The challenge faced by security professionals in measuring and reporting IT security performance is very appropriately summarized by Andrew Jaquith in the forward of this book. Jaquith says, “Information security is one of those funny disciplines where the best outcome in a given day is…nothing. Nothing bad happened.”

Security metrics are important not only for claiming the optimum share of IT budget, but also for creating security awareness across the company and improving the overall security posture of the organization. Measuring security is not throwing at management numbers generated by a security tool. It is all about identifying meaningful measures and communicating them in the most effective manner to the right stakeholders. This cannot be achieved on a sustainable basis without a comprehensive security metrics program.

Security Metrics—A Beginner’s Guide by Caroline Wong helps security professionals build a security metrics program. This is a beginner’s guide, as the title suggests, though some parts are relevant even to experienced and seasoned security professionals.

The book is divided into nine parts. The first three parts establish a foundation that the later parts build upon.

The first part of the book emphasizes the importance of the security metrics program. It talks about the changing profile of a cybercriminal. A computer nerd aiming to establish his technological superiority and satisfy his ego is replaced by an organized group of criminals trying to create financial havoc or committing cyberterrorism. With cybercriminals continually adopting new technologies, security professionals need to do their best every day.

An effective measurement program can equip security professionals with the right information to improve the security program.

Any security metrics program should start by identifying what to measure. The obvious answer is that security should measure what is important for the business. Ironically, however, this is not easy to establish. After establishing the importance of having a security metrics program, the book provides guidance on how to determine what should be measured.

Part four of the book elaborates on how to implement a security metrics program. It covers setting the objectives, defining priorities and obtaining buy-in from key stakeholders.

Any serious attempt at having a comprehensive security metrics program is incomplete without meaningful automation. It is simply not sustainable without automation, and automation is helpful not only in gathering the data, but also in processing and communicating the results. The book covers a range of automating options, from the most popular Excel sheet to the most advanced online analytical processing (OLAP) tools.

Another important aspect of a metrics program is communicating the results of measurement. Interpreting the results in the most meaningful manner and communicating in an effective way require analytical and presentation capabilities. While tools may help measurement and, to a certain extent, presentation, analyzing and correlating results are vital to ensuring the usefulness of a security metrics program. These aspects are adequately covered in different parts of the book.

Finally, the book covers the relationship between cloud computing and security metrics. The book also provides templates and checklists in the appendix.

The book, written in a very simple manner, is a must-read for those embarking on a journey of developing an organized and sustainable security metrics program.

EDITOR’S NOTE
Security Metrics—A Beginner’s Guide is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in the latest issue of the Journal, visit www.isaca.org/bookstore, email the Bookstore at bookstore@isaca.org or telephone +1.847.660.5650.