General Misconceptions about Information Security Lead to an Insecure World

It is becoming clear that Underground Hacking Industry as a whole (not just individual hackers) is continually gaining ground despite best efforts of Information Security Industry. It seems that the latter should have an overwhelming advantage - a multi-billion dollar industry staffed with hundreds of thousands of security professionals. However, the efforts of the Information Security Industry are almost always reactive, and in most cases amount to losing ground on the defensive. The unfortunate and seldom acknowledged truth is that the Underground Hacking Industry is always one step ahead. Why are we so slow to respond when all evidence indicates that such delays lead to enormous business losses? Is it possible that the fundamental way our Information System Security is organized has some inherited deficiencies, which are prohibiting us from successfully mounting an effective defense?

Today’s losses are becoming too great to say that we are just in need of some evolutionary improvements. Instead, we need to reevaluate the way we go about security business as a whole. In the following article, we are considering various processes common to both Information Systems and Information System Security based on both well-known cases and personal experience. This is our initial attempt to analyze how Information System Security is organized, and to suggest some core changes to its processes.

What is failing?
Continued information security failures are raising questions not just about security mishandling in such poster cases as TJX, but also whether basic Information Security (InfoSec) concepts as we know them are correct. Today there are far too many cases of such failures to simply place all the blame on sloppiness of just a few individuals.

For instance, let’s take a look at the recent FBI security assessment [1] and Department of Homeland Security problems [2]. It is very likely that both FBI and DHS invested heavily in their security infrastructures and have put a very sophisticated security programs in place… and yet, both have failed.

We would posit that the main problem is in the existing relationship between “Business Management” (BusMan) (which is coupled with Information Systems Management) and Security Management. For years this has been structured as a “subordinate” relationship, and that it is entirely incorrect. (Mental note – did you even question who is the “boss” in that relationship?). We will try to disprove this fundamental concept of corporate security management using some real life examples.

As a practical reading regarding corporate security management and “TJX case” in particular, as well as to gather some opinions, please refer to Bob Sullivan’s article on MCNBC.com [3]. The information presented in the article and following public opinion can help shed some light on the discussion below.

**Who holds the money?**

The need to separate Information Security (InfoSec) from Information Systems (InfoSys) and how to best do it have both been the topic of much debate in recent years. So far, however, there
is no universal solution to implementing the “separation of duties” to serve organization’s business and security needs.

In a small organization, you would typically see the same person taking care of general information systems services as well as other aspects of security. Enterprise level organizations with larger scale concerns about security can afford to and usually do keep two independent services in different branches of management. (However, it is not what US Government would agree with. In the case of DHS failures, CIO was responsible for InfoSec. Are they saving some money by integrating security in InfoSys?)

While we do not question that the two information services should be divided, it is further our contention that it does not matter how the division takes place on the management level.

The real issue is that there is no separation of the BusMan, who holds the money, from InfoSec. In most of literature discussing InfoSec we find the very popular opinion that InfoSec should always seek a good relationship, support, and understanding from BusMan for its planned activity. This is, to put it bluntly, because the “boss” can stop the flow of money.

The logical question to ask then is should the security of an organization, be it large or small, always depend on limited technical expertise and understanding of security matters of a business manager? This is especially troubling today where the complexity of both security systems and the threats they face can frequently be beyond the understanding of a manager with a very basic technical education covered in an MBA degree. An example of such managerial control is the “TJX case” and others. Please see the Bob’s article [3] and following discussion for examples of how the management and security personnel differ in their opinions about the security situation at TJX.
Why are we late?

Next, let’s discuss why InfoSec is frequently late in securing business assets. To illustrate, we would like to discuss a real life example.

L worked as a security analyst in a US government organization. During a routine scan for network vulnerabilities, L found 60 computers with blank administrator password. The network had several thousand computers, and roughly 1% seemed like a rather significant number. Moreover, considering that these computers were completely defenseless from unauthorized access (i.e. backdoor planting, deletion of the entire operating system, data theft/manipulation, etc.); it was a gaping security hole.

The decision was made to take up the case and to begin a course of action as required by the security manuals and procedures. L informed concerned users, departments’ ISSO, gave recommendations for a fix, and actively participated in the process by answering questions and logging activities. In general, changing administrator’s password takes approximately three minutes. The affected computers were distributed around the campus within a few buildings, at a reasonable pace, without the situation being handled as an emergency, it could take a couple of days for a single technician to walk around and fix all of them.

In the case discussed, however, it took the users and local security personnel exactly sixty days to fix sixty local machines sitting next to them. Given the magnitude of the failure to act in this example we began to seriously think about why officially approved and seemingly logical procedures are not working as expected.

Granted, most procedures do not consider the potential latency of the “human factor”, but even taking that into account, the situation described above took an unacceptably long period to remedy. We can refer to this as a “60-60” Rule: multiple management levels affecting security
delays exponentially. How did we end up with “rules of engagement” (policies, procedures, manuals, etc.) which result in a “60-60”? – see below for further analysis.

Local or global focus and the magnitude of the problem
Let’s consider the case in question from two disparate points of view. First, we can look at it from a purely InfoSys perspective. A blank password does not prevent a computer from functioning. A user can do his or her job, and the issue of a missing password has no effect on local business functions. There is no pressing need to fix it as quickly as possible using any and all available resources. Of course, any system administrator will tell you that having a blank password is not good idea, but the argument will be security not business based.

From InfoSec standpoint, having a blank password creates a huge exposure and should be fixed as soon as possible. Unsecured access to a machine located on a shared network could affect not just local computer but other parts of the network, potentially extending to the Internet around the world. One could say that “the world” argument is not brought up very frequently and is therefore perhaps not as compelling as risk to local systems. However, we do routinely configure our firewalls to prevent outgoing DDoS attacks, as well as block malware sent from our email servers to others.

The fact is that we do actively try to avoid polluting the outside world. And it is frequently not just for altruistic reasons. For example, no company wants to have their mail server blacklisted because a malicious intruder was able to send spam from a compromised corporate email server. Similarly, no one wants to incur the exorbitant bandwidth costs because hackers managed to launch a DDoS attack from a company’s PCs.

From this we can draw two important conclusions:
- InfoSec considers local, and as well as global interests while InfoSys approach almost always focuses solely on local business interest.
- The same issues that are not considered problematic from the InfoSys point of view could potentially present far-reaching problems for InfoSec.

**Home grown InfoSec**

InfoSec came about as a part and parcel of InfoSys, and subsequently, the style of management (goals and approaches) of InfoSys (more precisely – BusMan) has been accepted as a default for InfoSec. This resulted in a traditional “subordinate” relationship. In the case outlined above, this approach meant that InfoSys resolution style of slow multilevel response embedded in the security process virtually guaranteed to result in the “60 - 60” rule. Once we have been watching for four weeks as InfoSys services were installing a computer to start a consulting job. It was not the US government organization in this case. However, multi-layered structures with many dependencies tend to all act in the same way leading to the same problems.

Unfortunately, to date most security procedures have been created based on the InfoSys experience and with local business focus. It is still a widely accepted view that InfoSec exists only to “serve local business goals” and this opinion still prevails when security professionals discuss the issues they face.

**The case for reconsidering a partnership**

Today's businesses can no longer divorce themselves from or ignore issues of security. Companies all over the world are connecting to the Internet in the normal course of doing business. Global economy is based on the global access to resources. If Internet is crippled
because of our lack of attention to the security issues it faces, the global economy will suffer a major blow. A lot of information security problems come from outside the companies that end up dealing with them. And that means that what is happening in my backyard can easily affect others half a world away and vise versa. While remaining largely insignificant from business management point of view, a security event can pose a real threat to the company's livelihood, and other businesses as well. *The goals of business growth and security have become equally important.*

**What does the future hold?**

*When it comes to security issues, the time of slow, multi-layered response must come to an end.* Let's consider what an appropriate response to the password issue would be if the security administrator had a real Information Security standard in hands. Ideally, within a few minutes all the affected computers would be disconnect from the enterprise network as they represent a significant local and global danger. Next, the affected parties would be notified about the steps they need to take getting their computers back online. “ Interruption of business” concerns would be considered irrelevant at this point, because they would be overridden by the security concerns over possible security repercussions of leaving the unprotected computers connected to the internal network as well as to the world at large. From a non-InfoSec perspective, it may seem like an extreme reaction. An interim solution may be a group-wide email to soon-to-be-affected users (one hour delay) followed, one hour later, by a shutdown of the computers whose users did not report having fixed the problem. Even though the interim response assumes a risk of roughly two hours of grace period for the users, it is still infinitely more acceptable than a 60 day lag to fix 60 computers.
The age of local-centric thinking should be passing away as well. We would consider one more example to prove our case. Company X did not upgrade its anti-virus software, and its computers have been infected. Then, using this company’s email system, the virus has been transmitted to Company Y. Sloppy work of local systems administrators in Company X directly affected business of Company Y. We don't need to be concerned right now about why Company Y was not secured to such an attack in the first place. Company Y suffered measurable losses and, if those losses are significant enough, a simple case of negligence by Company X can morph into a lawsuit for damages by Company Y. This situation would not even be discussed within the scope of Information Systems, as they are considered local and cannot, in general, damage each other.

Risk estimate

Now, we would like to discuss what happens when an InfoSys application is transferred into security domain without appropriate considerations of underlying methodology, and thus setting false expectations in InfoSec.

Risk Management (RM) is considered to be one of InfoSec’s cornerstones. It traces its origins to financial applications, where it is generally possible to collect statistics and to then create a model to “measure” your progress in finding an optimal solution. Plenty of financial information is publicly available. A statistical model would consider a finite number of random financial variables (like stocks) and random events (weather, politics, speculations, etc.), as well as statistical dependencies between events and variables, affecting financial variables. Ideally, a model should have an infinite number of events and dependencies; otherwise it will fail in prediction sooner or later.
In the InfoSec world, we have a fairly similar situation: threats (factors), dependencies, and financial losses – exposures (asset value multiplied by an exposure factor). However, there are some important differences.

*The number of threats is close to infinite.* One must also consider heretofore unknown and continuously developing threats, such as viruses, malware, and others. There is no clear data on how many variations of these are currently floating around and how many more will be developed and released in the near future.

*Dependencies are mostly unknown.* This is probably the most significant problem and it has been part of an ongoing security conversation for years. There are no publicly available statistics on how the security threats affect victims. Keep in mind that we are only discussing Information Security related threats and accidents, not Physical Security issues (such as fires or floods). Frequently, Enterprises themselves are to blame for not disclosing this information. At present, Government neither provides nor requires such disclosure.

*Creating a database for all existing threats and exposures* is considered by many experts to be an exercise in futility. In part this is because no one knows of all the threats out there and in part because even known threats are constantly evolving and mutating into new forms. Collecting detailed information on and describing how a specific threat has affected computer users or companies is also practically impossible. There are too many variables to consider - users, computer environments, and business environment, among others. If there are no reliable statistics, there can be no statistical simulation, and therefore no “measured or measurable risk”.

These limitations unfortunately mean that today InfoSec Risk Management Quantitative Analysis is more of an art than science and cannot be relied upon to produce consistent and trustworthy data. If you are presented with a piece of software touted to “calculate” risk, ask your
vendor how large the database of threats and dependencies is, how many different kinds of
events and exposures it has, and whether the data is being continuously collected.
Qualitative analysis is a completely different story. Because it is based on common sense
(expert’s estimate), it can genuinely help in improving a company's security. What's unique
about qualitative analysis and what puts it above the quantitative is that by itself it does not set
false expectations or produce inaccurate numbers.

Jack of All Trades: The Security Analyst

One other aspect of InfoSys influence on security matters is personnel hiring. If you look at a
typical job requirements list for a system administrator, you will see a laundry list of operating
systems, hardware, software, etc. If you compare that to the job requirements of a security
specialist, you’ll see a very similar if not identical laundry list. This identikit quality comes from
management’s lack of understanding of InfoSec and its unique needs. If a system administrator is
extremely busy working on his assigned projects and fails to complete 10% of the tasks, it is, in
all likelihood, not a severe problem. If somebody’s computer does not perform well, fails to run
an application or print a document today, it could be perfectly acceptable to fix it tomorrow.
However, if we take the same approach to security tasks, we can all agree that a 10% failure to
complete is not acceptable. Just as you would not consider your house completely secure if one
in 10 doors is wide open, it could be dangerous to leave a firewall 10% misconfigured or for
10% of all computers to not have a security update when it is known that a new exploit is
coming. Clearly, it is unwise to hire security professionals by InfoSys rules. The InfoSec job is
all about security and cannot be treated as just an extension of a system administrator's job
function.
Managing technical expertise

Finally, the last problem we would like to discuss is the technical competence of the security management teams. While some level of technical expertise is expected from someone in a high-level management InfoSys position, the primary focus is on the business, not technical side. Here is how US Department of Labor sees an Information Systems Manager position [4] “Job opportunities will be best for applicants with computer-related work experience; a master’s degree in business administration (MBA) with technology as a core component, or a management information systems degree; and strong communication and administrative skills.” In other words, an MBA degree is usually expected, no technical degree like Master's or Ph.D. in Computer Science is required. While this balance between business and technology skills might be acceptable for an InfoSys position, it often spells disaster for an InfoSec one. We strongly believe that both technical education and technical certification of InfoSec management is critical to the success of the position. Furthermore, this balance should be shifted more toward technology and an MBA should not be required and in some cases, even desired. Check the Bob Sullivan’s article [3] and popular opinion for security management behavior and considerable aversion to techies.

Conclusion

If we want our InfoSec to function, we need to forget about our currently prevalent InfoSys approach. Each InfoSec function should be carefully researched and weighed in light of its primary goal - to protect. It is no longer a business goal; it is instead a security goal. How do you decide how much to spend on the security of your company? Any amount justified by an expert
opinion and thorough research is not a waste if it goes toward building up your company's
security infrastructure and systems. As has been illustrated by the TJX debacle, a single InfoSec
breach can incur hundreds of millions of losses, or in some cases bring an entire company to its
knees. Just as effective business goals are a must for security, security goals are a must for
survival of any business.

Management must understand that the information environment has changed drastically as
compared to what it was 20, or even 10 years ago. We have vastly improved capabilities for
sharing and transferring information, but at the same time, we now face a large variety of new
threats. Today, it is not uncommon to see an old style managerial structure fail to respond,
sometimes with catastrophic results, to an ever-escalating number and strength of cyber threats.

This new information environment requires new managerial structures and solutions.

References:

2. CIO On The Hot Sit; Information Week, June 25, 2007, 19.
   blog on Red Tape Chronicles; MSNBC.com:

   http://redtape.msnbc.com/2007/03/tjx_hack_more_o.html


   http://www.bls.gov/oco/ocos258.htm

Copyright © 2007, RuBos, Inc., www.rubos.com
Authors:

Daniil. M. Utin, MS, Director of Software Development, CIDC, Inc. www.cidc.com

Mikhail A. Utin, Ph. D., CISSP, Principal Consultant, RuBos, Inc., www.rubos.com

Jane Utin, BA, Project Manager, CIDC, Inc., www.cidc.com