

E-commerce security

Some day, on the corporate balance sheet, there will be an entry which reads, Information; for in most cases, the information is more valuable than the hardware which processes it. Grace Hopper 1906–92

Introduction

E-commerce is an inherently technical area, but the management of e-commerce security is about people, visibility and risk. Security management is an imperfect discipline. System designers must ensure that risks are clearly and continually assessed and that the controls placed to mitigate those risks can evolve with the wider environment.

Security structures must first acknowledge the architecture of information security risk. They must also be sufficiently flexible to respond to changes in business objectives and the threat environment. This would allow limited resources to be efficiently targeted at those areas where they would add most value. A coherent framework is vital; experience shows that the ad hoc application of technical controls is unlikely to be either cost effective or reliable as a means of mitigating risk. Organisations must therefore maintain a clear picture of their risk environment and apply a planned combination of technical, procedural and cultural controls to ensure that risk levels remain within acceptable limits. While this risk picture does not need to be complex, it does need to be formally planned and managed.

Every organisation has a different set of objectives and constraints, so it is not appropriate to mandate a standard security implementation at a detailed control level. There are, however, many structures that would indicate that organisations are managing security effectively.

Insurance companies do have a part to play, and one that is not currently well defined or widely in evidence. This is to encourage and reward the effective management of information risk, because this will encourage organisations to manage their information security by affecting their insurance cost base. This will increase the mandate for information security within organisations and ultimately dramatically reduce exposure to an increasingly complex risk environment associated with e-commerce.

E-commerce – a new way of doing old business

E-commerce continues to evolve as it brings significant advantages to business transactions in a wide range of areas, and its attendant security infrastructure must support this advantage. Security functions must be designed with business objectives in mind; an e-commerce system that is crippled by unnecessary or inappropriate security measures might be unable to achieve its objectives, and thus compromise the business function it is supporting. When implemented well, security is not a separate discipline, but an integral aspect of all business and operational management.

Once the preserve of only a few organisations that could justify the investment, today's technological environment has brought e-commerce capability within reach of every type of organisation. E-commerce can, however, be a confusing concept; a "buzzword" striking fear into the hearts of many who are not familiar or comfortable with its rules or risks.

Essentially, e-commerce is a way of communicating for business purposes using electronic means, although the debate continues among the technical community as to whether this is confined to simple commercial transactions or whether wider business activities might be involved. The important point to remember is that e-commerce, like any other form of business, is done by people, and that the technology is merely a platform on which business is conducted. Technology brings with it several diverse risks, not only to the actual business transaction, but also to the wider organisation and community in which the business activity takes place.

Information technology has evolved as a significant enabler for business, and while the essential business objectives and transactions often remain unchanged, the way that business is conducted often changes on a constant basis. New technologies and capabilities promise new opportunities and these in turn evolve new business practices that in turn drive technological development, and so the cycle continues. It is arguable that this has been the way of things since the first primates discovered that they could make natural tools more efficient by adapting them. Nonetheless, the rate of change is now so fast that to keep up to date has become a major challenge, even for specialists.

E-commerce from a security perspective

From a security perspective, the e-commerce environment brings several challenges that must be faced regardless of the size of an organisation.

There are many sources for this new set of risks, but generally, as developers struggle with the balance between technological complexity and customer demands for ease of use, they create situations in which much of the actual system activity undertaken by the tools is hidden from the people using the equipment. It is this shadowy area of “hidden technological activity” that provides a fertile breeding ground for potential risks. It is here that deliberate and accidental threats can evolve and exploit hidden vulnerabilities without being noticed by the people using the equipment. This means that in order to manage these systems, business users need to deploy controls and techniques to monitor and report what is going on in easily understood terms. As a result, users can become increasingly dependent on these monitoring and control tools to secure their systems. This further increases the complexity of the problem because these tools are effective only if correctly configured and deployed (and if we can correctly read the information they provide). More critically, users must be sure that the control tool is doing what it claims and is not the source of risk in the first place.

This dependency is often exploited by virus writers, who prey on fear and uncertainty in order to persuade people to run their viruses. Every year, several viruses appear that claim to be the fix to another threat, but are in fact a problem in themselves. Conditions of fear and uncertainty create an environment in which people are vulnerable to cleverly designed manipulation.

An example of how problematic this is can be found in connection with the management of security logs on computers and firewalls. The effective management of security logs is generally accepted to be an important part of any well-run security management system. Correctly interpreted logs can provide a clear insight into current levels of threat activity and expose potential and actual compromises of system security. The difficulty lies in understanding the information the log contains.

Effective analysis of logs requires a significant level of knowledge and understanding of both the technology and the threat. Several organisations offer log analysis services, although this service itself might be a significant risk in some instances in which it is not possible to validate the integrity of the organisation offering the service.

Information and communications technologies are becoming increasingly complex in order to operate more effectively; new threats and vulnerabilities appear on a daily basis, and many of these might be impossible to see or even understand without detailed specialist knowledge. The language in which they are articulated is also difficult, and in many cases serves to complicate and confuse even more than the technology it is describing.

It is not just about technology

E-commerce is often seen as being profoundly complex; steeped in technology, three-letter acronyms and appallingly complex terminology that would confuse even people with a generally comfortable understanding of today’s computer environment. This is often combined with a cultural resistance to the generic concept of security. The result is that e-commerce

security is often seen as an obstacle to business. Conversely, experience shows that many people harbour a deep fear of the internet.

One example of this relates to a woman who would not actually shop on the internet due to the “security risks”, but left her internet facing machine unprotected by firewall or antivirus software, despite the fact that her accounts and credit card details were stored on it. She had not realised that there was a problem because she could not visualise the attack route from the internet onto her machine. One could not blame her; she simply did not understand, and given that the personal computing paradigm is only 20 years old, she had no relevant reference points in her “real world” experience. Interestingly, the moment that the problem was sketched in a diagram on a piece of paper, it became very clear to her. This is an astute businesswoman and a national leader in her field; it is just that this field is not traditionally delivered using information technology.

The difficulty lies in the visibility of risk. If people cannot visualise a risk, they tend to either ignore it or magnify it disproportionately.

E-commerce is not simply about technology. It is about a complex and changing combination of technology, people and culture. Without a clear understanding of this complex structure, organisations are unlikely to achieve an effective balance of cost and security. However effective (or expensive) a piece of technology might be, it is unlikely to work effectively if it is not installed, maintained or used properly. In addition, although increasingly effective development tools are being created, ultimately system design continues to be fundamentally dependent on people. People are involved in the specification, design, production and use (or abuse) of IT, and people are not perfect!

A Royal Air Force pilot, trained to a high level to fly fast jets in combat, made an interesting observation that has relevance to the subject of e-commerce. He observed that traditionally the capabilities of a well-trained and competent pilot have been generally greater than those of the aircraft that they were flying. This meant that pilots could generally compensate for problems and “sort things out”. In recent years, however, the technical capabilities of the equipment has far exceeded the capabilities of the pilot and as a result it is now far more difficult to solve problems when they occur and increasingly a pilot is less able to compensate for technical failure.

This is true in an information security context, especially given the wide distribution of powerful computers and high-volume data communications in offices and homes, often managed by people with no detailed technical knowledge (or explicit requirement for it). The result is an environment that must be considered generally “unsafe”. Any system which users are unable to demonstrate is effectively managed and secured must be considered untrustworthy. Further, even in systems that can demonstrate proactive security management, users must accept that they might be subject to ongoing compromise. In the final analysis, no system can ever be assumed to be completely “safe”.

The operational implication is that every individual and organisation must take responsibility for system security and information managed and stored by these systems at every stage of processing.