Pragmatic Security: Making the Most of What You Have

Andrew S. Townley

BearingPoint, Inc.

Abstract

Security is about managing risk. These risks can affect the organization in many ways: its reputation, its information, its physical assets, its employees or its customers. However, only business decisions determine the acceptable level of risk in any situation, and each one of these decisions involves trade-offs. The only way to completely mitigate the risks to an organization is to not engage in any activity whatsoever.

Since there will always be risks, it is imperative to classify them effectively based on their potential impact to the business. It is quite easy to spend a lot of money on common security infrastructure components yet only address a small portion of the real risk to the organization. The most effective way to identify and manage the various risks is to perform a risk and business impact assessment as the first step towards implementing a comprehensive security policy.

A pragmatic approach to implementing the security policy involves prioritizing the risks and mitigating them by addressing the greatest risks with the fewest resources. Depending on the size of the organization, this approach may manifest itself in many different ways, but it allows business requirements to provide focus to security initiatives. Security policies should enable and support the business, not hinder it-whatever its size.

Introduction

Security is about managing risk, and managing risk allows the business to stay in business, but there are many ways to approach security. Approaching enterprise security pragmatically has value regardless of the size of the organization. From the individual user, to the small business to the global enterprise, it is sound business practice to spend money where it will do the most good. However, when it comes to security, how do you know where this really is?

The temptation is to follow industry "best practices" and hope. Everyone knows you need a firewall if you have systems connected to the Internet, but which one? How many systems need protection? Where are they? Do you really need spam filtering and anti-virus software? Are you sure?

Approaching enterprise security in this manner is a lot like playing Russian roulette: you may win, or it may kill you. The reality is that the biggest risk reduction may not be in the most obvious place. The only way you really know what is at risk is to do some sort of risk assessment and use that to define your enterprise security policy.

Like security policies, there's no one-size-fits-all risk assessment. It can be as simple as: "If this computer were to catch fire, the business would stop." It doesn't need to cost millions or even

thousands of dollars, but it must be done – the more detailed, the better [1]. Once this "set of guiding principles" has been created, it can be used to make intelligent business decisions and address pragmatically. Security is a business issue and should be treated like one [2], [3], [4], [5].

The process described in this paper is not a formal one, nor is it intended to be comprehensive; rather it intends to illustrate the activities necessary for providing security from a pragmatic perspective. There are several documented formal processes which may be useful and should be considered when implementing security within the enterprise [6], [7].

Getting Your Bearings

The first step to approaching security pragmatically is to understand the environment you're trying to protect. This understanding is not based on attempting to identify risk, it is simply so you know what you have already. This step is first, because if the organization doesn't already have a security policy, you will have to work with them to create one. You can't do this if you don't have some understanding of how they work and what resources they have.

This process really only requires leg-work, communications skills, a pen and a notebook. It may take some time, but it is important to answer these questions. The more information you gather now, the easier your job will be later.

This step also doesn't specifically require security expertise, although it helps when trying to ask the non-obvious questions. Also, in larger organizations, not all of this information may be in one place, or at one level. The management team needs to understand what you are trying to do, and why you need to ask the people with the answers. Bear in mind that some of these answers are often known only to lower-levels of an organization. I will call what we're building an enterprise field guide, because it will have a little bit of information about nearly the whole organization.

What Is It?

This question should not be overlooked when performing this exercise because in some cases, an organization is not all that it appears to be. Sometimes, it is much more. It is very important to understand the nature of the enterprise's business, because this understanding may guide the types of questions asked later.

Some key questions to answer are:

- What type of organization is it (public, private, partnership or not-for-profit)?
- Is any aspect of the business subject to legal controls (laws, regulations, guidelines or recommendations)?

How Big Is It?

The size of the organization is a very important consideration at all stages of security planning and implementation. The specific needs of a single, self-employed individual working from their home are much different from a multi-national enterprise, however their fundamental needs are ultimately the same: effective risk management.

Some of the questions which must be answered in this step are:

- How many employees?
- How many locations?
- How many departments?
- How many networks?
- How many computers (servers, laptops and desktops)?
- How many user accounts?
- How many applications support the business?
- How many other physical assets support the business (e.g. telephones, fax machines, specific industrial equipment and paper records)?

It is important to capture any elements of scope in this step which are critical to the business. When answering some of the other questions you may be adding more things to this list.

How Does It Work?

The detail of how work gets done on a daily basis has many implications for the types of security measures which may be required. The purpose of this question is to identify all of the supporting infrastructure required for the business to function. The focus is on anything not related to communication or information. The goal is identification of the important elements of the business, not to model existing business processes. Extreme detail is not required.

Some of the questions which must be answered are:

- What is the organizational structure?
- What kind of physical environment exists? How is it accessed (internally and externally)? Do people share workspaces? Do they have offices?
- Where do meetings take place? Are all meetings within the building, or are shared facilities used?
- How many computers does each person control (including laptops and PDAs)? Do they take one or more with them when they leave the building? What level of access do they have to the machine?

- What kinds of systems support the business (including versions and patch levels)? Operating systems? Shrink-wrapped applications? Custom applications?
- Where are these systems located? Are they in the building? Are hosting facilities used?
- Who manages these systems? How often are they monitored?
- How are these systems accessed? Is the same system shared by multiple people or does each person have a separate user account?
- How does data get entered into the systems? Is it done manually, or are there automated processes or batch jobs?
- How can data be retrieved from the systems? Are there nightly reports? Is there Web access?
- Where is data stored? In physical files? Electronically? What about the most critical business data? Is off-site storage used?
- What types of backups are performed? How often and what do they contain?
- What security measures are currently in place (both physical and electronic)?
- What is the visitor policy?
- What custom or industry-specific tools and equipment is used?
- Where do employees go for lunch?
- Where do employees go for drinks?

Answering the above questions should provide a decent understanding of how people work and what tools they require to do their jobs. It also provides information on where they are likely to gather outside of the organization to discuss work topics.

How Does It Communicate?
How an organization communicates is normally directly tied to how it works, but it deserves separate consideration from an information security perspective. People communicate with each other in many different ways. Some of them support their jobs directly and some support their life outside work.

Some of the questions which must be answered are:

- When and how do employees use email?
- When and how do employees use the phone?
- Do employees have company mobiles?
- Do employees have phones with cameras? Web-cams?
- Who has access to fax machines and copiers?
- Where are printers located? Who can access them?
- Are whiteboards and flipcharts used? Are they erased regularly or destroyed?
- Are computer monitors or other information visible to other people? From outside (day and night)?
- Are shared directories used for communication? Between individuals? Between work groups? With customers or partners (including computers used for presentations)?
- Do employees have access to personal email accounts from work? What about webmail?
- Do employees have access to instant messaging? Which ones?
- Are portable storage devices used (memory sticks and MP3 players)?
- Are documents destroyed after they are used? Are they shredded?
- Are wireless networks used? Are they secured in any way?
- How are physical networks connected? What connects the organization to the Internet? Are VPN connections used?
- Are there departmental intranet web servers?
- Does the company have a web site?
- Do employees have weblogs?
- Do employees present at workshops or conferences?
- Do employees write articles for publication?
- Is there a company phone directory? Is it printed?
- How is information moved from one physical location to another (inter-office mail, couriers, the postal system or shipping companies)?

Understanding these communication mechanisms is critical to ensure they are accounted for during subsequent security planning activities.

What Does It Communicate?
Enterprise information is not only electronic information [2], but includes physical information as well as information contained in the minds of employees. This step is critical for identifying the types of information that is communicated (or available) within the organization.

Some of the questions which must be answered are:

- What information is on people's desks?
- What information is taped to people's computers?

- What information is on mobile devices (phones, PDAs, laptops, portable storage and MP3 players)?
- What information is on bulletin boards? In the canteen? In reception?
- What information is in conference rooms (on the computer(s), on paper, on flipcharts and whiteboards)?
- Are documents classified based on their sensitivity to the business?
- What information is in the company phone directory? Does it include postal and email addresses?
- What information is in filing cabinets?
- What information is thrown away (including disk drives and removable media)?
- What information is accessible from the Internet? The internal network?
- What information is in electronic mail messages?
- What information is sent via instant messaging?
- What information is sent via email lists?
- What information is in external communications (presentations, workshops, articles and weblogs)?

While what is communicated and how it is done are normally investigated at the same time, it is useful to consider them separately. In doing so, it is possible to identify overlooked communication channels or certain types of information being transmitted in unexpected ways.

Who Does It?

In many cases the who is as or more important than the what or the how. People are an organization's most adaptable and dynamic resource [2], so it is very important to know what skills and talents [8] are available to implement the security policy.

Some of the relevant questions for this step are:

- Who owns or controls the organization?
- Who are executive management team (including the board of directors)?
- Who owns the building?
- Who built or decorated it?
- Who controls the budgets?
- Who is responsible for making security decisions?
- Who is accountable for security and business decisions?
- Who manufactures the products?
- Who supplied any custom or trade-specific equipment?
- Who manages the networks?
- Who manages the systems?
- Who supplied the systems?
- Who is officially in charge of each department (and who runs it, really)?
- Who uses which systems (and which systems need access to other systems or to the Internet)?
- Who created key innovations?
- Who works remotely?
- Who travels (and where do they go)?
- Who supplies physical security?
- Who supplies utilities (e.g. communications, power and water)?
- Who cleans the building (inside and out)?
- Who maintains the building (e.g. painting, heating, cooling and wiring)?
- Who provides the catering and vending facilities?
- Who fixes the copiers and printers?
- Who waters the plants?
- Who are the nearby law enforcement and emergency services?
- Who ships or handles company parcels?
- Who books the company travel?

The above is far from an exhaustive list, but serves to illustrate the number of people who interact with an organization on a daily basis. Some of them are potential assets while others are potential liabilities when viewed from a security perspective. Some may not be relevant based on the type of business or the size. Sensitive research facilities would pay more attention to the number of people who could possibly access their facilities and information than the self-employed landscape artist. When attempting to establish the scope of an enterprise from a security perspective (pragmatic or otherwise), it is better to have too many than not enough questions.

Assessing the Risks

Based on the information in your field guide, it should be quite clear that securing all of the information of an enterprise is well beyond the scope of a single set of technology tools [2]. Hav-

ing identified the individuals responsible for security, it is time to begin defining the security goals for the organization.

Historically, information security has not generally used formal methods for risk assessment [1]. From the pragmatic perspective, this is the first risk assessment issue to be addressed: how good is "good-enough"? Clearly formal methods of risk assessment have their benefits – they are nearly mandatory if the organization is of sufficient size or falls under certain regulatory controls. Since you have already gathered the information you need to make this decision, it is simply a matter of determining how precise you need to be. Remember, precision is different than accuracy [1].

Depending on whom you must convince, it may be sufficient to group risk ratings into basic categories such as "high", "medium" and "low." However, in larger organizations, there is generally more pressure to provide more representative cost ratios. Regardless, be pragmatic about it: the goal is to have a way to measure relative risk to the business.

How do you appropriately assign even three levels of risk to aspects of an enterprise? Unless you are responsible for the business, the answer is: you can't.

A traditional, bottom-up approach to enterprise security goes after the low-hanging fruit: infrastructure tools like firewalls, anti-virus, and intrusion detection tools [9]. The attitude is often, "Well, it can't hurt. Everybody knows you need them anyway."

I'm not saying infrastructure tools are a bad investment; I'm just questioning the priority of the investment. While you might not buy a house without locks on the doors, if you never locked them, they just cost you money without providing any value. Would they (in the general sense) say the same thing if the money came out of their pocket? What if the infrastructure tools were approved and installed, but the next day the Chief Scientist's laptop containing the only copy of her designs for the next version of the flagship product was stolen while she was at the airport? Which threat has the greater potential impact on the business?

Understanding the interrelationships of events, one of the tenants of Systems Thinking, cautions against the lure of the "quick fix" because it generally only leads to a false or, at best, temporary solution to the bigger problem [10]. Additionally, the above scenario is an example of the significance of context when making security decisions [3], [4].

An organization with a single computer and a dial-up connection to the Internet would be foolish to consider these types of security controls over, for example, locks on the garage where their tradesman tools were kept. If the computer was running Microsoft Windows, the use of a software firewall would certainly be advisable, but if the person was a Mac user, they would likely be relatively safe without one [11].

Ross Anderson says being able to make these kinds of decisions by "understanding the potential threats to a system" is the essence of security engineering [12], and this is what requires security expertise. Each of the answers to the questions about the enterprise can be revisited with a view to possible risks based on the types of potential attacks.

Ultimately, the final analysis will be done jointly between the people responsible for the business and its security to assign meaningful risk ratings. It is crucial to remember that while the same items may appear for similar organizations, the exact ratings will be unique to each organization [13]. The result of this exercise is a business impact analysis (BIA) [13].

The Security Policy

Even when implementing a pragmatic approach to security, a security policy is imperative. The role of the security policy is to establish the vision or focus of the security initiative. It articulates *what we are trying to achieve* in a concrete way and allows accurate measuring of the security gap. This gap indicates how much needs to be done to go from where security is now to where it needs to be [10]. Ideally, it should be extremely focussed on results [2], however it can be expanded into standards and procedures if so required.

Example policies might be as simple as: "protect the most important assets from the most serious threats" [5] or "ensure compliance with all relevant regulations by Q4 2005." Defining the security policy in this way makes it easy to define metrics and benchmarks which are necessary for accurate progress assessments at all levels [2], [1], [5].

How do you know what the "most important assets" and "most serious threats" are? You go back to your enterprise field guide and business impact analysis. For a large, e-commerce organization, a possible top threat might be software vulnerability exploits. For a purebred horse breeder, it might be the prize stallion and anything threatening its health. Different businesses have different priorities.

Based on operational intelligence, the security policy could also change – raising or lowering the priority of certain risks in relation to others. The security policy thus puts the security risks into a business context so they can be addressed relative to the needs of the enterprise. Its main goal is to focus organizational attention on the outcomes necessary to sustain ongoing business initiatives.

Applied Risk Management

Given that the security priorities will be different for each enterprise of each size in every industry, it is impossible to provide unqualified advice on where an enterprise will see the greatest return on investment (ROI). However, it is possible to discuss some approaches to likely items on any current risk assessment, independent of their relative risk to an organization.

Both Symantec and McAfee publish periodic lists of the current "top threats" to computer systems. These lists differ slightly in presentation, but two reports from 2005 indicate that the following items will likely be on any risk sheet:

- Exposure of confidential information via Trojan horses or phishing attacks
- Attacks against Web applications
- Viruses and Internet worms targeting Microsoft Windows
- Spam email containing spyware/adware
- Severe and easily accomplished remotely exploitable vulnerabilities

Symantec's statistics indicate that the time between when a vulnerability is discovered and an exploit has been released is now just over six days [15]. This statistic is very scary for security professionals responsible for managing any computer on a network – nearly every one of them. These two facts reinforce Gartner's claims that organizations should be focussed on eliminating these vulnerabilities [5]. Certainly failures to patch known vulnerabilities have resulted in high-profile security breaches, one example of this is the recent T-Mobile incident [16].

Since not all organizations can provide the same level of spam and email virus filtering [17], a potential option is to outsource at least the hosting of email accounts to a trusted third party. If there is sufficient trust that the supplier will not allow unauthorized access to organizational email, most hosting providers provide commercial-grade email filtering, however it is often an additional cost. For example, lunarpages.com provides spam and virus protection for between $2 and $1.25 per address, per month depending on the number of email addresses hosted. Filtering for 5 email addresses is $117/year, which might be a viable expense for a small business. A cost of $8000/year for a mid-sized business with 500 accounts might not be.

Other alternatives available to organizations hosting their own environments range from free, open-source email virus scanners to fully-supported commercial products from vendors like Symantec. Like any security solution, there are trade-offs. Open-source solutions generally require more in-house knowledge to deploy and maintain compared to commercial products, however they can often do as good or even better jobs. Either choice has a cost associated with it and a decision similar to buying or renting a home: you pay and end up with an investment, or you pay for a service and end up with nothing but a place to live. It is a business decision which one is the right choice.

Security in Context

Pragmatism in security recognizes that security is a fluid concept which is directly related to the context in which it is to be applied. According to Dourish et al., "Pragmatic users see security as a trade-off, one that must be continually struck as one balances immediate needs against potential dangers" [4]. Users of enterprise information have an enormous amount of potential in the application of security policies [2] because they understand this context. One of the reasons for this is that they are the closest to the information. They create it; they read it; they update it, but most importantly: they understand it. The data and the business processes which manipulate it are a large part of their lives.

Successfully integrating security into every employee's routine requires understanding users and how they use your systems [4]. One of the important points of research by Dourish et al. is the connection between a user's online and offline perceptions and expectations of security. This research explores how users deal with security issues during their normal activities and how they accommodate their security requirements into their work. They found that not only are users quite sophisticated at understanding their security needs, but that they adopt mechanisms outside traditional security protocols to ensure these needs are met.

These ideas, when combined with Sandhu's thoughts on "good-enough" security based on business objectives [3] could be the key to the most pragmatic security possible. The appeal of this approach is that it could be equally effective in a small business and an international enterprise.

One of the interesting consequences of the user's unified online and offline view of security is they naturally use media switching and physical space to facilitate their perceived security requirements. Both behaviours indicate a keen awareness of security on the part of the individual [4].

Media switching involves beginning a communication via one medium, email, for example, and continuing the communication via another, like the telephone. Dourish et al. indicate that this stems both from the perceived differences in the security of the medium (voice conversations are less likely to be stored for later processing) and from an apparent need to be aware of the visibility of a security system [4]. The visibility of the system in terms the user understands and how it might meet their needs also seems to directly correspond to a user's perception of its security.

Some examples cited by the research of effectively using physical space to accomplish security objectives were as simple as ensuring someone entering an office cannot see what is on the user's screen. Others include the use of barriers like tables and chairs to direct people to "safe" areas of the workspace and devising systems like using coloured folders to facilitate organization and tracking of sensitive documents while they are being used [4]. Visitors see the colours, but have no idea what they mean and are prevented from seeing the contents because they are both closed and under the control of someone. Established social norms are normally sufficient to prevent disclosure of information in these cases [4].

Given the apparent and dramatic differences between evidence of how users actually work and how traditional security systems are designed, it seems possible to devise a hybrid model. This model would integrate the security-related decisions with the normal activities of performing the tasks the policies were intended to secure, thus providing better security at minimal additional cost.

It is recognized that this model is not foolproof; humans make mistakes in both actions and judgment, however such a system should provide "good-enough" levels of security for most situations. This model might in practice exceed the total security of a non-integrated, conventional model because the user and the security system would be acting in harmony.

Conclusion

Pragmatic security is a business-driven approach based on mitigating risks in line with existing business objectives for organizations of any size. It attempts to reduce the most risk while using the least resources: people, time or money. It can only be successfully implemented once enough of the relevant risks to the enterprise have been identified and can provide a unified, strategic direction towards security that is documented in the organization's comprehensive security policy.

It is the process of discovering the enterprise and completing the risk analysis and business impact assessment that provides the foundation for the security policy. Without these two activities, it is not possible to determine a clear approach to implementing the security policy nor is any ability to easily identify changed risk priorities in light of new business intelligence available. All three combine to make a powerful security and risk management framework.

When thinking pragmatically about security, an organization should not forget its most adaptable resource. With minimal additional guidance, the people of an organization can leverage their inherent understanding of their own security requirements and those of the enterprise to provide significant increases in security without corresponding significant increases in cost. Users do what they would do normally, but they make security decisions in line with a common understanding of what security means to the enterprise. Successful security must be integrated into the work habits of those who are expected to keep the enterprise information safe. If this is done, enterprise information security will be "good enough" to protect critical enterprise assets.

References

[1] Slater, D., *The ABCs of New Security Leadership*, 2004, February 17

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

[2] Townley, A., *The Philosophy of Enterprise Information Security*, Information Security Bulletin, Volume 10, Issue 5, June 2005

[3] Sandhu, R., *Good-Enough Security: Toward a Pragmatic Business-Driven Discipline*, IEEE Internet Computing, January-February, pp. 66-68, 2003

[4] Dourish, P., Grinter, R.E., Delgado de la Flor, J., Joseph, M., *Security in the wild: user strategies for managing security as an everyday, practical problem*, Personal and Ubiquitous Computing, 8(6), pp 391-401, 2004

[5] Bunker, E., *Business Practical Security - How a Pragmatic Approach Enables Better Risk Management*, 2003

http://www.criticalwatch.com/press/businesspracticalsecurity.pdf

[6] SABSA Institute, *The SABSA Method*

http://www.sabsa-institute.org/sabsa_method.htm

[7 ZIFA, *Zachman Framework*

http://www.zifa.com/framework.pdf

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

[9] Wilson, P., *'Top-down' versus 'Bottom-up' - Different Approaches to Security*, 2003, December

http://www.insight.co.uk/downloads/presscoverage/Top%20down%20versus%20Bottom%20Up%20(Network%20Security).pdf

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

[11 Pogue, D., *How Susceptible Is Your Operating System to Viruses?*, 2003, September 18

http://www.nytimes.com/2003/09/18/technology/circuits/18POGUE-EMAIL.html

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

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

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

[14 Jaques, R., *Bots and adware top threats for 2005*, 2005, January 4

http://www.iwr.co.uk/news/1160264

[15] Symantec, *Symantec Internet Security Threat Report Highlights Rise In Threats to Confidential Information*, 2005, March 21

http://www.symantec.com/press/2005/n050321.html

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

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

[17] Jaques, R., *Consumers make it easy for e-commerce hackers*, 2005, April 18

http://www.vnunet.com/news/1162529

About the Author

Andrew S. Townley is a Manager 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.