@ISACA
RELEVANT, TIMELY NEWS
Volume 26, 18 December 2013

Are You a Fearmonger? Tips on How Not to Be

By Bruce R. Wilkins, CISA, CISM, CGEIT, CRISC, CISSP

Have you ever wondered why security organizations are sometimes viewed as purveyors of fear? Or why some security managers fall prey to the stereotype of being a fearmonger? A fearmonger in this context threatens and instills fear to obtain resources to mitigate risk. The mitigated risk may or may not be relevant to the organization's risk appetite or reside in the organization's technology, and the fearmonger, in the worst case, does not know the difference.

Read More

Win a Free Trip to an ISACA Conference

One of the many benefits of being a topic leader in ISACA's Knowledge Center is that you are eligible to win a free ISACA® conference experience. ISACA appreciates the efforts of topic leaders and has launched a recognition program to reward topic leaders for their active participation in the Knowledge Center.

Read More

Stay Connected—Renew Your ISACA Membership

ISACA® membership gives you access to the critical information you need to succeed and add value to your enterprise. The association offers resources you can draw upon to enhance your skills, expand your professional connections, and experience a vibrant local and global community of colleagues.

Read More

Share Your Passion—Become an ISACA Volunteer

The 2014-15 Invitation to Participate is now open through 13 February 2014. Visit the Join an ISACA® Volunteer Body page of the ISACA web site for information regarding volunteer service at ISACA and links and other important information related to the volunteer process and ISACA's volunteer bodies.

Read More

New COBIT and SecaaS Resources Available

Remember to Provide Feedback on Guidelines by 31 December

ISACA® has issued the following new publications: *COBIT®5: Enabling Information* and the *Security as a Service* white paper. Additionally, the IS Audit and Assurance Guidelines exposure drafts are posted for online feedback through year-end 2013.

Read More

Book Review: *The Rootkit Arsenal, 2nd Edition*

Reviewed by Ibe Kalu Etea, CISA, CRISC, ACA, CFE, CRMA, ISO 9001:2008 QMS

The prevalence of hacking attempts and the increased risk posed by stealth-type security threats, such as rootkits, create a need for in-depth guidance that unveils attack and defense techniques practically. The rather murky rootkit terrain is thoroughly analyzed by Bill Blunden in this 2nd edition of *The Rootkit Arsenal*.

Read More

Are You a Fearmonger? Tips on How Not to Be

By Bruce R. Wilkins, CISA, CISM, CGEIT, CRISC, CISSP

Have you ever wondered why security organizations are sometimes viewed as purveyors of fear? Or why some security managers fall prey to the stereotype of being a fearmonger? A fearmonger in this context threatens and instills fear to obtain resources to mitigate risk. The mitigated risk may or may not be relevant to the organization's risk appetite or reside in the organization's technology, and the fearmonger, in the worst case, does not know the difference.

How did this happen and where did we did we go wrong? Well, many times the issue is

security's overcommitment to professionalism. In their zeal to inform, some security managers can be viewed as merely threatening.

Are you a fearmonger? Why be concerned if you are or are not? The issue of becoming the stereotype is that the informal organization within the business will begin to evolve the enterprise without your participation.

Here is a quick checklist of fearmongering mistakes that can be corrected easily to make you a better team player:

1. If the above statement provoked the reaction, "They cannot evolve the enterprise without me because I have an approved policy that says I will be involved," you may be a fearmonger. A security policy is in place to define what is expected from an engineering perspective. This is truly easier and more predictable than instilling a sense of craftsmanship in our technologist. If a security policy were solely stated for defining internal controls, only audit would read it. Some people forget that we need to build before we can audit. Being an equal team member is critical to maintaining parity, which is critical to a healthy approach to maintaining a security posture. This could be an education issue with the engineers.
2. If you react poorly to technological changes that result in new protection strategies, you may be a fearmonger. Some security managers attempt to stop the introduction of a new technology into their organizations even though the technology may give the organization a marketplace advantage. We sometimes forget our job is to figure out how to say yes. We are entrusted with finding new protection strategies and abandoning old protection strategies to meet the needs of our organization.
3. In conducting a root-cause analysis of your open vulnerabilities throughout the enterprise, if you find that your security policy is the root cause a majority of the time, you may be a fearmonger. This could mean the policies are overstated and unachievable. It is best to work with technology experts to tailor the implementation approach from the policy. It is okay to have a secure vision that is reflected in policy, but when it is blindly applied across the whole technology suite, you lose creditability to the inherent capabilities that vary across technologies.
4. If your security policy contains technological solutions, you may be a fearmonger. The proper separation of governance, policy and procedures shows an understanding of a strong management of change within your governance framework. Constantly having to change policies and obtain approvals takes away from providing the attention necessary to other parts of the security program.
5. If your discussions mainly focus on threats outside the context of your organization's risk appetite, you may be a fearmonger. It is important to have threat discussions in the context of an organization's business model and risk appetite. Remember that, as security experts, we are protecting for the sake of the business model, not protecting just for the sake of protecting.
6. In reviewing your security organization personnel qualifications, if you find that no

one on your staff is an engineer or technologist, you may be a fearmonger. It is critical that the right protection strategy be applied to the correct technologies. Technical staff members give the security manager an honest broker to better understand the nuances of why and when protection strategies must evolve. Having these conversations among technical people is critical to a mutual understanding of the security posture of the organization.

7. If all audit findings must be fixed, you may be a fearmonger. Depending on the quality of the auditor, audit findings may be all over the board. Strive to mitigate findings, not necessarily fix findings. There are some findings that absolutely must be corrected; other findings are false positives, not applicable or simply do not fit within the current protection strategies. Remember, audits are opportunities to improve your business case for security.

There is no doubt that being a security manager is demanding and even worse in a heavily regulated business environment. But whatever your threat environment, understanding protection strategies and having a reasonable implementation approach softens those hard, but necessary, threat-oriented discussions. The idea of risk avoidance is just not salable. Taking a risk management approach and presenting options to your leadership in concert with the technology chiefs should lead to a more stress-free life. You will be less likely to be seen as a purveyor of fear among your colleagues and more likely to be sought out as a valuable resource.

Bruce R. Wilkins, CISA, CISM, CGEIT, CRISC, CISSP, is the chief executive officer of TWM Associates Inc. In this capacity, Wilkins provides secure engineering solutions for innovative technology and cost-reducing approaches to existing security programs.

Win a Free Trip to an ISACA Conference

One of the many benefits of being a topic leader in ISACA's Knowledge Center is that you are eligible to win a free ISACA® conference experience. ISACA appreciates the efforts of topic leaders and has launched a recognition program to reward topic leaders for their active participation in the Knowledge Center. The three topic leaders with the highest activity rating (based on discussions and replies) will be recognized in *@ISACA* and on the ISACA web site on a quarterly basis. At the end of the year, the topic leader with the highest participation rate will win a trip to the next ISACA conference in their region.

To become a topic leader and participate in the recognition program, visit the Become a Topic Leader page of the ISACA web site for more information. Browse all Knowledge Center topics to match your area of expertise. There are immediate needs for topic leaders on the following Knowledge Center topics:

- Business Continuity/Disaster Recovery
- Cybersecurity

- Information Security Management
- Information Security Policies and Procedures
- PCI DSS
- Privacy/Data Protection
- SAP
- COBIT® 4.1
- COBIT® 5

The next recognition program begins on 1 January 2014 and ends 31 December 2014. To be eligible, Become a Topic Leader. Once you are a topic leader, you must opt in to the contest and agree to the contest rules. Void where prohibited.

Stay Connected—Renew Your ISACA Membership

ISACA® membership gives you access to the critical information you need to succeed and add value to your enterprise. The association offers resources you can draw upon to enhance your skills, expand your professional connections, and experience a vibrant local and global community of colleagues.

When you renew your membership, you retain your membership level and benefit from the following free or low-cost benefits, among others:

- Access to the latest research and development to add value to your career and enterprise
- Exclusive access to the *ISACA® Journal*
- Exclusive, member-only webinars and virtual conferences that cover timely topics on today's most challenging IT and information systems (IS) issues
- ISACA's eLibrary, featuring hundreds of in-demand titles
- Print and/or electronic deliverables of peer-reviewed research, COBIT® 5 and other publications essential to your profession
- Opportunity to earn more than 70 hours of CPE credits annually at no additional cost
- Connections with like-minded peers across the globe with whom you can exchange information and ideas in ISACA's Knowledge Center

ISACA provides resources and solutions that help enterprises and individuals achieve success, resulting in greater trust in, and value from, information systems. Don't miss out on the opportunity to stay up to date in your field. Visit the ISACA web site to renew your membership before 15 January.

Share Your Passion—Become an ISACA Volunteer

The 2014-15 Invitation to Participate is now open through 13 February 2014. Visit the Join an ISACA Volunteer Body page of the ISACA® web site for information regarding volunteer service at ISACA and links and other important information related to the volunteer process and ISACA's volunteer bodies.

Participants in ISACA's volunteer bodies support education and certification programs, professional conferences, research, education programs and professional standards. They also drive the creation and maintenance of products, services and benefits for ISACA members and constituents.

In addition to volunteering, you can nominate individuals who you believe would be an asset to an international-level ISACA volunteer body. To nominate someone, use the Volunteer Nomination Form. Nominations should be submitted well in advance of the 13 February 2014 volunteering deadline to allow nominees time to submit additional application information by the deadline.

Volunteers experience ISACA in unique ways. Join us and help shape your profession and your future. Become an ISACA volunteer.

New COBIT and SecaaS Resources Available

Remember to Provide Feedback on Guidelines by 31 December

ISACA® has issued the following new publications:

- *COBIT® 5: Enabling Information*—This detailed reference guide is for the information enabler for the governance and management of enterprise IT (GEIT). It further explains the information model (based on the COBIT® 5 generic enabler model) and provides examples of fully elaborated information entities. *COBIT® 5: Enabling Information* should be considered the information equivalent of *COBIT® 5: Enabling Processes.*
- *Security as a Service*—This white paper presents the potential impact of Security as a Service (SecaaS) on the enterprise. It identifies prospective business benefits, challenges and risk, and it presents recommended governance and risk management practices to minimize risk and optimize value from investments.

Additionally, the IS Audit and Assurance Guidelines exposure drafts are posted for online feedback through year-end 2013. The guidelines were updated to support the newly issued IS Audit and Assurance Standards. After public exposure feedback is incorporated, the new guidelines are scheduled to be issued in the third quarter of 2014 and will replace those

currently in force.

Information on current research projects is posted on the Current Projects page of the ISACA web site.

Book Review: *The Rootkit Arsenal, 2nd Edition*

Reviewed by Ibe Kalu Etea, CISA, CRISC, ACA, CFE, CRMA, ISO 9001:2008 QMS

The prevalence of hacking attempts and the increased risk posed by stealth-type security threats, such as rootkits, create a need for in-depth literature that unveils attack and defense techniques practically. The rather murky rootkit terrain is thoroughly analyzed by Bill Blunden in this 2nd edition of *The Rootkit Arsenal*.

The book creates points of convergence among elements of antiforensic technology, network security, investigative tactics and defense strategies. *The Rootkit Arsenal* is clearly at the forefront of current rootkit guidance in terms of the depth and array of content it provides, clearly illuminating the often unclear subject areas of antiforensics. Split into four parts, the book is a collection of tactics including armoring, API tracing, false flags, FISTing, obfuscation, code morphing, file scrubbing and data contraception.

The 1st part serves as a refresher course for intermediate to expert readers while laying a baseline for beginners. Investigative and counterforensic techniques are introduced, as are basic concepts that would serve as keystones for rootkit forays.

The 2nd part discusses various tactics of frustrating forensic methods, e.g., volume, file-system and file-signature analysis. The nature and complexity of techniques outlined morphs from easy to complex as the text progresses. Static and run-time executable analysis—the two types of forensic executable analysis—are explained, as are the tactics to foil them.

The 3rd part elucidates on the various tactics a forensic investigator would apply, initiating and resolving live incident response. Rootkit intrusion discovery tools are reviewed, as are countermeasures to undermine such efforts.

The 4th part gives a broad overview of the salient considerations needed by both investigators and intruders. Emphasis is placed on caution and not underestimating the enemy. Blunden concludes with some strategic recommendations for rootkit advancement and his own thoughts on how stealth techniques and intrusion serve the same purposes on a higher level than operating systems.

Blunden assumes a pragmatic approach, encouraging his audience to experiment using kernel debugging and unearthing new techniques themselves. The collection of code manipulation techniques and practices depicts a stadium scenario with boundless terrain on which to exercise.

Ibe Kalu Etea, CISA, CRISC, ACA, CFE, CRMA, ISO 9001:2008 QMS, is a corporate governance, internal controls, fraud and enterprise risk assurance professional. He also serves as a member on the advisory council of the Association of Certified Fraud Examiners (ACFE).