

# Justifying Security Training

digg this story

Discuss in Forums {mos\_smf\_discuss:Opinions}

By Michael Roberts, Founder and President of Mile2

I am probably preaching to the converted with respect to the distinguished visitors at this venue. Notwithstanding, please humor me for a few minutes and carefully read and consider the assertions below in the hope that it may give you some ideas to help "loosen the purse strings" of those in your organization who make training budget decisions.

Unlike "commodity" training such as commonly available Cisco and Microsoft certification courses, IT security training investments require a higher degree of due diligence on the part of the student and on the part of management personnel responsible for Information Assurance within their organization.

Unfortunately the managers of many organizations have yet to grasp the severity of risks posed by the vulnerabilities invariably present within their network because many are yet to be identified. As such, they are often reluctant to invest in the security training those on the frontline are desperately seeking. This is akin to a bank being slow in deciding if it should have an armed guard in the foyer just because it has not had a hold-up since it opened in 1919, notwithstanding the crime indicators for the area escalating. If a decision was made to hire a guard and the bank enjoyed another 5-year period without a holdup, the "bean-counters" might argue that the guard is not needed. The question is how many holdups were thwarted by the guard? In the same manner, how many network breaches are thwarted by a network secured by personnel with relevant, efficient and up-to-date IT Security Training? It is not a measurable statistic, but the assumption that many breaches were probably thwarted does stand to reason.

Unlike almost any other IT problem an organization may face, a security breach is far more serious than a broken router or a crashed hard drive which can be routinely remedied. After all, information assets such as customer databases, trade secrets and intellectual property are probably the most valuable assets on a commercial organization's balance sheet; or, in the case of government or military entities, their databases contain some of the world's most sensitive secrets. Information assets are usually the worst things to lose because when they are stolen, they are probably not insured and invariably create irrecoverable or irreversible damage.

What I am attempting to articulate here is something fundamentally obvious, but which no one seems to have adequately addressed. What is the difference between a "specialty IT security trainer" and a "great general instructor with a mediocre to great book"? An executive director of a large Asian delivery partner asked this question recently and it is a great question. It occurred to us that the difference isn't in the quality of instruction, or in the curricula, or in the courseware, or in the frequency of updates, or in who is relying on the programs for their training

needs (name dropping). It's in the just-right combination of all these elements (except maybe the name dropping ;).

A premier IT security training vendor does not sell training programs, or instructor days, or courseware; he sells an organization's security. Program graduates secure their organizations because they know what to do, when to do it and how, and they understand why. Good IA training vendors deliver on this promise time and again because they don't train just anybody (we insist on prerequisites), they don't rely on books and their instruction is a mix of from-the-field experience and pedagogical excellence.

OK, I have managed to get this far without inserting a shameless plug for our business. However, what I need to say now can not be done generically as the methods outlined are unique to our company, so plug I must.

In an effort to provide the best possible protection for their clients' information assets, Mile2 Security Training Partners have elected to bring in "hired guns" from Mile2 to make sure students have everything reasonably required to create and implement effective security policies.

Mile2 Security Training Partners will continue to utilize their internal team of multifaceted instructors to provide great training value for "commodity" training courses such as Microsoft, Cisco and Citrix to name but a few. However, with respect to IT Security Training, they bring in the experts. This decision allows local students a quality alternative to the "class in a box" security options offered by other training vendors and delivered by all-purpose trainers. These courses are generally obsolete by the time the courseware or book is shipped, let alone presented in class. IT Security evolves constantly and in keeping, related curriculum should be printed only a week or two before each event to allow for crucial last minute updates; hence, covering the latest threats.

Mile2 Security Training Partners are also the only organizations authorized to deliver Mile2's popular information security awareness and update seminars. Often there is no charge and they are not sales pitches; they are genuine community awareness presentations by Mile2 Instructors when in town on assignment. Frontline security techs should encourage their management personnel to attend these events. The seminars are eye openers and have the tendency to relax the purse strings of managers with respect to training budgets, thereby benefiting personnel tasked with the defense of their organization's security.

You may be the decision maker for training budgets or you may have to go "hat in hand" to management for funding; either way, before you make a decision on what training to pursue, do a quick mental check list of EVERYTHING your organization can least afford to lose. Once you have the list, estimate the losses if that information is lost or stolen. If it is a customer database, how much would you lose if your customers lost their trust in your organization and went elsewhere with their business? This "scenario planning" is a great way to justify the training budget you need.

When management compares the cost of potential losses against the relatively low training fees, they will find an excellent return on investment. Quality information security training programmes equate to a very low insurance premium for your priceless information assets.

Michael Roberts is the founder and President of Mile2 which has offices in USA, Australia, Malaysia, Singapore, United Kingdom and Europe. He first became involved in Information Assurance as an Investigator with the Australian Telecommunications Commission in the 80's and now lives between the United States and Europe where he coordinates Mile2's partner activities. Mile2's penetration testing courses have become the de facto standard for the US Military with dedicated classes being delivered at US Air Force bases as well as US Marines, US Army and National Guard. Mile2 has also taught personnel from the United Nations, NATO, foreign Military and Government personnel and a large number of Fortune 100 companies. Traditionally, student participation has also come from a wide spectrum ranging from charities, banking, insurance, health, communications, transport, law enforcement and education to almost any sector imaginable.