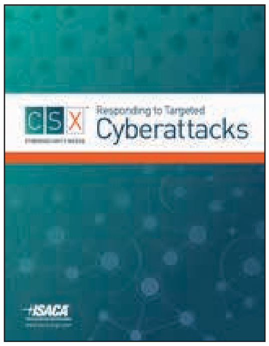
# Responding to Targeted Cyberattacks

Organizations today are concerned about information security primarily due to the fact that the type and nature of attacks are undergoing a lot of changes that make them difficult to detect and prevent. One example is targeted attacks. A targeted attack is a combination of multiple attacks faced earlier by organizations with a focus on stealing information or sabotaging the operations of the targeted organization, and which is difficult to detect. To help address this threat, ISACA® has issued *Responding to Targeted Cyberattacks* with experts from Ernst and Young, as an initiative under ISACA's Cybersecurity Nexus (CSX) program.

This 88-page book is divided into six chapters and two appendices. The chapters follow the natural sequence of cybersecurity activities; after an introduction, there follow chapters on preparation, investigation, eradication, post-eradication and conclusion. The appendices include questions relating to other issues that the investigation team should address and tools required for investigations.



This book is useful for security professionals, consultants and students pursuing cybersecurity as it provides guidance for identifying/detecting, responding and eradicating targeted cyberattacks. Information systems (IS) auditors can use this book to understand what they should be looking for while performing an IS audit to assess the preparedness of the auditee to respond to targeted cyberattacks.

Chapter one introduces the changing landscape of cyberattacks, covering the life cycle of targeted attacks and advanced persistent threats (APT). Organizations require this information to understand the nature of attacks and plan for investigations.

The book then describes the basics of information security that are required to detect and respond to targeted attacks. Early detection helps in controlling the spread of an attack and the damage due to an attack. The basics of information security include risk management, asset management, incident management, emergency response management and building intelligence.

The third chapter covers conducting investigations of security breaches and references the incident response life cycle. The chapter also addresses the focus of investigation and evidence collection for forensic requirements. It emphasizes getting answers to who attacked, determining how the attack might have happened, and identifying the spread and objectives of the attack.

The fourth chapter discusses eradicating an incident and the need to do so more efficiently and faster to prevent the attacker from reestablishing the attack. The chapter offers a great deal of detail on eradication planning and executing the plan with precision.

The next chapter discusses post-eradication activities, e.g., monitoring for reentry, verifying and strengthening controls, and documenting lessons learned. It also emphasizes the possibility of making relevant changes to the strategic plan (if required).

The book concludes by emphasizing the importance of being prepared to respond to cyberattacks. Appendix A provides a useful questionnaire for the investigation team.

Although small in size, the book addresses the current security threat of targeted attacks and guides readers in preparing to detect and respond to these attacks.

## Editor's Note

*Responding to Targeted Cyberattacks* is available from the ISACA® Bookstore. For information, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

**Reviewed by Sunil Bakshi**, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP, visiting Faculty and Industry expert at the National Institute of Business Management (India) and a consultant and trainer in IT governance and information security.