Chapter II
The Complex New World of Information Security

David Porter
Detica UK Ltd., UK

ABSTRACT

This chapter discusses the latest developments in the shifting threat landscape and their impact on the world of information security. It describes how we are now moving into a “third wave” of cybercrime, where sophisticated criminals are applying relatively “soft” techniques that are more pervasive in their execution. It argues that, as a consequence, information security countermeasures based on the latest information intelligence technologies will need to be complemented by softer, more pervasive techniques drawn from disciplines such as process engineering, policy development, behavioral science, psychology and benefit management. The chapter also considers how these countermeasures can be fully realized in today’s business environment and concludes by discussing future directions such as the growth in complexity and the rise of the surveillance society. The author hopes that by understanding these new imperatives, information security practitioners will be in a stronger position to protect their organizations from today’s threats — and those of tomorrow.

INTRODUCTION

The Rise of the Cybercriminal

With the industrial and mobility revolutions of the 19th and 20th centuries behind us, we now find ourselves in the grip of the 21st century digital revolution. The widespread diffusion of telecommunications and computer technology is now having a profound effect on the way we live. From online banking and shopping through to social networking, the digital revolution is
creating entirely new ways of working and socializing as well as challenging, and even destroying, many others.

The world of the financial criminal is evolving in a similar way. To put today’s and tomorrow’s threats in context, let us begin with the recent past. A couple of decades ago the techniques used were relatively “hard” — high on violence and low on intellect — and focused in execution, such as armed robbery and mugging. Traditional security countermeasures comprised of guards, dogs, fences and locks. As the digital revolution gathered pace in the late 1980s, criminals (both existing and newcomers) graduated into cybercrime, where the techniques used were “softer”, requiring more intellect, less muscle and involved a broader range of execution. The new threats included hacking, virus attacks and various forms of electronic fraud involving credit cards, ATMs, checks, mortgages and insurance.

A range of preventative countermeasures similarly involved, such as access control systems comprising firewalls, website/e-mail content scanners and the like. Detection systems based on a body of rules (often wrapped up inside behavioral scorecards) that define the way that fraudsters and money launderers typically carry out their activities were also deployed. These rule-based systems are often founded on the “three Vs” of profiling — the volume, value and velocity (timing) of transactions. Countermeasures also included process controls such as recruitment screening, segregation, supervision and training. In the case of money laundering, much of this centered on the principle of “know your customer”: training front office staff to verify the identity of customers opening new accounts and spot suspicious deposits or withdrawals. Last, but not least, information security standards have been deployed such as ISO17799.

Over the past few years, and into the present, we have seen a “second wave” of cybercrime, where criminals have moved further into “softer” and more sophisticated techniques that are more pervasive in their execution. This has been clearly demonstrated by the significant growth in:

- the Internet as a general vehicle for committing all kinds of frauds;
- Card Not Present (CNP) fraud as a result of the move from magnetic stripe to Chip-and-PIN credit cards;
- identity fraud (application fraud and account takeover) as a result of the significant increase in remote online banking and shopping as well as the indiscriminate publication and sharing of personal information on blogs, instant messaging, wiki pages, file sharing and social networking websites;
- sleeper fraud in which organized criminals imitate the behavior of genuine customers over an extended period of time, gain as much unsecured credit as possible and then default. This type of fraud is specifically designed to exploit the limitations of traditional record-matching technologies. The perpetrators are experts at distorting information to remain undiscovered until it is too late;
- insider fraud, where the perpetrators range from temporary contractors to permanent staff and all the way up to the most senior executives. All are in positions of trust and exploit inadequate processes, systems and internal controls. The original “opportunity takers”, or people who exploit gaps in the system through temptation, incentive or pressure, have been joined by “opportunity makers” or professional criminals who have infiltrated a company and are immune to, and will indeed exploit, an organizational culture of trust and caring. Businesses where there are high levels of organizational or process change have been particularly vulnerable as well as those where there is unchecked staff authority, high staff turnover or low staff morale.

A “second wave” of cybercrime countermeasures have been, and are being, developed as a result: