

Accounting For information Security: Does it Add Up ?

Simon Walker and Javvad Malik

A Blast From the Past

A few years ago our family doctor had a heart attack. Which in some ways is kind of ironic since she was always telling her patients to lose weight, eat healthy and exercise more.

But then again, doctors aren't very good at taking their own advice. Which makes it a good thing that they can't self-prescribe any medication. Perhaps this is what happened in the case of the recent RSA hack. It's far easier to give your patients good advice and securing their data that it is to secure your own.

But that would be an over-simplification of the issue and the analogy being an analogy doesn't quite fit.

The question still remains, when RSA can be hacked so thoroughly, what does it say about Security-practice Vs. Security-policy? Or maybe more appropriately, the question is, what does it say about the security industry as a whole? To paraphrase Michael Moore:

"We like nonfiction and we live in fictitious times. We live in a time where we have fictitious security standards, that are governed by fictitious security committees and implemented by fictitious security professionals. We live in a time where we have companies spending millions on security products for fictitious reasons."

A bit of a harsh assessment? But think about it for a while. Is there an immediately obvious business case for information security, other than "It's the right thing to do". You can try to convince someone till you're blue in the face, but it just doesn't add up. Security is a cost and a high one at that.

So what happens? Everyone takes shortcuts to build their business with the least cost. After all, that's the objective of a business, to make money and not spend it all.

CloudNine Communications was one of Britain's earliest internet service providers. It had been in business for six years. It was voted ISP Review ISP of the Year 2000 and was listed in the Top 10 rated UK ISP's (on ISP Review) from October 2000 through to January 2002 (Reuters, 2002) . Its core offerings were email services and software, web site hosting and was one of the first companies providing Software As A Service (SaaS). Formed in 1996, it had approximately 30,000 business customers.

In January 2002, it was subject to a Distributed Denial of Service attack. A denial-of-service attack causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computer resources of the target.

As a consequence, the management were forced to sell the business to a competitor, Zetnet. This was significant because:

- CloudNine had recognised the risk of a DDOS attack, but had deemed the cost of countermeasures to be prohibitive, relative to the risk
- It was the first known instance of a company being "hacked out of business", although high profile attacks had previously taken place on high profile sites such as Register.com (an online computer trade journal) in 2001 , and the Eire Department of Finance website (also 2001).
- DDOS attacks have subsequently appeared as a weapon of cyberwarfare, for example during the 2008 South Ossetia war, the 2009 Iranian election protests.

This case represents a clear instance of a management team making a conscious risk management decision based on faulty assumptions; i.e. that no existential threat existed for them, when in fact there was already some evidence to show that this was not the case.

Accounting For information Security: Does it Add Up?



1 Cornhill, London EC3V 3ND +44 (0) 20 7125 0364
info@quantainia.com www.quantainia.com

Accounting for garbage

Externalities can be defined as costs and benefits which are not naturally captured in the pricing of the activities to which they attach. This may also pertain where the costs and benefits of an activity are felt by different parties, resulting in a misalignment of incentives, as argued by Anderson and Moore (Anderson 2006) This results in the oversupply of goods and services where there are negative externalities, such as pollution, or undersupply, where there are positive externalities, as would be argued to be the case where information security is concerned.

It may therefore be useful to draw lessons, where possible, from innovative models used in other areas where externalities are a significant factor. One good example would be waste management – at an abstract level, it displays many commonalities with information security. For example:

- Neither is generally thought of as a revenue generating activity
- Both are display classic characteristics of public goods, with free rider problems and undersupply unless provided by a centralised authority (e.g. municipal governments for waste management and driven by central government legislation for information security)
- In both cases, failure to supply has negative effects, but these are difficult to accurately quantify in advance

Comparative data exists on consequence, but is incomplete and its applicability would be open to challenge. For example, ineffective sewerage resulted in cholera outbreaks in 19th century London, but only way of modelling the probability and effect of a major sanitary failing, other things being equal, in 21st century would be theoretical.

The State of Florida uses a full cost accounting approach for its solid waste management. Full Cost Accounting is a systematic approach for identifying, summing, and reporting the actual costs of an activity. It takes into account past and future outlays, overhead (oversight and support services) costs, and operating costs. In this respect, it can be seen to overcome the objection to ROSI that it is unrealistic to fixate on capital expenditure over revenue expenditure when considering information security expenditure.

Bebbington and Thomson (Bebbington 1996) lay out a series of layers of cost to be considered in a Full Cost Accounting model. These are laid out, in a form adapted for information security, in the table below

Tier	Description	Content
0	“Usual costs”	Direct and indirect costs which would be associated with an activity using a conventional accounting approach, including both revenue and capital expenditure.
1	“Hidden costs”	Additional costs usually found in overheads/general accounts. These would include regulatory management systems, and monitoring costs, both revenue and capital in nature.
2	“Liability costs”	These costs would not be incurred in the present period in a conventional accounting sense. These would emerge dependent on other events, for example changes in legislation, and their likelihood can only be estimated. Examples might include fines and other regulatory costs.
3	“Less tangible benefits”	Costs and benefits that are likely to arise from improved security management. These costs and benefits could include the effect of goodwill arising from a project; changed attitudes of suppliers, customers, and employees.
4	“Environmentally focussed benefits”	Costs that would be incurred if a security focussed approach was taken in a project can be estimated. Costs to ensure that a project has a net positive effect on information security could be estimated. These values would be informed by estimates of the industry and social impacts and alternatives.

Accounting For information Security: Does it Add Up ?

A cost/benefit model that excludes Tier 4 would not be a full accounting model, rather only “fuller” than ISACA’s ROSI. Working through the tiers systematically would enable an organisation to produce a holistic picture of the costs and benefits of its information security expenditure.

The ACCA (Bebbington 2001) define a number of steps that would be required to deploy this model in an environmental context. Adapted for information security, these would be :

1. Define the cost objective- for example, a new project or process. This is critical – in particular the end-to-end extent of an activity. Failure to do this would result in incomplete consideration of costs and benefits.
2. Specify the scope of analysis – this serves to determine what sub-set of all possible externalities are to be considered. Moreover, this would be important in identifying the various layers of externality – these might include, for example, regulatory impacts. It would not be useful to try to include all conceivable externalities (e.g. impact on competitors); rather, only those externalities which can be directly identified with a particular project or activity should be included.
3. Identify and measure external impact – this requires an explicit link to be made between the cost objective and the externalities which arise from it. This requires the gathering of data on both the cost objective itself and the identified externalities. The first set can largely be drawn from boundary transactions – i.e. where there is a consumption or movement of resources resulting in a monetary transaction. With regard to externalities, there is a less exact and more variegated set of data which could be drawn on – for example, secondary data sets such as reported costs of incidents from the latest PWC/BERR reports and historical fines under the Data Protection Act from the Information Commissioners Office. Although this information set has obvious drawbacks, it has the benefit of being publicly available.

4. Cost external impact (e.g. monetisation of the externalities. In many respects, this is the most problematic stage – for example, it would be dependent on a convincing scope having been identified earlier in the process. As was identified through the survey, this often the area regarded as most subjective and subject to challenge, as it will tend to be “story dependent”.

This therefore produces a theoretical model for a full cost analysis would be a summation of costs from Tier 0 to Tier 4. However, this still leaves the problem of the uncertainty of assertions about probability, and the relative balance between costs and benefits. This rather suggests the need to apply both prudence, and an adaptive management approach. In other words, the calculations should articulate clear assumptions about facts (e.g. the economic climate, which has an impact on the overall level of criminality), and should be expressed in a flexible way (i.e. “best case”, “medium” and “worst case”). This would allow conscious decisions about confidence levels, and would provide a clear rationale for revisions if specific assumptions are proven incorrect. Furthermore, it would allow for improved confidence in decisions over time, both from a psychological perspective and by providing internal benchmarks which can be refined over time. This is something that ROSI notably does not do, as a specific application of it will only ever be “generally in line with events” or “not aligned”. Turning this into a model for determining the return on a particular activity would therefore produce:

$$\text{Return} = \frac{(A + B + C) + (D + E + (F \times \text{probability of } F))}{(D + E + (F \times \text{probability of } F))}$$

Where:

- A is the direct benefit of the activity/project (as per Tier 0)
- B is less tangible benefits (as per Tier 3)
- C is positive network effects (as per Tier 4)
- D is Tier 0 costs
- E is Tier 1 costs
- F is the cost of contingent liabilities (as per Tier 2).

Accounting For information Security: Does it Add Up ?



1 Cornhill, London EC3V 3ND +44 (0) 20 7125 0364
info@quantainia.com www.quantainia.com



So What Does It All Mean?

The answer is that, like it or not, there is no easy answer for the formulation of business cases for information security. That's not to say that information security doesn't make sense from an economic point-of-view. It just means that, as a profession, we need to think more broadly about how we structure the approach and think creatively about how to apply lessons from elsewhere. It took accountants (probably the third oldest profession) several thousand years to come up with double-entry book keeping and then agree on uniform standards. Hopefully, information security can manage to reach this point somewhat sooner; and security professionals should apply some pressure on industry bodies, to make it so.

Bibliography

Bebbington, J. G., R.; Hibbitt, C.; Kirk, E. (2001) Full Cost Accounting: An Agenda for Action

Bebbington, J. T., I. (1996). Business Conceptions of Sustainability and the Implications for Accountancy. London, Association of Chartered Certified Accountants.

Reuters, "How CloudNine Wound Up In Hell", 02/01/02
Retrieved from 15/09/2010 from
<http://www.wired.com/techbiz/media/news/2002/02/50171>

Quantainia
1 Cornhill, London EC3V 3ND
+44 (0) 20 7125 0364
info@quantainia.com
www.quantainia.com