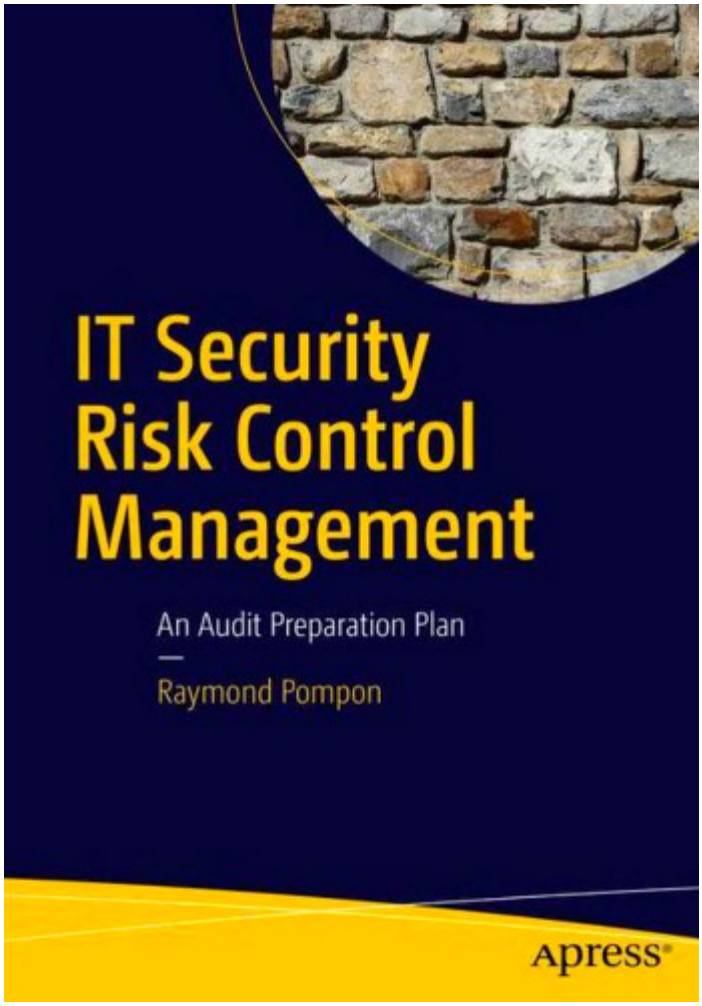
BOWLING GREEN DAILY NEWS

'IT Security' finally starts to make sense

Posted: Sunday, November 27, 2016

"IT Security Risk Control Management: An Audit Preparation Plan" by Raymond Pompon. Seattle, Wash.: Apress (Springer Science+Business Media), 2016, 311 pages, $49.99.



"Imagine a network worm using a variety of attacks to infect the most popular operating system on the internet," Raymond Pompon writes in "IT Security Risk Control Management: An Audit Preparation Plan," his primer on keeping us safe in an increasingly uncertain world. "It was called the 'Morris worm' after its creator Robert Morris, a computer scientist. The author of the worm was so technically skilled that, within hours of being launched, it infected one out of 10 machines on the internet. The worm hit in 1988, before some people in the security field were even born."

The reality is that most of us have either been the victim of a security breach or we know someone who has suffered from having their personal data compromised. In many instances, these incidents can be far-reaching in scope, inflict considerable damage to individuals and organizations and even rattle the foundation of society itself. Full disclosure: My interest in this subject matter in general and this book in particular sprang from watching one of my favorite shows this summer, "Mr. Robot." If you have not seen this exceptionally written dark drama, created by Sam Esmail and starring a talented cast that includes Christian Slater, Rami Malek and Carly Chaikin (among others), you might want to check it out. By most reports, the depiction of what hackers can do when sufficiently motivated is chillingly realistic.

"Most of the time, you shouldn't work too hard at being exceptional," Pompon explains, in reference to how some cybersecurity specialists approach their assigned responsibilities. "You're better off first making sure that you avoid doing anything too stupid. If you are hacked because of some unpatched hole that's been sitting around for months, you will look stupid."

"We know that no matter how secure we make our systems, new vulnerabilities will be found," the author continues a little later. "Your challenge is to find and fix the holes before the attackers exploit them. The process you use is called vulnerability management. It is a process that combines both technical and administrative controls, calling upon many different aspects of security and coordinating work between different departments."

Pompon goes into a rather detailed description of the four sequential yet interlocking activities associated with vulnerability management: hardening standards, vulnerability discovery, prioritization and patching and remediation. One of the features I liked about this book was the down-to-earth style that tends to characterize much of the narrative. Make no mistake, the prose can get extraordinarily dense in several places; consider the following passage from "Starting the Audit," the 21st chapter. Pompon explains the principles inherent to performing an effective systems audit; i.e., one that keeps those desiring to circumvent the integrity of our networks from being successful in their quest.

"Each principle has its own control objectives and associated controls. In summary they are as follows: Security Service Principle: Controls covering governance, security awareness, risk management, control monitoring, operations and change management. Availability Service Principle: Controls covering capacity management, data backup, and system recovery. Confidentiality Service Principle: Controls covering system acquisition, system disposal, system boundary protection, third-party confidentiality, service providers, and user awareness of confidentiality. Processing Integrity Principle: Controls covering management of processing errors, system input integrity, data processing accuracy, data storage, output accuracy, and modification protection. Privacy Principle: Privacy policies, privacy notices, privacy consent processes, data collection processes, data usage and storage limitations, internal access controls, third-party disclosures, IT security controls, data quality, compliance monitoring."

In a nutshell, everything you need to know in order to keep a computer network safe and secure can be found in the interplay between these five principles. Although the text may seem incomprehensible on first pass, I found I was able to follow Pompon's analysis and reasoning to a remarkable extent once I had time to appropriately reflect on what he was actually saying – and in light of the detailed yet remarkably clear explanation he provided throughout the remainder of the chapter. Once you understand the basic concepts and applications that form the architecture on which network security is invariably based, it all starts to make sense. There is indeed a method to the madness here that starts to become self-evident once you begin to glimpse the larger picture he is meticulously constructing with each subsequent page.

"IT Security" consists of an introduction and 24 chapters arranged in four major sections: "Getting a Handle on Things" (chapters 1-5), "Wrangling the Organization" (chapters 6-10), "Managing Risks with Controls" (chapters 11-20) and "Being Audited" (chapters 21-24). As is becoming common practice with many books, references and other supplemental materials can be found at the publisher's website. The author manages to strike a good balance between the technical dimensions associated with the often tedious work of providing network security and the practical implications and consequences that often evolve from those efforts.

"Today, a majority of IT security attacks still originate over the network," Pompon cautions in "Network Security," the 17th chapter. "The attacks that don't originate from a network still usually involve a network in some manner. It seems that every device and application is now Internet aware, where even our household appliances are supporting social media accounts."

I found this to be a very sobering book. Certainly, my respect for those charged with keeping our digital world safe and secure has grown immensely as a result of my exposure to Pompon's extraordinary and frightening treatise on the new normal. If you are interested in learning more about what we are doing to keep our world safe from those who seek to harm us from the comfort of their laptops, this is one you might want to add to your personal library.

Reviewed by Aaron W. Hughey, Department of Counseling and Student Affairs, Western Kentucky University.