Assessing Information Security

Strategies, tactics, logic and framework

A Vladimirov • K Gavrilenko • A Michajlowski

Second edition

itgp™

Assessing Information Security

Strategies, tactics, logic and framework

Second edition

A VLADIMIROV
K GAVRILENKO
A MICHAJLOWSKI

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

First published in the United Kingdom in 2010
by IT Governance Publishing: ISBN 978-1-84928-035-8

Second edition published in 2014
ISBN: 978-1-84928-599-5

PREFACE

When a new software version is released, an updated ‘changelog’ file outlining all changes since the previous version is supplied. It has been five years since the first edition of this book was published: a remarkably long period for the modern information technology milieu, but perhaps not so for its information security shadow or counterpart. This preface is, effectively, a brief changelog for both the book and the environment it applies to in practice.

Strategy-wise, all of the key principles outlined in the first edition stay in place unchallenged. We did not have to change a single epigraph to any section, and remove or replace any quotations forming the book’s logical backbone. The schematics that reflect high-level process structures also remained unaltered. In a nutshell, no Black Swans overriding any of the first edition fundamentals have flown by since. Even some of the technical examples (sadly) remained relevant, and we decided to leave them where they belong while providing new examples and reflecting novel technological challenges where necessary. This particularly applies to the areas of application security testing, client-side gaps, and some rather peculiar physical level and wireless risks. If anything, accelerated technological developments such as expansion of cloud networks, application services, business use of BYOD (Bring Your Own Device) and BYOA (Bring Your Own Application), together with all kinds of interconnected mobile devices, have only strengthened the strategies we have elaborated by forcing downstream security tactics to be more aligned with them.

They have made the *information security zone* more fluid, its borders/attack surfaces less certain, *information security anti-patterns* more pronounced, and the roles of the human factor and processes more critical to security organisation.

The common 'combined arms' approach of modern-day cybercrime makes it sometimes difficult to tell where 'technical hacking' ends and 'social engineering' begins. With the dramatic increase in outsourcing, offshore/nearshore out-staffing, and the use of remote freelance contractors, the border between 'insiders' and 'outsiders' is also blurred. Security audits that have been appropriately selected, planned, executed and responded to are becoming indispensable to address the rising information security issues, whether process, technical or human. Even reasonably educated guesswork on behalf of the would-be designers, implementers and maintainers of security controls just won't do the job any more.

Perhaps the most important update of the second edition is that it has become more 'defender-oriented'. We do concentrate more on what the applicable countermeasures and corrective actions should be, and attempt to supply as much information relevant to the auditee side as this book's scope and purpose would allow. Hence, we hope that it has somehow shifted from a targeted treatise on "what a CIO, CTO, CISO, Director of Information Services, or other concerned manager or professional should know about information security assessments" towards a more generic guide to good information security practices, written from both the auditor's and the auditee's perspective. Nevertheless, the auditor's view – or even the attacker's – is still preserved as the predominant, so that the dynamics of this work (and

the entire field) are not stalled, and the seeds of the passive check-list attitude are not planted in the readers.

Inevitably, paying more attention to design and implementation of security controls means dedicating more time to the relevant standards and compliance-based frameworks. The most significant compliance change since the first edition of *Assessing Information Security* is the ISO27001:2013 release that has finally superseded the battered 2005 version of this key international information security management standard exactly a year ago. It took us another year to realise the practical significance of this transition by working as both ISO27001:2013 auditors and implementation consultants (for different customers). Describing ISO27001:2013 in detail, or the differences between it and the previous 2005 version of the standard, are not the aims of this work – such publications are already abundant. Where appropriate, however, references to ISO27001:2013 and its Annex A have been added, and overall the second edition of the book is more heavily ISO27001:2013-based. As a side note, we find the following peculiarities introduced in the new version of the Standard worth mentioning in the context of this preface:

- ISO27001:2013 does not mandate the use of PDCA (Plan-Do-Check-Act) cycle anymore. So, for instance, an OODA loop or any combination of nested OODA loops can be applied instead. Nevertheless, we still recommend the hybrid of PDCA and OODA as suggested in the first edition of this book (see *Figure 7*).
- ISO27001:2013 does not explicitly mandate asset-based risk management. So, an ‘asset’ now could be what we call a “centre of gravity” using the terminology of military strategy. This could provide a very effective

approach to both assigning ownership of risks (a requirement of the new Standard!) and prioritising their treatments.

- Talking about risks, we were pleasantly surprised to see that ISO27001:2013 has adapted a new definition of risk based upon uncertainty, almost as if the standard's authors took to their hearts all that we wrote about 'friction' in the previous edition. Saying that, the more traditional definition remains in use here as more practical for the purpose of quantifying risks.

To summarise, we do hope that this renewed edition of *Assessing Information Security* will become a useful supplementary guidance for ISO27001:2013 auditors and implementers alike. It is not limited to this specific standard, however, and should be helpful in obtaining and maintaining compliance to the PCI DSS (version 3.0 is referenced), SSAE16 SOC1/2, and any other standards or regulations where performing information security assessments, whether third-party or internal, and handling their outcome is a key requirement. Besides, to our knowledge, this book continues to be the only printed source that addresses managing information security audits at all levels and of all types, from physical security checks to social engineering and penetration tests, on both the auditor's and the auditee's sides, regardless of compliance dependencies and adopted frameworks. In fact, it aims to provide a generic strategic principles-based framework, which can always be applied when there is none, and has been proven by many years of practice. It can be consulted when you need an independent security assessment, or want to set up an internal audit team, or review your vendors' or partner companies' levels of security, or even run your own

information security services business. Taking into account the possible requirements of government organisations, the real use cases, perhaps, go well outside the original scope we envisioned.

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.

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 – including successfully passing an audit – must cover why and what kind of assessments have to be performed subject to a particular situation. This, in itself, depends on a variety of variables, both external (regulations, litigation, customer requirements) and internal (business strategy, plans, politics, culture). Such a thorough treatise is further 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. On the auditee side, it must cover justifying controls or their absence, presenting objective evidence to the auditors, executing corrective actions and providing sufficient evidence of their execution. Everything we have just listed,

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

however, is mere technicality. If you concentrate on them too much and without applying a sufficient level of abstraction and generalisation, you risk missing something of a much greater importance: their logical, strategic, and even philosophical backbone.

You will fall into a trap of adhering to rigid, mindlessly executed 'if-then-else' mechanical instructions. These can easily become outdated and flawed, even by a subtle change in the operating environment – not to mention business, organisational, market or regulatory change. A smart opponent can outwit them using non-conventional methods. Until the new, appropriate schemes are generated – usually by someone else and late – you are lost. Any approach without a solid strategy is destined to remain reactive.

Conversely, 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, and with minimal expense. Even more, you can shape the change yourself, 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 will 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 to describe what we have alluded to as "a sufficient level of abstraction", coupled with a rapid and precise low-level, 'ground' act.

Unfortunately, when we have scoured for what others have said about 'the philosophy of information security' and its implications towards security assessments in specialised texts, we were strongly disenchanted. We stumbled across multiple security management sources presenting solely

managerial perspectives; technical displaying purely technological perspectives; and legal offering exclusively legal perspectives. Numerous works are written on the subject of social engineering, but they are neither produced by expert psychologists nor take into account technological means that enhance social engineering attacks in a sufficient depth. The existing information security standards are presented as some kind of an infallible verity that contains everything a security specialist might need. Adaptation and implementation in every particular case is left solely to the experience of implementer, as if no hints could be provided. 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”, “security through obscurity never works”, or “everything is vulnerable” are omnipresent. We are not implying that these are somehow entirely incorrect. They have their time, place, value and significance – but they do not form a coherent integral framework that can be easily adapted to a variety of relevant situations in both theory and practice.

Then we have turned to other disciplines for guidance. For instance, we have looked at modern mathematical chaos and game theories. In fact, we have borrowed from them. These are fine examples of applicable ‘coherent integral frameworks’ that offer useful insights. It was the philosophy of war and its core principles, however, that truly hit the nail on a 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 would be repeated in this book. We have left them in place for the second edition, too. At that time, we found the high suitability of statements written more than two thousand years ago to what is still considered a cutting edge technology today at the very least amusing. Besides, they provided a necessary symbolic martial arts link. In this work, however, the assertions, opinions, estimations and judgements of master strategists of all times are not just some fancy spice-up citations and epigraphs to attract certain categories of audience. 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 – no toying around!
- Realism and utilitarianism (one who does not apply it properly may be doing it for the last time!).
- Simplicity and clarity of statements (often at lack in numerous security policies we came across).
- Clear distinction between strategy and tactics (a flaw more common in ISMS we have observed than one might think).
- Taking into account wide selection of variables (organisational, technical, but – above all – human!).
- Reusable terminology (which is also not technology-specific and can be comprehended at any organisational level).
- Multidisciplinary approach (as is the field of information security itself, ranging from applied cryptography to personnel background checks).

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 Carl von Clausewitz's infamous saying, '*Everything is very simple in war, but the simplest thing is difficult'*, and see where it might lead your thoughts. Then perform this simple exercise every time you encounter a classic martial citation in this book.

Of course, applying philosophy and strategy of war to other disciplines is not news. In particular, this was extensively (and, perhaps, excessively) done in business management. We have even encountered a linguistic opinion stating that "Sūn Zǐ Bīng Fǎ", traditionally translated as "Sun Tzu's Art of War", actually means "Sun Tzu Competitive Strategies". The Boston Consulting Group book, *Clausewitz on Strategy*, 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 its 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 CEO is not a general and is not

likely to wield such power. Attempts to do so may actually lead to some of the anti-patterns we warn against later in this book, namely the "stovepipe" and "management by perkele". But perhaps the mightiest blow comes from 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, at least to an extent they are cooperative. They involve rather complex relationships between different sides with net gain or loss. There is a mutual benefit even from some forms of intercourse with direct competitors. As a security consultancy, we are not at other information security companies' throats. We have met their professionals during numerous industry conferences and informal gatherings. We have exchanged ideas and shared research. We have had many beers together. We may outsource some work to a competitor when specific resources or expertise are scarce. They may outsource it to us under similar conditions. It does not even have to involve commission in all cases. It could be an act of a goodwill to a customer, or birth of a partnership. This is good for business and develops the industry, thus it eventually benefits us all whether we think about it or not. Even the compliance auditors are not enemies no matter how harsh they might be. Years after graduation, many come to realise that the harshest examiners brought the most benefit and, perhaps, were the best.

When it comes to real aims of safeguarding your information and other assets, however, please consider the following suppositions:

- *'At the end of the day, information security is a form of warfare'.*
- *'In essence, it has plentiful similarities with "traditional" counter-intelligence and counter-insurgency efforts'.*

- *'Unlike the information security industry, such efforts existed and have evolved for centuries, if not millennia'.*

These are 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 "decentralized and flexible network structures". Now we can observe such never-ending global scale conflict in everyday news. These researchers also proposed the somewhat ill-fated term 'cyberwar', which is constantly abused and misunderstood by media and general public who think it's all about 'hacking'.

Returning to game theory:

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

Cooperating with a cyber criminal does not make more sense than collaborating with a burglar who broke into your house. The same applies to a disgruntled employee who has decided to sabotage business or sell internal data to a competitor. The reasons for it could vary, and the perpetrator might even have a point. However, the latter is for the court to decide, and in this book we are interested in the end result. One can, and should learn a lot from security incidents, but this is not cooperation. Collaboration with criminals, no matter what the possible justification, is a crime per se. Cooperation 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, when real security issues are dealt with.

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

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

It is not merely a system, process, approach, service, set of methods, mindset, and so forth. It is all of those things listed and 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 information in electronic format'*.

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

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

They can and should be about more than 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 and a Nobel Prize winner 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 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 to be 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 closer 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 a 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 cyber crime', 'war on SPAM', or 'war on web application insecurities'. It may motivate some people to do something about these issues in your organisation, 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 'Neo-Clausewitzian'. This is particularly evident in the second chapter of the book, which is dedicated to directing and shaping effects that policies, governance and compliance have on information security assessments and their outcomes. Note that the political approach is always heavily at play when security budget and other resource 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', especially those with no security-centric background. It is reflected in viewing security as a mere part of business continuity, disaster recovery and prevention, or even service availability. In application development, security flaws might be viewed on par with other bugs, with no priority given to their elimination. It is often expressed by the essentially defeatist 'c'est la vie' statements, such as "everything can and would be hacked anyway", "we can do our best, but sensitive data will still leak out", or "by providing our information to the Cloud we are losing control over it anyway". 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 no matter how correct it* ***seems*** *to be.*

Such a cataclysmic approach to information security reduces initiative, decreases morale, and promotes passive defensive, reactive responses, 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'*.

Having said all of the above, of course, it does not matter that the company or organisation should not have implemented a quality incident response and business continuity and disaster recovery plans. Information security standards do not include these within the list of controls (such as ISO27001:2013 Annex A 16 and 17) by accident. What we imply is that these are only one line of what should be a multi-layered defence. The last line.

Comparing a natural disaster or unfortunate accident to premeditated malice is senseless. Even if the end effects and even some of the countermeasures appear to be the same, both preventive and reactive responses will have to differ. Assessing the related risks, and predicting their likelihood and 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 only'*.
- *'Active security incidents happen due to the combination of error and hostile action'*.

Practically every successful attack involves some mistake on the defender's side. Infectious disease happens when virulence of the microbe and lack of immunity of the infected host, augmented by poor hygiene, are superimposed.

- *'Passive security incidents can easily pave the way for their active counterparts'.*

An accidental access control flaw or sensitive information leak are likely be deliberately abused later. It is better to be prepared for the worst and base any impact estimations on it.

- *'Security assessments must evaluate probabilities and potential impacts of both 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 on all systems involved.

4. the enforcing software is present on all corporate systems that contain, or may contain, sensitive data (mind BYOD and telecommuter systems!). It is correctly installed, configured, maintained and documented. Users cannot easily disable it, and such action will trigger a policy violation alarm.

Alternatively, the prohibition of use can be substituted by appropriately employing strong cryptography to protect data on portable computers, smartphones and mobile media.

However:

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

In the example above we will have to add the fifth point: verify that our USB port blocking software cannot be circumvented. If this is possible, then it becomes necessary to discover how much effort and skill such a hack would require from a potential attacker. And then the sixth: check whether other mobile storage media that does not rely on USB ports can be and is used to carry information. For instance, can sensitive data be automatically copied to any such media over Wi-Fi, Bluetooth or any other wireless connection? If encryption is employed, strength of ciphers, keys and its actual implementation, key management in particular, must be analysed. Again, one must estimate how much skill, effort and time the attacker has to expend to break it. Are there any publicly available tools or exploits one can simply download and run? In a nutshell, all these additional security auditing means are a form of *penetration testing*, which is always active and highly intrusive intervention.

Thus, we have finally arrived to 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, worms and other malware, you are not battling an inanimate piece of code. It is nothing less than your 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, fraudsters, cyber criminals, 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 intelligent 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, just like intrusion prevention or antimalware are on the IT side. If Clausewitz meant anything like it when he wrote about war being aimed at human weakness,

he would have explicitly written about 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 both "matter" and "intelligent force" 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 because they are inseparable. Therefore, both have to be synchronously implemented, maintained, audited, analysed, measured and improved, so that all available reasonable 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 contributory proportions of such things – in particular technologies – 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'. As a reminder, FUD is a common abbreviation standing for Fear, Uncertainty and Doubt. FUD undermines will and leads to paralysis of action.

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

- *fear* of being successfully compromised (or failing an audit!) 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 or mitigate the breach.

A typical attacker FUD encompasses:

- *fear* of being discovered, caught and persecuted.
- *uncertainty* regarding defender preparedness, 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 favour the attacking side. Fear, though, often reinforces competent defenders: in the case of

defeat, the (legal) repercussions for attackers are often 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 defenders' victory. '*The key factors for winning the FUD game appear to be resolve, initiative, good observation and orientation, foresight, cunning and swiftness. Chance always plays its role and cannot be dismissed. 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 underlying logic is clear. It can be formulated in a minute. Here it comes from the (independent) auditor's viewpoint:

- Find out about the assessment's goals and conditions.
- 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.
- Ensure that you have collected a sufficient volume of quality objective evidence.
- Analyse it.
- Pull the analysis results together.
- Measure and analyse relevant risks.
- Consider realistic remedies.
- Generate an impressive report.
- Work with the customer on any follow-up acts if needed.

A mirror version of this scheme as seen from the auditee's perspective is also easy to generate and you can try it as an exercise. It will have to be more strategic in nature. To an extent, it is defined in the recent ISO27000 and Annex SL aimed at streamlining various ISO standards. 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 timespan of a few days. More often than not, only glimpses of what is really going on in the audited entity are caught. For the auditee it is an element of some larger long-term security program that does not end with passing the assessment. Or, at least, this is how it should be.

Wing Tsun is an effective and increasingly popular Chinese martial art. Bruce Lee 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 a thousand 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 very rare cases where the governing principles do not have to be built into a resistant and inert (physical, organisational, corporate) body by dedicated, sustained effort, things are not straightforward. Knowing the major winning strategies will not instantly make you a chess grandmaster. And chess is only an ancient board game with an immutable set of rules.

Unlike chess, in the field of modern information security there are no defined winning strategies accepted by everyone, anywhere, at any time. 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, or are expected to test and analyse them. When, instead of the expected positive outcome, the auditor uncovers a major program, planning or process non-conformance, it comes as a big surprise. A typical example of such a situation relevant to ISO27001 is paying more attention to Annex A controls than to the body of the standard and thinking "if all Annex A controls are implemented, we will pass". An auditor might also concentrate on Annex A since it provides a comfortable checklist, providing that the requirements of the Standard body appear to be *formally* fulfilled. This approach reduces information security and its assessments to nothing more than craft.

The other extreme tends to be the opposite. Personal experience, judgement and professional intuition are proclaimed as infinitely superior to all other ways, which are usually viewed as too conservative and formal. Detailed planning is often disregarded, and minor non-conformances could be ignored regardless of the real risks they may be associated to. This attitude is common among many security auditors. However, even fine arts have certain rules, and the so-called 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. Nor 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. Exactly the same applies to passing the audits from the auditee's side ('the defender') and, on a more general note, to designing and implementing

a workable information security management system and its controls. After all, military science does research and has employed such fundamentals for centuries. Is sustaining and assessing 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, whether internal or external, must be performed. They come from both managerial and technical perspectives. The majority of these reasons are maintenance-related and can be summarised as 'if things are not regularly verified, analysed and improved by specialists they would go wrong and eventually collapse'. Alas, the 'improvement' part (Section 10 in the body of ISO27001:2013) is frequently understated. More often than not, in the real world these reasons are simply ignored. Companies or organisations that subscribe for professional security auditing usually do it because:

1. compliance and regulations, or customer contracts demand it.

Today, the PCI Security Standards Council seems to be the most successful at that. SSAE16 (usually adapted by

service providers), FISMA and HIPAA in the US, and FSA (primarily its chapter on IT Controls) in the UK definitely deserve some credit. ISO27001 is also gaining popularity, at times because large customers demand it and it is easier to certify to the Standard and pass one monitoring assessment per year rather than several assessments from such customers. Failing a customer (second party) assessment could lead to a contract loss. If the profit brought in by such a contract exceeds the costs of formal certification the latter should be opted for without a second thought, not least because of the additional benefits brought in. Quite often, certification to an internationally recognised standard is a market opener, especially for foreign companies that begin operating in the West.

2. a serious 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. It does take some pain to realise that if no preventative action is taken its reactive counterpart can become a never-ending loop. Besides, at times only security auditing (often external) can help to establish the root cause of an incident.

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

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

4. the company or organisation is a lucrative target for cyber criminals 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. So, 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, services and software for their vendors.

The mindsets of ignorance

Overall, it is more educating and informative to analyse the surprisingly persistent 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 managers' 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"/"it always happens to other people" mindset'*

We will not tell hair-raising stories about wily cyber criminals and sly insiders in return. This is constantly done by today's media – just visit any major news site. The hype is such that at times even the report of a not-so-critical and specific technical security issue makes it to the top ten read on BBC News. 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 'it will never happen to' because they are not prepared. Consider it 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". Pick up any company that claims so and verify their incident detection and response processes and controls if you disagree.

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 a 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 waste time and effort 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 launching DDoS (distributed denial-of-service) attacks, whether commercially or politically motivated. Or sending SPAM. Or distributing 'wares and pr0n'. Or anything else. Nowadays, no sane attackers will ever perform any such activities from systems that can be traced back to them. It even comes to selectively targeting countries with weak cyber crime laws to establish a foothold for further attacks from there. Until a few years ago, Brazil was the favourite. After its legal system was improved the focus shifted to Vietnam. On some days the overall number of attacks launched from (read – 'via') this country could reach a half of all registered attacks in the world. To underline this point, modern cyber crime is a big business, botnets are lucrative, and there are hundreds of things that could be

done (ab)using a hijacked system or service. Very few of these have a relation to that system's original purpose. Besides, many attacks are simply opportunistic and indiscriminate, like spraying bullets in the dark.

It has been said that selling information security is akin to selling insurance. However, insurance typically covers what we might call 'passive' incidents. The difference in approach towards the passive and the active has been already reviewed in the preface.

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 and preparation for them. 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 any technology. Recall the discussion of 'human' and 'matter' factors in the introduction. Guns alone never win wars. 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 or physical 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.

Did anything really change from the first edition of this book? Well, the *"shiny box with flashing lights"* mindset has been complemented by its "*shiny SaaS (software-as-a-service) app with colourful buttons*" service equivalent. Subscribing to a third-party service is more economical, and is it not run by the real specialists in the field your company cannot afford? It usually is, but do they really know about your business requirements, organisation, politics, typical user behaviour, environment changes, and so on? Even moving everything to the Cloud may not resolve all of the associated information security problems, rather creating a comfortable and affordable illusion of such a resolution. A new section (A.15) on analysing security (and reliability) of suppliers and supply chains has been added to ISO27001:2013 for a good reason.

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 adopt the "devil is not so black as he is painted" view. However, common sense tells that you cannot reduce, retain or transfer risks without a prior professional, desirably independent risk evaluation. How else could you justify exclusion or inclusion of controls (now mandated by ISO27001:2013 in relation to its Statement of Applicability)? 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, such as customer databases, customer data 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 and, in fact, in doing anything involving information security at all. Even during a financial crisis no highly skilled professional auditor or implementer wishes to toil for pennies. At the same time, selling security services is a raw spot of all companies that offer them.

Information security audits are 'intangible'. Many countermeasures and controls are just as intangible: consider what is often referred to as 'the change in corporate security culture'. We have already discussed the "shiny box with flashing lights" mindset, its current state and expected outcome. Even those who understand the need to perform security assessments often purchase 'the shiny box' or subscribe for 'the shiny service' first and only then ask the auditors to test its usability and integration. This is potential financial and man-hour loss. The assessors may or may not recommend getting the 'box/service/app' in the first place. They could advise you to get a somewhat different solution or position it at the bottom of the risk treatment/corrective actions priority list.

They may suggest that a cheaper solution 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. Avoid making uninformed guesses, and note that the availability of numerous third-party services to subscribe to, often run by little-known start-ups, makes it all only more confusing for the decision maker.

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 the ancient Chinese strategist Ho Yanxi, '*when trouble is solved before it forms, who calls that clever?'* We have already stated that subscribing to regular security assessments is somewhat akin to getting an insurance policy, but 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. They are 'a matter of life and death', however, that 'may be taken up lightly' by many.

Thus, from the financial standpoint information security audits (and security in general) are always viewed as 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, a significant part of this loss is, again, intangible. Have a look at the costs of IT failure as stated in the ITILv3 "Service Design". In accordance with this widely

accepted set of best practices for IT service management, the tangible costs can include:

- *Lost user productivity*
- *Lost IT stuff 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, ITILv3 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'*. Indeed, designing any financial metrics on information security remains difficult unless we talk about specific cases of online services' availability and their downtime due to attacks. The majority still sticks to the traditional metrics, such as the number of incidents per period of time, and will continue to do so.

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 a 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 regularly attacked by cyber criminals 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 like marauders.

Is it possible to consider information security as a potential source of profit? ITILv3 "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, all three are covered in the corresponding sections of ISO27001:2013 Annex A, and 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. What was a differentiator in the past has become the enabler.

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. This is especially true in the areas where trust is the key, as when the customer entrust their key business processes, commercial secrets or employees' personal data to a third-party service or product. 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 mitigation and implementation services as parts of a complete service package.

Of course, using information security as a selling point to achieve service or product warranty superior to that of your competitors carries its share of risks. It must be done with caution, since the detrimental effects of any security blunder in a commercial proposition of this sort 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. This approach is by no means impossible, however. It only takes some initiative, confidence and solid skills:

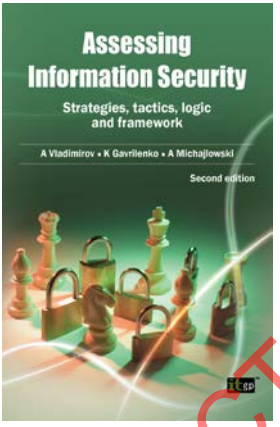
- *'Therefore armed struggle is considered profitable, and armed struggle is considered dangerous.' (Sun Tzu)*

- *'For the skilled it is profitable, for the unskilled it is dangerous.' (Cao Cao)*

Thus we conclude this brief discussion of 'why's' in respect to finance and choice and can safely turn back to more 'philosophical' strategic matters.

<<< END OF EXTRACT >>>

Assessing Information Security: Strategies, Tactics, Logic and Framework



- Shows how to use principles of military strategy to defend against cyber attacks, enabling organisations to have a more structured response to malicious intrusions.
- Explains the priorities for robust cyber security, helping readers to decide which security measures will be the most effective.

Buy your copy today

www.itgovernance.co.uk/shop/p-363-assessing-information-security-strategies-tactics-logic-and-framework-2nd-edition.aspx

www.itgovernance.co.uk/shop/p-363-assessing-information-security-strategies-tactics-logic-and-framework-2nd-edition.aspx

www.itgovernance.co.uk/shop/p-363-assessing-information-security-strategies-tactics-logic-and-framework-2nd-edition.aspx