A Paradigm Shift in Operational Information Security

Michael Barwise

I was reminded the other day that the World Wide Web is 20 years old, and it came as a shock to realise that I've been involved with it for all but the first three years.

Things move very fast in IT: ten years is a lifetime, and 20 is a whole era. Why then, after more than 15 years of general public access to the web and almost as much of burgeoning web services for business, has there has been no significant overall improvement in operational information security? I believe it's primarily due, not to technological issues, but to the psychology that underpins the dominant security paradigm. We have so far consistently taken the defensive in a guerrilla war against a proactive enemy who is at least as competent and determined as ourselves, and we have almost exclusively used technology-driven reactive tactics. We generally assume that “until it’s attacked it’s secure”, so post-hoc tests that (possibly fortuitously) come up clean are construed as a measure of security, and protection measures get deployed once the calibre of the flying bullets has been recognised. As a result, lots of us get shot. This is typified by the Citigroup breach discovered in early May this year, in which some 200,000 customer accounts were illicitly accessed via a trivial and well-known URL parameter tampering attack. More recently, it's been reported that Ubiquisys femtocell 3G mobile telephony base stations can be breached via a flaw in the remote firmware update system - the update image is digitally signed, but the public signing key can be stored in an unencrypted file on the device, and it's apparently also possible to download from it an unencrypted backup image.

We continue to make mistakes like these because we're concentrating on individual narrow technological issues rather than thinking the problem through holistically.

A change of emphasis is long overdue. The protectors of our corporate information assets are responsible for the wellbeing of the business. They need to become proactive and to concentrate on the information rather than just the technologies. After all, the information is where the real business value lies. This means the business side must provide them with a business-oriented plan of campaign: an information security strategy which forms an integral part of corporate governance, creating a robust infrastructure that will remain resilient in the face of the unexpected.

A strategy is not a mission statement. Neither is it a technological or even a policy framework. Granted, much of the front-line weaponry is technical, but the deployment of forces must be based on soundly identified business priorities. What's needed is a paradigm shift from technocentric "IT security" to business-centric "Information Assurance". Instead of relying exclusively or even primarily on "impregnable walls" around the enterprise, the potential losses occasioned by abuses of information assets must be weighed against the costs of protecting those assets to an adequate level. Only then can we decide how best to allocate and apportion our inevitably limited security budget.

The identification of these priorities is an absolute prerequisite to a trustworthy security implementation. Get it wrong, and we could spend millions on elegant solutions to the wrong problems, while unwittingly failing to protect the business against real threats. So how to get it right?

First off, we must be able to make reliable, consistent and accurate risk assessments. Only after that can we define appropriate, affordable mitigation. But how good is our judgement? One of the least acknowledged factors in information security prioritisation (aka “risk assessment”), is that any evaluation includes two independent sources of uncertainty: the likelihood of the object under review existing or happening (systemic uncertainty), and the likelihood that one’s estimate of the systemic uncertainty is right (epistemic uncertainty). The first is intrinsic to the object under review and is in principle determinable given sufficient data, but the second is intrinsic to the evaluator and is much more difficult to quantify. In information security, epistemic uncertainty often dominates the equation, due, not only to a serious shortage of data upon which to base judgements, but more importantly to the inherently unstable statistical properties of an event space mainly populated with human purposive actions. But the greatest contributor to epistemic uncertainty in infosec is nevertheless a profound lack of understanding of both probability theory and the psychology of judgement on the part of most people conducting risk assessments. Unfortunately, all these contributors to uncertainty are almost universally ignored by information security practitioners, leading to optimistic and generally unfounded confidence in the reliability of judgements made by privileged “risk assessors”, often unsupported by evidence.

If we want to get our information security priorities right, we need to reduce these uncertainties, and we need to do that urgently. Although the long term goal must be improved education for our risk

decision-makers, we can't afford to wait until that's accomplished. So given the current general lack of awareness of first principles, this will require considerable effort. It will require the input of several disciplines. No single department or section, let alone a single officer (regardless of grade), can perform the whole task. It needs a pool of expertise covering the specifics of individual business processes, legal, actuarial, financial and technical specialisms, and Board level representation of broader business strategy. It is a whole-business activity that must be tailored to the business to work. But, however it's implemented, the universal prerequisites are rigour, consistency, objectivity, evidential support for decision-making, and of course, assurance of the expertise of those involved. Most of all, success depends on excellent communication and a complete absence of any political agenda. These prerequisites may seem hard to achieve, but they are fundamentally necessary. If they seem impossible, remember that the only penalty for failure is to remain insecure. That is not illegal (yet).

Originally appeared on the Infosec Reviews blog, August 2011