

Computer security for fun and profit

Hank Wolfe

For years we have been trying to sell the importance of computer security. As a security evangelist, I have addressed audience after audience talking about the importance of security hoping that one day I would hear someone stand up and shout "Halleluiah!! I believe!!." As you might imagine, it has never happened and probably never will – for me or for anyone else.

Top management tends to be part of the problem rather than part of the solution. For example, a large local unnamed organization's top executive and their deputy will not sign off on implementing the organization's formal security policy document because within it, is a policy that directs that all passwords should be changed regularly and have certain restrictions on their makeup. The two individuals have used the same password for several years and do not want to be required to change it now — in this example, top management are definitely a part of the problem.

Promoting security here in this forum is like preaching to the converted; however, perhaps we have missed an opportunity. If

we were to approach the idea of security and position it as an overhead line item in the scheme of the profit and loss statement a little differently, we all might be able to convince management that in times of economic hardship, that security should not be one of the first things to be cut back. We might also strengthen our position when proposing a new or updating an

The idea is to consider security expenditure as a PROFIT line item...

old security measure if it is couched in this form.

Most insurance companies are very well off so the technique works

Some years ago, I had the privilege of hearing Ira Somerson of Loss Management Consultants, Inc. explain another way of promoting security. Ira deserves credit for the idea and put forward a compelling case and I will attempt to put it forward here as best I can. I have never heard it used anywhere else, but it never the less makes a lot of sense to me.

The idea is to consider security expenditure a PROFIT line item. Here's how:

- Actuaries calculate the probabilities of many events and produce tables containing these probabilities.
- Many personal factors are used in the calculation and over a population, on average, the probabilities are pretty accurate.

	Annualized Probable Timing (years)	Total Forecast \$ Cost	Annualized \$ Cost
Event Description (no protection) 1 event	10	10,000	1,000
Event Description (no protection) 2 events	20	20,000	1,000
Event Description (<u>WITH</u> protection) 1 event	20	10,000	500
Security Measure (Annually over 20 years)	20	7,000	350
PROFIT/LOSS		\$ 3,000	\$ 850

Figure 1: Security for profit

- They are used to decide when it is likely that each of us will die so that our insurance company can charge an appropriate premium on each person's life policy that will, collectively, cover all losses and yet make a tidy profit.
- Most insurance companies are very well off so the technique works.

The same technique is used to forecast a plethora of events as well. What we need to do is make use of these probabilities to discover the average amount of time over which an event can be expected to occur. For example, a fire that would adversely impact a server installation can be reasonably predicted – perhaps once in 10 years or once in 20 years. For our example, let's use once in 10 years. The expected cost of that event can easily be calculated. It is comprised of the cost to replace equipment plus the cost of setup and data restoration plus the cost of loss of directly and indirectly connected revenues – in our example \$10,000. If the cost of preventative measures is less than the cost of the event and those measures prolong the time frame (10 years) or reduced the recovery time and cost, then that expenditure (for the preventative measure) makes a profit.

In the example outlined in figure 1, the measure would extend the probability of the adverse event occurring by 10 years and reduce the expected cost when it did happen over 20 years from \$20,000 to \$10,000. The cost of the security measure over 20 years in the example is \$7,000 and, therefore, implementing this security measure makes a profit of \$3,000.

See Figure 1 for a clearer outline of the calculation.

It seems like this is just a juggle of figures but it's not. It's just a different way of seeing what actually occurs. The difference is that the viewer should be able to see the justification of

appropriate security measures not as optional overhead during good times but as a moneymaker not to be "reduced" in bad times.

In any case, implementation of any security measure should be economically justified and take into account the related cost versus expense in money as well as other costs that are not so easy to quantify. These are issues like:

the viewer should...see...security...as a moneymaker not to be "reduced" in bad times

- Reputation.
- Credibility.
- Public embarrassment.
- Potential loss of revenues that cannot be calculated.
- Other intrinsic issues that have a serious impact on the organization.

Some measures will be put into place merely based on these intrinsic reasons rather than any specific economic justification and they should be separated, perceived, addressed and

Preaching security may...be a thing of the past because current "best practice" will dictate the minimum security elements

categorized differently than the others.

The other aspect, of course, that must always be addressed when promoting information assurance/computer security is the ongoing and continuous requirement for protecting business continuity. In today's world, computing and information technology are no longer optional. They play a vital role in every business and are as important as having a product to sell. Without either, there is no business.

The current trend seems to favour the point of view that an organization's directors may be held liable if it were to fail and that failure was attributable to security "best practice" not being in place. If this trend is adopted in most jurisdictions, then preaching security may also be a thing of the past because current "best practice" will dictate the minimum security elements that must be in place.

If you have questions or comments (critical, complimentary or helpful) please do contact us.

About the author

Henry B. Wolfe has a long computing career spanning more than 43 years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago located in Dunedin, New Zealand where he is an associate professor.

Contacts:

Dr. Henry B. Wolfe
 Computer Forensics & Security
 Information Science Department
 Otago School of Business
 University of Otago
 New Zealand
 Email: hwolfe@infoscience.otago.ac.nz