Data Security and Improving Quality:

A look at how working on three points can help a security manager improve the quality of overall data security within his organization

Tim Plona
Océ - USA
SANS GIAC Certification Level 1
August 2000

Table of Contents

Introduction

Within the last year I became Manager of Server Operations for a medium sized corporation here in the USA. Previously, in addition to running my own PC consulting company, I held Information Technology positions that included, Technical Supervisor, LAN/WAN Coordinator, and Manager of PC Services. While information/data security was always something that I had heard about, it was not a concern of mine. My attitude was simply that I did not work at a company that was a potential target of corporate espionage or Internet hackers. Who would want to steal data or deny service at a trucking company, a manufacturer of gaskets or a company that makes copiers?

My attitude changed earlier this year with the proliferation of havoc wrecking viruses. The Melissa and the ILOVEYOU virus outbreaks in the Spring of 1999 and 2000, caused me great concern. While the company that I worked for endured the outbreaks rather easily, I had really left the experience believing that we survived out of sure luck. What really began to concern me was the question – "What would we have done had we lost significant amounts of data?"

The need for a greater understanding about my corporation's security needs were driven home when my job description was changed early in the Summer of 2000 to include the responsibilities of the Data Security Officer. Now I was responsible not only for my own group's security efforts, but also those of the entire company. How was I to do this alone? Where do I start? What impact can one man possible have on years of neglect?

Two things happened later that summer to help me sort out the steps that I should take to help insure the integrity, reliability and security of the data that my corporation had built up over the years. First of all I attended a conference on security that exposed me to the reality that although I worked for a small copier company (in comparison to a XEROX) we were a potential loser in the data security area. Denial of Service attacks, Script Kiddy attacks, disgruntled employee revenge and simple poor processes could all cause a loss of data and productivity for the entire company. Additionally, in the summer of 2000 I was able to take a graduate level course in Applied Managerial Statistics and Quality. The course was able to give me tools and ideas on how quality in data security management could be achieved. What follows is a look at three factors that could ultimately affect how successful a manager, responsible for data security, could be in ensuring that his or her company is poised to protects its data assets.

Analysis

Adopting a new Philosophy

The job of information technology (hereafter referred to as IT) has changed since it inception earlier in the 1960s and 1970s. Originally, IT was responsible for the design and implementation of computer systems that produced data that helped eliminate jobs (clerks and manual accountants), create more accurate data, and created a means to better manage different aspects of the company's business (i.e. accounting, forecasting, HR functions). IT worked on an island; there were no connections to the Internet, other companies and employee's homes. The knowledge that IT had was self-contained, not many outside of the profession knew what went on in the IT departments and not many cared.

However, ‘the times they are a changing’. Today, IT is responsible for much more. We now manage WAN connections to points all across the country and the world. We have thousands of employees that have a growing knowledge of IT concepts. We now have resources that are appealing to people outside the department. The Information Age has brought IT into the multimedia world with its grasp extending into all areas of the company; from production lines, through sales and marketing, to compensation, vendor relations and customer management. Bill Gates in his book Business @ the speed of thought says, “In thirty years IT will have grown from 5 % of total business equipment spending to more than 50 % by the year 2000.”[1] IT is now an integral part of the corporate life.

With this new importance in the corporate environment it is now important more than ever to change our attitude and philosophy. We are no longer able to think that data security, reliability and availability are a side note to our IT careers. We must change our attitude and core philosophy. For example: computer assaults this year will cost businesses $1.6 trillion globally and $226 billion in the USA.[2] The dollar amount alone is not so significant as much as the fact that these attacks can be caused by a hand full of people and it can have affect within only a few days. For us as security managers to have an impact on the quality of data/ network security that we provide we must change everyone’s attitude about the importance of security. We must start with upper level management in an effort to convince them that data security is a must that requires support from above. The SANS Institute in a recently posted article stated that the number two mistake that Sr. IT Executives make is – Failing to

[1] Gates, Bill. Business @ the Speed of Thought. New York: Warner Books. 1999

[2] Hoffman, Lisa. “Computer Viruses Will Cost US $1.6 Trillion This Year” http://chblue.com/Article.asp?ID=604v (14 August 2000)

understand the relationship of information security to the business problem-they understand physical security but do not see the consequences of poor information security.[3] Additionally, we must focus on those technicians and engineers in the trenches to convince them that data security is a critical part of their job. By working both ends against the middle we can accomplish our goal. A change in philosophy about the importance of data security is crucial if we are to improve the overall quality of that data's integrity, security and reliability.

Drive out Fear

Fear is a means to stop people from acting, just as a robber stops when a police officer shows his gun and shouts "Stop our I'll shoot." When the topic of data security, reliability and integrity enters the workplace fear abounds. Many people allow their minds to run off in many directions. Many fear the policies they believe will be put in place. Others fear the discoveries that will be made when the topic is expressed and exposed. Others fear the financial investment that will be involved. But after all is said and done, fear will stop any effort to take a serious look at the issues.

The response to fear, inactivity, will stop any efforts to bring quality into the role of the security manager. If a security manager desires to begin to improve the overall quality of data integrity, reliability and security he may encounter fear and inactivity. It is the security manager's response to that fear and inactivity that will ultimately determine the overall effectiveness of any quality security initiative. The security manage must not stand back and count his losses, he must continue in his efforts. One key thing that a security manager can do to help erode fear and cause movement

[3] SANS Institute. "Mistakes People Make that Lead to Security Breaches" http://www.sans.org/mistakes.htm (14 August 2000)

is to inform the people around him of the risks involved in inactivity. He must show the senior staff that data loss or a denial of service attack can be very costly to any company in this e-commerce global economy.

Additionally, by driving out fear a security manager could not only build momentum to the issues but could also help introduce the concept of quality to other areas. As the evaluation of the security efforts are reviewed other system's lack of quality could be exposed and then refined. The implementation of a quality minded effort could have far reaching impacts across the entire IT department and eventually corporation.

Institute a Vigorous Program of Education and Retraining

Once the new policy of looking for quality begins to take form and the fear has begun to be driven out from the masses a new program of education and retraining must begin. Remember, it is a new philosophy and attitude, and it needs to be taught. IT departments often live in a world similar to the Old West with gunslingers and sheriffs. Many things are tried and implemented without any formal procedure written or testing performed. It is run and shoot. Run and shoot works for a time, but it does not provide a quality product. According to the SANS Institute the worst mistake a Sr. Executive could make in regards to security is "Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job".[4]

Take the example of preparing web site servers for connection to the web.

[4] ibid.

Without a well educated and trained group of technicians who are following a set of written procedures, five engineers will security harden five different server five different ways. This is where education and retraining need to come in. The staffs must be trained in the importance of following procedures and same methodologies. Only then can you be sure that all the boxes have been done the same. Of course, some sampling and testing should be done as in any process, but at least you have a base from which to assess the boxes.

Beyond the basics of data/network security the technical side of security will require regular education. The type and style of attacks and intrusion will constantly be changing and evolving. The viruses of the mid 90's that took months to spread and needed the physical moving of a diskette from one box to another are all but gone. Today's ever changing technology gives the hacker a wide set of more and more technical tools with which to attack. Our engineers and technicians must be provided the education and training necessary to meet the challenge

Conclusions and Recommendations

The role of security manager is a challenging one. It is one fraught with the danger of responsibility without ability. A security manager has the responsibility to keep it all together, but the burden of convincing others of the need for the policies and expense. The security manager has the need to keep up to date on trends in the industry while not having the time. The security manger has to make decisions that will affect the entire organization, even though the organization may fear, reject and spite those same decisions. What follows are a few suggestions to help make it through the storm.

In terms of Adopting a New Philosophy, the key is to inform. You must convince those around of the need of your pleas. Help them all to see that data/network security, integrity and availability are crucial to business in the Information Age. This can be done is several ways:

- Keep them aware of stories about security breaches in the news.
- Do some basic internal self assessment to expose current weaknesses (use discretion)
- Share with everyone in IT how they can be a part of an overall quality security plan.
- Help expose everyone to the reality that one whole in perimeter defense is enough for sufficient damage.

In terms of Driving out Fear, once again the concept of providing information is key. Knowledge drives out fear, so use it to your advantage. Once again you have to help people understand what you are trying to accomplish. They need to understand that policies and procedures that will be put into place are for the good of the company. Yes, they may seem restrictive and overbearing, but they will help the company succeed in the modern era of Hackers and Attackers. Some ideas:

- Don't surprise anyone, let everyone in the IT department know of the initiative
- Involve others – this allows others to help be a part of the team and not part of the fear mongers
- Work slow and deliberate – speed in and of itself can scare people, give people time to adjust.

While Instituting a Vigorous Program of Education and Retraining there will be obstacles. Some will be resistant to the new ideas, they are comfortable and don't want to train. You have to push on, you can not have a quality security program if aren't willing to change the ways of the past. The patterns of the past are changed using retraining. An engineer that still is convinced that security is essential to the success of his company won't be much help if he does not know how to harden that new server. Everyone must be trained. Some suggestions:

- Have your technicians certified on the products they support.
- Subscribe to third party security resources (search for Security Newsletters on the web)
- Become intimately knowledgeable of your key vendors website and e-mail notification offerings.
- Have your technicians be exposed to as much of the overall business as possible, in this way they gain understanding of the need to protect the business process.
- Have your lead technicians attend classes, seminars and conferences on security. The networking with other security professionals will alone pay for the expense.

Information security is a challenging, dynamic and growing field. It is not meant as an afterthought, it should be in the forefront of every IT person's mind. In order to help assure that you are part of a quality security initiative remember that you will need to help change the overall attitude and philosophy of the people involved, you will need to drive out fear and you will need to educate and retrain those involved. All of this takes time, patience and resources. Don't be afraid – the reward of knowing that you are prepared for the next virus outbreak, script kiddy, hacker, disgruntled employee or corporate spy is one that is well worth it. Your data will be secure, your network sound and your business processes in order, all thanks to some hard work on your part.

Bibliography

Computer Security Institute. "Information Protection Fundamentals" http://www.gocsi.com/ip.htm (14 August 2000)

Gates, Bill. 1999. *Business @ the Speed of Thought*. New York: Warner Books.

Hoffman, Lisa. "Computer Viruses Will Cost US $1.6 Trillion This Year" http://chblue.com/Article.asp?ID=604v (14 August 2000)

Overly, Michael. 1998. *E-Policy: How to Develop Computer, E-Policy, and Internet Guidelines to Protect Your Company and Its Assets*. Long Beach, CA: Amacom.

SANS Institute. "Mistakes People Make that Lead to Security Breaches" http://www.sans.org/mistakes.htm (14 August 2000)

Tucker, M. "Security is the Key." http://www.scmagazine.com/scmagazine/1999_12/editor/editor.html (14 August 2000)