# FOREWORD

*By Howard A. Schmidt*

The overall mission of this book, and the reason why it is important, is that it bridges the gaps that separate security experts, technology experts, business experts and strategic planners. We hope that you see this book as such a bridge and that you use it as a way to increase your organization's understanding of the full dimension of e-threats.

Keep in mind, security must now be part of your core day-to-day business processes. Corporate security has been an important topic in business news for well over a decade. However, in the last two to three years, there has been a bewildering change in how companies protect important information assets. Threats have grown more complicated, and so have the solutions.

Technology enabled business strategies have become the standard. These have continuously manifested themselves in a proliferation of web-enabled business strategies that have opened up enterprise networks to not only close business partners, like suppliers and key customers, but now to the global online market. This has increasingly put a company's important information assets at a level of risk that did not exist in the past.

In the previous generation, the approach taken to protect critical assets was similar to the bricks and mortar approach — companies would "build a wall around it." Therefore, a company would construct a perimeter security, manned by technologies such as firewalls and intrusion detection systems, all with the goal to keep people out. But new threats and business technology strategies are emerging between and within corporations, spawning initiatives to enhance collaboration and interconnectivity. These initiatives highlight the need to knock down "silos" of protection and implement policies, procedures and technologies that protect the creation of, the sharing of and the access to data. Rather than building walls around data and applications, top managers are now looking at business processes and trying to secure them. That has made security much more of an interdisciplinary and operational issue for the global enterprise.

In the past, it was common to have security deployed as a reaction to an event or almost as an afterthought. The Chief Operating Officer (COO) would get the strategic direction from the Chief Executive Officer (CEO) and then work with the Chief Information Officer (CIO) to implement a technology infrastructure to support the new business processes. The Chief Security Officer (CSO)/Chief Information Security Officer (CISO) would then come in and do what he or she could do to protect the infrastructure. Well, that's no longer a viable technique.

As new processes develop and new technologies are introduced to the enterprise, the CSO/CISO must be involved at the beginning to ensure that the vulnerabilities and security threats associated with those technologies are identified and mitigated. Protecting data is now a considerably more dynamic situation for corporate America, elevating security to an important strategic issue that requires attention from senior management.

In the past, management may have been accustomed to handing security off to a CSO/CISO as a reactive function. Now, it needs to get the "business of security" built into the business process and understand the security implications of their business strategies, as well as that of the technology roadmap that they decide to follow over the next few years. They must adopt greater and earlier security awareness, as part of their strategic thinking.

Simultaneously, the skill sets associated with securing these business processes must respond and evolve. Before, security departments would have silo expertise, e.g., security professionals who were experts at implementing firewalls, or at patch management or at vulnerability assessments. That fragmented approach to point security is no longer viable for all the reasons previously stated.

There is a growing need within security to integrate its pool of activities and to understand the impact of those security activities on business processes. Not only must security professionals be more interdisciplinary within the field of security, but they must also be able to understand the business objectives. This requires innovative ways to protect technology, data, and business processes in an integrated manner.

Because threats continue to evolve and the originators of these threats are akin to terrorists, the threat does not have to be coordinated. There are many different people that are active in a variety of areas trying to develop and implement different types of threats. They don't have to coordinate with other attackers to do damage to an enterprise; they just have to succeed once. The situation now exists where corporate security officers must have a full understanding of not only what security technology does, but also the business imperatives of their company, and be able to prioritize the allocation of resources to those priorities.

You can't secure everything 100%, so you must understand what needs to be secured the most, and prioritize accordingly. Then, at the same time, you must have a growing understanding of the new types of threats that are launched on a daily basis. This is a big challenge for the corporate security community.

Important is effective communication among the CSO/CISO and the other senior executives in the organization. The CFOs who must underwrite and fund these initiatives, the COO who is implementing new business processes, and the CEO who is looking for a new direction, must all understand whether the new directions are viable from a security standpoint.

In the pages of this *Black Book on Corporate Security,* many of these dimensions are explored in great depth. They are also validated with a series of surveys that were conducted to identify what the market is saying about corporate security and what the experts, who are developing new responses to threats, are saying about these threats.