INVITED TALK 1

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

1

Security Should Pay: It Should not Cost

William Hugh Murray, Executive Consultant, Information System Security,
Deloitte & Touche, Ten Westport Road, P.O.Box 820, Wilton, Connecticut 06897-0820. 203-761-3088,
Facsimile: 203-834-2200.
49 Locust Avenue, Suite 104, New Canaan, Connecticut 06840. 203-966-4769, 0-700-WMURRAY,
Facsimile: 203-966-8612, Cellular: 203-326-1833.
Stepping Stones, 705 Weed Street, New Canaan, Connecticut 06840-4017.
whmurray@dttus.com 5126,1722@Compuserve.com WHMurray@DOCKMASTER.NCSC.MIL
315-8580@mcimail.com DXBM57A@Prodigy

1. Security -- A Cost of Doing Business

There is a television commercial in the U.S. that shows an automobile mechanic. In one hand he has some worn piston rings. In the other he holds an oil filter. The mechanic looks from hand to hand and says, "You can pay me now, or you can pay me later." The point of the commercial is that friction is inevitable. It is a cost of running an automobile. It is inescapable. You will pay. The only choice that is open to you is how you pay. You may pay in a regular and orderly manner, or you may pay in a destructive and unpredictable manner, but you must pay.

So it is with information protection. It is a cost of doing business. It is unavoidable. You will pay. The only choice that you have is how you pay. You can pay in a regular, orderly, and business-like manner, or you can pay in an irregular and unpredictable manner, but you must pay.

Now, I know what you are thinking. You are thinking that those rings came from an American car, not from a Mercedes or a BMW. You are thinking of all those stories that you have heard about the little old lady who drove her 500 SEL for a million kilometers without ever changing the oil, much less the filter. Perhaps you can get away with not changing your oil filter. Perhaps you will be lucky.

But the mechanic in our advertisement portrays himself as a friend, giving friendly advice. He is trying to help us understand our choice so that we will make the one that is best for us. He too has heard the story about the little old lady; he's even seen some of those cars. But he understands that those cars are the exceptions. While one driver may get away with it, for most drivers and cars, periodic changes of oil filters is a smart and efficient policy.

While one department or manager within your organization may get away with poor security, taken across all departments and all managers, security can pay and its absence will put the health of the business at risk. You are in the role of the friendly mechanic. It is your job to convince management in general and managers in particular to change their oil filters.

2. Security Should Pay; not Cost

Security should pay, it should not cost. Management has a fundamental responsibility to conserve and protect the assets and interests of the institution and its constitutents. However, it should spend no more to do that than will contribute to the objectives of the institution, at least across the whole institution and across time. Security is a means, not an end. As with safety programs, personnel programs, recognition programs, and the like, we have security programs because they contribute to the bottom line.

3. Efficiency

Some of you, with keen ears for English, might have noted that I said "security can pay." It does not necessarily do so. As with anything else, it is possible to pay too much for security. Of course, if you do, then it will not pay. Courtney's second law says, "You should spend no more to deal with a risk than tolerating it will cost you."

Security must be efficient. That is, it must be effective without waste. A security measure is efficient when it costs less than the alternatives, including the alternative of doing nothing. A collection of security measures is efficient over time when the sum of the cost of losses and the cost of the measures is at a minimum. Infinite security means infinite cost, and zero security means intolerable losses.

Of course, there is part of the problem. This is a difficult number to know. While we can measure the cost of security measures, the frequency of large losses is low and the period long. The cost of frequent, but controllable, losses is often beneath our notice and, when noticed, is not seen as related to the cost of security. Therefore, it is difficult to identify the value of our day-to-day activity, to convey it our management, and to motivate our peers and colleagues.

We have a saying in English, "No one promised you a rose garden." No one promised that management was easy. If it were easy, it might not pay so well and offer such nice working conditions.

One important form of efficiency is consistency. It is important that security measures result in a similar level of security across like parts of the institution and similar resources. We do not want to spend a great deal of money to raise the average height of a fence by greatly increasing the height of one section while leaving most of it alone. Therefore, efficiency requires that like resources receive similar protection. It requires that all resources receive the appropriate protection, while reserving expensive measures for only those resources that need them.

4. Efficient Management Systems

Having said that, we can now begin to identify efficient management systems and efficient measures.

It may be that there are some institutions that are so homogeneous that one level of protection would serve for all but a small, easily identified, set of their resources. I have not encountered one in my 25 years in this field. It may also be that there is a management system, other than classifying resources by their sensitivity or according to the protection measures that they measures that they should get, that will ensure that everything is properly protected but expensive measures are reserved. Again, I have not encountered one, but wonders never cease. In the meantime, I do not expect to see an institution the size of those represented here that has an efficient security program that does not require management to classify and label information resources.

5. Efficient Measures

While we tend to focus our attention on the effectiveness of security measures, efficiency is inversely proportional to effectiveness. That is to say, the most effective measures are rarely efficient. Either they cost too much, or they have too large a negative impact on our ability to accomplish other objectives. The most important factor in efficiency is the breadth of the measure. Those measures that are most efficient are those that address the largest set of risks, including:

- Direction to employees
- Management supervision
- Physical security
- Access control
- Encryption
- Data base backup
- Contingency planning.

Tell your people what you expect and what you rely upon them for. When employees fail to do what we expect, it is far more often the result of a failure to communicate on our part than of any failure of motive or intent on theirs.

Supervise. Note variances from intent or expectation and take timely corrective action. Management supervision is the most general, flexible, and effective of all controls. We use others only to the extent that they are more efficient.

Provide a safe environment. The test should be that what is safe for people will generally be safe for computers and information. The skills and special knowledge of your people makes them irreplaceable, while property is cheap, and information easily copied.

Limit access to sensitive and valuable resources. The more valuable the resource, the more layers of control and the fewer the number of people with access.

When you cannot limit access to information, then record it in codes that only the intended parties can read. Modern cryptography can be fully automated and arbitrarily strong. It enables us to protect information independent of the media on which it is recorded or the environment through which it must pass. We can implement both logical envelopes and logical signatures. We can compose these to simulate any control that we have ever been able to implement with paper. Using the computer, we can do these things in a manner transparent to the user and too cheap to meter.

Create multiple copies of important data and distribute them over space such that not all copies are vulnerable to the same event. Consistent with the needs to keep the copies current and confidential, the more the better.

Use slack time and resource before a disaster to reduce the cost and duration of the outage. You will survive and recover from most disasters. The issue is not whether you will survive but, rather, of how much it will cost and how long it will take to return to normal. Do not focus on tactics that might fail, or might not apply, but on strategies that must succeed.

None of these measures is one hundred percent effective against any hazard; all involve some residual risk. Therefore, their efficiency does not result from their effectiveness versus their cost. Rather, it results from the number of hazards that they address. While not completely effective against any exposures, they are efficient because they marginally reduce our exposure to a large number of risks and vulnerabilities, some of which we cannot even identify in advance.

Now, that is all there is to it. That is a quarter of a century of experience in a nutshell. That is all you really need to know. But it is only the beginning of what you must do.

Note that what is good for one security objective may be bad for another. The more copies of the data, the lower the likelihood that they will all be destroyed, but the greater the chance that one will be disclosed. Security is the act of balancing the cost of security measures against the cost of losses. The balance is not stable; It requires the continual application of experience and judgment.

6. The Price of Security

So we see how we should manage and what measures we ought to employ. All of this begs the question of how much we ought to spend. It may be that what I have said so far is all that can be confidently said on the issue. On the other hand, my experience suggests that these answers are not satisfying. To say that "you should spend less than it would cost to do nothing" is unsatisfying if the cost of doing nothing cannot be readily known.

Most organizations cannot tell you with much confidence how much they spend on security. Their books are not set up to measure things so small. Neither can they tell you much about the cost of losses; the books are not set up to track things that occur so seldom.

Early in my career, I used to respond to this question by saying that if you were spending more than three percent of your budget on security, then you were not likely to be efficient.

The longer I am in the business, the lower the number gets. Perhaps it is as little as one-tenth of one percent. That is to say, perhaps one employee in a thousand works full-time in security.

How much you spend may be a measure of intent, but it is not a measure of accomplishment. Accomplishment is measured by how well you spend. We maximize our chances of spending wisely by spending on the efficient measures. Now it is time to get on with it.

You can pay me now, or you can pay me later.