

# **FUNDAMENTALLY INSECURE: DEBUNKING 10 MYTHS OF INFORMATION SECURITY**

## **THIRD EDITION**

**BY ANDREW PLATO, CISSP OF ANITIAN ENTERPRISE SECURITY**

**COPYRIGHT © 2004-2005 ALL RIGHTS RESERVED**

Information Security has become a billion-dollar a year industry. In 1996, when I began working with security technologies, most organizations spent less on information security than they did on coffee. The irony is that this has not changed much. Although information security is generating a tremendous amount of interest and focus, the fact remains that most organizations are not investing in real information security improvements.

The ultimate reason for this is a common problem – hype. Information security is merely the dot.com hype of the 2000s. In 1996 everybody was going to get rich selling basketballs and pet food on the Internet. Now those same people have suddenly become experts in how to secure complex business systems. It's not with a touch of irony that some of the same people, who could not make Internet dot.coms work, are now promising to secure networks from intrusion.

### **Rationale for this Paper**

Hype is a double-edged sword. While information security hype has generated tremendous of interest, that hype has also generated a lot of misleading information (and misleading individuals.) For the past decade, I have worked in information security in many different roles. As the owner of an information security consulting firm, I have had the opportunity to see security from many different perspectives.

Over time, I have found our consultants and projects routinely combating a growing number of misunderstandings and misconceptions about information security. This has lead to numerous discussions and debates among peers about the role of information security in organizations. The common complaint was that a lot of people are getting a skewed view of how information security functions within an organization. The origin of these misunderstandings were from numerous sources. Security amateurs, technology vendors, and general ignorance seemed to be the most common culprits.

This paper is therefore the culmination of Anitian's research and analysis of these common misconceptions. Our findings are based upon our experience with Anitian's customers as well as discussions with peers in the information security community. This paper distills down ten of the most common misconceptions, or myths of information security.

## Assumptions

It is important to understand our assumptions regarding information security and technology as you review this paper. Like any analysis, we approached this topic with a series of assumptions. These are:

- **Security must be balanced with business and personnel issues.** Good security is a balancing act between diverse and sometimes disparate issues within an organization. Information security is not solely a technology or management problem. It affects all aspects of an organization.
- **Security must be practical and transparent if possible.** Strong security measures pose as little disruption to an environment as possible. Based on my own experience, security measures that are cumbersome or overly complex will be ignored. Thus invalidating whatever benefits those solutions might have provided for the organization.
- **Technology is only as useful as the user.** Technology is a tool, and a tool is only useful when it is in the hands (figuratively) of a competent user. Likewise, a powerful tool in the hands of an inexperienced or negligent user can be dangerous or detrimental.
- **Bias and inexperience lead to bad decision-making.** Most bad decisions come from people rushing into things too quickly or being misled into a solution based on faulty recommendations. People with obsessions over technology are much less likely to analyze a situation logically and rationally. They will see every issue in terms of their own agenda.
- **Given a choice between security and productivity, most organizations choose productivity.** This may seem like common knowledge, but it is also supported with a vast array of scientific data. Organizations, especially developing ones, view security as a nuisance. Ultimately, this is a reiteration of the second assumption on this list. If security measures are overly complex, companies will ignore them and place productivity over security.

As you will see, these assumptions tend to color the ideas and concepts presented in this document.

## Myth 10 – Open Source is More Secure than Commercial Software

John Viega, the author of the *Secure Coding Cookbook* (O'Reilly, 2004), wrote an excellent article titled *Open Source Security: Still a Myth* for O'Reilly's web site where he discusses the myths of open source security. In the article, Viega discusses the open source maxim of "many eyeballs." The concept basically states that the more people there are that look at the source code, the more likely security weaknesses will be discovered.

While this theory may be conceptually solid, in practice it does not hold for open source. The fact is, not very many open source users EVER look at the source code. There is minimal, if any, troubleshooting done by the grand majority of users.

This issue was recently illustrated in the problems that afflicted Sardonix. Sardonix was online "community" that provided a central point for the open source community to audit open source code and report flaws. It was a great idea and won high-praise and plenty of news coverage. Sardonix turned out to be flop. Few people ever submitted any reviews. Most of the content on the boards consisted of people *talking* about secure code. Few, if any, ever actually conducted comprehensive security analysis of code.

Sardonix's failure is a quick lesson in the central problem of group dynamics. It is easy to talk about doing something. Buckling down and actually doing the work is much harder. Most people are unwilling to make the leap from talk to action, unless there is something to be gained (like money). Sardonix was going to offer a rating system where top analysts could earn praise and bragging rights. Apparently, that was insufficient to compel the open source community to audit their code. Communities need leadership and incentive to propel themselves forward and accomplish great things. Open source has a dearth of both. Leaders are few and far between and incentive has always been a problem. It's hard to get people to work for free.

In fact the majority of security holes in applications, both open source and commercial, are being detected by security manufacturers. Since 1999, Internet Security System's (ISS) research group, X-Force, has detected and reported over 55% of the "high" level exploits to both commercial and open source technologies. ISS is rivaled by other commercial security companies including eEye Digital Security and @Stake. Only a tiny fraction of the "high" risk vulnerabilities discovered since 1999 have been the result of individuals or open source groups. The open source community is simply not auditing their own products. They are leaving that up to customers and for-profit organizations – sound familiar?

For years, the main complaint open source advocates leveled against commercial software providers was that the commercial companies turned customers into de-facto security auditors. By releasing incomplete, unaudited technologies that nobody could open up and look into the source code, the commercial providers were in effect saying "trust us to be secure." And trust is supposed to be verifiable.

This has changed. Commercial software vendors have a strong, central motivating force – money. Insecure software scares away customers. And customers are beginning to demand more secure software if they are going to shell out money for technology. This has forced almost all commercial software providers to begin conducting comprehensive security reviews of their applications before they are released to the public. Software vendors have started investing in secure coding and testing practices. Even software goliath Microsoft, who is often the focus of open source ire, has started to invest heavily in security methods.

Furthermore, merely having the potential to be more secure does not mean a technology is actually used in a secure manner. You could lock a Windows® 95 machine in a Fort Knox vault and it would, arguably, be more secure than any Linux box on the Internet. Of course, it would not be terribly useful.

The ultimate measure of any technology is not its “potential” for security, but its actual security. Actual security is the result of many factors including design. However, how a system is implemented, managed, and used has a considerably more profound impact on the security of a system than its design. A well-designed system can become totally insecure if it’s managed or implemented in an insecure manner.

Furthermore, the total numbers of vulnerabilities that exist for a technology are not terribly meaningful yardstick for security either. A system that is maintained well with good access controls, adequate security logging, and routine patching, instantly mitigates this problem completely. A product could have thousands of vulnerabilities, but if they are all patched and/or mitigated, then those vulnerabilities are not a factor any longer. This applies equally to open source and commercial products.

So what is the result of this? Should you avoid open source technologies? No, of course not. Open source technologies offer a veritable bounty of outstanding tools. Some open source products are arguably many times better than their closed source cousins. Apache, for example, is widely considered a more secure web server than Microsoft’s Internet Information Server (IIS). The point of this myth is not to discourage the use of open source technologies, but merely to place them in perspective.

## **Myth 9 – Some Organizations are not a Target of Attacks**

This is just a patently false statement, and it is something I hear an awful lot. People are constantly misleading themselves into thinking they are protected with a little mantra of, “we’re not a target” or “we don’t have anything they want to steal.”

During a recent presentation Anitian sponsored in Seattle, Washington, I had the opportunity to speak with some noted information security experts. One of those experts was Patrick Gray from Internet Information Systems. He was a former FBI investigator who helped track down hackers over the past few decades. According to Mr. Gray, when hackers were asked “why did you do it?” the number one answer was “because I could.” Interestingly, the second most common answer was, “because my boss is an <expletive deleted>.” Most hackers do not care about your systems. The fact that you process or store boring or low priority information does not make you more secure.

Denial is also not a replacement for security. And denial extends to the corporate board. Ignoring security or pretending that it’s not a big deal for your organization is basically asking for problems.

Furthermore, even the existence of security protections does not necessarily lower your target profile. New intrusions are coming out that specifically target information security. In June, 2004, an exploit was discovered that attacked Symantec security technologies and anti-virus. Cisco, ISS, McAfee and many others have all seen worms directed at their technologies.

Complacency is a dangerous problem that can infect organizations of all sizes. Security demands a certain level of constant vigilance.

## Myth 8 – Patching is Critical

Patching operating systems has become a metaphor for the fundamental problem with information technology. If systems were designed and built to more exacting standards and there was an expectation on organizations to manage and use those systems in a diligent and responsible manner, patching would become a casual process; not the mad dash to plug the holes that it has become at many organizations.

The real problem is ultimately an issue of conflict of interest. Too many organizations are depending on patches from the manufacturers to solve security weaknesses. Yet manufacturers have a compelling interest in NOT patching systems until it's almost too late. Microsoft has rolled back their "patch at will" process just recently and moved to a regular monthly patching process.

Thus, organizations are now placing the security of their organization on the good will of a manufacturer to get the patches out in time to prevent the propagation of a serious attack.

The patching problem is further compounded with the shrinking amount of time between when new vulnerabilities are discovered and when exploits are released. According to a September, 2004 report from Symantec, the average time between the discovery of a new vulnerability and an exploit being released has decreased down to 5.8 days. Most organizations are struggling with basic project management issues. The idea that an organization has the ability to identify and correct such a problem before it is in the wild is absurd.

In 2001, I decided to test the concept of patch mania. I started with the theory that a properly secured system could be installed on the Internet and never need patching. I installed a Windows 2000 server with Service Pack 2 for use as a security appliance. The system was hardened such that no unnecessary services were exposed to the Internet. Access controls and restrictions were enforced on the system such that no processes were allowed to run without explicit credentials. The system ran for 337 days straight without any intrusions, downtime, or faults.

Now it is unrealistic to expect every organization to harden their systems to the point where access is so limited. However, the current patch mania is not working. The ideal way to manage systems is such that patches can be tested first and then rolled out when IT staff can dedicate the resources. Fortunately, many security vendors have seized upon this problem and now infuse host-based security technologies with the ability to defend systems from vulnerabilities before patches are released. ISS, for example, has led the way with their desktop protector agents, which can proactively defend a system and give IT administrators some time before patching. This is a nice capability (for a price of course) and offers organizations to get control over patching and have it return to a non-critical function.

## **Myth 7 – Security Should Be Easy**

This is the first of many rants against the technology manufacturers and vendors. Somewhere between their power lunches and pipeline reports, sales people for the technology industry realized that promoting products as “easy to use” was a great sales tactic. Whether those claims are actually true or not is essentially a matter of personal opinion. When challenged on the complexities of their products, the sales people will sheepishly counter, “Well, it’s easy for me to use.”

Behold the power of marketing to transform any intricate, complex, or nuanced problem into a sound byte. I realize that marketing is a necessary evil. Companies always want to make their products look good to customers. But the “security is easy” routine is causing more problems than it purports to resolve.

Security is not easy. Marcus Ranum, Bruce Schneider, and all the other security experts have all said similar things. Security is a difficult and often daunting challenge that deals with a great deal of gray areas. And while it is always preferable when engineers make complex systems more easy to use, a simple GUI does not mean security can be relegated to the janitor. You can put a child in front of a microscope, but that does not mean they are a biochemist. There is a little more to being a biochemist than wielding tools.

Security is in the details. One error in an application can render an entire system insecure. Thus, simplifying those systems where many of the details are hidden is the anathema to security. This leads to the “Default Disease.” That is, organizations installing and using complex information systems in “default mode.” They never learn the system at a layer deeper than the GUI.

Running is not the same as running securely. A server may function just fine and dish up web pages in a diligent manner. Yet, if the system has an insecurity that is exploited, it could stop running quickly, or worse, start running something it should not be running.

Organizations need to take claims like “our product is easy to use” with a grain of salt. “Easy to use” does not mean “easy to secure.” A technology might be easy to setup or install. That does not necessarily translate into security of the organization being easy.

## Myth 6 – Awareness will Make Us Secure

One concept that gets a lot of talk among security people is security awareness. The idea is that if your executives, users, and the public are aware of security issues, then they will wake up and start taking security seriously. Unfortunately, experience has shown this is seldom the case. Being aware of a problem does not mean people are doing anything to resolve it (see Myth 10 and the concept of “many eyeballs.”). In fact, awareness without a solution is almost worse than flat-out ignorance.

Talk is cheap. People find it more entertaining and satisfying to talk about what they are going to do then to actually sit down and do it. This is especially the case in organizations where there is no incentive for IT people to take risks. Holding meetings and attending classes is fun. Reconfiguring 100 servers to prevent theft and fraud is hard. That takes time, and there is risk. A server could crash and cause somebody to scream.

This problem is exacerbated by the overall vagueness and impracticality of the security standards which are supposed to help organizations translate awareness into action. ISO17799, CoBIT, and Common Criteria are all very interesting to read. They have great ideas and content. Unfortunately, the information within them is rather arcane. Without some training in security, it is extremely difficult to implement these changes. Consider this example from ISO17799:

*Changes to information processing facilities and systems should be controlled. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. Operational programs should be subject to strict change control. When programs are changed, an audit log containing all relevant information should be retained. Changes to the operational environment can make an impact on applications. Wherever practicable, operational and application change control procedures should be integrated (see also 10.5.1). In particular, the following controls should be considered:*

- a) identification and recording of significant changes;*
- b) assessment of the potential impact of such changes;*
- c) formal approval procedure for proposed changes;*
- d) communication of change details to all relevant persons;*
- e) procedures identifying responsibilities for aborting and recovering from unsuccessful changes.*

That is all good advice. However, most organizations have trouble keeping track of their pens, let alone tracking every change in the environment. Being aware that change control is important is not the same as actually performing change control. Somebody has to put all that awareness into action. Otherwise, the awareness is wasted.

Further compounding this problem is the prevalence of “high-talkers.” That is, consultants, advisors, and trade-show presentations that present information on high-level, strategic issues and ignore how to translate that information into the operational or day-to-day functions of an organization.

It gets worse. Awareness can also lead to liability. If you are aware of a problem and do nothing about it, then you are liable when that problem leads to something bad. Awareness of a problem is a common thread in all corporate liability lawsuits. If an organization knows they have security issues to handle, but fail to fund or support those initiatives, then they become liable for anything bad that happens as a result of security weaknesses.

If your organization is not translating awareness into action, then you might as well go back to being oblivious. Ignorance might not stop the long arm of the law, but at least you can enjoy the bliss before you get caught.

Awareness is good. Acknowledging that you have security issues is the first step on the road to correcting them. But awareness is a first step, not the only step. Put that awareness into action.

## Myth 5 – Regulations are Important

A handful of security-related regulations have created more FUD (fear, uncertainty, and doubt) than all the crackpots on the Internet, worried about raw sockets. Regulations like the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley have created a whole subculture of consultants and advisors to support the provisions of these acts.

At the core of all of these regulations is the idea that businesses should be responsible and diligent with their information systems. What is disturbing is that regulations like this even need to exist. Businesses should already behave in a diligent and responsible manner. Unfortunately, as the recent accounting scandals have proven, most corporate boards are clueless about the function and operation of the business they oversee. This cluelessness filters down the chain until everybody has ignored the problem.

In all fairness, GLBA, HIPAA, and Sarbanes-Oxley are necessary evils. They do offer incentive to prod corporations in the right direction. And ultimately, that is a good thing.

However, if you read the regulations you quickly realize that they are fairly vague in what they recommend for information security. The HIPAA regulations are probably the most specific. But once again, without some training in security, these issues can be very arcane:

Consider this excerpt from the HIPAA regulations:

*(ii) Implementation specifications:*

*(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.*

*(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.*

*(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.*

*(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.*

*(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.*

Again, this is very good advice. But honestly, an organization should not need a government regulation to tell them to run backups. If an organization is turning to government regulations to tell them how to run their business, then the organization has larger problems than failing to meet the criteria of those regulations.

Regulations are only important for organizations that are being irresponsible about their information systems. If you are being diligent and responsible, the regulations become *almost* irrelevant. Regulations are important, to a point. Avoid the temptation to base your information security standards or issues solely on regulatory pressures.

#### Myth 4 – Technology will Make Us Secure

About a year ago, I was flipping through a magazine and came across an advertisement for a security technology. The ad was for a particular brand of firewall. In huge, black letters the ad confidently stated:

**If you're not using <name withheld>, you're not secure.**

The hubris in such a statement is matched only by the sheer nonsense of its content. I realize some marketing person thought this was a bold statement. It is also an insulting and completely misleading statement. It assumes that their product (or the reseller who will hook you up with this product) has transcended all complexity, hackers, and business processes and can now deliver you a product that will secure your network so you can go fishing all afternoon.

Technology is too often relegated as the solution for all of an organization's ills. "Do you have users abusing the Internet? Just buy this rack-mounted, best-of-breed, high-performance box of wires that will magically turn all of your employees into productive little automata."

Technology is a tool. And tools are only as good as the user. A kitten at the console of a nuclear submarine does not mean our country is safe. Likewise, an unskilled, overworked, underpaid, uninterested, semi-disgruntled, machine-gun owning employee armed with megatons of security equipment does not mean your organization is safe and you can go back to fishing all day. People need direction, motivation, and focus. Mostly, they need somebody demanding them to be qualified and skilled at the systems and technologies they are managing.

Compounding this problem is the lack of useful post-purchase help. Technology vendors have become so focused on getting you to buy their technologies, that once you have bought them, they have little incentive to actually make them work. This results in poorly implemented, poorly managed, or unused systems that are not delivering even close to what the vendor promised.

Before working as a security consultant, I worked as a technical writer. One day I noticed that a customer of mine was investing \$3,000,000 into marketing their new product. Yet they were only willing to spend \$200,000 on documentation and training. That was the moment I realized that getting people to buy a product was valued far more important than getting them to use the product. And the network of resellers and integration partners that push these products have fallen completely in-line with this mentality. Once you have signed the purchase order, they could care less if it works.

What is the answer? People. Technology does not solve security problems. People using technology in the right way solve security problems. Invest in your people and hold them to high expectations. Pay them what they are worth and train them well. A single qualified, motivated, experienced person can have a more profound impact on security than all the boxes of wires in the world.

### Myth 3 – All Software has Security Flaws

A few weeks ago I was flying home from a business meeting. Somebody had left a copy of one of those entrepreneur magazines in the seat pocket. Without anything to do, I flipped through the endless number of pyramid schemes and other get-rich-quick nonsense. The magazine had an article about information security.

A line in this article really struck me as oxymoronic:

*Since software isn't finished before it is shipped, software companies continually offer bug fixes, security patches, and new features.*

How many people buy something that is not finished, use it for a while, and hope the manufacturer will fix it eventually? Or more appropriately, imagine going to the store and purchasing a stereo. When you get home, the stereo works, but a huge arm comes out at night and unlocks all your doors and feeds your dog antifreeze. Would you want this product? So why are you purchasing or developing software that could do the same thing to your company?

The notion that companies are shipping unfinished products is not new of course. The technology industry is notorious for making the users become unwilling participants in mass beta testing.

Unfortunately, this lax attitude toward software often extends into internal development resources within organizations. Since Microsoft releases buggy software, developers then feel that they, too, can release applications that are only mildly tested.

In all fairness, there is a shred of truth behind this myth. The sheer complexity of modern technologies dooms them to be in a constant state of repair. It is understandable that technologies have to undergo periodic maintenance and improvement. It is also understandable that no organization can spend an eternity testing new software.

The problem is really one of attitudes. Organizations too often see software as this isolated package that gets installed on a machine and either works or does not work. Therefore, companies have designed their development processes around maximum functionality and marketability. This is ultimately why people have become tolerant of buggy software. If the software works, they do not notice the fundamental security flaws that exist until it's too late.

This is coupled with the fact that many organizations do not test or evaluate software before they buy it. They become enamored with the features and potential of the software and fail to address the realities of using it in their environment.

The solution is once again a matter of diligence. Organizations must become more diligent in deploying software. And software manufacturers need to be held to higher standards. It's not acceptable to release software that works, but contains hidden weaknesses that allow exploitation.

## Myth 2 – Security is an Endless Journey

Even Frodo from the Lord of the Rings made it to Mt. Doom. Sure, it was an epic journey, but all good things must come to an end. Securing an organization can often seem like Frodo's journey, full of Orcs, Wraiths, and other assorted creatures. Yet at some point, you have to reach an end and say, "We have arrived."

All journeys have points where you stop and assess your situation. Even Frodo stopped and questioned his journey. Likewise, organizations need to stop and examine their progress.

The genesis of the "security is a journey" concept is clearly from the amateur ranks of security consultants and other self-proclaimed experts. End points are frightening concepts for people who do not really know what they are doing. If you stop and assess what you are doing, it may become painfully obvious that...you do not know what you are doing.

Companies and governments have long accepted that they must manage risk. The entire insurance industry is built upon the foundations that risk is inherent in everything and you can pay somebody to assume that risk for you. In order for any company to survive, it must engage in some kind of risk management.

Yet if you walk around the server rooms of America, risks are everywhere. And nobody notices or talks about those risks. They just exist. They are never analyzed, reviewed, or managed. The result is this journey mentality; that risks do not, or cannot, be properly analyzed because they will just keep changing and evolving.

It is understandable how people then get into this mode. Security threats are constantly evolving. New worms, exploits, and hacker tricks are being invented everyday. Yet almost all of these problems boil down to the same kinds of risks. If organizations would start thinking in terms of risks rather than individual threats, they would realize that there is a finite and rather static set of risks. If those risks are being mitigated or assumed, then you can arguably reach a conclusion. Sure, the management and the maintenance of technologies require constant attention. But that process can reach a point where you can reasonably ask some basic questions like:

- Are we more secure this year than last year?
- How many risks have we mitigated this year?
- How many risks have been problems this year?
- Have we become more productive?
- How have we saved more money?

If your IT department cannot answer these questions on an annual basis, then perhaps they need to go to Mt. Doom and talk to Sauron.

**Myth 1 – Trust Us**

One day, you decide to take a vacation to Hawaii. You arrive at the airport. At the gate, you notice the pilot waiting to board the plane. He walks over to you and strikes up a conversation. He talks to you about his airline's amazing stock performance this year and how many customers they have. He boasts about some new initiatives they have this quarter to make customers buy more plane tickets. Then he tries to get you to upgrade into First Class for just \$99.95 more. When you look at him perplexed, he says, "Hey, what is it going to take for me to get you into first class?"

We trust surgeons to operate on us, not sales people. We trust pilots to fly planes, not sales people. Why then would you trust the security of your organization and its valuable assets to sales people?

Sales people have a challenging job. It can be very difficult to build up a customer base and meet quotas. And unfortunately, many organizations treat their sales force poorly or make unrealistic expectations of them.

I put this myth at the top of the list because it is the most sinister and pervasive problem in the technology and security industry. Organizations get mired in a sort of "vendor funk" that infects them whenever a new sales person comes out to visit them. Sales people are masters at convincing organizations that they have problems they may or may not actually have. It is easy to forget that most salespeople do not care about your security, smooth operation, or responsible business practices. Salespeople just want you to buy something. And frankly, many of them will tell you exactly what you want to hear.

While good sales people are very knowledgeable about the products they sell, they are rarely qualified to design complex information security solutions. Most sales people get the bulk of their information from marketing material. This makes them good to tell you the basics of a product or service, but rarely can they delve into the details of a technology. Moreover, most sales people lack the expertise to handle a complex business governance issue.

Sales people are also masters at compartmentalizing problems. If you approach them with vague problems (like security), they will solve them with whatever equipment or service they can sell you that yields the largest commissions. Security is not a single technology, service, or policy. Security is a state you strive to attain through a combination of many things. You cannot simply buy equipment or services and become secure. You must expend both capital and intellectual effort, and then you will begin to move toward a more secure and reliable environment.

Another trick sales people play is the price game, and a lot of organizations fall victim to this game. The idea is to get everybody fighting over price, and not value. Price is an easy fight to win, especially for big, discount resellers who just move products. And the organizations that fall for this game wind up with lots of cheap products, but no skills to make them work. These places know the price of everything, but the value of nothing. Rather than become a slave to this price game, try to focus on the value your organization is receiving from products and services. Make vendors and consultants talk about their value proposition. Why they are better and how they will improve your business. This will rapidly weed out the people who just want your money.

Vendors and resellers are an important part of building a secure IT department, but choose them wisely. Do not let sales people mislead you into solutions that are not right for you. Sales people exist to help. A good sales person does not pressure you into a decision or mislead you with meaningless metrics. He/she helps you get the information you need to make an informed decision. A really good sales person genuinely cares about your business and satisfaction and will earn your trust.

However, remember that trust is more than just a word on a brochure. Just because somebody wears a vendor's shirt or works for a big reseller does not mean they know what they are talking about. Trust is something that is earned and it's based on a person's (or company's) credibility. Would you trust a pilot who is more interested in his golf swing or the condition of his aircraft? We trust people who can demonstrate their expertise with consistent results. We trust companies because they can deliver what we want and add value. Stock value, total sales, number of employees, etc. all are misleading metrics of success. They don't demonstrate capability or ingenuity, just size. And big, is not always better.

The core of this problem is bias and hidden agendas. Sales people have an agenda – selling. You have an agenda – to become more secure. And those two agendas do not always align properly. People's biases and their agendas color their advice and decisions. And bad decisions come from people who fail to critically analyze the information before them. Some sales people and vendors expect and depend on you not critically analyzing your options.

Lastly, when you need to secure your business, you need to be prepared to handle a lot data that does not always lend itself to clear answers. Security is all about “gray areas.” There are no clear cut answers. And “gray areas” are where both bad and good ideas and decisions lurk. This is why trust must always be earned.

## Conclusion

The last point for this paper is to summarize the main themes of this paper. You may have noticed that I touched on these concepts multiple times throughout this presentation:

- **Practice *risk management* rather than *threat avoidance*.** Analyze the risks to your organization and find ways to mitigate, eliminate, or assign those risks. Do not try to just plug holes with technologies or solutions that merely patch up threats.
- **Build IT and security operations that focus on *personal responsibility* and *accountability*.** Require IT people answer to their environment and its security. Train IT staff to be experts in their area and hold them accountable to understand not only the technologies, but how they serve the organization.
- **Balance people with technology.** Invest in your people and their skills. A single skilled, intelligent, and motivated IT person can be more valuable than racks filled with equipment. However, technology works 24 hours a day, people do not (at least not for long). Parse off mundane tasks to technology, and require your people to analyze and master the output of those systems.
- **Chose your partners carefully.** Some resellers, vendors, and security amateurs have a vested interest in misleading you. Pay attention to the priorities of your partners. Are they more interested in selling you a technology or helping you build a better organization? Experts are involved in your business and their profession. They take their jobs seriously and make your needs a priority. Also, avoid looking solely at the price of technologies and training. Address the value things will provide your organization. Buying a firewall for \$5.00 less at some discount store might seem like a good business decision at the time, but can that shop support you when you need help? You may be better off to pay a little more and work with a specialist that has a long history of expertise with the technology you are using. Expertise is ultimately more valuable than any single piece of technology.
- **Security is a game of *gray areas*.** Be prepared to deal with issues that do not lend themselves simple answers.

If you have any comments or suggestions about this paper, please contact me at [andrew.plato@anitian.com](mailto:andrew.plato@anitian.com).

*NOTE: None of the companies or organizations mentioned in this document sanctioned, prompted, or compensated Andrew Plato or Anitian Enterprise Security in any way for this document. The opinions in expressed in this document are those of Andrew M. Plato.*

*This document is the exclusive property of Andrew M. Plato and the Anitian Corporation. Redistribution is permitted; provided the contents are not altered in any way and Andrew M. Plato and Anitian Enterprise Security are clearly noted as the authors.*