The ethical challenge for information protection management

The most fundamental ethical challenge faced by protection professionals lies in finding a way to convince upper management to identify and fulfill duties to protect. The refusal of higher level decision makers to identify and fulfill their duties to the public puts the ethical professional in a bind. The code of ethics of most protection professionals does not codify the protection of the public well being, but the code of ethics of most of the engineering professions do. Engineers, particularly professional engineers who are certified or licensed by government, have some leverage in asserting professional responsibility and are rarely overruled by management on technical issues such as the strength of a load bearing wall or the proper gage of wire for a building. When they are, they are faced with an ethical choice that often involves peoples' lives and many, if not most, will refuse to compromise safety. Replacing the engineer will only get more refusals and whistle blowing. But in the protection profession, there are few, if any, mandated standards for protection, there are no government approved professional certification or licensing programs except for internal government programs, and protection professionals who refuse to yield are typically fired and replaced by someone – anyone – who will do what management wants.

The task of the protection executive is to find a way to influence management so as to properly specify the duties to protect and, based on these duties, to fund the protection efforts. Depending on the size of the infrastructure provider, the individual tasked with protection may be the same person who implements it and has other tasks and they may report directly to the chief operating officer or board, or they may work for a director within a department in a division in a business unit and never encounter any executive high enough to even communicate directly with anyone who sets policy. The further from top management the harder it is to influence or identify duties to protect, and the more skilled the individual has to be in order to succeed. And the more embedded they are within the information technology area, the less able they are to work around the obvious conflicts of interest of the CIO. While you wouldn't ever put a corporate financial auditor under the CFO (they should be working for the audit committee of the board of directors), the people tasked with reviewing information protection are often working for the very people they are supposed to review.

As industry analysts, we need to clarify that there is no product or service offering that can fix a fundamental flaw in the approach taken by companies. While a good consultant will tell their clients when such a situation exists, there is nothing they can really do to change it, and if they point it out in a document, they are also likely to be terminated from further consulting. Which is to say that, just like most good CISOs get fired before too long because they do their job “too well”, most really good security consultants are systematically weeded out in favor of those without the knowledge to identify that the emperor has no clothes. In short, the outlook for poor quality consultants is excellent, and the outlook for real experts is poor.

Our analysis shows that unless and until the top executives and/or boards of directors learn enough to recognize that they need an independent security function, companies will continue to spend more and more for less and less in the security arena, will continue to take unnecessary and unjustified risks with their shareholders' money, and will fail to meet even the minimal standards of due diligence that thoughtful people could not deny.

