is underlined. *In the event of any security incident, both will be simultaneously affected as they are inseparable. Therefore, both have to be synchronously audited, analysed, measured and protected so that all available means of defence are employed, yet you do not overreact.*

You may still ask 'what the 19th Century military strategist could know about the role and contributive proportions of such things in modern times?'. Collate his words with the following extract from the current US MCDP (Marine Corps Doctrinal Publication) 1 *Warfighting*: '*No degree of technological development or scientific calculation will diminish the human dimension in war. Any doctrine which attempts to reduce warfare to ratios of forces, weapons, and equipment neglects the impact of the human will on the conduct of war and is therefore inherently flawed*'.

Based on multiple observations, we have developed our own little model of the 'clash of wills' in typical information security conflicts. We call it 'the FUD game'. FUD is a common abbreviation standing for Fear, Uncertainty and Doubt. FUD undermines will.

The rules of the 'FUD game' are simple: the attackers are trying to maximise FUD of defenders while diminishing their own and vice versa. The first to increase the opponent's FUD above the breakpoint of their will, gains the upper hand. A typical 'defender FUD' can be described as:

- *Fear* of being successfully compromised and held personally responsible for negligence and blunder.

- *Uncertainty* regarding how, where, and when the effective blow will occur.
- *Doubt* in one's abilities to prevent the breach.

A typical 'attacker FUD' encompasses:

- *Fear* of being discovered, caught and persecuted.
- *Uncertainty* regarding defender knowledge, skill and means.
- *Doubt* in one's ability to disengage without leaving a give-away trace.

The situation is asymmetric. In the real world, the Uncertainty element tends to favour the attacking side. Fear, though, often reinforces competent defenders: in the case of defeat the (legal) repercussions for attackers are far more severe. The defending side has another important advantage: there is no actual draw. Repelling the opponents and simply avoiding the breach counts as the defender's victory. *The key factors for winning the FUD game appear to be resolve, initiative, good observation and orientation, foresight, cunning and swiftness. Chance also plays its role. Other factors are subordinate, providing that neither side has enormous superiority in technological prowess.*

With this observation we shall complete this hopefully provocative preamble that sets logical and philosophic grounds for the principal work.

CHAPTER 1: INFORMATION SECURITY AUDITING AND STRATEGY

'We should base our decisions on awareness rather than on mechanical habit. That is, we act on a keen appreciation for the essential factors that make each situation unique instead of from conditioned response.'

MCDP 1 *Warfighting*

Rephrasing Clausewitz, to produce a workable scheme for information security assessments, is one of the tasks that are inherently simple, yet the simplest thing is difficult to implement. It is simple because the underlining logic is clear. It can be formulated in a minute. Here it comes from the (independent) auditor's viewpoint:

- Find out about goals and conditions of the assessment.
- Plan the appropriate actions.
- Select the corresponding methodologies and tools.
- Check and test everything you can within the limits of budget, requirements, time and means.
- Pull the results together.
- Measure and analyse risks.
- Consider realistic remedies.
- Generate an impressive report.
- Work with the client on any follow-up acts if needed.

A mirror version of this scheme, as seen from the auditee perspective, is also easy to generate. It will have to be more strategic in nature. The auditor receives goals and directions, but it is the management of the auditee that formulates and sets them. It must also select suitable auditors for the task and a qualified manager to oversee the process. At the end of the day, for the auditors, the assessment is often a separate assignment within a limited time span. For the auditee, it is an element of some larger long-term security programme. Or, at least, it should be.

Wing Tsun is an effective and increasingly popular Chinese martial art. Bruce Lee has derived his Jeet Kune Do from it. There are only eight principles in Wing Tsun. Some even reduce them to four: forward pressure, sticking to the opponent, using the opponent's strength, and centreline control. Reading and comprehending these fundamentals 1,000 times will not make you a formidable fighter. That would require many years of intense practice. Still, there is no guarantee that you will win every single fight. Even in cases where the governing principles do not have to be built into resisting and inert (physical, organisational, corporate) body by dedicated sustained effort, things are not straightforward. For example, knowing the major winning strategies would not instantly make you a chess grandmaster and chess is but an ancient board game with immutable rules.

Unlike chess, in the field of modern information security, there are no defined winning strategies which are accepted by everyone. This leads to two extremes. One is reducing everything to specialised schematics, detailed local standards, checklists and guidelines, and ad-hoc 'technical' countermeasures and safeguards. Correspondingly, the auditors would be asked to test and analyse them. This reduces information security and its assessments to nothing more than craft. The other extreme is exactly the opposite. Personal experience, judgement and professional intuition are proclaimed as infinitely superior to all other ways, usually viewed as too conservative and formal. Detailed planning is often disregarded. This attitude is common amongst many security auditors. However, even fine arts have certain rules, and chaotic systems are mathematically deterministic while looking random at the first sight.

We do not believe that a healthy balance between these extremes cannot be reached. Neither do we think that there are no general strategies, principles and philosophies that can increase the effectiveness of information security audits and streamline them, while preserving necessary adaptability, diversity, creativity and initiative. After all, military science has researched and employed such fundamentals for centuries. Is sustaining and assessing the information security of a company or organisation of any size, more complex than waging a modern interstate combat? Some theoretical groundwork for a potentially productive approach to this issue was already laid in the introduction, and a few broad principles were formulated. But prior to proceeding further with this ambitious exercise, we need to address that annoying 'why' question.

To do or not to do?

'Military action is inauspicious – it is only considered important because it is a matter of life and death, and there is the possibility that it may be taken up lightly.'

Li Quan.

There are many sound theoretical and logical reasons why information security assessments must be performed which come from both managerial and technical perspectives. The majority of them can be summarised as 'if things are not regularly verified, analysed and improved by specialists they would go wrong and eventually collapse'. More often than not, in the real world these reasons are simply ignored.

Companies or organisations that do subscribe for professional security auditing usually do it because:

1 Compliance and regulations demand it.

Today the PCI Security Standards Council seems to be the most successful at that. FISMA and HIPAA in the US and FSA in the UK definitely deserve some credit.

2 A security incident has happened.

One that's been caned is worth two that haven't, for sure. At least some of the security audits we have performed in the past were follow-ups to computer forensics.

3 There is someone with high security awareness and understanding amid the executives who lobbies it through.

This usually applies to specialised hi-tech companies or government agencies.

4 The company or organisation is a lucrative target for cybercriminals or malcontents and knows it.

This is commonly complemented by points 1 and 2. Aspiring to 3 is warmly recommended.

5 There is an internal security auditing team in the company anyway.

They should be kept busy to justify their salaries.

Other, less common causes can drive such a decision too. For example, we ran (internal) IT security assessments for companies where the IT management head had just changed. The new IT director wanted to 'clean the house', get a better grasp of what is going on and, no doubt, show the bosses that his predecessor was incompetent. We have also performed independent security reviews of novel pre-production appliances and software for their vendors.

The mindsets of ignorance

Overall, it is more educating and informative to analyse the reasons explaining why companies and organisations do not perform any information security assessments. If they have a turnover of six digits or more, we can safely bet that these reasons are within the manager's skulls no matter what they might say about the budget. There are three most common 'mindsets of ignorance':

1 The 'it will never happen to us' mindset.

We will not tell hair-raising stories about wile cybercriminals and sly insiders in return. This is constantly done by today's media – just visit any major news site. With his metaphor of knights and dragons, Ira Winkler has already examined the security media hype very well – consult his *Zen and the Art of Information Security* book if interested. What we will note, nonetheless, is that 'it' always befalls those to whom 'it will never happen to' because they are not prepared. Consider it to be our modest contribution to Murphy's laws. By the way, 'but it has never happened to us and we are in business for many years' should be translated as 'we don't have an effective monitoring system set up and maintained, and audit trails are not our strongest point'.

Another variety of this tune people frequently whistle to is 'our data (systems, networks) are not interesting for any assailants-to-be'. First of all, one has to be in the attacker's shoes to know what is intriguing for such person and what isn't. Then, how would the assailants guess that 'it is not interesting' until they gain access to it? And if it is truly the case, why to waste time and effort spent on gaining this access while it can be used for other amusing things? Such as hacking into 'more interesting' systems to hide their tracks and preserve resources at your expense. Or sending SPAM. Or distributing 'wares and pr0n'. Or else. Besides, many attacks are simply opportunistic and indiscriminate, like spraying bullets in the dark.

2 The 'shiny box with flashing lights' mindset.

The 'it will never happen to us' is a major overall information security issue. The 'shiny box with flashing lights' mindset is more pertinent to information security assessments. It is human nature to associate security with something palpable, like walls, doors, locks, safes and barbed wire. Vendors actively exploit this perception for profit. Buy this appliance and you will become secure. Buy that software and you will become compliant. To stay secure and compliant, however, you need a whole complex of interrelated measures, many of which are not technical or cannot be solved by technology. Remember the discussion of 'human' and 'matter' factors in the Introduction. Guns alone never win wars, and even on a purely technical level, the safeguard must be properly positioned, configured, maintained and usually interconnected with other relevant systems and applications. Adversaries should not be able to bypass it by either a frontal or lateral attack. To ensure that all of this is done right and eliminate inevitable errors, timely IT security audits are a must. Otherwise, there is a good chance that you have simply wasted your cash on that precious intrusion prevention system, content filter or firewall.

3 The 'we are glad to accept this risk' mindset.

This attitude is typical for people who are able to see through the media and general public hype. As a result, they adapt the 'devil is not so black as he is painted' view. However, sanity tells that you cannot reduce, retain or transfer risks without a prior professional risk evaluation. Which brings us back to the topic of security assessments.

Are there any companies or organisations that actually do not need any information security audits at all? At the very minimum, such an entity would have to:

- Stay away from personal and other sensitive data, like customer databases and trade secrets.
- Thoroughly vet and fully trust all its employees, partners and guests.
- Be disconnected from the Internet and other untrusted networks.

We have never encountered such a corporate or governmental body in the real world.

On monetary contemplations

'Benefit and harm are interdependent, so the enlightened always consider them.'

Ho Yanxi

The budget is the main restricting factor in performing information security assessments. Even during a financial crisis, no highly skilled professional auditor wishes to toil for pennies. At the same time, selling security assessments is a raw spot of all companies that offer these valuable services.

Information security audits are intangible. We have already discussed the ‘shiny box with flashing lights’ mindset and its outcome. Even those who understand the need of performing the assessments often purchase ‘the shiny box’ first and only then ask the auditors to test it. This is potential financial loss. The assessors may or may not recommend getting the ‘box’ in the first place. They could advise you to get a somewhat different solution or position ‘the box’ at the bottom of the risk treatment priority list. They may suggest that a cheaper ‘box’ will suffice. In any case, if you have decided to seek professional advice (which is a necessary outcome of any proper security audit), get it first and then put it to good use.

To make the situation worse, practical end results of information security audits are usually ‘negative’. By negative we mean that auspicious security assessments do not make easily recognisable good things happen. They stop the bad ones from unexpectedly popping up. In the words of ancient Chinese strategist Ho Yanxi, ‘*when trouble is solved before it forms, who calls that clever*?’ Many published sources have stated that subscribing to regular security assessments is akin to getting an insurance policy. However, paying for something not to occur is not even an insurance premium. It is more like charges for in-depth private medical examinations. You do not undergo them to increase your direct income, and the procedures can be rather costly. However, they are ‘a matter of life and death’ that ‘may be taken up lightly’ by many.

Thus, from the financial standpoint, information security audits (and security in general) are viewed as a necessary evil. Psychologically, everyone wants to save on this evil and convince themselves that it isn’t so necessary, after all. Information security is traditionally valued only in terms of reducing loss, and practically never as a profit generating factor. To aggravate the issue, significant parts of this loss are, again, intangible. Have a look at the costs of IT failure as stated in the ITIL V3 'Service Design'. In accordance to this widely accepted set of best practices for IT service management, the tangible costs can include:

- *Lost user productivity*
- *Lost IT staff productivity*
- *Lost revenue*
- *Overtime payments*
- *Wasted goods and materials*
- *Imposed fines or penalty payments.*

The intangible costs can comprise:

- *Loss of customers*
- *Loss of customer goodwill (customer dissatisfaction)*
- *Loss of business opportunity (to sell, gain new customers and revenue, etc.)*
- *Damage to business reputation*
- *Loss of confidence in IT service provider*
- *Damage to staff morale.*

Regarding the second category, ITIL V3 states that '*it is important not simply to dismiss the intangible costs (and the potential consequences) on the grounds that they may be difficult to measure*'.

To emphasise, the damages listed above are assumed to result from accidental failure, disaster or seldom lapse. In the case of a directed and planned act of hostile intelligent force they would be naturally magnified. Additional legal and investigative expenses are likely to be incurred. External public perception of the events would also be unfavourably different. Everyone is sympathetic to victims of a genuine cataclysm. In our highly competitive world, this is not so when *avoidable* trouble is deliberately caused by fellow humans. *Vae Victis* – '*Woe to the vanquished!*' There is at least one bank that none of the authors would use because it has suffered far too many security incidents that led to sizeable losses. This is not misfortune: every bank is getting regularly attacked by cybercriminals and other fraudsters, but the outcome is different. This is negligence.

Examine another curious observation we have made: if the act is deliberate, tangible and intangible losses tend to be more interconnected and amplify each other to a larger extent. According to Clausewitz, '*it is chiefly the moral force which is shaken by defeat, and if the number of trophies reaped by the enemy mounts up to an unusual height, then the lost combat becomes a rout*'. Making things worse, the disclosed security incidents often attract more assailants. The bad guys start viewing the victim company or organisation as a soft target and step in alike marauders.

Is it possible to consider information security as a potential source of profit? ITIL V3 'Service Strategy' explicitly names security as the essential element of warranty. The other key elements are availability, continuity and capacity. Note, that all three are dependent, or at least can be heavily influenced, by their security counterpart. Indeed, from the security specialist's perspective, availability is the 'A' in the infamous CIA triad. '*Warranties in general – continues the ITIL – are part of the value proposition that influences customers to buy*'. Nowadays, utility alone would not suffice.

This, no doubt, can be effectively exploited in marketing and advertisement. There are a great deal of services and products that come from different vendors, yet their utility is essentially the same. As everyone is catching up with the general technological side, the difference in security can provide the margin needed to overcome competition. At the same time, such a difference may not be very difficult to achieve. We have effectively partnered and regularly worked with IT integration and maintenance companies. Our assistance has allowed them to offer customers discounted security audits and other security services as part of a complete service package.

Of course, using information security as a selling point to achieve service and product warranty, superior to that of your competitors, carries its share of risks. It must be done with caution, since detrimental effects of any security blunder in case of such commercial proposition would be magnified. The balance of expenditure on the security element of the offer, which can easily grow to an unacceptable level, must be constantly checked against the additional profits gained. However, this approach is by no means impossible. It only takes some initiative, confidence and solid skills:

- *Therefore armed struggle is considered profitable, and armed struggle is considered dangerous (Sun Tzu).*
- *For the skilled it is profitable, for the unskilled it is dangerous (Cao Cao).*

Thus we conclude this brief discussion of ‘whys’ in respect to finance and choice and can safely turn back to more philosophical strategic matters.

The fundamentals

'War is only a part of political intercourse, therefore by no means an independent thing in itself. ***It has certainly a grammar of its own, but its logic is not peculiar to itself****.'*

Carl von Clausewitz

By definition, this is the most vital section of this book. Comprehending and putting the rest of the material to good practice depends on gaining a firm understanding of the fundamental principles. A lot of them are pure logic and common sense. Nevertheless, until the maxim is clearly formulated, its meaning and use will remain beneath the surface. That is, in the realm of intuition.

We have already expressed some of the basic postulates in the Introduction. To rehearse the most relevant ones:

- *Information security is a science and the art of protecting data.*
- *IT security is the science and art of protecting data in electronic format.*
- *Information security assessments are a practical way of improving the information security state.*
- *Security assessments must evaluate probabilities and potential impacts of passive and active security incidents.*
- *To assess the likelihood of passive security incidents it is usually sufficient to analyse controls, their implementations and enforcement.*
- *To assess the probability and impact of active security incidents a more aggressive and all-encompassing path must be taken.*

- *'Human' and 'material' information security elements have to be synchronously audited, analysed and measured.*

Like the scheme in the beginning of this chapter, these principles are sufficiently general to be applied to any security assessment, in any given situation. When we have looked at information security auditing from the 'bird's eye' perspective, trying to dissociate ourselves from narrow technological and procedural aspects, 20 such principles have surfaced. Let us list and analyse them in brief.

1 *Information security assessment is an act of corporate or organisational politics.*

This is a pure Clausewitzian statement that goes well with his infamous '*war is not merely a political act, but also a real political instrument, a continuation of political commerce, a carrying out of the same by other means*' quote. At the end of the day, it is the politics and strategic goals of a company or organisation that leastwise determine:

- Whether an audit will be undertaken.
- When and by whom it is going to be done.
- Its overall scope and type.
- How it will be managed on the auditee side.
- Which actual follow-up reactions will be performed.

This reflects the planning of large-scale security programmes by the auditee management, of which security assessments should be the integral parts.

2 Information security assessment is always shaped by political, administrative, technical and human 'terrain'.

Having strategic and political aims at its roots, the character and performance of information security assessments will be inevitably influenced by the auditee policies, operations and procedures, technology, relationships and personal traits of the people involved, etc. This is similar to effects terrain, environmental conditions, channels of communication, quality and quantity of troops and their armaments, etc. have on any battle.

3 Information security assessment must shape information security systems of its target.

Any action is reciprocal and triggers reaction. The absence of a tangible response is a type of reaction too. Even if the security assessment did not identify any gaps, it should still trigger (or prevent) change.

4 Information security assessment is never complete.

This can be compared with '*the result in war is never absolute*' (Clausewitz). Neither, in accordance to the strategy classic, it has to be: '*but this object of war in the abstract, this final means of attaining the political object in which all others are combined, the disarming the enemy, is by no means general in reality, is not a condition necessary to peace, and therefore can in no wise be set up in theory as a law*'. There is always something else to check, test, verify and analyse. You cannot discover all the existing flaws. You cannot 'disarm the enemy' by foreseeing and preventing every opportunity for hostile acts. Some security auditors are devoted perfectionists, but this perfectionism must be controlled to bear fruit. The approach based on prioritisation of risks is the key. Some actions can be placed at the bottom of the priority list and postponed for later. Which brings us to the commonly repeated maxim that ....

5 Information security assessment must be a part of a continuous process.

The environment changes. What was secure yesterday is not so today. What was sufficient to become compliant a month ago may be unsatisfactory now. Standards alter. Technology constantly moves forward and can introduce significant correctives. The audit methods evolve. Besides, as stated when examining the previous principle, the next audit can accomplish what the previous did not. On any hand, it is clearly required to verify both completeness and correctness of any follow-up reaction to its predecessor. Information security auditing is a powerful *way of monitoring the information security state*. A stand-alone assessment completely misses this point.

6 Information security assessment should maintain a proper balance between tempo and depth.

As often, the art is in doing as much as you can in as little time as you have. Because the conditions change, a protracted audit can end up with findings of its beginning becoming obsolete or irrelevant when the end is reached. All critical vulnerabilities and gaps should be promptly analysed and reported – '*each minute ahead of the enemy is an advantage*' (Gen. Blumentritt). However, hurrying up and missing important discoveries are another highly unpleasant extreme.

7 Information security assessment must always exceed its ***perceived*** *scope.*

This principle can be easily misunderstood. It does not mean that you have to go after more targets than were