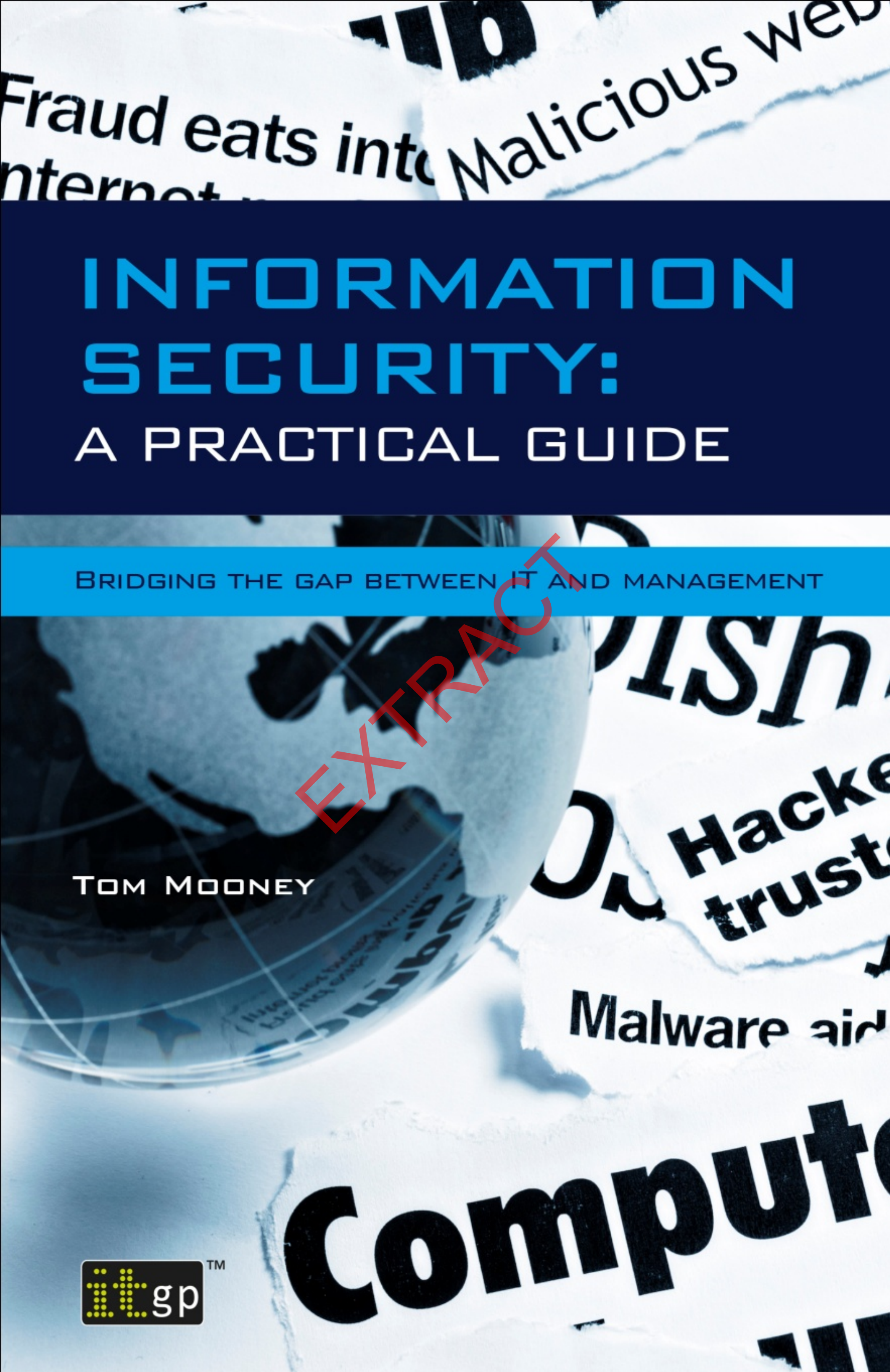


INFORMATION SECURITY:

A PRACTICAL GUIDE

Bridging the gap between IT and management

Tom Mooney

itgp™

Information Security: A Practical Guide

Bridging the gap between IT and management

TOM MOONEY

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 publisher and the author cannot accept responsibility for any errors or omissions, however caused. Any opinions expressed in this book are those of the author, not the publisher. Websites identified are for reference only, not endorsement, and any website visits are at the reader's own risk. 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 4EA
United Kingdom

www.itgovernance.co.uk

First published in the United Kingdom in 2015
by IT Governance Publishing
ISBN 978-1-84928-741-8

ABOUT THE AUTHOR

Tom Mooney has more than ten years' IT experience working with sensitive information. His current role is as a security risk advisor for the UK Government, where he works with project teams and the wider business to deliver key business systems securely. His key responsibility is to act as an intermediary between management and IT teams to ensure appropriate security controls are put in place. His extensive experience has led him to develop many skills and techniques to converse with people who are not technical or information security experts. Many of these skills and techniques are found in this book.

He has a BSc (Hons) in information and computer security, and is also a CESG certified professional.

CONTENTS

INTRODUCTION

When I started my career in information security many years ago the thing that struck me most was the lack of engagement with people who weren't of the information security profession. IT in other departments would shy away from speaking to me as they feared security would stick its nose in and either stop their work or make things more difficult. The business viewed it as a dark art and as long as their security guy said it was okay then that was fine. Most people regarded security as a blocker rather than an enabler. I resolved to change that; I wanted people to see security as an enabler: something that can help you do more business and to create more services. An analogy I like to use when describing security is that of a car: would you get into a car that had no brakes? The answer is no, and so security is like the brakes on your car: you need them to drive. Some people counter that brakes stop you going forwards, to which my response is: do you drive around with your foot on the brake pedal? No, you have brakes to slow you down when you come to a junction, traffic lights or some other hazard. You use them as a control so that you can slow down and assess the situation before proceeding safely. Every driver can see the value in brakes, and this is exactly the viewpoint I want to build for information security. In the information age where everything is connected to the Internet, information security is as important as the brakes on your car: if you don't have it, you're going to have a nasty accident at some point.

I set about creating and building techniques so that I could better work with my peers, increasing their understanding of security. Helping a business understand the risks means it can make more informed decisions and encourage it to grow.

The chapters in this book have been used by myself over a number of years as tools so that I could help my employers build safer systems. Each chapter shares one common focus and that is communication; nothing in this book has been suggested without giving you real value and helping you to better collaborate with your team. I have come across many long-winded documents or overly technical diagrams that are created and then simply filed away to tick a box for some compliance. Each of the things you create from following this book are meant for re-use; they are meant to be changed as the system changes and the risks change. Each chapter is written with examples; the idea is that you read the chapter, understand the technique and then implement it referring to my example if necessary. The book is written in order of how you would follow the techniques described, and each chapter builds upon the previous chapter. The techniques described can be adapted and changed – in fact I encourage it – as I have applied these on many Agile projects and adapted them each time to suit the people I worked with, so you should do the same.

I would like to offer one key piece of advice that is more important than anything else. Make sure you take the time to educate your team on security in a way that they will understand. Make sure you regularly take the time to understand their security concerns and always give them a response ensuring they understand the reasons for your decision. Having your team buy into security and making it part of their day to day work is one of the most valuable information security cultures you can foster; your people will truly become an information security strength.

CHAPTER 1: DAY ONE AS A SECURITY PROFESSIONAL

Chapter Overview

This chapter gives you guidance on bedding yourself into your new role in security. It will help you to get your bearings and explains some of the early tasks you need to carry out to understand your role much better.

The chapter first reinforces the confidentiality, integrity and availability (CIA) mantra, explaining its meaning and how to use it in your role. I then describe the people you should look to meet as soon as possible so that you know what is going on within the organisation and who you will need as allies. The chapter then explores how you can begin to understand the organisation's security culture in order to realise how much influence you have in your role.

Objectives

In this chapter you will learn the following:

- How to build a foundation for communication using CIA
- How to understand the security culture of the organisation
- Building relationships with key personnel
- Identifying the gaps in the organisation's security set up.

Your First Day

Your first day in an information security role can be extremely daunting, especially if you are new to the profession. Often information security is seen as a dark art performed by some elite person, and your peers will have a higher expectation of you and your knowledge of information systems. During a security incident even senior managers will look to you for advice and guidance, so you should be prepared to take on this responsibility and lead when needed.

It is important that you have an overall understanding of the organisation's IT strategy and what systems are being changed and deployed. Remember, in security the attackers only have to win once, whereas you have to win every time. This means there only needs to be one mistake or oversight and a vulnerability could be exploited in your organisation that could have a tremendous impact.

From day one you must get to know the organisation as quickly as possible, its people, its strategy and its culture. You will not be effective in your role until you understand those things.

Confidentiality, Integrity and Availability (CIA)

The CIA mantra is the bread and butter for every information security professional. These three key areas form the foundation of information security. Think of CIA as your weapon when discussing security with IT and business staff alike. Set this foundation for anyone you are going to work with regularly, as it will allow you to develop a mutual understanding. In my experience people pick up the CIA mantra extremely easily.

Confidentiality means that only those who should have access to the data do, and those who do not have a need to access the data cannot. Data is protected from unauthorised access, and this is the traditional view of security.

Integrity means that the data is accurate and that we can rely upon it. Data that is incorrect or suspected of being incorrect has no value as we cannot rely upon it. When discussing integrity ask how much of the data's integrity would need to be compromised before confidence is lost in its entirety, as this will help you gauge how important integrity is.

Availability relates to the information being available to those who are authorised to access it when they need to access it. Information that is not available for use is of no use to us. You may have heard the anecdote of taking the data, putting it in a safe and then dropping that safe to the bottom of the ocean. If that's what we have to do to protect the data then why keep it at all? We can't make any use of the data, and it is a liability not an asset. This is the part people have most difficulty in understanding. Sometimes people think of the data as a physical asset, so for example if the data is stolen, they assume we no longer have access to it. In fact, theft could be a mixture of both availability and confidentiality. It is important to be clear that availability is about whether we can or cannot access the data.

Getting to Know the Business

It is often easy to forget that you and the IT department are there to serve the business; you are a tool and resource to be used for the business to achieve its objectives. This is why it is important to understand the business and what it wants to achieve. In this section I will introduce the different roles and explain their importance.

Senior Managers

When I talk about senior managers in this context I am referring to those who are one level under the Board; typically this will be heads of departments or divisions. Senior managers will often have high-level responsibility in ensuring their department is working to fulfil the organisation's business objectives. The key for you is to ensure information security is on their radar, that when they are overseeing the implementation of their objectives that they consider security. If you don't have buy-in from the top, you will find it difficult to prioritise security within the various IT teams.

Explain to them the CIA mantra so that they understand what each of the three points mean, and it will help if you apply CIA to a specific area. They will then be able to conceptualise security at a high level.

Senior managers are important when trying to change the culture of the organisation and the way it works. Unfortunately people are often resistant to change, but by ensuring senior management buy-in you will have high-level backing to get things done when you encounter resistance.

Business Analysts

Building strong working relationships with business analysts will provide a great insight into the views of the wider organisation. They spend most of their time understanding the business and its needs and then translating this into requirements for IT systems. By understanding their findings you can implement more effective security controls. For example, you implement a new password policy that means passwords now have to be at least 15 characters long. People in the organisation have trouble remembering their passwords so they begin writing them down and attaching them to a sticky note under their keyboards. This security control would actually increase the risk to the organisation of a security breach rather than reduce it. However, as the person responsible for security, people are unlikely to volunteer that they are willingly breaking this rule, so this is where your relationship with business analysts is important. By understanding their work you can better understand the security culture of the organisation and improve it over time, as well as ensuring they factor in security concerns.

Senior Information Risk Owner

The senior information risk owner (SIRO) is a role that you may have not come across before. It is often found in UK government. The SIRO is typically a Board member who has overall responsibility for ensuring effective information security and that it remains a priority on the organisation's agenda. If you are fortunate to work in an organisation that values information security then it may be worth suggesting this role to the Board.

Although the SIRO will champion information security at Board and strategic levels, it is unlikely they will have any in-depth knowledge of information security. Ensure the SIRO understands CIA so that you can develop a common understanding. The SIRO will be key in changing the organisation's security culture as they can raise your concerns at the highest possible level. The SIRO will often come to you with their concerns and rely on you to understand and explain the wider impact on the organisation.

Lawyers

The lawyers or legal team are often forgotten about, but they can be as much of an asset as an enemy. They have great power within an organisation as it is their job to ensure the organisation remains compliant with the law. Ensuring compliance with various laws can be a minefield, hence the need for a legal team. If you are fortunate enough to have a legal team within your organisation, I recommend you meet them as soon as possible. It is useful to build a relationship based on mutual respect: security professionals often have a high-level understanding of the various IT-related laws but it is the lawyers who interpret the law to its fullest. Use the legal team as a resource for advice and also an escalation point when you have legal concerns. As part of this relationship the legal department should ensure it keeps you informed of any proposed new legislation. By having early sight of legal changes you can make sure any security considerations are made early and that the organisation is prepared.

Key IT Personnel

The next step in acclimatising to your new role is to meet the IT staff you will be working with on a more regular basis. Your organisation likely has slightly different roles based on its size, but I would expect the following roles to be covered even if you have people covering several roles.

In this section I will introduce the different roles and their importance. This is also a two-way relationship. If you can build a rapport with these people then they will keep you in the loop with the work going on in the IT department. This is much more important than you think, since when an organisation’s security resource is limited you won’t be able to be as involved with all aspects of the department as you would like. This can often be troublesome as teams go about their business without considering security and its requirements. By meeting these people and teaching them the CIA mantra you will give them the tools to realise when there is a need for security and encourage them to approach you when you might not have been involved with the work.

Change Management Team

Who

How organisations manage change and deploy IT systems varies widely. Some organisations and small silo teams take care of their changes, whereas others have one overall change-management team with responsibility for all changes. Either way this team or teams have responsibility for determining what and when IT changes and deployments happen.

What they do

Deploying or changing IT systems is rarely a simple task. Who the change affects, what other systems the change will affect, what to do if it all goes horribly wrong and when to implement the change all need to be considered. The change-management team takes the lead on informing the people who the change will affect and if needed provides advice and guidance on the new system. They are also aware of other systems that it affects; for example, if we were upgrading our email system, any IT systems that send email would be affected, not just the users. Also, if we allowed everyone to change systems whenever they wanted, we'd have chaos and probably a broken IT infrastructure. By grouping and scheduling changes we can make small changes to IT systems over time, which also means that if a change breaks a system then we can quickly identify the change and fix it.

Why they are important

The change-management team are the final step in any change-management process. They should keep a record of changes that have been and will be implemented. By understanding their change schedule you can ensure no changes that could introduce weaknesses into IT systems are implemented. I recommend you insist on becoming part of the approval process for changes. By this stage you should be aware of any changes, but this final step will be a catch all for anything that has slipped past.

Network Team

Who

The network team is an obvious one for most people, as this is the team responsible for managing the network. They have a better understanding of the network and the infrastructure it connects than most in the organisation.

What they do

The network team have more responsibility than just the day to day running of the network. They often have the following responsibilities as well: firewall set-up and monitoring, intrusion detection/prevention system (IDS and IPS) and overseeing the efficient running of the network. Monitoring of the IDS and IPS is extremely involved, and because of their understanding of the network the team are best placed to understand the result of this monitoring system. As useful as these systems are, without constant tweaks they flag up a lot of false positives and will not be configured to recognise the latest threats.

Why they are important

Your relationship with the network team will centre around three key areas. Firewall maintenance, in particular rule changes, IDS/IPS changes to ensure they are up to date, and finally any network changes.

When firewalls are installed effort goes into configuring the rules to ensure maximum protection, but over time these rules can be weakened as new systems are implemented. Often the network team are aware of the potential for introducing weaknesses into the network by changing firewall rules, but they may come under pressure from other teams. By forging a strong relationship you can ensure that weaknesses aren’t introduced and that more secure solutions are found instead.

IDS and IPS changes will be more of a hands-off role for yourself, as it is likely you will not have the deep technical understanding that the networks team have. Where you can help the networks team is by keeping an eye on trends within security and ensuring they are aware of the latest attacks, as well as which attacks are being most commonly used. This will help the team tweak the IDS/IPS rules and interpret the log records.

Finally we come to network changes. If the network has been implemented correctly, it will be segregated into different security and function zones; this ensures any compromise doesn't affect the entire network but only a small segment. As with the firewall rules this segmentation is well thought out initially but in time segments may become bridged, or even worse segments that should never have any connection have connections introduced. By working with the networks team you can ensure these segments and good network security practice remain in place.

IT Services Team(s)

Who

This team likely has a different name in your organisation. They are responsible for maintaining the different services and systems within your organisation, for example, email, shared drives, office applications and your general desktop infrastructure. Typically these teams focus on getting new systems implemented and working and often security can be an afterthought.

What they do

Their responsibilities vary greatly depending on the organisation. However, they are responsible for the installation, maintenance and general day to day running of the organisation's IT systems. One key aspect of this role is the application of security patches: by keeping systems up to date most known vulnerabilities can be mitigated, and patching is a basic housekeeping task that can have a big effect on how secure an organisation is.

Why they are important

You can assist the team by ensuring security patching remains high on their agenda. I recommend procuring a patch-monitoring service so that you are always aware of the latest security patches for your systems; it is easy to overlook or forget a patch when working in a high-pressure environment. The other way you can assist is by confirming the change-management schedule in time for them to apply security patches.

Finally, when the team is considering implementing a new IT system you need to make sure security requirements are taken into account. This can include whether the new system meets industry best practice, checking historical vulnerabilities found in the system to determine how secure it is, and how much maintenance is likely to be involved in the running of the system. I also recommend all new systems once fully configured and in place undergo a full penetration test.

IT Help Desk Team

Who

The IT help desk or service desk are the first line of support for your IT users. It is their job to log user IT issues as incidents and then provide advice or forward the incident on to the relevant expert. Sometimes this function is outsourced, so getting to know this team on a more personal issue may prove difficult.

What they do

The help desk are the first point of call for IT users and sometimes customers. They log calls and provide advice where possible, usually trying to fix the caller's issues immediately providing a first-time fix. Where this isn't possible they create a problem record and inform the relevant team. As the help desk is the first line of support, they are aware of any issues first. The help desk should be made aware of any current IT issues so that when they receive calls they can advise and appear to be up to date with the situation. They collate metrics and show patterns in incidents being raised, which is important during a security incident.

Why they are important

As a security professional the help desk is often a bridge between the IT user and customer security incidents and the organisation. For example, if a spam attack is underway using your organisation's email domain, you are unlikely to be aware of it until complaints are logged. Another example is malware spreading through your infrastructure with IT users raising the issue with the help desk. It is important that you remain in the loop with the help desk and are an escalation route for them when a security incident(s) is raised.

You can also be proactive in this area. If you are made aware of a security incident early, you can inform the help desk so they can offer advice to callers. A proactive approach reduces the impact of reputational damage due to a security incident as the organisation appears to be in control of the incident.

Architects/Designers

Who

Architects and designers are responsible for the overall IT strategy of the organisation and provide direction to the organisation. IT architecture is a multidisciplinary function and architects specialise in specific areas such as software, infrastructure and data to name a few.

What they do

Some may argue the difference between architects and designers, but for the purposes of this book I consider them both responsible for the high-level decisions regarding what and how IT systems are implemented and how they should function. They have a long-term view of the organisation's IT strategy and how it will be implemented, and produce the designs for their respective systems.

Why they are important

By influencing the architects early on in the designs you can ensure security is included from the start. Building the architects' understanding of the CIA mantra means they are well placed to ensure security considerations are raised early in the design process. Also, given the architects' technical knowledge they can provide options on how a security issue can be managed; you can help the architect by exploring the benefits of these options and even provide further design options if needed. If you fail to build a good relationship with the architects, you may find that security is often a contentious issue with those responsible for implementing the systems. Security can be quickly seen as a blocker rather than an enabler, which becomes a real issue when people exclude you from design discussions as they believe you will block their decisions rather than help them develop their design.

Software Development Team

Who

The software development team code and develop IT systems, which includes websites and databases. They are among the most technical staff and have some of the deepest understanding of systems. Unfortunately this introverted view often means they fail to consider other issues and systems.

What they do

The software development team is responsible for the low-level design and creation of software code. They work to specific development methodologies; two of the most common being Rational Unified Process (RUP) and Agile. RUP works by developing over a number of predefined cycles planning in changes in an iterative process. Agile is more user centric and focuses on their needs, delivering functionality that can be demonstrated in each user cycle.

Why they are important

A good relationship ensures newly developed systems are secure and that existing systems are maintained.

As we mentioned with the architects it is important that security is included from the start rather than added at the end. Often the software development team focuses on writing code that works rather than the security of that code. Introducing secure coding standards can reduce the number of vulnerabilities and weaknesses in your software. However, sometimes it can be difficult to demonstrate the value of secure coding. I recommend introducing Open Web Application Security Project (OWASP), in particular the OWASP top ten vulnerabilities found in web applications. OWASP explains how these vulnerabilities work and provides guidance on how they can be fixed. The more technical the person, the better it is to demonstrate what you are trying to explain. Showing the developers how some of these vulnerabilities can be exploited will engage them as they will have an appreciation for how the exploits work.

Maintaining systems, especially legacy systems, can be difficult as often they are not as well documented as they ought to be. The software developers have the best understanding of these systems as they were probably the ones who developed them. It can save time knowing who built a system and therefore who can answer your question. This is important if potential security issues are raised and your in-house developed software needs to be patched and fixed.

Incident Management Team

Who

The incident management team manage and coordinate any IT incidents that require immediate action. An example could be the loss of the organisation's email system as the impact is likely to be widespread and great for the business. It is also likely the business will put great pressure on IT to get the issues resolved. It is unlikely you will have a dedicated incident management team (unless IT incidents are commonplace...); instead the team will be brought together and made up of a multidisciplinary group from within the organisation. As a security professional you should be part of this group.

What they do

The incident management team convenes whenever there is a major IT incident that requires management. They typically manage the incident from discovery through to resolution and often look at lessons learned afterwards. They ensure the right people are involved and decide what needs to be done to fix the issue and then coordinate the fix. They also provide constant updates to the business to assure them the incident is being managed properly, and part of this includes an estimated fix time.

Why they are important

It is important that security is represented at incident management meetings, at least initially. The incident may not first appear to be a security issue but until this is confirmed you should be involved. If you have a security risk log, it is important during the management of the incident that you see if the security incident was a potential risk that was previously raised. If it was then the incident could be used as motivation to implement a long-term fix. If the incident was unexpected then the organisation may need to revise its threat landscape and consider the security risks to it.

What is the Security Culture?

Now that you have met the key players from the business and IT, you should have a feeling for the security culture.

To help you decide what the culture is like I have noted three key areas that you should consider:

Priority – What is the organisation's priority when considering security? Is it something they think about at the start or do they assess security at the end? When you had your discussions with the business what was their balance of security vs business opportunity? If security has a higher priority then your job should be straightforward. However, if the organisation puts business opportunity first then you must make a strong argument for any security controls you wish to implement. You also need to be careful that you don't come across as someone who is trying to stifle the business through excessive control; remember you are there to facilitate business opportunity.

Attitude – When you were meeting the organisation staff members, what was their attitude? Did they give you plenty of time and listen to what you had to say or were your meetings rushed? I have had people fail to attend arranged meetings, which defines their attitude towards security. Understanding their attitude means you know what level of engagement you are likely to get. When engaging with those who have a poor attitude towards security you may need to ensure you have senior management backing, which should encourage them to be more receptive.

Power – How much power does the security team have? Can the security team veto deployment of new systems if they believe the risks are too high? Does the security team have such little influence that they could shout as loudly as they wanted and no one would listen? If it's the latter then you really have your work cut out. You will probably need to find other ways to reinforce your proposals and arguments. If this doesn't help then perhaps your services will be best used elsewhere...

Identifying the Gaps in Security

Now that we have spent time getting to know the organisation and understanding the culture we need to understand any gaps in security. As you should know, security isn't just about perimeter firewalls but also about process and management. In this section I discuss some of the best ways to understand the gaps in security and how to address them, assuming the organisation has the appetite to do so.

What accreditations does the organisation have?

The fastest way to identify gaps in security is to look at any accreditations the organisation might have. Typically accreditations have a scope. What does this scope include? Is the scope organisation wide or does it cover a standalone server hidden in a room somewhere? Many accreditations are regularly audited by an independent organisation, so read the audit reports and understand the findings. Often an organisation will do its utmost to paint a glossy picture of how it complies with an accreditation; if the auditor identifies any areas of concern, these areas should be of concern to you.

Even if an audit for an accreditation isn't due, it may be worth employing a consultant to carry out a pre-accreditation assessment. Explain that your accreditation isn't at risk of being lost based on the assessment and that you are using it to find areas of weakness. Encourage those involved to be open and honest and that it is much better to identify issues now rather than later.

What is the business appetite for accreditations?

The appetite for accreditation varies from organisation to organisation. Broadly speaking it fits into three categories.

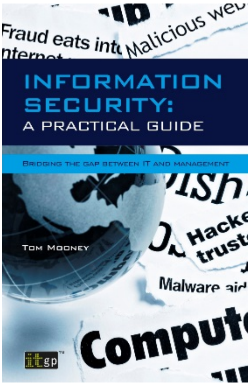
No appetite – The organisation sees little to no value in achieving an accreditation. This can be the most frustrating stance as often achieving accreditation not only proves the organisation is working effectively but can also raise morale as the good work of staff is acknowledged and is meeting a baseline standard.

Appetite for the badge only – The organisation wants the badge that comes with the accreditation but doesn't actually see the value of working to the standard the accreditation defines. A good example of this is ISO27001, which defines the need for various polices. An organisation taking this stance has the required policies but the quality of those policies is questionable; in essence the policy exists to tick a box rather than promote good working practice.

There is appetite for the accreditation as the business see the value and understand the advantages that the accreditation can offer. If the organisation believes itself to follow industry best practices then often it will want these to be recognised as this can prove the quality of service they offer. If your business operates in a particularly competitive market then this could provide an edge over competitors. The other benefit to this is that where an assessment to achieve an accreditation is undertaken any gaps it identifies are likely to be resolved so that the organisation is successful in its assessment.

<<< END OF EXTRACT >>>

Information Security: A Practical Guide



Provides an overview of basic information security practices that will enable your security team to better engage with their peers to address the threats facing the organisation as a whole.

“One of the most impressive……This book is well worth an hour of your time, whether as a refresher, or if you are finding yourself facing more work on the info-security side. Recommended.”
Mark Rowe, Editor at Professional Security Magazine

Buy your copy today

www.itgovernance.co.uk/shop/p-1701-information-security-a-practical-guide-bridging-the-gap-between-it-and-management.aspx

www.itgovernanceusa.com/shop/p-1472-information-security-a-practical-guide-bridging-the-gap-between-it-and-management.aspx

www.itgovernance.eu/p-1126-information-security-a-practical-guide-bridging-the-gap-between-it-and-management.aspx