

Join the Discussion
Connect

Ambiguous Threats

By Ronald L. Mendell

This article discusses the ambiguity factor in threats and explains how psychological influences such as confirmation bias, comfort zones, and seeing only the “big picture” inhibit reducing ambiguity in assessing threats.

Abstract

Being able to recognize that not all threats present clarity in their potential level of harm increases an information security professional's decision-making powers. This article discusses the ambiguity factor in threats and explains how psychological influences such as confirmation bias, comfort zones, and seeing only the “big picture” inhibit reducing ambiguity in assessing threats. It cites recent examples of how ambiguity in threats prevented the installing of appropriate countermeasures. And, the article concludes with practical advice about detecting bias, recognizing and auditing comfort zones, and paying attention to small details within the big picture like USB drives or password management.

The classic dilemma

Many threats possess clarity. The information security professional correctly assesses initially the potential risk and impact to the organization. Well-documented and recognized attacks on networks fall into this category, which produces generally accepted countermeasures such as firewalls, intrusion detection systems, and DMZs. But, some threats have a “gray” quality. They do not sound immediate alarms for security decision-making. They remain ambiguous because of three psychological fac-

tors. First, we tend to seek out only facts that validate our existing mindset: the confirmation bias. Second, we lessen our sense of danger in situations or environments where the perception of hostility or threat is low: a comfort zone. And third, when concentrating on a big-picture security solution, we tend to overlook details, which enable workarounds for an adversary penetrating our major defenses.

A few definitions are in order. *Ambiguity*, in the information security context, means information that does not immediately fall “out-of-bounds” with regard to established security principles. It lacks being either clearly white or black, and to borrow from intrusion detection terminology, such grayness may lead to accepting a “false negative”: something not recognized as hostile or dangerous. An ambiguous threat is an event or series of events that remains below the daily concerns of information security professionals and their clients. Due to not recognizing them as something seriously hostile, though capable of causing significant harm, they stay submerged. Such a threat may simmer or dwell below the threshold of detection for significant periods of time due to the cited psychological factors. *Asynchronous threats* in information security become attacks that track differently from what defenders intended. Often smaller in scale and even in sophistication than the defensive countermeasures in place, these attacks rely upon surprise and breaching defenses on unanticipated

fronts. They have a “time-is-out-of- joint” quality (to borrow from Shakespeare) that blindsides defenders. Operators of web-sites and networks that do not consider themselves as targets, doing only a minimal vulnerability assessment occasionally, fall prey to this species of attack. (An alternate term having currency in security circles is *asymmetrical threat*, where the attacker has limited resources compared to the target but still can deliver debilitating attacks. Anonymous is an example of an organization that delivers both asynchronous and asymmetrical attacks.)

The classic dilemma of information security rests in handling High Impact/Low Probability events. Conventional thinking dictates that a High Impact/High Probability (HI/HP) event should be visible on everyone’s radar, so little challenge lies in recognizing the threat. Usually HI/HP threats get the needed resources. The risk matrix or table, where the severity of impact graduates from low to high on the table’s left side and probability does the same across the top, serves as a useful tool in categorizing threats (see Figure 1). After the categorizing is over, however, the challenge becomes what to do about low probability events. Are they to be totally disregarded? Low probability events do happen, but even in cases where the impact could be high, justifying the allocating of resources for countermeasures may be difficult. After all, a common adage in security is “to defend everything is to defend nothing.”¹ Thinking beyond the high/low probability dichotomy may become necessary, however, in an age of asynchronous threats.²

Asynchronous threats tend to be those that your security planning does not anticipate. And, most often they present themselves ambiguously. Responding to asynchronous threats requires breaking one’s thinking mode. As a part of changing that mode of thinking, we need to realize that even a high-impact and high-probability event can be ambiguous when the event regularly happens behind the scenes. Unintentional sensitive information leakage or corporate espionage both come to mind. So, ironically, ambiguity is not the exclusive province of the low-probability security incident. Perhaps the most common HI/HP event, which remains ambiguous, is corporate espionage. Whether one’s upper management ac-

IMPACT	Probability		
	Low	Medium	High
Low	Subscribers not a likely target, no history of problems (comfort zone established, confirmation bias working)	We have no previous experience to warrant this level of probability (a confirmation bias)	We have no previous experience to warrant this level of probability (a confirmation bias). Impact not evaluated.
Medium	Subscribers not a likely target	We have no previous experience to warrant this level of probability (a confirmation bias)	Not analyzed because the probability is initially assessed as low.
High	If an industry trend develops, more research may be warranted. Comfortable with past history so full impact not assessed.	If an industry trend develops, more research may be warranted. Comfortable with past history so full impact not assessed.	Not analyzed because the probability is initially assessed as low.

Figure 1 – Example of a High Impact/Low probability matrix – Kiplinger Case

knowledges the issue or not, all businesses of significant size face this insidious, invisible threat. Its failure to register on the daily radar creates its ambiguity. The “busyness” and hectic demands of daily business challenges hide corporate espionage from being recognized as a high-impact and high-probability event, and a loss of what Professor Michael A. Roberto calls “*sense making*” occurs: an inability to discern patterns outside of one’s regular frame of reference.³ (In the January 2012 issue of *Popular Mechanics*, an article on corporate and industrial espionage, “The Secret War” by Adam Piore, argues that American business frequently becomes a victim of this threat, causing an erosion of our technological base.)⁴

It is in the nature of human psychology to assimilate new information into existing patterns or images.

Analyzing ambiguous events

The binary risk/assessment table or matrix of impacts and probabilities cannot reduce consistently the issue of ambiguity, even in high-probability events.⁵ In considering, however, mid-range events, where the impacts and probabilities have a moderate or medium scale, the issue of eliminating ambiguity becomes even more problematic. Richards J. Heuer, Jr., in

1 The adage, based upon a quotation from Frederick the Great, may seem trite, but it reflects the plethora of information and admonitions available to users regarding threats. Michael Kassner in a blog posting asks the question regarding what security advice should computer users ignore. In reality, even the best-intentioned consumer of information security warnings cannot react to everything, some filtering is necessary. The aim of this article is to examine the psychology behind the filtering process. (See <http://www.techrepublic.com/blog/security/are-users-right-in-rejecting-security-advice/3275>.)

2 Defense Business Agility Forum, <http://dcmo.defense.gov/dbaf/about.html>, asynchronous threats as the new paradigm. (Note: The U.S. Department of Defense has closed access to the content of this site due to current security conditions.) The website of Anonymous has similar references to asymmetrical or asynchronous threats at <http://www.wecareanonymous.eu/2011/11/ufouo-asymmetric-warfare-group-sniper.html>.

3 Michael A. Roberto discusses the issue of “sense making,” the art of discerning patterns during ambiguous events, in Lecture Seven of *The Art of Critical Decision Making*, The Teaching Company, Chantilly, VA, 2009.

4 Ronald L. Mendell, *The Quiet Threat*, second edition, published by Charles C. Thomas in 2010, covers at length why industrial espionage stays under the radar most of the time. *Popular Mechanics* in the January 2012 article, “The Secret War” by Adam Piore, also echoes this theme. The pattern remains ambiguous because it works subtly in many cases behind the scenes. Usually, headlines occur only when all the damage is done. And, organizations do not always perceive themselves as possible victims, when in reality any company can become prey.

5 William Arthur Conklin, Greg White, et al, *Principles of Computer Security*, McGraw-Hill, 2010, p.533, Figure 20.3, “Binary Assessment.” A binary assessment is a dichotomy between high and low impacts and/or probabilities. Obviously, one can widen the scale to include mid-range impacts or probabilities, but that step often does not eliminate ambiguity.

the *Psychology of Intelligence Analysis*, struggles with threats that do not fall at either end of the spectrum.⁶ In reviewing the problem, he argues that we tend to perceive what we expect to perceive. Usually, mindsets have an intractable quality, which means that they tend to form quickly, but they become resistant to modification and change. It is in the nature of human psychology to assimilate new information into existing patterns or images. This quality of our minds makes it difficult to critique the same information from multiple perspectives. When confronted with initially ambiguous data, or what Heuer calls “blurred stimuli,” we

A comfort zone becomes an area of unaudited trust.

end up with a skewed or even a blunted perception, even in cases where later and better information becomes available. To lessen ambiguity, Heuer counsels that we should identify “the degree and source of uncertainty,” which involves considering alternate explanations and scenarios for the pattern that we initially perceive for the event. Concrete examples of sources, in order of increasing certainty, are the following:

1. Internal human sources
2. Other information security professionals
3. Documented case studies

The primary internal human source for many security professionals is their boss or another co-worker. But while these sources obviously deserve serious respect, their perspectives may be skewed. Other security professionals may offer a broader viewpoint in accessing a threat if a significant degree of ambiguity still remains. Documented case studies, however, available in information security publications both online and in print, offer the greatest opportunity in recognizing threats that have succeeded elsewhere against data similar to your sensitive data. No single source eliminates ambiguity in threats. Yet, when confronted with a possible high impact, investigating beyond in-house thinking may confer additional clarity.

Examples of ambiguous threats

Reviewing some examples of low- or mid-probability events should aid in understanding better the psychology of ambiguous threats. (In choosing these examples, I considered the perspective of the data’s owner. Based upon their security actions prior to the loss or attack, the ultimate compromise or loss of their data resulted from limited vulnerability analysis because the threats did not rise to a high level of visibility to the data’s owner.)

On June 25, 2011 Kiplinger Washington Editors, the publishers of *Kiplinger’s Personal Finance Magazine*, discovered that customer account data for over 142,000 subscribers to their magazine had been compromised through a break-in by an

unidentified third-party.⁷ A spokesman for the magazine commented that the greatest challenge in investigating the breach was in identifying what the hackers were after. The victimized company did not know exactly what information the intruders absconded from the database. In other words, the company did not fully understand why it would be a target for information thieves. Whatever controls were in place did not effectively block access to sensitive customer information and did not permit detection and tracking of any data compromised. Obviously, magazine subscriber data fell into a mid-range of vulnerability. It lacked the technological allure of say the latest smart phone device’s specifications, or that of cutting-edge laser weapon technology. Yet, mundane or even “boring” data of customers’ names, addresses, and other identifying credentials are targeted by data predators, whether the victim is Sam’s Pizza Parlor on the corner or General Motors.

And, in fairness to Kiplinger, they are not the only victim of the plunders of mid-range data. In a July 7, 2011 report, the *Washington Post* had 1.27 million user IDs and email addresses compromised from their jobs website.⁸ Again, the victim was somewhat surprised at the attack. Neither financial nor highly sensitive customer information became prey in the attack. In retrospect, however, the *Washington Post* concluded that the customers’ email addresses had value in phishing attacks. Also, the user IDs offered possible entrance into various computer systems and networks. The lesson learned from this attack involves perspective. From the perspective of the *Washington Post*, the data on their jobs website was a low-to-medium security risk or target. But, one has to consider the perspective of the attacker in protecting information. Unfortunately, one person’s insignificant data is another person’s treasure. And mining the foothills for valuable data is nothing new. In pre-Internet days, the trick was to go into a dumpster and find credit card carbons in order to get credit card numbers. The same idea applies today: even “insignificant data” can be a stepping stone to more valuable information.

The aim, however, is not undue criticism of the *Washington Post* or *Kiplinger’s Personal Finance Magazine*. Failing to consider the attacker’s perspective, when evaluating a medium- or a low-range threat, becomes a common pitfall arising from ambiguity. And in some cases, a reasonable cost-benefit analysis produces the decision not to devote resources against threats in the medium-to-low range. This article stresses that this needs to be a conscious decision, not a lapse in analysis. An organization should not drift into this security posture.

Another area of ambiguity involves the psychological comfort zone. At times, security becomes less because the organization is operating within its security perimeter or in an area that is perceived as safe. Sutter Gould Medical Foundation, in a July 5, 2011 account, revealed that a box containing 1200

6 Richards J. Heuer, *Psychology of Intelligence Analysis*. CIA, Washington, D.C., 1999.

7 <http://www.databreaches.net/?p=19522>, “Kiplinger Magazine” July 8, 2011 (from Bloomberg, July 8, 2011)

8 <http://www.databreaches.net/?p=19487>, “Washington Post Jobs site” July 7, 2011.

patient records ended up in a landfill.⁹ A vendor under contract to scan patient records inadvertently sent the box for disposal after scanning. The vendor was an entity that the organization felt comfortable with, and there was not an auditing procedure in place to account for scanned materials as the operation progressed. Such a comfort zone becomes an area of unaudited trust.

In another variation on the comfort zone “trap,” Plymouth State University in New Hampshire revealed that on May 18, 2011, 1059 student records were unaccounted for.¹⁰ These records contained student names and social security numbers. Stored on an external hard drive, these records were to be sent to the state licensing board in New Hampshire in order to establish certifications for teacher candidates. Unfortunately, the external hard drive, which was used internally within the university offices, disappeared. The university’s comfort zone had two aspects: the drive was used internally (and was deemed safe within the security perimeter) and the sending of the data was a routine matter. The routine nature of the university’s activities regarding this data created the ambiguity, for the process was not regarded as having significant risk. And again, no harsh criticism is intended of these two victims. Rather, comfort-zone ambiguities occur daily, and many times they are difficult to recognize.

Steps in reducing ambiguity

What then are some steps information security professionals can take to reduce ambiguous threats? Asking a series of questions during the evaluation process may aid in analyzing these threats. But screening questions are far from foolproof. Ambiguous threats always remain a minefield for the information professional, but proper questioning and self-examination can filter out some of the biases that lead to ambiguity.

Confirmation bias

The first question seeks to overcome what Michael Roberto calls “confirmation bias.” This bias emerges when the security professional only looks at information that confirms pre-existing viewpoints or perspectives regarding the threat.¹¹ For example, if we assume that no one would be interested in our data because it is not a “top target,” then we are not considering any threat agents who do not share that perspective.

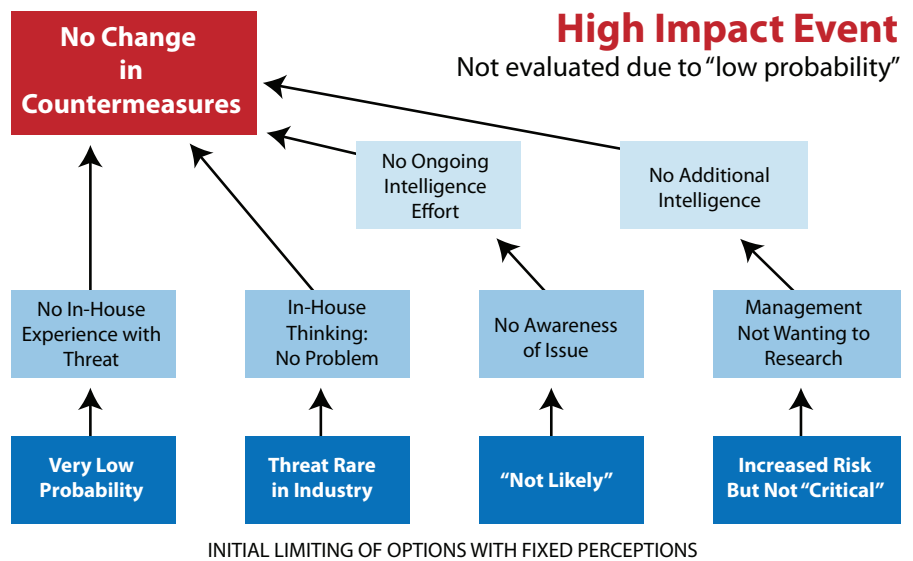


Figure 2 – An attack tree example illustrating confirmation bias

Who would be interested in our data? In asking this question we should accept all possible answers, even if initially they appear off-the-wall. Once we list all possible answers, then we can weed out those threats that cause minimal damage. We can also use a tool such as an attack tree to visualize threat agents and their methods, mapping an attack upon data that at first glance appears to have minimal value (see Figure 2).¹² Seeking out attacks that can escalate from simple footholds in data and cause significant damage should be the analytical goal.

Comfort zones

Detecting comfort zones leads to the next question. What assumptions are we making about the safety of our internal data and our internal trust relationships? In other words, do proper auditing controls exist on data handled internally? The rule of thumb should be that any personally identifiable information (PII) or data that could lead to the discovery of PII requires secure processing, no matter how comfortable we feel about its location during processing. The same attitude applies to sensitive business information, whether it be financial data, trade secrets, or other proprietary data. During all processing, audit checks need to be built-in to ensure that the data is not lost or compromised. (For example, in the Sutter Gould Medical Foundation case, checking *in* and *out* boxes on a control log could have prevented the loss. They were expecting to get their files back after the scanning, but had no cross-checking process to ensure the immediate return.) In referring back to Heuer, always consider alternate scenarios where internally handled PII or sensitive business data falls

9 <http://www.databreaches.net/?s=Sutter+Gould+Medical+Foundation>, “Sutter Gould Medical Foundation” July 5, 2011.
 10 <http://www.databreaches.net/?s=Plymouth+State+University>, “Plymouth State University” breach of May 18, 2011, listed on site July 5, 2011.
 11 Michael A. Roberto discusses “confirmation bias” in Lecture Two of *The Art of Critical Decision Making*. The Teaching Company, Chantilly, VA, 2009. Confirmation bias happens when one looks only for information that reinforces a position or perspective already held.

12 Attack Trees: An example of an attack tree is found on ISACA’s Web site at <http://www.isaca.org/Journal/Past-Issues/2007/Volume-3/Pages/Analyzing-the-Security-of-Internet-Banking-Authentication-Mechanisms1.aspx>, and Bruce Schneier’s paper on Attack Trees at <http://www.schneier.com/paper-attacktrees-ddj-ft.html> has become a standard reference. The website <http://www.isograph-software.com/atpover.htm> offers a demo and a trial version of software to create attack trees. And, the PDF document found at <http://www.amenaza.com/downloads/docs/AttackTreeFundamentals.pdf> “Fundamentals of Capabilities-based Attack Tree Analysis” provides a good overview on developing attack trees.

into the wrong hands. Again, attack trees can be a useful tool in identifying these alternate scenarios. And as Microsoft's *Threat Modeling* points out, "understanding the adversary's view" becomes critical.¹³ Always consider the entry points, the trust levels, the assets being protected, and the exits from any system or process. In other words, map out where your information assets move about your system and what vulnerabilities they face along the way. Information flowcharts and diagrams can identify where adversaries may insert themselves or even where

information assets may become lost as in the Sutter Gould case (see Figure 3).

Effective intelligence can minimize the ambiguity.

Offsite Document Scanning

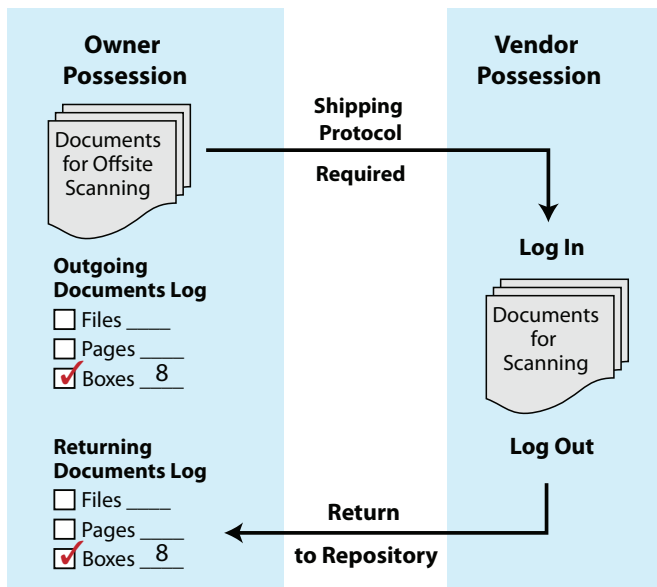


Figure 3 – Information flow diagram example – Sutter Gould Case – possible safeguards

Avoiding the big picture

Finally, avoid seeing all problems from just the "big" perspective. A great deal of the focus in information security surrounds big threats like state-sponsored terrorism, international crime rings hacking into networks, and state-sponsored industrial or corporate espionage. Of course, there is nothing wrong with focusing on these areas. Yet, the information security professional must not overlook that even small events sometimes do generate big losses in these arenas. If we focus on just the big picture in, say, industrial espionage by concentrating on large-scale technology as the main countermeasure, we can miss the tight coupling and the multiplier effect of small holes in our security (see Figure 4). "Tight coupling," described by Michael Roberto, happens when one event directly causes another, for example, when one user responds

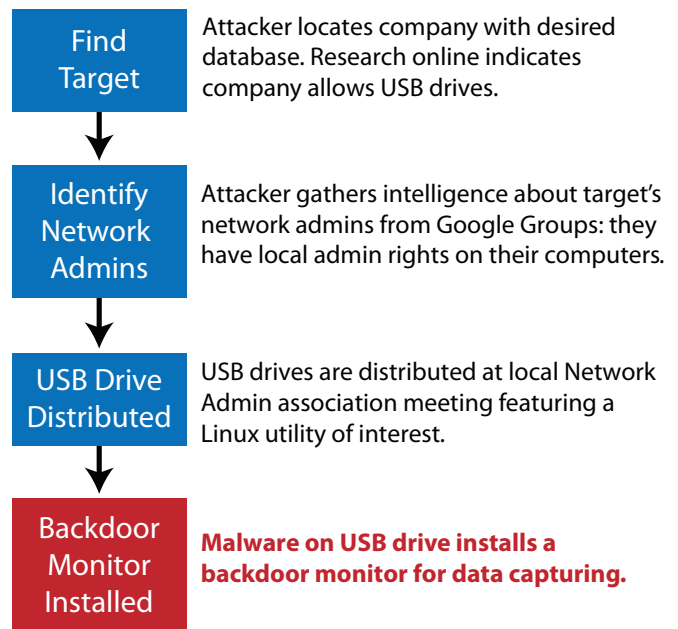


Figure 4 – "Tight Coupling" – USB drive attack tree example

to a phishing attack and immediately all the other users in his email address book receive the attack.¹⁴ The old proverb best explains it: "For a want of a nail the horseshoe was lost, and for the want of a horseshoe, the horse was lost, and for the want of a horse, the rider was lost." Asynchronous attackers are not intimidated by your vast infrastructure of technological countermeasures. A recent article in *Popular Mechanics* identifies the USB drive as the most effective way to get behind the perimeter defenses of any network.¹⁵ Once plugged into a machine, the USB drive is quite capable of loading various malware to create a back channel for a would-be attacker. And the malware can easily multiply across numerous machines. So, always supplement large-scale thinking with a small-scale analysis.

In addition to USB drives, a simple flaw in managing passwords is another detail that can generate considerable harm. The recent attack by Anonymous against the national security consulting firm Stratfor (Strategic Forecasting, Inc.) in Austin, Texas, caused the unauthorized disclosure of over 800,000 email addresses and an equal number of hashed passwords of clients.¹⁶ However, the subsequent deciphering of thousands of hashes using Hashcat by The TechHerald revealed many clients used poor, easy-to-guess passwords. Such

14 Michael A. Roberto explains "tight coupling" in Lecture Seventeen of *The Art of Critical Decision Making*, The Teaching Company, Chantilly, VA, 2009.

15 Adam Piore, "The Secret War," *Popular Mechanics*, January 2012, describes the USB drive as one of the small things, which can cause great harm especially in corporate or industrial espionage.

16 "Even Experts Use Awful Passwords, Hack Reveals," FoxNews.com, January 5, 2012, http://www.foxnews.com/scitech/2012/01/05/even-experts-use-awful-passwords-hack-reveals/?cmpid=cmt_email_Gigya_Even_Experts_Use_Awful_Passwords%2C_Hack_Reveals; "New Analysis of Stratfor Anonymous Breach," Identity Finder, December 30, 2011, <http://www.identityfinder.com/blog/post/Update-Identity-Finder-Releases-New-Analysis-of-StratforAnonymous-Breach3b-Warns-Victims-to-Beware-of-Phishing-and-Change-Passwords.aspx>; "Report: Analysis of the Stratfor Password List," Steve Pagan, January, 2, 2012, <http://www.thetechherald.com/articles/Report-Analysis-of-the-Stratfor-Password-List>.

13 Frank Swiderski and Window Snyder, *Threat Modeling*, Microsoft Press, 2004.

revelations increased the embarrassment of Stratfor's clients and seriously affected the firm's reputation. The firm was not enforcing a password policy commensurate with sensitivity of the information and the ultimate privacy needs of its clients, which numbered among Fortune 500 companies. Consider the little ways where attackers exploit small, but effective holes in your armor.¹⁷ Regular penetration testing of your network's defenses can identify these holes early in the game. And a comprehensive vulnerability scanner can audit password policies and do compliance checks, alerting password weaknesses before a serious breach.

As an adjunct to these ideas for countermeasures, let us not forget the need for good intelligence gathering. The process can be as simple as doing Internet searches for similar attacks against the kind of data that you are trying to protect. Most attacks on data have happened before and will happen again because of the ambiguous nature of the threats. Effective intelligence can minimize the ambiguity. As Sun Tzu counsels in *The Art of War*: "Foreknowledge cannot be solicited from spirits, nor from the gods, nor by analogy with past events, nor from calculations. It must be obtained from men who know the enemy situation."¹⁸ Learn from others in cyberspace, and by networking with other security professionals to gain the additional perspectives that you need to reduce ambiguity in threats.

Summing up

Reducing the ambiguity of threats requires overcoming confirmation bias, recognizing comfort zones, and by not overlooking details, even when implementing a "big picture" security program. Being able to step outside of one's mindset is essential to minimizing confirmation bias, and attack trees are a useful tool for identifying alternate viewpoints about a threat. Comfort zones are essentially trust relationships. Analyzing these trust relationships with a skeptical yet constructive eye can identify needed controls to ensure the trust model is not compromised. Attack trees and information flow diagrams aid in identifying weak points. Finally, consider how overlooking small details like the internal use of USB drives or minimal password controls provides "end runs" around the security infrastructure. Regular gathering of security intelligence and penetration testing can aid in identifying the small details that can lead to major problems.

About the Author

Ronald Mendell, M.S., CISSP, is an information security consultant and writer specializing in the psychological aspects of IT security. He is currently a full adjunct



¹⁷ David Kilcullen in *The Accidental Guerrilla*, Oxford University Press, 2009 and in "One Nation Under Arms" by Todd S. Purdum in *Vanity Fair*, January 2012 discuss some of the pitfalls in maintaining just a large-scale, broad focus on security problems. The resolution of big-scale issues may lie, unfortunately, in increasing attention to small-scale details like the use of USB drives.

¹⁸ Sun Tzu, *The Art of War*.

professor in the Computer Science department at Austin Community College in Austin, Texas. His previous articles in the *ISSA Journal* include "Information Security – Overcoming Organizational Obstacles," in July 2011 and "The Psychology of Information Security," in March 2007. He may be reached at rmendell@austincc.edu.

CONNECT
LEARN
ADVANCE

Supporting the Development
of Information Security
Professionals Worldwide

WWW.ISSA.ORG