Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Successfully Building Security into Business Projects

Copyright SANS Institute
Author Retains Full Rights

AD

© SANS Institute 2008, Author retains full rights.

Successfully Building Security into Business Projects

GSEC Gold Certification

Author: Alex Clayton, sans@alexanderclayton.co.uk

Adviser: Richard Genova

Accepted: July 2008

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

1 Abstract 4

2 What is the problem? 5

3 Things to say – using soft skills 6

3.1 Influence 8

3.2 Be "known" 13

3.3 Educate 13

3.4 Consider language, terminology and context 15

4 Things to know – be prepared! 17

4.1 Security best practices 17

4.2 Standards 17

4.3 Money makes the world go round 18

4.4 War stories 19

4.5 Understand wider project process 20

5 Things to do 22

5.1 Secure buy in from management 22

5.2 Create alliances with other parts of the business 23

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

5.3 Establish a formal security process for projects 23

5.4 Integrate security process into project process 24

5.5 Use Risk Assessments and security plans 25

5.5.1 Definition of risk 25

5.5.2 Risk assessment techniques 25

5.5.3 Security plans 29

6 Top 10 tips for successfully building security into business projects 31

7 Conclusion 33

8 References 34

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

1 Abstract

Security is only one of a range of considerations that a project manager needs to deal with when delivering a project to the business. What tools and skills does a security professional need to ensure that security is built into the deliverables in a timely and effective manner? To answer this question this paper identifies important soft skills, key knowledge, and good practices, e.g. security risk assessment, that when combined are a convincing argument to persuade project managers to bake security into their projects.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

2 What is the problem?

All too often security is a last minute consideration when delivering projects. On the one hand this is understandable from the view of a project manager. He is juggling timescales, budget and usually a changing list of things to deliver. The last thing he wants is the project to be complicated or changed due to additional security controls.

From the perspective of a security professional this is bad. Either a project goes live with poor security or it is delayed to incorporate additional security controls or even reworking of previously tested and approved functionality. In either case, the security professional is not seen in a good light.

This perspective is shared by many of my fellow security professionals and a recent online article by Mathias Thurman:

Never mind that the real cause of the delay is the failure of project managers to give security a thought until just before they plan to roll out the new application to users. It's the security manager who says, "No, this can't be used in our environment without a security assessment." It's the security manager who seems to have no compunction about negating months of hard work with orders for reworks that mitigate the security problems.

Add to this the cost of reworking project deliverables to incorporate additional security

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

controls and this cyclical occurrence is unpleasant. This paper will provide security professionals with a set of tools and advice to break this cycle and get security incorporated into projects at the beginning of the process and not the end. This will save money for the business and raise a more positive reputation for the security professional.

3 Things to say – using soft skills

Security professionals are human beings who work with other human beings to get their job done. Human nature is not simple and not logical. This sentiment is summed up by two famous people's comments on the subject:

Albert Einstein, "Two things are infinite: the universe and human stupidity; and I'm not sure about the universe."

Anatole France, French Writer, member of the French Academy and Nobel Prize for Literature in 1921, 1844-1924 "It is human nature to think wisely and act foolishly."

Therefore, it is important that security professionals understand how to deal with people and not treat them as logical and predictable robots. This section details some of the softer, more human, skills that will aid security professionals in getting alongside their colleagues and ultimately persuading them to the security cause. These skills are not security specific and could be utilised by anyone who needs to influence those around them.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

To help contextualise this from a security perspective, I would like to introduce the fictional Bruce Stapleton, a security manager for a mid-sized finance company in the UK called Winalittle Ltd. Bruce is 45, married with 3 challenging teenage children and rarely has time to sit and read his favourite magazine, “Security for You”. He is stressed at work. Every day seems like a battle. He is either on the offensive telling project managers that they can’t deploy their insecure solutions or on the defensive when he is dragged into project board meetings to explain why he has caused project delays due to “unnecessary” security controls.

Bruce is an intelligent chap with a degree in electronic engineering and has completed all the industry standard qualifications for security, e.g. CISSP (https://www.isc2.org/cgi-bin/index.cgi). He knows that security is important and does not want to be responsible for security breaches in his company. However, his personal skills are not quite so well qualified. He is not considered a team player and rarely lunches with his colleagues. Due to the constant barrage of problems he has become quite bitter and short when discussing problems with people in his department. He finds it hard to communicate difficult technical and security concepts and does not seem to be perturbed when projects are halted due to his last minute insistence that the deliverables are insecure. He is not liked by his fellow professionals and consequently they do not come to him for advice about security issues they are facing.

What can Bruce do to improve his work situation, become less stressful and provide a better security service to the company? It wouldn’t hurt Bruce to begin with a positive attitude

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

as confirmed by George Bernard Shaw:

"People are always blaming circumstances for what they are. I don't believe in circumstances. The people who get on in this world are the people who get up and look for the circumstances they want, and if they can't find them, they make them" (as cited in Gilbert, 2005, p.132).

It is important to say at this point that the material in this section does not take in to consideration all the cultural variations on how to effectively manage people. The material is largely geared towards Western cultures and, in particular, the United States and the United Kingdom. However, most of the principles should be applicable to most international engagements.

3.1 Influence

There are a myriad of books and electronic media in print that detail the techniques of how to handle humans and situations. I have relied heavily on the famous "How to win friends and influence people" by Dale Carnegie that details a set of principles by which any person can secure popularity, have influence and enjoy life. I have taken a few gems from this book to highlight how Bruce can persuade others to his cause.

Negotiate. Rather than being draconian and absolute in his insistence about deploying security controls, Bruce needs to understand that "security is a trade-off", (Schneier, 2008)

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

and must be considered within the context of business risk, operational considerations and cost.

The ability to negotiate with other parties, e.g. project managers, goes a long way to getting suitable security into projects as well as allowing other parties to get what they want as confirmed by Carnegie (1981),"Each party should gain from the negotiation"(p.46).

Negotiation is a technique used to positive effect by politicians, business leaders and family members and the best ones have learned, supported by Gilbert (2005), that "It's not the cards you are dealt, but how you play your hand"(p.112).

Be Pragmatic. According to Wikipedia (2008), "pragmatism refers to behaviour which temporarily sets aside one ideal to pursue a lesser, more achievable ideal." In other words this is a practical approach to problems. In the security world this means understanding that sometimes, for example, people are willing to take security risks for the benefit of business functionality or advantage.

As an example, company A is rolling out Service Pack 2 for Windows XP on all of their laptops and desktops. It is a significant piece of work, requiring a project framework, project manager and a team of 30 people to roll this out across the global network. The project team approached the security team to see if they could roll this out without DEP

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(http://support.microsoft.com/kb/889741) – a useful tool to stop buffer overflows. Now, the security team knew that the timeline of this project was compressed due to business pressure and the project team were nervous about DEP as they had heard that it caused problems with their Citrix clients. What did the security team do? They allowed the rollout without DEP understanding that they already have a few layers of defence against buffer overflows and understanding the context of the rollout, i.e. deploying a solution that caused all Citrix client sessions to fail would be a catastrophe. The project team got what they wanted and the security team were highlighted as being co-operative and helpful by senior management. In other words the security team had gained some popularity points and, more importantly, a few chips to bring to the next negotiating table.

It would benefit Bruce to sometimes concede some security controls to help the business achieve their objectives with a clear understanding that he has bought himself an advantage the next time security need to insist on a security control.

Avoid arguments. According to Carnegie (1981), "I have come to the conclusion that there is only one way under high heaven to get the best out of an argument – and that is to avoid it" (p.116). On the one hand it would seem logical that Bruce needs to argue the security case in a direct manner. Who else is defending the security corner? However, history tells us that those who achieved the most influence and impact did not go head strong into

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

argumentative debate to get their way. This is supported by Carnegie (1981),"Nine times out of ten, an argument ends with each of the contestants more firmly convinced than ever that he is absolutely right"(p.117).

Don't say "You are wrong". Robinson states "if we are told we are wrong, we resent the imputation and harden our hearts" (as cited in Carnegie, 1981, p.126). This is further supported by the same author:

I am convinced now that nothing good is accomplished and a lot of damage can be done if you tell a person straight out that he or she is wrong. You only succeed in stripping that person of self dignity and making yourself an unwelcome part of any discussion.

Bruce, instead of being argumentative and direct, could adopt a more conciliatory position, cease putting peoples backs up and gain some co-operation from his colleagues.

See things from the other persons view. Bruce is often forced to derail project timelines due to finding security problems close to the live date. He is frustrated that he has not been involved in the project at the initial design stage. His responses are usually direct and lack any consideration for the other objectives of a project and the people therein. An alternative approach would be for Bruce to understand the wider context of what the project is delivering and other pressures on the project to deliver it on time and to budget. Instead of saying "This

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

project is delivering insecure products and should be stopped from going live" he could say "I understand that this project is really important to the department and the business and know that there have been many problems with our third party supplier. Unfortunately, I have identified a security issue which needs to be looked at as it is my responsibility to make sure that our systems are secure. I will do my best to make sure that I keep the disruption to a minimum. It would be helpful to me and the rest of the department if security was considered earlier in the project progress to avoid situations like this."

Carnegie supports this position:

Stop a minute to contrast your keen interest in your own affairs with your mild concern about everything else. Realise then, that everyone else in the world feels exactly the same way!

Bruce could use this piece of advice from Dr Gerald S. Nirenberg to his advantage:

Starting your conversation by giving the other person the purpose or direction of your conversation, governing what you say by what you would want to hear if you were the listener, and accepting his or her viewpoint will encourage the listener to have an open mind to your ideas (as cited in Carnegie, 1981, p.171).

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

3.2 Be "known"

A popular, friendly person is more likely to persuade people to their point of view than someone who has a negative and grumpy demeanour. The famous American President Abraham Lincoln is known to have said:

It is an old and true maxim that 'a drop of honey catches more flies than a gallon of gall.' So with men, if you would win a man to your cause, first convince him you are his sincere friend (as cited in Carnegie, 1981, p.145).

It follows that in order to gain these friendly alliances Bruce needs to be more involved with the department. Perhaps he could attend the weekly chess club and get to know, Mira Stoppard, the AJAX programmer a bit better. This may smooth over some of the clashes they have been having recently over the security policy for application code. Perhaps Bruce could be on the organising committee for the company Christmas party. He would be engaging with people in his department outside of the remit of security and this would build stronger links with his fellow colleagues.

3.3 Educate

Bruce's job would be easier if his fellow professionals already knew how to implement good security rather than Bruce causing project delays by insisting that project deliverables are re-worked.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The best way to do this is to educate people in the ways of security best practice. Bruce could use all three of the following suggestions to get a better level of security understanding and sympathy across the business.

Security is an enabler. Security technologies provide businesses with huge opportunities for flexibility and cost savings which would otherwise not be possible. Remote working using VPN and other encrypted communication tunnels across the Internet have given rise to a more agile work force. The online shopping industry owes its existence to technologies such as SSL which provides secure communications when customers are supplying their credit card details whilst purchasing goods. Emphasising these facts can change the perception that security solutions are always a blocker.

Business wide security awareness campaigns. If end users are aware of good security practice then they will ensure that security is built into their business requirements, e.g. we want a system for our customers so that they can see their orders but we must ensure that their data is kept confidential. After all, the IT department is there to deliver what the business wants.

Bruce could have some fun here as well as raising his own and security's profile within the business. He could perhaps run a campaign for "hunt the hardware keylogger and win a bottle of champagne". He could utilise the company intranet "message of the day" facility to

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

send some important security tips. Perhaps he could run a set of workshops where he educates users in how to secure their home PCs and wireless network at the same time as sending out some key messages for responsible working within the business.

Inform project process about how security works. It is important that project managers know how the security process works within a project. A security professional needs to explain that, for example, a security risk assessment is conducted against the draft technical design from which a security plan is established. The plan contains the security controls required for the project. If the project manager is aware of this he can incorporate this time and resource into his plan which then leads to an increased chance the project can be delivered on time and budget.

3.4 Consider language, terminology and context

Bruce finds it frustrating that people do not understand him when he explains security issues and what needs to be done about them. He uses the same language and terminology whether he is in a security forum with other security professionals, project meetings or talking to non-technical business people.

A good communicator is one who is able to gauge the audience and shape their ideas, thoughts and words in such a way so that the recipient clearly understands what is being said.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The concept of risk is a common thread through the work of security professional. Many businesses are also au fait with risk management and this is a really useful term to use when discussions cross the boundary of IT and business.

For example, a project is looking to deliver an online solution for the marketing department. Bruce has spotted that the username and password is hard coded into the database connection string (hidden from the public) that connects the web servers to the back end database server. This does not comply with the agreed security policy on credential management. At the go live meeting, Bruce could relay his concerns to the project team (composed of both technical and non-technical people) in terms of risk. He could explain that the system will go live with a medium risk and ensure that the project team understand and, if they decide to go ahead, accept the risk. This is a better scenario than Bruce insisting that the project can't go ahead as the solution is insecure.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

4 Things to know – be prepared!

When Bruce is negotiating and working with his colleagues on projects he needs to be able to present information to the decision makers about the reasons why certain security controls should be deployed within a certain project. This section outlines some of these.

4.1 Security best practices

The security industry is becoming more mature as it attempts to provide protection against organised crime and other computer based criminal and malicious activity. One way of doing this is to agree a way of working that is seen to be best practice that others can follow. The knock on effect is a more co-ordinated posture that reduces the risk of bad things happening.

Bruce needs to know these best practices and adopt them within the department. Which senior manager or project manager would blatantly disagree with incorporating a security control which is seen as the best solution in the eyes of everybody in the security industry?

4.2 Standards

Using a collection of internal and external security standards will help Bruce demonstrate that defined security controls for a project are in line with previously agreed

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

standards that have been ratified by senior management.

Again, this is a powerful tool when negotiating security into projects. Specifying security controls for a project that are documented within approved and ratified standards provides a level of consistency and removes any need for arguments or personality clashes. The security controls are in a previously agreed document and not just made up.

One such industry standard is ISO/IEC 27001 and forms part of the BS ISO/IEC 17799:2005 standard (formally BS7799), commonly known as ISO 27002. This is an internationally recognised standard relating to Information Security Management. The standard provides a framework by which an organisation may establish an Information Security Management System (ISMS) to ensure the ongoing security of information and to ensure best practice controls are implemented.

4.3 Money makes the world go round

The nature of commercial activity is that it all comes down to money. The importance of money is confirmed by this famous quip by Oscar Wilde, “When I was young I used to think that money was the most important thing in life. Now that I am old, I know it is.”

The decisions that management make are usually focussed on the bottom line. What is our margin on the sale of this product line? Can we save money if we outsource these

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

processes offshore? What is the cost benefit for moving the office to another location?

In terms of security, Bruce needs to be aware of the context in which he operates. He could use cost as an argument to get security built into the project process at the design stage rather than a last minute consideration. It is inevitable that security catered for within the original design is always cheaper than having to re-work project deliverables at the last minute. All the resources required to change documentation, re-code applications and re-test solutions are all expensive and avoidable activities. This is supported by Ellison (2006) when he says that, “reengineering a system to incorporate security is a time consuming and expensive alternative.”

Showing management that this is the case is a strong argument which many decision makers would find hard to ignore.

4.4 War stories

A useful tactic in convincing project managers, management and the board members about the need to take security seriously is to share war stories.

These war stories need to be a clear, relevant example of what could go wrong if security is not built into the systems.

For example, as Bruce is part of a UK finance company, regulated by the Financial

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Services Authority (http://www.fsa.gov.uk) he could describe how much money and reputation has been lost by a similar company because they had a data breach or even just because they had poor security controls (http://www.theregister.co.uk/2008/06/19/fsa_fines_msgl/).

It is very likely that Bruce will get support from the decision makers to take security more seriously. This in turn will make sure that project managers cater for security in their projects.

There is no shortage of IT security blunders that Bruce could cite. For example, he could talk about TJX who were in breach of the PCI (https://www.pcisecuritystandards.org/index.htm) standards and were subsequently fined 40.9 million dollars (http://news.zdnet.co.uk/security/0,1000000189,39291249,00.htm).

4.5 Understand wider project process

As mentioned in the abstract, a project manager has to plan and deliver suitable products that adhere to the functional and non-functional requirements, of which security is only one. It would benefit Bruce if he understood the entire project process so that he can help the project and be a team player.

Technical professionals are usually very busy people who are juggling lots of project and operational balls. It may be that a project manager has forgotten to schedule a

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

penetration test in the testing phase. If Bruce is aware of the current projects and their statuses he could prompt the project manager to include the test in the testing plan. This is a 'win win' situation. Bruce gets his security test (with plenty of time for any required remedial action) and the project manager delivers his project on time.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

5 Things to do

5.1 Secure buy in from management

It is absolutely critical for Bruce to ensure that management, i.e. the decision makers, agree that security is a vital part of delivering successful IT. Without this support, Bruce will have a huge uphill struggle in convincing others in the company that security should be taken seriously.

Fortunately, many of the recommendations in this paper can also be applied to senior management to show them that they ignore security at their peril. For example, Bruce could demonstrate that other leading IT departments are using security industry standards to determine their security measures.

The more convincing arguments are those associated with money. Therefore, Bruce could describe some real life examples of how much money a company lost when they lost customer data or, more tangibly, could present accurate figures showing how much money could be saved if security was built into the beginning of the project process rather than re-working project deliverables at the last minute.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

5.2 Create alliances with other parts of the business

The IT department is usually only one part of the professional services within a company. Commonly, there are roles that cover, for example, compliance, legal or audit. These functions are the “brothers in arms” of the security professional. They are working to a similar end and a close and productive working relationship with these areas will give weight to an argument to deploy security measures into projects.

For example, a UK financial institution is required to adhere to FSA regulations. The compliance team within the UK company ensures that it adheres to the rules and regulations issued by the FSA. This is largely to do with the identification, protection and security of information. Using our example, Bruce can insist that security controls are put in place to comply with regulatory requirements. No project manager willingly wants to jeopardise the company’s reputation by ignoring these controls.

In a similar way, an internal audit team compares how a company operates against industry best practices and regulatory requirements and monitors its compliance against them. Again, Bruce can use these recommendations as mandatory requirements for appropriate security controls in projects.

5.3 Establish a formal security process for projects

This security process typically involves a risk assessment of what is to be delivered

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

with an associated security plan that details what security controls are required to ensure that the project products are fit for purpose. The composition of this process needs to fit into the structure and culture of the business. For some, a thorough and detailed process is required that is accompanied by significant documentation whereas other companies would be comfortable with a lighter model. Section 5.5 takes a look at a few techniques currently used in the security industry.

For Bruce, this is really helpful as he has a method which is repeatable. This means that his workload is reduced. Another benefit is that the method of defining security controls for projects is consistent. This also means that project managers can anticipate the amount of time and resource required for a security assessment and plan. Further to this, Bruce will be lining himself up against industry best practice. This is confirmed by the control specified in the international security standard ISO27001 (2005), “A management authorisation process for new information processing facilities shall be defined and implemented” (p.14).

5.4 Integrate security process into project process

It is vital that once a formal security process is established it is then incorporated into the project process. More specifically, the security function is consulted for approval at various checkpoints within the project. The most significant gate is obviously the go live date and it is essential that the project requires security sign off before it can be commissioned.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

5.5 Use Risk Assessments and security plans

This section details some risk assessment techniques including those used commonly by industry and an example of a business specific method.

5.5.1 Definition of risk

According to the industry standard project management technique, PRINCE2, “risk can be defined as uncertainty of outcome” (p.251). In terms of security there is a classic definition for risk which is supported Cole:

The classic definition of risk is ‘risk = threat * vulnerability’. Vulnerability is defined as a weakness in a system that could be exploited...A threat is any event that can cause an undesirable outcome.

The management of risk is the cornerstone of managing security within a business.

5.5.2 Risk assessment techniques

Security risk assessment tools such as CRAMM (http://www.cramm.com) and OCTAVE (http://www.cert.org/octave) provide a thorough risk based strategic assessment and planning technique for security. These are commonly used by Government departments and large organisations and require significant effort to complete. The U.S. Department for Homeland Security promotes the Trustworthy Computing Security Development Lifecycle

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/project/38-BSI.html)

The SANS 401.3 section on IT Risk Management details a set of risk management steps that culminate in a business case for management to use to make informed decisions. This process is summarised by Schneier (2000):

It's not enough to simply list a bunch of threats, you need to know how much to worry about each of them. This is where risk assessment comes in. The basic idea is to take all the threats, estimate the expected loss per incident and the expected number of incidents per year, and then calculate the annual loss expectancy (ALE) (p.301).

The steps are as follows:

1. Threat assessment and analysis. This step is to identify what bad things could happen and how they could occur within the business.

2. Asset Identification and Valuation. All businesses are limited by the amount they can spend on security. This step will give good visibility of the priority with which defences are deployed.

3. Vulnerability Analysis. It is all very well identifying what could happen but equally important is the evaluation of how susceptible systems are to these threats.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

4. Risk Evaluation. This step is effectively multiplying steps 1, 2 and 3 together (threat * vulnerability * asset value) to provide an overall level of risk for each issue identified.

5. Report. The final deliverable is a document that provides the detail of steps 1-4 but also includes recommendations on what management should do.

An example of a tailored risk management tool is one that I have used in a company that was reasonably lightweight but worked really well within the project process and addressing other wider security issues.

The process is divided into 2 sections; risk assessment and security plan. The risk assessment identifies risks giving them a value of 0-3 for threat, vulnerability and asset value. These risks are grouped by their impact on confidentiality, integrity and availability of data and systems. The higher the value, the higher the risk. The next page shows an extract from a risk assessment document that tables the risks identified.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

5 Risk Assessment

The integrity and confidentiality of information within this project is paramount. However, the availability of the information would become critical in the event of this service being operational.

Integrity					
Risk ID	Description	Threat	Vulner ability	Asset value	Risk Score
1	Data corruption in transit (over the internet) and at rest (disk corruption)	2	3	3	18
2	Synchronisation does not function correctly and data is corrupted in either location	2	3	2	12
3	Malicious code gets into mailboxes at XXXXXXX, e.g. when user logs on through webmail solution on an infected PC during evocation	3	2	2	12
4	Mis-configuration of XXXXXXX, XXXXXXX or XXXXXXX equipment leads to data being corrupted	1	2	3	6
Confidentiality					
Risk ID	Description	Threat	Vulner ability	Asset value	Risk Score
5	Data in transit is intercepted either over the Internet or across XXXXXXX network	3	2	3	18
6	Domain passwords (used for accessing the web mail application) are compromised when stored at XXXXXXX or in transit	2	3	3	18
7	Hacker gains access to mailboxes via the web mail browser	3	3	2	18
8	Data stored at XXXXXXX is accessed by unauthorised users	1	3	3	9
9	A device within XXXXXXX could act as a Man-in-the-Middle and intercept XXXXXXX data	1	1	3	3
Availability					

With this information a suitable security plan that details the controls for the project can be defined.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

5.5.3 Security plans

A security plan is a list of the controls that are required for a project. Continuing from the previous section, the risk assessment determines the priority and level of security required for the solution. The table on the next page is an example of the controls required for the risk assessment detailed above.

The controls are divided into logical sections, i.e. those controls that are administrative, e.g. policy, technical, e.g. firewalls and physical, e.g. locks on doors. The controls are further defined into the types of controls that they are, i.e. preventative, detective, corrective or a deterrent.

These controls are effectively a checklist for the project to deliver against. It is the project managers' responsibility to implement these controls with the assistance of the security function.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Security plan for

	Prevent	Detect	Correct / Recover	Deter
Physical	•Access controls in place to only allow authorised users to enter zones within the XXXXXXX site [risk 8]	*No new controls in project*	*No new controls in project*	*No new controls in project*
Technical	•Malicious code protection for web client [risk 3] •Malicious code protection within database [risk 3] •Data is encrypted to adequate level in transit (over the Internet and XXXXXXX network) [risk 1,5,6,8,9] •Separate disks for XXXXXXX at XXXXXXX [risk 8, 11] •Web client with "baked in" security, e.g. caters for SQL injection attack. [risk 3,7] •Synchronisation software designed to tolerate and handle corrupted or malformed data, e.g. does not commit corrupt data to the database. [risk 2,4,5,9] •DOS attack mitigation at the XXXXXXX gateway [risk 12]	•IDS within XXXXXXX network [risk 9] •Monitoring software, e.g. for disk capacity [risk 11]	•Reliable and proven backup and restore technology [risk 1,2,3,4,5,8,9,11,12]	•Disclaimer on the web client [risk 7]
Administrative	*No new controls in project*	•Full audit trail of physical access to site [risk 8]	•Thorough and proven backup and restore procedures [risk 1,2,3,4,5,8,9,11,12] •Careful admin and rollback procedures [risk 4] •Detailed and proven processes for responding to a "disaster" at XXXXXXX [risk 13]	*No new controls in project*

6 Top 10 tips for successfully building security into business projects

Just in case Bruce needed a summary of the advice in this paper, the table on the next page contains a short description of the 10 things that a security professional can say, know and do in order to ensure that project managers bake security into their projects.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Tips for successfully building security into business projects	
Things to say	
1	Be Influential by using negotiation, pragmatism and other people skills
2	Raise the profile and importance of security within the business
3	Consider language, terminology and context when interacting with colleagues
Things to know	
4	Security best practice and standards
5	Money makes the world go round – and motivates management
6	War stories – when things go bad when security is poor
7	Understand the wider project process
Things to do	

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

8	Secure management buy in – if they take it seriously everyone else will!
9	Create alliances with other departments within the business
10	Establish a security risk assessment and plan process and plug it into the existing project process

7 Conclusion

Bruce did, in fact, adopt the advice and tools detailed in this paper and began to deliver a better more co-operative security service and assisted project managers in delivering secure projects on time and on budget. One particularly good example was the delivery of a new remote access system for his company. The old system was littered with security problems because Bruce was only consulted at the last minute and he insisted that the authorisation mechanism be changed. The original solution only required username and password to gain access whereas Bruce insisted on retro fitting a further PIN to provide another layer of security. Due to the rush to get this added security requirement, the code was not properly tested and later, during a penetration test, an ethical hacker was able to login to their systems without genuine credentials. The project was delivered very late and 30% over

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

budget.

The new system architecture was presented to Bruce during the design phase of the project where Bruce had an opportunity to assess the solution, identifying the high risk associated with the solution providing access to the company's critical data from the Internet. Bruce produced a security plan which detailed the use of SecureID to provide 2 factor authentication. This was incorporated into the project schedule and budget. A penetration test was also scheduled which proved that it was exceptionally unlikely that the system could be hacked.

The system went live on time and on budget providing management options to increase workforce flexibility and with the confidence that unauthorised people could not gain access to their critical information. Bruce is now much happier. He is delivering better security, his interaction with the department is less confrontational and he has a better work life balance.

8 References

British Standards (2005). *BS ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements.* Standards

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Policy and Strategy Committee.

Carnegie, D (1981). *How to win friends & Influence People.* New York: Pocket Books.

Cole, E (2007). *Security 401.3 Internet Security Technologies.* SANS Institute.

Einstein, A (n.d.). Retrieved June 18, 2008, from Quoteworld.org: http://www.quoteworld.org/quotes/4109

Ellison, R (2006). Security and Project Management. *Build Security In.* Retrieved June 18, 2008, from https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/project/38-BSI.html

France, A (n.d.). Retrieved June 18, 2008, from Quoteworld.org: http://www.quoteworld.org/quotes/4894

Gilbert, A (2005). *Go MAD – the art of making a difference.* Leicestershire: Go MAD Books.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Office of Government Commerce (2005). *Managing Successful Projects with PRINCE2.* London: TSO.

Pragmatism (non technical usage). (2008) In *Wikipedia.* Retrieved June 18, 2008, from http://en.wikipedia.org/wiki/Pragmatism_%28non-technical_usage%29

Schneier, B (2008). The Psychology of Security. *Essays and Op Eds.* Retrieved June 18, 2008, from http://www.schneier.com/essay-155.html

Schneier, B (2000). *Secrets and Lies.* New York: John Wiley & Sons, Inc.

Thurman, M. (2008). Security Manager's Journal: Enough of being the bad guy. *Computerworld.* Retrieved June 18, 2008, from http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=project_management&articleId=316095&taxonomyId=73&intsrc=kc_feat

Wilde, O (n.d.). Retrieved June 18, 2008, from All Great Quotes: http://www.allgreatquotes.com/money_quotes.shtml

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Last Updated: February 13th, 2016

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Northern Virginia - McLean 2016	McLean, VAUS	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Munich Winter 2016	Munich, DE	Feb 15, 2016 - Feb 20, 2016	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Feb 16, 2016 - Feb 23, 2016	Live Event
SANS Southern California - Anaheim 2016	Anaheim, CAUS	Feb 22, 2016 - Feb 27, 2016	Live Event
SANS Secure India 2016	Bangalore, IN	Feb 22, 2016 - Mar 05, 2016	Live Event
RSA Conference 2016	San Francisco, CAUS	Feb 28, 2016 - Feb 29, 2016	Live Event
SANS London Spring 2016	London, GB	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Philadelphia 2016	Philadelphia, PAUS	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Abu Dhabi 2016	Abu Dhabi, AE	Mar 05, 2016 - Mar 10, 2016	Live Event
SANS 2016	Orlando, FLUS	Mar 12, 2016 - Mar 21, 2016	Live Event
ICS410 Dubai 2016	Dubai, AE	Mar 13, 2016 - Mar 17, 2016	Live Event
SANS Secure Singapore 2016	Singapore, SG	Mar 28, 2016 - Apr 09, 2016	Live Event
SANS Secure Europe 2016	Amsterdam, NL	Apr 04, 2016 - Apr 16, 2016	Live Event
SANS Northern Virginia - Reston 2016	Reston, VAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Atlanta 2016	Atlanta, GAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
Threat Hunting and Incident Response Summit	New Orleans, LAUS	Apr 12, 2016 - Apr 19, 2016	Live Event
ICS Amsterdam 2016	Amsterdam, NL	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Secure Canberra 2016	Canberra, AU	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Pen Test Austin	Austin, TXUS	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Copenhagen 2016	Copenhagen, DK	Apr 25, 2016 - Apr 30, 2016	Live Event
SANS Security West 2016	San Diego, CAUS	Apr 29, 2016 - May 06, 2016	Live Event
SANS Baltimore Spring 2016	Baltimore, MDUS	May 09, 2016 - May 14, 2016	Live Event
SANS Houston 2016	Houston, TXUS	May 09, 2016 - May 14, 2016	Live Event
SANS Stockholm 2016	Stockholm, SE	May 09, 2016 - May 14, 2016	Live Event
SANS Prague 2016	Prague, CZ	May 09, 2016 - May 14, 2016	Live Event
SANS Secure Japan 2016	OnlineJP	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced