The Philosophy of Enterprise Information Security

Andrew S Townley

BearingPoint, Inc.

Abstract

Enterprise Information Security (EIS) must consider anything that would put the enterprise's information at risk or in danger. Unfortunately, the risks and dangers facing today's enterprise are great indeed: spyware, spam, phishing, Internet worms, viruses, crackers, natural disasters, corporate espionage, increasing regulation, eroding customer confidence, disgruntled employees and possible criminal prosecution of executive management. These dangers are far beyond the scope of hardware or software detection and prevention tools alone.

Enterprise information includes not only the sum of all data stored or transmitted by its networks and computer systems but must also include the knowledge in the minds of its employees. All this information is the lifeblood of the enterprise. This information is also the differentiator from its competitors. Therefore, it is no surprise that the scope of EIS has expanded to include physical security, non-electronic data storage, document destruction, emergency preparedness, regulatory compliance and even employee protection in both normal and abnormal circumstances. The answer to how an enterprise has any hope of successfully protecting its information lies in Weinberg's Second Rule of Consulting: "No matter how it looks at first, it's always a people problem."

People are the biggest asset an enterprise has in dealing with the totality of EIS. Of course, its people can also be one of the largest causes or contributing factors to these risks and dangers as well. Only through understanding the critical role of people in the end-to-end information security can an enterprise establish security policies which will be embraced rather than be rejected as unnecessary distractions from "getting the work done." Policies don't provide security; people do.

Introduction

Philosophy normally invokes images of Socrates, Plato, Aristotle, Lao-tsu or Confuscious, however an investigation of the word turns up some perhaps lesser-known meanings [1]:

- The critical analysis of fundamental assumptions or beliefs
- A set of ideas or beliefs relating to a particular field or activity; an underlying theory
- A system of values by which one lives

The above are three of the eight definitions presented. By examining these definitions in the context of Enterprise Information Security (EIS), it is possible to illustrate the broad scope of information security which must be considered by any enterprise. Once the scope has been discovered, it is then possible to address the last two of the above definitions and create a holistic security policy which directly affects the day-to-day operations of every individual in the enterprise.

The Issues

There are several contributing issues to modern Enterprise Information Security which must be understood before attempting to analyse the underlying assumptions and beliefs that will allow us to define a philosophy for managing EIS. The key issues in this area are customer trust, the growing regulation of security, preparing for unexpected events, the role of employees in enterprise security incidents and the threats relating to intellectual property.

Customer Confidence

The many recent, high-profile security breaches such as LexisNexis, ChoicePoint, T-Mobile, Bank of America and even Paris Hilton's Sidekick account reinforce what security professionals have known for many years: security cannot be an afterthought; it must be thoroughly integrated within the activities of the organization at every level. Unfortunately, security has generally not been the top priority, so it should not come as a surprise that security breaches of all types are a regular occurrence [2].

Until recently, there was nothing to force disclosure of security breaches. Organizations were not especially eager to let breaches of their systems become public – especially in the case of on-line retailers. Businesses depend on customers trusting them with their personal data. As Arik Hesseldahl wrote in a 2003 Forbes.com article [3], *"No company wants to puncture their own reputation as a safe place to shop online."* This attitude can naturally be extended to businesses in any industry.

Customer loyalty relies on maintaining a degree of trust between the consumer and the supplier of a service. When those customers happen to be capable of defining or influencing legislation or regulations and this trust has been violated, something is generally done about the problem.

Regulations and Legislation

In 2003, California passed the *California Information Practices Act* primarily due to a security breach of the state's payroll records, resulting in the financial information of 265,000 employees potentially being exposed [3]. Some of these 265,000 happened to be the state lawmakers. Mr. Hesseidahl points out that this law affects not only companies based in California. Any U.S. or International company who has customers resident in California is also accountable under this law.

The recent publicized breaches mentioned above are having an impact in Washington D.C. as well. Using the Thomas service [4] from the U.S. Library of Congress, there are currently at least 50 pending Bills for the 109th Congress dealing with privacy and security. At least two of these are modelled on the California law. Lawmakers are reacting to legitimate concerns about the potential uses of compromised data – specifically, fraud and identity theft. According to a Federal Trade Commission report, over 600,000 U.S. consumers have reported fraud and identity theft complaints during 2004 [5]. International law firm White & Case additionally reports in a press release that *"identity theft costs US consumers and businesses $50 billion annually"* [6]. These figures are difficult to ignore for both lawmakers and businesses.

Expanding the view to regulations relating to controlling international terrorism, the count of U.S. Congressional Bills is currently also 50, but the European Union's *Legislative Observatory* [7] lists nearly 200 Parliamentary procedures currently in progress. At least in the U.S., regulations like *Executive Order 13224* prohibit *"doing business with terrorists,"* according to longtime Chief Security Officer Bob Hayes [8]. However, the wording of Executive Order 13224 states it applies to *"individuals and entities that provide support, services, or assistance to, or otherwise associate with, terrorists and terrorist organizations designated under the Order"* [9]. Compliance with this regulation means checking every customer, supplier, visitor, employee and service provider against the list of known terrorists and terrorist organizations.

Examples like Executive Order 13224, Sarbanes-Oxley, Basel II, BS7799, ISO17799, the Can-Spam Act of 2003, HIPAA, the Gramm-Leach-Bliley Act, AS/NZS 4360:2004, FISMA, FIPS, FACT Act, PCI Data Security Standard, Data Protection regulations and others require organizations covered by them to provide evidence of compliance. Compliance failures can vary from fines to imprisonment of company chief executives or both, as former CEO of HealthSouth Corp. Richard Scrushy is likely to find out when the verdict is decided in the first Sarbanes-Oxley prosecution [10]. Of course, evidence in the case clearly seems to indicate wrongdoing on the part of Scrushy, but what if similar accusations were made against your enterprise? The only way to sensibly respond to allegations of this nature is to have proof that the appropriate security measures are in place to prevent inaccurate recording of the company's financial transactions. This proof will be necessary for both periodic compliance audits as well as for potential legal evidence in court.

Unexpected Events

Natural disasters and other disruptive events are also a threat to the security of the enterprise's information. Remembering that critical enterprise information is in the minds of its employees and physical records as well as the data on its computer systems and networks, anything which would put any of these at risk or in danger must be considered.

What happens if the CEO is injured or killed? Is the critical strategic direction for the organization documented? What if the communications link for the support centre was severed by workers at a building site down the road? Who will answer the customer calls? What if there is a fire in the central computer room that shuts down the systems running the enterprise? Does the business stop in its tracks? What happens if the Senior VP of Sales has his laptop stolen? Is the data on it backed up?

What could competitors gain from the data on the machine?

Answers to the questions in the preceding paragraph are provided by having a well-defined *Business Continuity and Disaster Recovery* plan (often abbreviated BC/DR). It is no coincidence that the essential first steps in creating a comprehensive security policy and a BC/DR plan is a risk and business impact analysis [11]. Without accurate risk and impact assessment, it is impossible to define the appropriate protection for specific information resources within the enterprise.

People Problems

In 1985, Gerald Weinberg proposed three fundamental Laws of Consulting in his book *The Secrets of Consulting* [12]. The second of these laws: *"No matter how it looks at first, it's always a people problem"* can be applied in both the negative and the positive in relation to Enterprise Information Security.

According to a Gartner report [13], *"more than 70 percent of unauthorized access to information systems is committed by employees, as are more than 95 percent of intrusions that result in significant financial losses."* A recent article in the on-line version of SC Magazine echoed the tone of Gartner's findings by saying *"upwards of 80 percent of network attacks are facilitated by employees opening attachments of unknown origin or even by providing their username and password to someone else"* [14]. While these are staggering statistics, the question is really if the employee intended malice or if these events are the result of negligence. The short-term business costs are the same, but the solutions to the problems are dramatically different.

Security expert Ross Anderson is of the opinion *"most actual computer frauds involve staff accidentally discovering features of the application code that they can exploit in an opportunistic way."* However, he adds that they may *"just be abusing features of the applications that they were trusted not to"* [15]. While initially accidental, the continued abuse of application functionality would definitely fall into the malice category as would running a network packet sniffer on an internal network without previous authorization or repeatedly attempting to log in to systems to which the user did not have access. The classification of opening unknown attachments and giving out usernames and passwords is much more difficult and should be examined on a case-by-case basis.

Intellectual Property

The threat of *Intellectual Property* (IP) loss also is a growing concern. IP losses can take several forms, but broadly falls into two categories: counterfeiting and confidential or trade secret information. For the month of February 2005, IP theft accounted for 36% of global counterfeiting relating to brands, trademarks and copyrights [16]. Clothing, entertainment and software contributed $50 million of the total losses. This is a small portion of the approximately $300 billion in costs absorbed each year by U.S. companies according to figures published by CSO Magazine [17].

Confidential and trade secret information vital to the business is also under extreme risks. It may exist in many places: company servers, on laptop computers, portable storage devices, backup tapes, paper documentation, emails, but most importantly, in the brains of the employees. Any one of these things can be attacked or compromised. Improper handling of employee terminations, either due to poor performance or cost cutting, can create severe security risks for the company's IP [17]. As much as an employer may like, they ultimately have no control over what is in the employee's brain when they walk out the door for the last time.

The issues discussed in this section cover a very broad spectrum of information security at a high level. Each issue contributes unique challenges for anyone responsible for providing solutions to ensure the enterprise's information is safe. All hope is not lost, however. Now that the main issues are illustrated, we can explore the assumptions often accompanying them so that we can define a philosophy for approaching the problem.

Challenging Assumptions

Assumptions are everywhere. Every time you interact with someone or something, a set of explicit and implicit assumptions actively influence your actions. The problem is that it is normally the implicit assumptions which get you in trouble. The process of recognizing these implicit assumptions and understanding their influence is part of the discipline of Organizational Learning, and is the positive side of Weinberg's Second Law of Consulting. People *can* alter their behaviour.

For it to be successful, a security policy's standards and procedures must be integrated into the day-to-day operations of an enterprise. Often, well-structured and considered security initiatives put in place by company executives fail to achieve the desired results. In this respect, the security policy does not differ from many other management initiatives. From the employee perspective, it is simply regarded as another collection of rules which must be followed and which will just get in the way of doing productive work. If this attitude is adopted, the standards and procedures will be implemented completely or correctly if they are implemented at all. Employees in this state conform to Lao-tsu's 2500-year-old observation: *"the more laws, the more lawbreakers"* [18].

The work of Peter Senge on *Organizational Learning* indicates these policy failures are linked directly to conflicts between what they say and fundamental assumptions of how things are or should be done in the minds of employees [19]. As described by Weirich and Sasse, *"many users construct their own, often wildly inaccurate models of security threats"* [20]. Given this conflict, the aforementioned behaviour is certainly understandable. Therefore it is absolutely necessary that these fundamental assumptions are brought to the surface so that they can be

addressed either during the creation of the security policy or during its implementation.

Assumption: security training is only necessary for the IT staff

It is important that the IT staff responsible for implementing and managing projects have a good understanding of security, regardless of their level. As previously mentioned, security should be a consideration from the very beginning of a project.

However, John Golden's article [14] points out that in most organizations, IT staff are distinctly the minority within the organization. Most will be non-IT users likely having only specific computer skills. They will not generally have the awareness that attachments from unknown sources could pose any threat to the organization at all. The users in the sales, support, marketing and finance departments need to gain an understanding of the threats from seemingly benign things like email as part of a program of basic security training for every department. People have no hope of behaving accordingly if they do not understand the nature of the threat.

Assumption: anti-virus, firewalls, intrusion detection systems and other technology solutions will keep networks and systems secure

Technology tools are vital to the overall enterprise security architecture, but they are only one piece of the puzzle. *Symantec* documented the discovery of over 2,600 new software vulnerabilities in 2003. This means that there was an average of seven new security vulnerabilities discovered each day [21]. It takes time to investigate these threats and provide meaningful fixes. Therefore, it is virtually impossible for any reactive hardware or software system to provide a complete security response to this kind of threat.

The solution to this type of threat is a proactive one and should be addressed as part of the basic security training mentioned above. To paraphrase a story from one of my colleagues, *"if it doesn't need to be there for the system to run, why is it?"* should be the standard way of thinking. People are the most adaptive system in the organization; therefore, they are the best place to start dealing with problems of this magnitude.

Reliance on technology solutions and inadequate human monitoring of security advisories directly led to the T-Mobile security breach [22] which lasted from October 2003 to October 2004. This failure of T-Mobile's security allowed a 22-year-old using 20 lines of Visual Basic to gain full access to customer passwords, Social Security numbers and other personal information. With critical, 24x7 systems like T-Mobile's WebLogic application servers, security updates and patches must be planned and tested. Automatic updates similar to Windows Update are not a viable option.

Assumption: information security threats will not come from trusted business partners or customers

Trust relationships are one of the most difficult things to manage in any security environment. Before establishing a relationship with a new business partner, the level of data access should determine the level of credential verification performed. However, this verification has limits.

The ChoicePoint security breach [23] involved access to secured customer information via the establishment of a customer account *"using stolen identities and altered documents."* No illegitimate access to any ChoicePoint computer system was involved. The failure actually occurred in the credentialing performed on the identities before establishing the trust relationship allowing data access by suspected members of organized crime [24].

In practice, the credentialing solutions used could be influenced by governmental regulations similar to Executive Order 13224. However, the ChoicePoint case illustrates some of the potential risks relating to trust relationships. ChoicePoint personnel trusted the issuers of the supplied credentials, apparently without properly determining their validity.

Assumption: passwords for "normal" users are not as important as for "administrator" users

Passwords are only as good as the person holding them. Anderson [15] stresses that a password policy must be considered in relation to the expected types of attacks. The main goal of anyone trying to breach security on a computer system is to first obtain access to the system. The attacker's typical exploitation path would be to first obtain control of a regular user account. Once they have access to the system, they can begin more sophisticated attacks on administrator accounts using known exploits for the system.

Also, the above presumes that the "normal" user does not have access to sensitive enterprise information. The process of social engineering is still one of the greatest threats to enterprise information, because the easiest thing for an attacker to do is to extract information they want from the people who legitimately have access to it *"by telling some plausible truth"* [15].

Two high-profile cases of social engineering are LexisNexis and Paris Hilton's T-Mobile Sidekick account. LexisNexis illustrates a combination of social engineering to trick a user into executing malicious code and following the textbook system exploitation path [25]. After discovering a user account and password for a LexisNexis computer system, users were able to locate an administrative account for the Texas state police department. Again using social engineering, the attackers tricked an administrator into resetting the password on the account, allowing full access to the system and it's information. The Paris Hilton case was straightforward social engineering [26]: attackers convinced a T-Mobile employee to give out account details

which were then used to access private user data stored on the system.

The only serious deterrent to social engineering attacks is the education of the complete user community. As has been shown, any account on any system can provide a foothold for an attack. While in the majority of cases intrusions can be detected once they have occurred, ones related to social engineering can often be prevented before they happen. Preventative measures, if successful, will also avoid potentially damaging public disclosure of a security breach under any of the relevant legislation. Such disclosures may undermine customer confidence and lead to loss of revenue.

Assumption: security of backup media is a lesser priority than the security of the running systems

Backup facilities should be a part of any business-critical system be it electronic or paper-based because they provide a recovery mechanism from both physical and logical disruptions to a given point in time. However, in order to provide this facility, backup media introduces a confidentiality risk [15] because the backup media is normally replicated to multiple locations and also subject to differing security controls.

If an attacker can gain details of how the backup tapes are handled, they now have an additional possible route to the information. Based on the difficulty of accessing the live system or the backup, the backup media may be a much easier target. Once they have the backup media, they can attempt to restore it to a similar system with essentially unlimited time. If this is successful, the information will be compromised.

The above scenario was mostly likely the goal in the Bank of America case [27] where backup tapes containing the personal information of 1.2 million workers of the U.S. Government were apparently stolen during transport to a backup centre. From a U.S. national security point of view, the loss could endanger the nearly 900,000 employees of the Department of Defense in addition to the very real threats of fraud or identity theft. The loss must also have a negative impact on the trust of the Bank of America customers.

Assumption: all critical data in the enterprise is regularly backed up

While data stored in enterprise applications is generally backed up on a regular basis, a full Business Continuity and Disaster Recovery plan must address all enterprise information. The backups are no good to the business without the correct systems. The reality is *"most people don't really know how many servers they have, or how they're configured, or what applications reside on them"* according to security and disaster recovery experts [11]. If service to critical systems is interrupted, it is difficult to keep the business running without this information.

Failure to consider data on portable devices such as laptops is also common. Mobile users may not regularly be in the office to participate in scheduled backups. Even remote connections over VPN links have limited capability in this regard due to slower than normal network speeds. If a laptop is the only location for critical business information, losing it can cause significant liability to the enterprise.

People are key in addressing this assumption. If processes and procedures are in place for accurately recording changes to the system, employees can do a lot to ensure such information exists somewhere other than in their heads with only minimal effort. Without these procedures and facilities, people become the primary repository for this information – and a significant risk.

Assumption: copyrights and patents are sufficient protection for intellectual property

Copyrights, patents and other legal protections are very similar to the function of locks on doors – they keep honest people honest. Criminals or unscrupulous competitors are not easily deterred by such protection because there will always be a window between when IP is stolen and when they are caught. Trademark and brand related IP theft is particularly troublesome because these are easily copied, cheaply produced and there is significant consumer demand for such items. Manufacturers are currently exploring technology solutions like digital rights management, nanotechnology, RFID and various methods of secure printing in attempts to protect both brands and intellectual property from unauthorized duplication [16]. However, a more proactive, if more difficult, solution may be to attempt to address the level of consumer demand for counterfeit goods.

In the case of "soft" IP theft, exposure of the information is the chief concern. Once the information is exposed, it is impossible to make it secret again [17]. Social engineering is also a major factor in IP theft, because people are the easiest way to access protected information. As illustrated by Weirich and Sasse [20], *"trust is the key criterion"* for accessing sensitive information followed closely by proximity. People skilled in social engineering can easily build up this sort of trust with most people very quickly resulting in disastrous effects for the enterprise.

Like other areas subject to social engineering attacks, making people aware of the sensitivity of the information under their control can prevent some breaches of this type. People may think they are cleverer than someone else suspected of this kind of attack and can turn it to their benefit, but in reality they often give away much more information than they get in return.

The above assumptions represent a very small list, but are given to illustrate that failures to understand and address the underlying assumptions involved with security issues could easily result in the exposure of critical enterprise information. They also illustrate the relationship between people and their fundamental assumptions. Nearly every

security breach, and certainly the ones discussed, can be traced back to an assumption that proved to be false. Even if these assumptions have been addressed, they need to be periodically assessed to ensure the environment has not changed. Doing so could invalidate many more assumptions.

Defining the Philosophy

A successful philosophy for enterprise security must aspire to securing enterprise information for both individual employees and the organization as a whole in a manner consistent with a comprehensive security policy. Only aspiration provides sufficient motivation because it requires that information security is the ultimate goal. Other possible motivations for compliance include coercion or persuasion. While persuasion is intended to induce belief and can be useful in instilling the philosophy as the ultimate goal, if focussed in the wrong direction it will be ineffective. The philosophy must get people to genuinely care about security such that it becomes essential to the nature of their work.

Fear is the primary motivating factor in coercion, but it is an emotion which is only effective in short bursts. If relied on for governing day-to-day behaviour, people will mentally adjust to deal with the fear, making it a less effective motivator until its efficiency is eliminated completely. This phenomenon can be observed by anyone who overcomes a fear of flying, animals or heights. Overcoming or living with fear is not something unique to people; it can manifest itself in organizational behaviour as well. It is unlikely that Richard Scrushy's $2.7 billion accounting fraud [10] started without a certain level of fear of being caught. However, during the six-year period it was committed, Scrushy clearly overcame any fears he had of discovery. The consequences of his actions could be hundreds of years in prison, but, like any fear, the longer he was exposed and the more confident he became, the less influence his fear of prosecution held over his actions. This illustrates the dangers of relying on fear to provide a long-term motivation for compliance, be it with government or industry regulations or with an enterprise's security policy.

Weirich and Sasse [20] explore the relationship between a user's actions and *"their mental constructs, e.g. their knowledge, beliefs and attitudes"* in the context of persuading the user to comply with security policies for passwords. Senge calls these same constructs "mental models" [19]. I believe that using the types of persuasion described by Weirich and Sasse to accomplish security is doomed to fail because it really only equates to two of Senge's levels of compliance [19], meaning either the person does what they're expected because they want to keep their job or the person only does exactly what is expected – no more; no less. Senge differentiates his levels of commitment from enrollment by stressing the "free choice" aspect of enrollment vs. feeling responsible for making something happen. Weirich and Sasse argue using persuasion to enable compliance, not to create an intrinsic belief that security is important.

Security failures due to people are more prone to happen in unusual circumstances because the person is not in their normal frame of mind. When under stress, the person who has been persuaded or coerced to comply with the security policy will often fail to do so, because the current environment may have rendered individual standards and procedures impossible to follow. However, an enrolled or committed individual will comply with the security policy in these cases because they believe in it; they have internalized it and it contributes to their every action. These differences can be crucial during BC/DR scenarios. In some cases, not only the business but also people's lives may be at stake.

The fundamental belief of an effective security policy is that people are the ultimate security enablers. Even faced with the alarming statistics of employee-related security breaches [13],[14], the positive role of people within EIS cannot be understated. People:

- assess the risk to the enterprise
- develop and implement appropriate BC/DR plans and procedures
- determine relevant regulatory requirements
- define the security policy for the organization
- define and implement the security standards and procedures
- design and implement the systems implementing these standards and procedures

Ultimately, people are responsible for keeping the information free from risk or danger. They build the systems, choose the hardware and software, monitor security advisories, keep the systems up-to-date, respond to unexpected events, and monitor the physical security of the facilities. Even with the application of industry "best practices", the onus of putting it all together is on the people, not the products.

Implementing the Philosophy

There are a number of common sayings summarizing the problem faced when implementing any security policy, but specifically when trying to instill an organization with a new philosophy. Weinberg states it in his *Buffalo Bridle Principle*: *"you can make buffalo go anywhere just so long as they want to go there"* [12].

The main question is how to get the buffalo wanting to go the right direction.

Buckingham and Coffman [28] rightly point out *"each individual employee can decide what to do and what not to do."* They equate the solving of this problem with learning how to manage by remote control. Getting employees to do the right thing involves unwavering focus on the outcomes to be achieved and not the mechanisms. However, they caution that at the same time rules relating to

safety and accuracy must be "the foundational part" of every employee's job.

Allowing employees to choose their own path while still adhering to the security policy is possible. If the security policy, standards and procedures are defined in terms of actual requirements with measurable criteria, meeting these criteria can be integrated into the performance review process at all levels of the enterprise. By focussing on the requirements rather than on the way the requirements must be met, employees can integrate the security policy into their own, individual styles of working – giving exactly the desired result of making security an essential part of everyone's job. Behaviour identified by Weirich and Sasse to reinforce this [20] is also recognized by Buckingham and Coffman [28]: *"A manager's job is to encourage people to do more of certain productive behaviours and less of other, unproductive behaviours…In most cases, no matter what it is, if you measure it and reward it, people will try to excel at it."*

Both Weinberg and Buckingham and Coffman recognize that attempting to over specify how an outcome can be achieved can result in exactly the desired outcome not being met. If the steps or the importance of them overshadows the desired outcome, the steps are no longer useful [28].

Communication is absolutely essential in implementing this philosophy successfully. According to Senge, *"In organizations, goals erode because of low tolerance for emotional tension"* [19]. Emotional tension occurs when communication is not open within an organization. If people have difficulty meeting deadlines or performing their jobs because they attribute it to overhead imposed by security requirements, they must be able to express these concerns to supervisors and managers. Buckingham and Coffman stress *"the most efficient path from A to B is always the path of least resistance"* [28], so the temptation will always be to avoid what people consider to be irrelevant. By encouraging open communication between employees and management, this "short circuiting" of security may be avoided, but only if the organization is as actually committed to the security policy as it says it is. By voicing concerns about being able to successfully implement appropriate security measures, both the security requirements and the business process can be reexamined to determine the best way to accomplish both objectives.

Open communication is also the only way to ensure that everyone shares the same mental models within the organization [19]. If the philosophy and the mental models are not synchronized, security within the enterprise will suffer. Another important observation by Buckingham and Coffman is *"companies must change the way people speak if they are to change how people behave"* [28]. If the language used to describe security within the enterprise does anything other than paint a picture of a wholly integrated activity, people will de-emphasize it. However, if the message of a holistic approach to security is communicated consistently, the behaviour of the organization will eventually reflect it. This phenomenon is an expression of how powerful mental models are over perception and behaviour [28]. Therefore, the enterprise must foster mental models that internalize security as the fundamental part of everyone's jobs.

Conclusion

The totality of Enterprise Information Security includes a wide spectrum of considerations including customer confidence, employee safety, business continuity planning, disaster recovery, regulatory compliance, protection of intellectual property, physical security and the protection of the information infrastructure. The only way to adequately address these considerations is by establishing a comprehensive security policy, tailored to the unique requirements of the enterprise, and by relying on the enterprise's most adaptable system to implement it-its people.

A security philosophy must be defined and adopted along with appropriate assessment metrics to ensure that implementing the security policy is a fundamental aspect of everyone's job. Based on this philosophy, the organization must provide open communication, allowing any implicit assumptions relating to implementing the policy to be surfaced and discussed. This process allows the organization to establish consistent mental models which are vital to implementing the security policy successfully.

These steps will allow security to be integrated into all activities across the enterprise. No longer will it be an afterthought. People must be recognized as a key source if enterprise information and as the ultimate security enablers. The people within an enterprise have the ability to adapt to any threat and create the security atmosphere which can keep its information free from risk and danger. No combination of hardware or software products alone can ever fill this role.

References

[1] Dictionary.com

http://www.dictionary.com

[2] Kirby, C. (2005, May 16), *Security breaches not on rise. Privacy watchdogs say incidents are being disclosed more often*

http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2005/05/16/BUG1HCORRK1.DTL&type=printable

[3] Hesseldahl, A. (2003, November 21), *Regulating The Hacker Chase*

http://www.forbes.com/2003/11/21/cx_ah_1121hack.html

[4] U.S. Library of Congress, *Thomas: Legislative Information on the Internet*

http://thomas.loc.gov

[5] Federal Trade Commission (2005, February 1), *National and State Trends in Fraud & Identity Theft: January - December*", 2004

http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf.

[6] White & Case (2005, April 12), *Data Security Breaches No Longer 'Dirty Secret' Says White & Case Lawyer*

http://www.whitecase.com/news/news_detail.aspx?newsid=11490&type=News%20Releases

[7] European Parlament, *The Legislative Observatory*

http://www2.europarl.eu.int/oeil/index.jsp?language=en

[8] Scalet, S.D. (July 2003), *Chaos in a Three-Ring Binder*

http://www.csoonline.com/read/070103/chaos.html

[9] Office of the Coordinator for Counterterrorism (2002, December 20), *Executive Order 13224 Fact Sheet*

http://www.state.gov/s/ct/rls/fs/2002/16181.htm

[10] Reuters (2005, May 19), *First Sarbanes-Oxley Prosecution Under Way*

http://www.cioinsight.com/article2/0,1397,1817852,00.asp

[11] Slater, D. (2004, April 8), *The ABCs of Business Continuity and Disaster Recovery Planning*

http://www.csoonline.com/fundamentals/abc_continuity.html

[12] Weinberg, G.M (1985), *The Secrets of Consulting: A Guide to Giving & Getting Advice Successfully*, Dorset House, New York.

[13] Hunter, R. (2005, February 11), *Enterprises and Employees: The Growth of Distrust*

http://www.csoonline.com/analyst/report3317.html.

[14] Golden, J. (2005, May 18), *Infosec: no longer just the IT department's concern*

http://www.scmagazine.com/features/index.cfm?fuseaction=featureDetails&newsUID=221d0d41-78d1-4cab-b5c0-a9ff26896d91

[15] Anderson, R. (2001), *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, New York.

[16] ArriveNet (2005, March 15), *IP Theft surges to 36% of Global Counterfeiting: Survey*

http://editorials.arrivenet.com/bus/article.php/3850.html.

[17] Slater, D. (2003, December 9), *The ABCs of Intellectual Property Protection*

http://www.csoonline.com/fundamentals/abc_ip.html.

[18] Tzu, L., and Star, J. (2003), *Tao Te Ching, The Definitive Edition*. New York: Tarcher/Penguin, 2003.

[19] Senge, P.M. (1994), *The Fifth Discipline: The Art & Practice of the Learning Organization – Paperback Edition*, Currency Doubleday, New York.

[20] Weirich, D. and Sasse (2001), M.A., *Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World*, Proceedings of the 2001 workshop on New security paradigms, Cloudcroft, New Mexico, pp. 137-143.

[21] Symantec (2004, June 2), *The Changing Threat Landscape*

http://www.symantec.com/symadvantage/022/landscape.html

[22] Poulsen, K. (2005, February 28), *Known Hole Aided T-Mobile Breach*

http://www.wired.com/news/privacy/0,1848,66737,00.html

[23] U.S. Securities and Exchange Commission (2005, March 4), *United States Securities and Exchange Commission, Form 8-K*

http://www.sec.gov/Archives/edgar/data/1040596/000095014405002087/g93611e8vk.htm

[24] KTVU (2005, February 28), *Outrage Growing Over ChoicePoint Security Failure*

http://www.ktvu.com/news/4232683/detail.html

[25] Zetter, K. (2005, May 25), *Database Hackers Reveal Tactics*

http://www.wired.com/news/business/0,1367,67629,00.html

[26] Millman, R. (2005, May 20), *Hacker and sidekick Sidekick hack trick exposed*

http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=1f137662-ca40-4bfe-bb0b-21462e50ac98&newsType=Latest%20News

[27] Morrison, J. (2005, February 26), *Bank loses credit card info of 1.2M federal workers*

http://www.computerworld.com/securitytopics/security/story/0,10801,100061,00.html.

[28] Buckingham, M. and Coffman, C. (1999), *First, Break all the Rules, What the World's Greatest Managers do Differently*, Simon & Schuster UK, London.

About the Author

Andrew S. Townley is a Senior Consultant with BearingPoint, Ireland. He is currently the Principal Architect for the delivery of the Irish Government's Public Services Broker (PSB): the SOA backbone of Ireland's e-government initiative. The PSB provides a portal and a common messaging infrastructure to facilitate the diverse needs of citizens, businesses and government agencies. As part of his current work, Andrew is working to define and codify the security policies and requirements for the PSB including service access control, federated identity management and inter-service message security in addition to leading several internal initiatives around raising the awareness of designing for security and writing secure code.

Prior to joining BearingPoint, Andrew designed a highly-secure, data capture system along with the corresponding IT infrastructure for capturing individual and corporate income tax returns on behalf of the Irish Revenue Commissioners. He has also helped shape the single sign-on implementation for the multi-channel portal of a 3G telecommunications operator. Andrew draws on an extensive background in distributed system software development, testing and implementation for large and small clients in both the US and Europe.