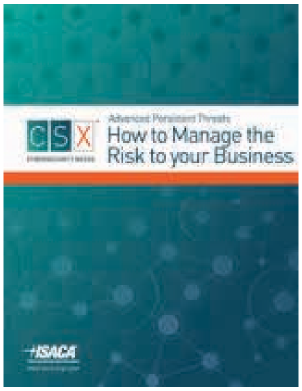
Advanced Persistent Threats: How to Manage the Risk to Your Business

Reviewed by Larry Marks, CISA, CISM, CGEIT, CRISC, CFE, CISSP, CSTE, ITIL, PMP, who is a risk manager with extensive experience in managing and implementing processes, policies and technology regarding risk, security, governance, program management, compliance, internal controls and information security in financial services, insurance, health care and telecommunications industries. He has helped manage project management offices at various Fortune 100 firms. Marks has been published in the *ISACA Journal,* the *(ISC)*^{2} *Journal,* the *PMI Journal* and *ProjectManagement.com.*

What are advanced persistent threats (APTs)? What is their impact? An APT is a specific targeted and sophisticated attack that keeps coming after the victim and is not easily stopped by a defensive program. Everyone is at risk for these attacks, and they make it necessary to prevent, detect and respond to attacks on a timely basis to ensure the confidentiality, integrity and availability of critical data.

The Trojan horse malware package Zeus, which was identified about nine years ago, is used to steal credentials for banking and credit card payments or for logging into a social network. Zeus is considered an APT because it is a set of programs or tools that can catch victims through phishing or encourage them to visit an infected web site. Zeus then commences a man-in-the-middle attack to capture a user's web strokes. In 2010, more than 100 people were arrested in the United States, the United Kingdom and Ukraine on charges to commit bank fraud and money laundering after using Zeus to steal US $70 million.[1]


CSX
Advanced Persistent Threats
How to Manage the Risk to your Business
ISACA

Current events, such as the recent Society for Worldwide Interbank Financial Telecommunication (SWIFT) breach, underscore the emphasis security professionals place on the importance of using a defensive approach. Thinking about breaches should be from the perspective of already having been attacked or the attacker already being present in the company's system. *Advanced Persistent Threats: How to Manage the Risk to Your Business* begins by presenting a control framework to assess the risk of an APT. The valuable takeaway from this section is the importance of doing an inventory of critical assets and data. Where do they reside? Who owns these data? Has the business or system owner been educated on the risk that is impacting his/her data? It introduces a way of thinking that helps identify prospective countermeasures. The book talks about managing the APT incident as it unfolds. But a user cannot reference a manual during an attack, thus continued security awareness training and scenario testing has to be encouraged.

Among some of the most useful content from the book are its appendices. Appendix A contains a dozen questions that the manager can ask, such as "What is the impact of an APT attack to my firm?," "How exposed are we?," and "How ready are we?" Appendix C guides the reader on how to perform a COBIT® 5 gap analysis of the controls in its business framework and prospective recommendations. This practical guidance will help enterprises better address APTs.

The book provides out-of-the-box controls and recommendations that are for varying levels of knowledge, from a layperson to an experienced technical professional. Even though a glossary is provided, the level of writing by the authors encourages the reader to understand controls based on the context of the measures, control and potential threat.

The recommendations provided in the book are not intended as the ultimate encyclopedia of recommendations to protect and prevent an APT, but as a starting point for discussion. The security professional still has to communicate the ultimate understanding that APTs can be mitigated, remediated, controlled, escalated to management, and budgeted for further understanding and further remediation, but cannot be entirely prevented.

Editor's Note

Advanced Persistent Threats: How to Manage the Risk to Your Business is available from the ISACA Bookstore. For information, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

Endnotes

[1] Cybersecurity Nexus (CSX), *Advanced Persistent Threats: How to Manage the Risk to Your Business*, ISACA, USA, 2013, p. 23