

The Challenges for the Security Sector: Thinking About Security Research

Martin Gill

Perpetuity Research and Consultancy International, 148 Upper New Walk, Leicester LE1 7QA, U.K.
E-mail: m.gill@perpetuitygroup.com

Security Journal (2007) 20, 27–29. doi:10.1057/palgrave.sj.8350041

The study of security: some reflections

Probably, the most disappointing thing about the study of security is that, in some aspects at least, it has progressed remarkably little since the first volume of the journal in 1989. It is still neither common for security companies to employ researchers nor for the security sector to sponsor quality-independent research and publish the findings. You could be forgiven for believing that, all too often those involved in the practice of security have seen research as an irrelevance. I do not criticize them for that (not too much anyway), after all much of the research that has been done has not been objective, the topics covered have often been viewed as marginal to mainstream interests, and the way that the research has been presented has often not taken account of the needs of security practitioners. Within Universities, the study of security has been mostly a marginal interest, and even then good courses have been more common than good research. Indeed, there are a few handfuls of dedicated security scholars around the world who have been responsible for much of the scholarly output.

It is not my intention to sound negative, actually there are some positive signs. There are some dedicated scholars who have “stuck with it” over many years (and most have published in this journal at one time or another). And there have been some excellent studies that have contributed to the security body of knowledge. The recent *Handbook of Security* (Gill, 2006) published by Palgrave (who publish this journal) contained a range of good discussions of the state of the art knowledge in this area. Increasingly, we are seeing some good evaluations, although there are far more that do not find their way into the public domain. However, it is not the case that the findings from even good security research finds its way into improving security practice. That is a challenge for the future.

Does security work?

It is always important to define what one means when discussing “security”. In this short essay, I am concerned with corporate security and security companies providing security products and services, such as manned guarding or installation companies. It is an incomplete definition, but sufficient for what space allows for here where it is only possible to refer to general trends.

One such trend is the plethora of research that has shown that all too often security measures do not work. And summarizing briefly, the principal reason is that they are not used properly. This is an important finding. I am continually amazed about what technology can do, it is impressive, and it looks set to continue to offer even more options going forward (Smith, 2006). The problem is that end-users are now sceptical. All too often in the past, they have been the guinea pig for the latest idea that worked great in practice, but was fraught with problems in the field (see, Gill and Spriggs, 2005). Yet, end-users are not free from blame in the security failure scenario. We knew years ago (Hearnden, 1996) that they get advice about security direct from suppliers. Sometimes, this is good practice based on a partnership and a good understanding borne of mutual professionalism, but not always. At a conference about a year ago, I was talking about this very issue when a supplier came up to me afterwards and said: “Martin, I am one of those suppliers you have spoken about and let me be honest with you. I sell CCTV, if I am called into to a client to give him a quote, and I wander around the building and think actually he needs some alarms rather than CCTV, do you really think I am going to tell him when I don’t sell alarms and I only sell CCTV?”.

In work that I and others have carried out (e.g. see Gill and Spriggs, 2005), security has been compromised by poor understanding of the problem that needs to be tackled, inappropriate measures being applied, poor coordination of the various stakeholders, technology measures that are technically deficient, and poor back-up in terms of a human response. Within the crime prevention field, we refer to these types of issues as “implementation failure,” and it is extremely common. And despite the many excellent installations that characterize a large part of the security sector, these types of initiatives attract widespread attention.

The fact of the matter is that solving security problems is not easy, it often looks easy but it is not. And we have been far better as an industry or sector in advancing the case of security services and technology, than we have the case for understanding all that it takes to make it work properly. Research studies have highlighted these (e.g. see Hayes and Blackwood, 2006). Part of the problem is that the focus on technology has been at the expense of a focus on procedure and process across business functions, that all too often are more important in managing a range of threats and risks to an organization.

Many times, security providers have provided solutions to only a fraction of the security threats faced by organizations against a background where client organizations have not adopted a well thought-out and holistic approach to managing all security threats, that is they have not evolved a meaningful security strategy or master plan. Security departments within companies have often been marginalized by the appointment of heads of security, who do not have a business background. In my view, it is still the case that the qualification that is most commonly looked upon as being the best in consideration of the appointment of a new senior director is a pension from the military or law enforcement. The common criticism – not always justified – is that they are not able to speak the language of business, further alienating security from where it most needs to be at the heart of the business. After all, security is relevant to every single business function.

For me, it is a pity that security has never realized its true potential to be viewed as something other than an unwelcome cost on the bottom line. Let us be clear, if a CEO had to cut money and focus on departments that were least likely to generate profit, security is something of an easy target. In my view, security does add value to the bottom line, and it is equally possible to see security as ‘value-added’ as it is a cost, but it means generating

metrics that show that, and a commitment to proving that it provides a worthwhile Return on Investment. I am currently researching this area and so, more in due course; it represents an opportunity to view the whole security function in a more positive light.

Research: looking forward

There are lots of areas that merit further research, and it is possible to highlight only a few here.

1. We need more evaluations of what works? We need much clearer pointers as to why things do and do not work. With this information, it is possible to rectify current problems and more easily able to replicate the good points in roll outs of the initiative/project/concept.
2. We need to better understand what the perfect security strategy or master plan should look like. How it will involve all people in an organization, what processes/procedures/incentivization approaches are necessary to engage them, what sort of data streams can inform good practice, what is needed to ensure there is the right link between different security technologies and crucially between technologies and humans.
3. We need to better understand the best methodologies for influencing practice, those at the sharp end. Conducting good research is one thing, making it meaningful for those who are busy and have other priorities is a real test. We need to better understand the value of security. It is not possible to see security as an unqualified good (certainly some academics do not, see, Loader, 1997; Zedner, 2003).
4. In the real world where the bottom line rules security needs to understand how it contributes to adding value (even profit) to companies and organizations. This has been a much under-discussed issue.

There are many more, of course. However, things are improving. Hopefully, when we get to the 40th volume, we will be able to reflect on an established security profession across the world, drawing upon a recognized and distinct body of knowledge, and highlight the role played by influential security studies in general and this journal specifically, now there is a challenge!

References

- Gill, M. (ed.) (2006) *Handbook of Security*. London: Palgrave.
- Gill, M. and Spriggs, A. (2005) *Assessing the Impact of CCTV*. Home Office Research Study number 292. London: Home Office <http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf>.
- Hayes, R. and Blackwood, R. (2006) Evaluating the Effects of EAS on Product Sales and Loss: Results of a Large-Scale Field Experiment. *Security Journal*. Vol. 19, No. 4, pp 262–276.
- Hearnden, K. (1996) Small Business' Approach to Managing CCTV to Combat Crime. *International Journal of Risk, Security and Crime Prevention*. Vol. 1, No. 1, pp 19–32.
- Loader, I. (1997) Thinking Normatively About Private Security. *Journal of Law and Society*. Vol. 24, No. 3, pp 377–394.
- Smith, C. (2006) Trends in the Development of Security Technology. In M. Gill (ed.) *Handbook of Security*. London: Palgrave.
- Zedner, L. (2003) Too Much Security. *International Journal of the Sociology of Law*. Vol. 31, No. 3, pp 155–184.