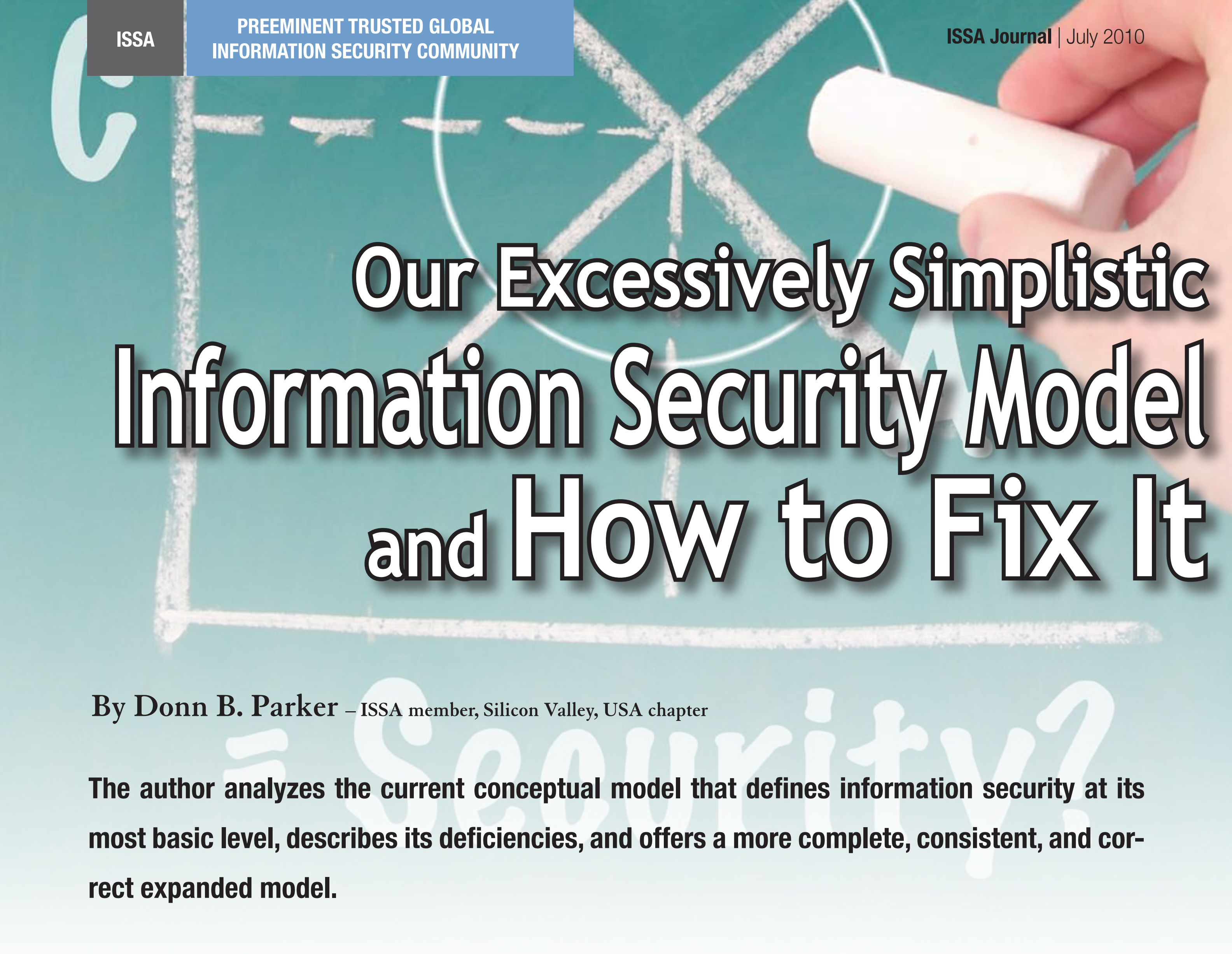


Our Excessively Simplistic Information Security Model and How to Fix It

By Donn B. Parker – ISSA member, Silicon Valley, USA chapter

The author analyzes the current conceptual model that defines information security at its most basic level, describes its deficiencies, and offers a more complete, consistent, and correct expanded model.

Abstract

I present and analyze here my version of the Current Conceptual Definition Model that defines information security at its most basic level. The purpose is to show its deficiencies and offer an expanded New Conceptual Definition Model that I claim is complete, consistent, and correct at the level of abstraction that I have chosen. I end this article with some take-away ideas for immediate use and a reading list for more in-depth study.

The basic level that I have chosen here is ideal for use in organizing categories for threat and vulnerability analysis and controls selection. It helps greatly to avoid overlooking important potential threats, vulnerabilities, and security solutions that are the most common problems in conducting organizational security reviews. Information security is an open-ended art and definable with both more and less detailed models than presented here. However, at other levels the number of descriptors required grows rapidly and becomes even more open-ended with unknown descriptors to foil us in our battle against intelligent perpetrators.

Examples of models with more or less detailed levels of abstraction might include attack vectors such as phishing, malware, spam, denial of service, and many more poorly defined jargon-named ones or at a more advanced level including computer-related fraud, theft, larceny, embezzlement, conspiracy, sabotage, extortion, espionage, and so forth. More detailed abstractions become confusing because the descriptors are defined differently in different literature and law jurisdictions. The identification of actual controls would also be required in more detailed abstractions rather than just control objectives or control purposes, and actual controls would expand to include many variations that grow in wordage, features, and complexity, becoming impossible to make complete, consistent, and non-redundant. I claim that my new model is complete to the extent that no experts so far have been able to show that there are additional descriptors needed, and I offer this as a challenge to security experts.

The current model

I derived the Current Conceptual Definitional Model (Current Model) from the study of several organization policies many years ago, and it is still representative of the security literature today. This model is simple, easily and quickly explained to management, information owners and users, and legislative assistants that write our laws. However, we are dangerously deceiving them by its simplicity, errors, and deficiencies.

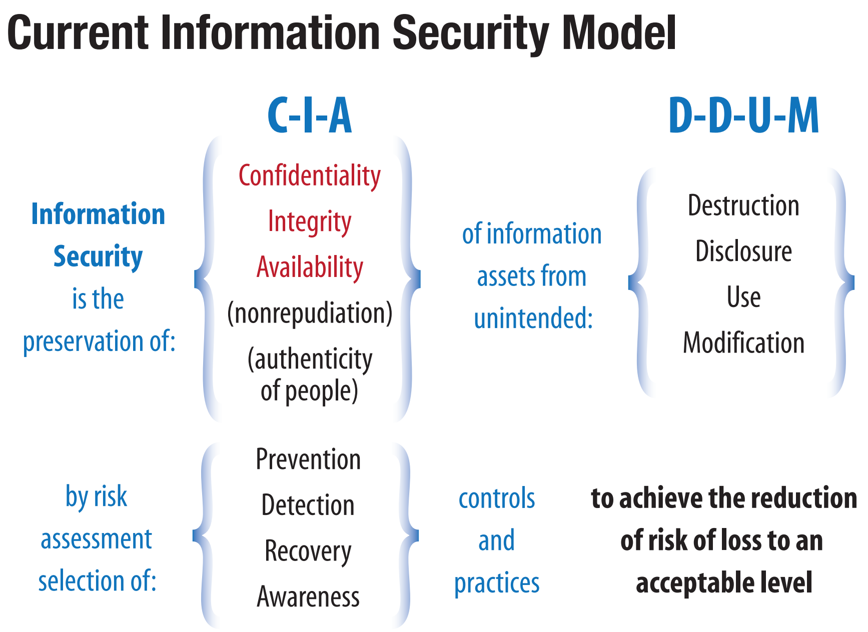

Current Information Security Model
C-I-A
D-D-U-M
Information Security is the preservation of:
Confidentiality
Integrity
Availability
(nonrepudiation)
(authenticity of people)
of information assets from unintended:
Destruction
Disclosure
Use
Modification
by risk assessment selection of:
Prevention
Detection
Recovery
Awareness
controls and practices
to achieve the reduction of risk of loss to an acceptable level

Figure 1 – Current Conceptual Definitional Information Security Model (Current Model).

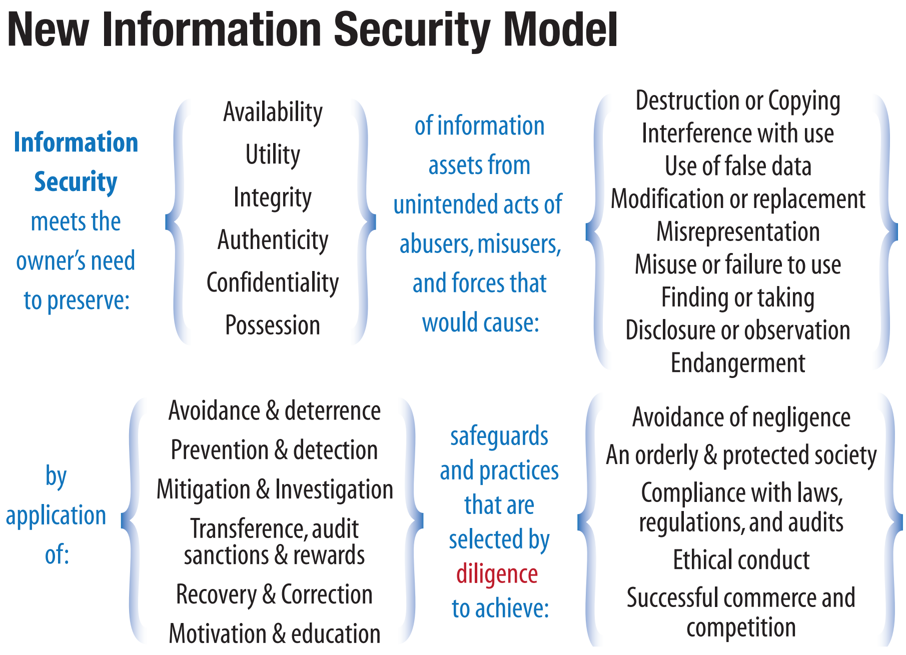

New Information Security Model
Information Security meets the owner's need to preserve:
Availability
Utility
Integrity
Authenticity
Confidentiality
Possession
of information assets from unintended acts of abusers, misusers, and forces that would cause:
Destruction or Copying
Interference with use
Use of false data
Modification or replacement
Misrepresentation
Misuse or failure to use
Finding or taking
Disclosure or observation
Endangerment
by application of:
Avoidance & deterrence
Prevention & detection
Mitigation & Investigation
Transference, audit sanctions & rewards
Recovery & Correction
Motivation & education
safeguards and practices that are selected by diligence to achieve:
Avoidance of negligence
An orderly & protected society
Compliance with laws, regulations, and audits
Ethical conduct
Successful commerce and competition

Figure 2 – The New Fundamental Conceptual Information Security Model (New Model).

The Current Model (Figure 1) contains the descriptors common to most of the policies I have examined. Several policies included additional descriptors where the writers attempted to account for deficiencies. For example, the U.S. Government rightly agreed that *confidentiality*, *integrity*, and *availability* (CIA) were not enough security states of information, so they added *non-repudiation* and *authenticity* of people. I believe the International Standards organization then added these additional security information state descriptors to their definition to follow suit. This makes the list of descriptors of security states of information more inconsistent and incorrect than CIA alone.

Here are my reasons for rejecting this particular expansion of CIA in my New Model (Figure 2). Repudiation may be valid or false, and it is not clear which is meant. Why would repudiation be important enough to add to the list but not its equally significant inverse, deception, that would cover social engineering and spam attacks at the same level of abstraction? Misrepresentation would be a better descriptor including both repudiation and deception, but misrepresentation is an act and result of an act that belongs elsewhere in the Model and "non-misrepresentation" is an awkward double negative word. Another failing is that the second added state, authenticity, applies to the identity of people whereas the other three descriptors refer to the secure states of information.

Many of the reasons for expanding and restating parts of the Current Model to form the New Model are obvious and left for the reader to grasp from simply comparing the current and new versions of the model. The rest of this article is devoted to explaining how and why I evolved my New Model from the Current Model in the less obvious ways. For example, I find it appalling that some security professionals would not already be using all of the descriptors in the New Model. For example, *observation* as well as *disclosure* is a violation of confidentiality, and solving security problems should start with avoidance and deterrence before prevention and detection. There is some redundancy in both models, but this is necessary to achieve comprehensiveness in dealing with likely intelligent and ingenious potential perpetrators who will always take advantage of any shortcomings in our defenses.

Model overview

Notice that the New Model focuses on stakeholders and wrongdoers not found in the Current Model. Information security has not concentrated sufficiently on the role that people play in perpetrating and defending against information-related loss. Security is about people (and forces or acts of nature such as storms, heat, cold, or shaking), not just technology. The New Model concerns forces and what people do as owners, users, custodians, and defenders of an organization's assets and the abusers, misusers, or wrongdoers that would cause harm. I also refer to more inclusive "unintended" acts in both the new and current models that do not necessarily do harm but are not desired rather than using "unauthorized," " harmful ," or "intentional and unintentional" acts (errors and omissions.) I leave undefined who decides what is unintended in these models.

The security states of information

Ross A. Leo, Chief of Technical Operations and Assurance for The Data Trust Company, claims he coined the triad states of confidentiality, integrity, and availability (CIA) of information in 1986. CIA is widely used including this quote from the Wikipedia: "The term information security… [has the]… goal of protecting the confidentiality, integrity and availability of information." *The Business Dictionary* defines information security as "Safe-guarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity."[1] CIA is often stated at the beginning of articles and papers defining information security but then is ignored in the remainder of the work. Sometimes security analysts use the CIA states as column headings to delineate kinds of threats, vulnerabilities, controls, losses, and risks. They do this at their peril as I shall explain.

U.S. Government definitions of CIA are stated in *The Guide for Applying the Risk Management Framework to Federal information Systems*, National Institute of Standards and Technology (NIST) Special Publication 800-37-rev 1, Appendix B Glossary:

- **Confidentiality** – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- **Integrity** – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- **Availability** – Ensuring timely and reliable access to and use of information

NIST has used CIA for many years primarily to define information security. Lawyers and politicians adopted the definition and put it into law (The U.S. Code, Title 44, Chapter 35, Sec. 3542.) NIST quotes the definition from the law in the glossary of the *Guide* and its many other publications. Actually the glossary entries are not definitions of CIA; they are explanations of how to achieve CIA of information. The definitions of CIA are implied by the explanations.

Confidentiality and possession

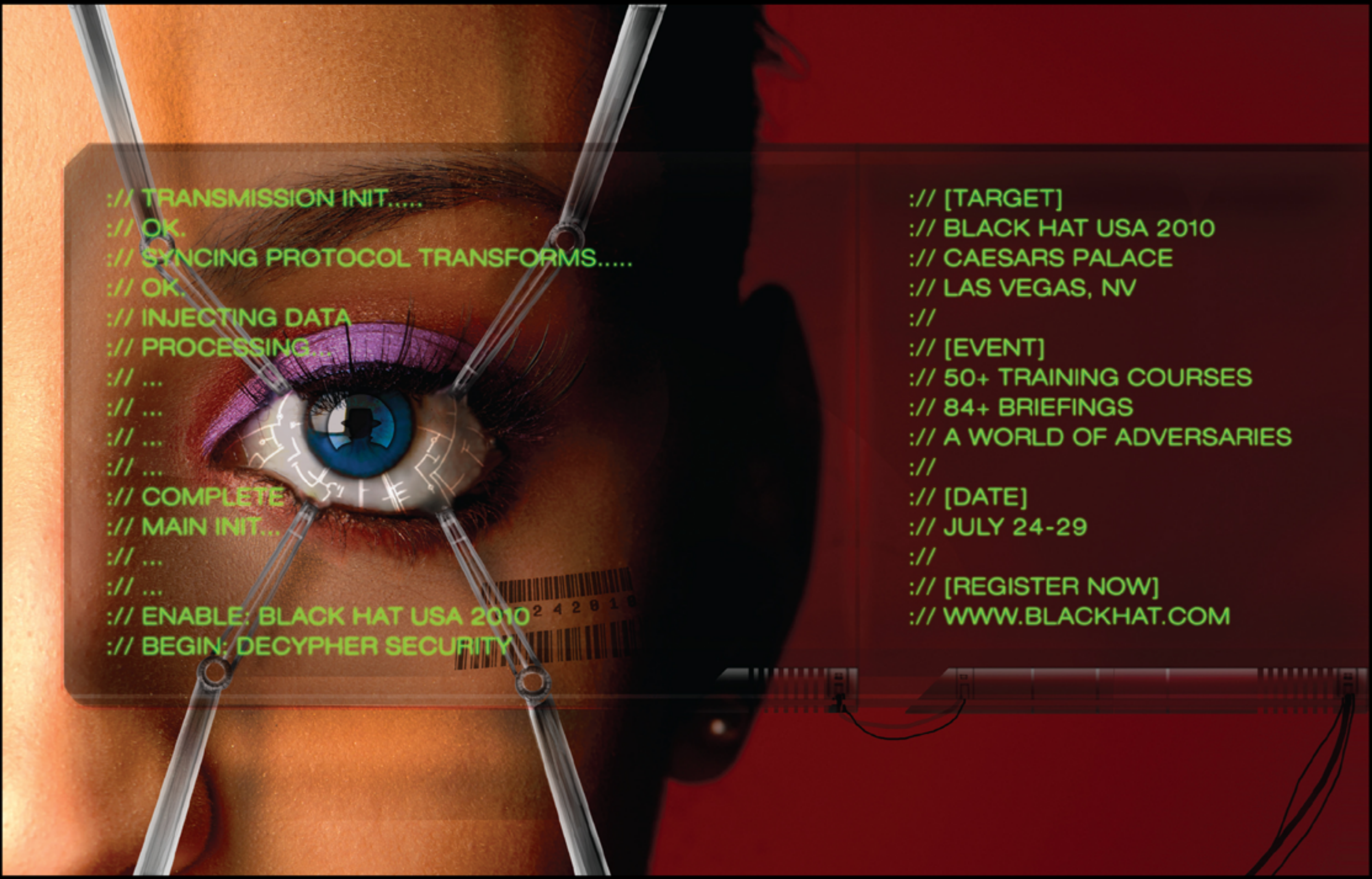
Confidentiality *(quality or state of being private or secret; known only to a limited few)* can be violated by both disclosure, as stated in the NIST definition, and by observation that is not stated but is at least as important. A common form of observation or espionage results from "shoulder surfing" or observing the contents of other users' monitor displays. Much of the security literature ignores this important distinction and identifies only disclosure. NIST apparently chose to include observing or reading implicitly within the more general term, *access*. However, the problem here is that access is an ambiguous term that makes it unlikely to bring observation to mind. Access here as a verb according to dictionaries means to enter, approach, or locate information but does not mean to observe it. Disclosure or observation would be another step after access. Only disclosing and observing violate confidentiality, and access should not be included since it is not the means of disclosing or observing, although information may be accessed at some time before it is disclosed or observed.

The controls to preserve restriction on *disclosure*, *observation*, and *locate* are very different. Both disclosure and observation, and only those two results of abuse, should be identified in the violation of confidentiality. Locating confidential information would be a violation of confidentiality if existence or residence of the information is also confidential, but existence or residence is separate information from the confidential information to which it refers, and disclosure and observation information apply separately as well.

The NIST definition of confidentiality includes protecting personal privacy and proprietary information. Personal privacy is a human right preserved by law and does not belong in a definition of security and state of confidentiality. I notice that frequently privacy is identified separately from information security. Holding information confidential is one aspect of achieving privacy; privacy and confidentiality are not synonymous.

Personal and proprietary information are two kinds of information that could be confidential or not confidential. For example, the quarterly financial report of a public corporation is proprietary and confidential information before the end of the quarter and is published, proprietary and public after the end of the quarter. After it is published it must still be protected but from unauthorized modification (preserving authenticity and integrity) and protected from lack of availability and utility, not observation or disclosure (confidentiality) since it is public. If proprietary information is to be included in the NIST definition, then it should be called confidential proprietary information, and equally important other kinds of confidential information such as copyrighted information should then be included as well. (Even though copyright has limited meaning in government, it is important for government contractors.) Clearly listing the several kinds of confidential information is not desirable at my definition level of detail since the list would be open-ended and never complete

[1] http://www.businessdictionary.com/definition/integrity.html.


:// TRANSMISSION INIT.....
:// OK.
:// SYNCING PROTOCOL TRANSFORMS.....
:// OK.
:// INJECTING DATA
:// PROCESSING...
:// ...
:// ...
:// ...
:// ...
:// COMPLETE
:// MAIN INIT...
:// ...
:// ...
:// ENABLE: BLACK HAT USA 2010
:// BEGIN: DECYPHER SECURITY
:// [TARGET]
:// BLACK HAT USA 2010
:// CAESARS PALACE
:// LAS VEGAS, NV
://
:// [EVENT]
:// 50+ TRAINING COURSES
:// 84+ BRIEFINGS
:// A WORLD OF ADVERSARIES
://
:// [DATE]
:// JULY 24-29
://
:// [REGISTER NOW]
:// WWW.BLACKHAT.COM

(e.g., personal, proprietary, accounting, scientific, alphabetic, etc.)

In addition there is the more philosophical question about whether taking and using confidential information without humans observing or disclosing it is a violation of confidentiality, for example in acts of extortion. I will leave that as an issue for law journals with one exception. Adding the state to preserve possession along with the security state of confidentiality, as I do in the New Model, covers restrictions on unintended taking (stealing) or using information since possession means that the possessor could control its being taken or using it.

Also all copies of non-confidential information could be stolen and held for ransom and would be a case of loss of possession or availability and not necessarily covered by loss of confidentiality, integrity, authenticity, or utility. For example, the information could be in encrypted form or recorded on or in a medium for which the perpetrators have no means of reading it, or the perpetrators might not ever be aware that it contains confidential information. This would be a violation of possession first and then possibly a violation of confidentiality depending on what the perpetrators do next such as selling it to a party that could take advantage of the confidential information. If possession is not considered, a possible control of defense-in-depth might be overlooked. This provides another reason for including possession as a security state.

It is difficult to imagine, but true, that NIST defines security with only the three states of CIA and non-repudiation of information and omits the state of a copy of information having been stolen whether confidential or not and even whether applying any of the other NIST definitions or not. It makes more sense to include confidentiality and add possession *(a state of having in or taking into one's control or holding at one's disposal; actual physical control of property by one who holds for himself, as distinguished from custody; something owned or controlled)* as another, independent state of security.

Finally, whether it is intended that information be confidential or public, if it is owned, its possession should be protected from acts such as those leading to plagiarism or false attribution. For example, valuable public documents and websites are owned and protected legally by proprietary rights addressed by trade secret, copyright, and trade mark laws and require application of security controls and practices to ensure exclusive or desired possession. Information security implies protection of only confidential information in the Current Model. Adding possession as I do in the New Mode facilitates inclusion of protecting ownership and source of public as well as confidential information.

Integrity and authenticity

The NIST description of integrity (not a definition but how to achieve integrity) is not correct. Preserving integrity *(unimpaired or unmarred condition; soundness; entire correspondence with an original condition; the quality or state of being complete or undivided; material wholeness)* means guarding against unintended modification of the unimpaired condition, quality, and wholeness of information and does not include preserving the content or meaning that would otherwise destroy its authenticity (according to all authoritative dictionaries.) An unintended material deterioration in condition (e.g., "1234567890" that is so faint that you can barely read it) would be a loss of integrity and different from an unintended but readable modification (e.g., "2134567890") that changes content and authenticity. Information may be improperly modified but still have integrity, or it may be authentic (what the stakeholder expects it to be) but has lost its integrity. Destruction is correctly included in the NIST description of integrity since the information would be impaired and certainly not whole. Authenticity *(authoritative, valid, true, real, genuine, or worthy of acceptance or belief by reason of conformity to fact and reality)* must be included as a separate state along with the other states and not included within the meaning of integrity.

The NIST definition of integrity includes non-repudiation. However, non-repudiation is an issue of authenticity and is incorrectly included within integrity. The integrity of information has nothing to do with whether it is repudiated or not. It could be rejected because of its condition but not repudiated since repudiation refers to the meaning of its content. In any case repudiation is no more or less important than other threats such as stealing, false data entry, or deception. (Deception is the inverse of repudiation. False repudiation is claiming that information is not authorized or not valid when it is and was, and deception is claiming that information is authorized or valid when it is not authorized or valid.) Note that invalid information and information that lacks integrity could be authorized on purpose and exactly what the owner desires when, for example, the faulty information is used for test purposes. Misrepresentation of information is a better term to use since it includes both false repudiation and deception (although non-misrepresentation is an awkward double negative word).

The primary issue here is difference between condition (integrity) and validity (authenticity). Note that the security controls and practices to preserve each state are quite different. It is inconsistent and incorrect to make integrity mean both integrity and authenticity when information could exclusively have one of these states of security but not the other.

Availability and utility

Availability *(capable of use for the accomplishment of a purpose, immediately usable, accessible, may be obtained)* is assured by having timely access to information as stated correctly in the NIST glossary entry. However, the NIST inclusion of preserving reliability is not necessary for information to be available. I suspect that NIST intended that reliability means reliably available rather than the information being reliable. Information being reliable is a form of being unimpaired and valid and thus having integrity and authenticity, not availability. I conclude that claiming that information is available is sufficient to conclude it is reliably available.

Also information may be available and therefore usable but it doesn't necessarily have to be in useful form to be defined as available. For example, encrypted information for which the key is unknown may be available (usable) for cryptanalysis but might not be useful in its present form. Usable and useful are not the same. That is, information may be usable but not useful or may be useful but not usable. Therefore, a sixth independent state, utility *(useful, fitness for some purpose)*, is needed along with the other five states.

Conclusion about states of security

I have added possession–authenticity–utility to confidentiality–integrity–availability, constituting six security states of information. Prof. Mich Kabay at Norwich University fondly calls all of them together the Parkerian Hexad that replaces the incorrect and incomplete well-known CIA triad. I have also put the descriptors into a more logical order, e.g., if information is not available, the others do not matter; if information is not useful, the remaining ones do not matter very much; if information is not available and in useful form, then integrity is meaningless; and so on. We must also protect the intended precision and accuracy of information, but I assume these characteristics fall within integrity and authenticity respectively.

Note that I only refer to information assets and do not identify systems, communications, networks, facilities, or any other containers or media of information assets. Of course, protection of information requires protection of all of the containers and media of information including systems, communications networks, filing cabinets, flash memories, mobile devices, data centers, humans, symbols chiseled in stone, holes in paper or wood, ink on paper, and horses pawing their hooves on a theater stage.

All known abuses and misuses of information are addressed by violating the six states that I have specified. Complexity of having six descriptors is a concern when explaining security to lay persons, but I believe having completeness, correctness, and consistency are more important. One solution is to have the six states in three pairs: Confidentiality and possession, integrity and authenticity, and availability and utility.

We must make information security more than an open-ended, faulty, and imprecise art. It must be successful in protecting against the hoards of intelligent, observant, and determined enemies that take advantage of every weakness we create. We must start using correct, complete, and consistent security states of information in our threats and vulnerabilities analyses and controls and practices selections if we are to successfully compete with wrongdoers.

Destruction, disclosure, use, modification

The Wikipedia defines *information security* to be protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. In this list access and use of a computer are redundant, and accessing information is difficult to define. Disruption of information makes little sense. This leaves destruction, disclosure, use, and modification in the Current Model as the meaningful descriptors of the unintended acts and immediate results of those acts in the definition, and it is terribly deficient.

Identifying all vulnerabilities in the most generic terms would be a short and useless list: physical, human, logical, electronic, and mechanical. A long open-ended (incomplete) detailed list would be impractical since just about everything is a vulnerability under the appropriate circumstances (With a big enough hammer you can break anything.) Since we never know all of our vulnerabilities, I list instead most if not all of the possible basic acts and results of those acts. The vulnerabilities may be derived or cataloged at a more detailed level of abstraction in specific instances and circumstances.

Knowing the unintended acts and results (from start to finish called attack vectors) is necessary to identify vulnerabilities and choose the functions (from the next box in the model) of security controls and practices to be applied. For example, an attack vector might consist of:

- Learning about and taking advantage of vulnerabilities, including social engineering opportunities
- Identifying and locating unlocked information
- Discovering and avoiding or overcoming controls
- Overcoming need-to-know and need-to-withhold specifications
- Deleting evidence of the attack
- Seeking and taking opportunities to profit from newly acquired possession

The result would be unintended finding, taking (stealing), and profiting from the attack vector.

(By the way, just finding the existence or location of sensitive information whether taken or not may be a significant violation not often recognized, and need-to-withhold is just as important as the inverse of need-to-know.)

The list of acts and results in the New Model is abbreviated here to only a small degree to keep the Model as simple and useful as possible. For example, destruction includes damage. The list is complete to my knowledge in that any and all acts fit under the general categories listed in the New Model no matter what new technologies inevitably arise to introduce variations (describable at a more detailed level than this Model provides.) For example, as stated previously misrepresentation is included to cover both false repudiation and deception. (False repudiation is the act of denial that valid information is valid, and deception is the claim that invalid information is valid.)

Note the inclusion of endangerment in the New Model. This could be the most common violation of all time, and I find many security professionals overlook it. It is often the result of the practice of information security professionals in their failure to adequately protect the most sensitive information that they hold, namely the information that recursively concerns the security of the most sensitive information of the organization. It is a gross violation of security to publicly reveal details of installed or missing security controls and practices, vulnerabilities, locations, assets, and loss experience that aids potential perpetrators. This leaves us with a serious deficiency of being unable to share useful security information. However, we can overcome this limitation by one-on-one or small-group sharing based on a mutual trust among security professionals.

Motivation does not even appear in our security vocabulary.

Failure to use or more generally failure to engage in potentially harmful acts when there is a legitimate need or instructed by higher management to do so is another violation often missing from others' lists. For example, and as stated previously, computer programming requires that the coder produces and uses false data for testing his program, and testing information security may include attempting to violate controls and practices (having first alerted all stakeholders of the tests for ethical reasons.) Also sometimes emergency situations arise in poorly designed systems requiring unintended actions. For example, a security practitioner may find it necessary to destroy copies of sensitive information rather than let them be used in insecure circumstances or fall into the hands of an industrial spy.

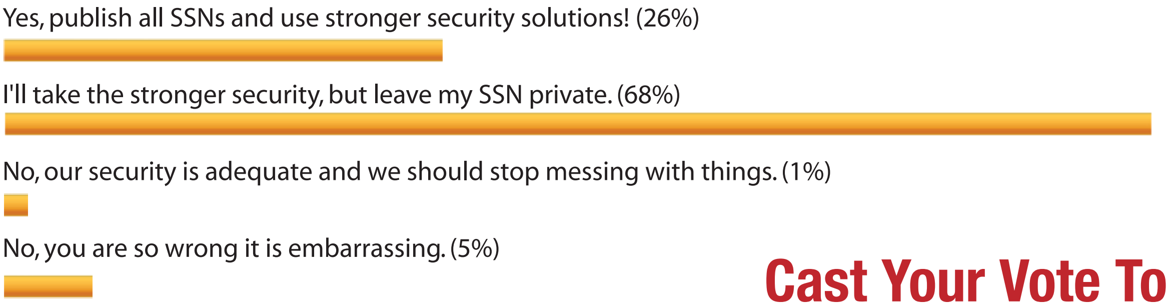
Types of controls and practices

The third box in my New Model contains the control types by function or objective of security controls and practices listed

ISSA Connect Survey

Should ISSA spearhead an initiative to make SSNs public?

It's time to convert old, weak techniques for protecting against identity theft into stronger options.
Should ISSA form a committee to target appropriate officials to publish SSNs and outlaw their use as secrets?



Total Votes: **99**

Cast Your Vote Today!

http://connect.issa.org/poll.jspa?poll=1033.

in a useful order. First, in selection of security controls and practices you should consider avoidance of security problems and vulnerabilities. Most lists of control objectives that I have seen do not recognize the importance of avoidance that eliminates having a security problem to solve in the first place. Avoidance is accomplished by:

- Removing a potential threat away from a targeted asset
- Removing an asset away from the potential threat to the asset
- Removing any vulnerabilities facilitating the potential threats
- Assigning the security problem to a more qualified or appropriate party

If avoidance is not possible, insufficient, or undesirable, then deterrence may be the next practice to apply so that potential perpetrators would not likely want to engage in the wrongdoing. Avoidance and deterrence are the most desirable solutions because the potential perpetrator does not act. If avoidance and deterrence are not possible, insufficient, or not effective, then prevention is called for. If prevention is not possible or not sufficiently strong enough, then detection of the act is necessary to record the attempt and produce an alarm or notification. Next, you should attempt to mitigate an ongoing misuse or abuse. After mitigation and termination of a loss, investigation with application of expert forensics and recovery should proceed followed by corrections so that justice and avoidance of possible recurrence are accomplished. Copycat recurrence of cybercrime and repeat computer errors and omissions are common because of the automation of crime and ease of repetition.

Transference, next in the list in the New Model, means turning the security loss problem over to another party more appropriate to deal with it such as reporting it to an insurance company, calling in law enforcers, or retaining forensic specialists. Auditors or consultants commonly are called in to take responsibility for completion of handling an event. Litigation and regulatory actions are common outcomes of complex adversities such as wrongful termination, due diligence, and privacy violation suits, and care must be taken with evidence and treatment of all parties in anticipation of legal actions.

Motivation of stakeholders to be alert to resist and report wrongdoings that they witness and to increase their support for security, in general, and education are important security practices and next in the list. Yet motivation does not even appear in our security vocabulary. Experts commonly recommend awareness at this stage and overlook the importance of motivation before trying to make stakeholders aware of the need for security. Security experts write entire books and articles without once mentioning security motivation, yet much of the effectiveness of security is in the hands of users, owners, and custodians of information with whatever motivation they may or may not have. After all, the constraints imposed by security are universally hated by users. Nobody likes having to use passwords, carry tokens, backup files, and pay for lost productive time, inconvenience, and out-of-pocket expense. Therefore, stakeholders must be sufficiently and explicitly motivated to support security and then effectively educated for motivation to be beneficial. Otherwise, awareness efforts alone are insufficient and may result in the negative effect of teaching users how to avoid security and make security non-functional. Users tend not to believe violations of security will make them victims until it happens to them or close associates, but even then memories are short, and poor security practices return.

We need to explicitly motivate security stakeholders with rewards for exemplary security and penalties for failures to support security just as management motivates employees to do other things disliked or resisted. The requirement with stated and enforced penalties and rewards should be included in all job descriptions and performance reviews. Never install a control or security practice until you are sure that all people affected by it are sufficiently motivated to support its successful function from the beginning of its use. Otherwise, they will beat you every time, and make it ineffective.

Security objectives

The traditional and obvious objective of information security is the reduction of risk as I have stated in the Current Model. However, risk-based security requires security risk assessment as I also include in the Current Model, and this contin-

ues to be practiced today and is required by law, regulators, and auditors. Unfortunately, security risk management and risk assessment are the emperor's new clothes and are not valid processes since security risk cannot be measured sufficiently to accomplish its purpose of justifying and prioritizing cost-effective protection.

Risk-based security takes a negative approach to security. It requires us to promote and measure our security by how much crime, errors, and omissions we attempt to predict could occur if we do not spend sufficient money in effective ways. My New Model does away with the negative concept of security risk altogether (and the need to estimate and declare when "the sky will be falling down" and what the impact may be.) I replace it with positive diligence-based security.[2]

Diligence security guides, measures, justifies, and prioritizes improved security architecture and selection of controls and practices based on:

- Benchmarking the exemplary security found in a few other select organizations (such as competitors)
- Good (not indeterminable best) controls and practices identified in the literature
- Standards and guides
- Tradition and experience
- Advice from the information security products and service industry
- Business requirements
- Audits, laws, and regulations

without resorting to the estimations of uncertainties of undeterminable future frequencies and impacts of negative adversities.

Diligence-based security is a positive process that more often will succeed, while risk-measured security will result in introducing uncertainty into security improvements and intimidating management. Risk measurements are likely to be wrong in outcome because of the constant presence of unknown potential perpetrators and threats, rapidly changing circumstances, and known and unknown vulnerabilities. In addition, the diligence approach may be applied separately and independently to each security issue that arises; whereas, the risk approach must be applied simultaneously to all of the organization's security with significant complexity. This includes the risks coming from all trusted people, all known controls, threats, assets, vulnerabilities, and systems within the organization and among the trusted business partners of the organization, especially with proliferation of cloud computing. The reason for this is because all risks are interdependent in contributing to the organization's total risk. The change in any one risk will cause other risk values to change up or down thus affecting the overall risk because of the flexibility that potential perpetrators have in choosing and changing their attack vectors as controls and practices change and new malware tools become available.

The objectives of information security in the last box of the New Model meet all of the expectations of a sound and comprehensive policy and practice within any organization. The reduction of risk is likely serendipitously achieved from application of diligent efforts in meeting the objectives as indicated.

Using the new model

The New Model is complete, consistent, and straightforward, and you should use it to upgrade your organizational security policies, standards, and guides. It also provides the basic subject headings to conduct thorough vulnerability and threat analyses, security architecture revisions, selections and improvements of controls and practices, and their justification and prioritization for implementation. As indicated by omit-

[2] See Donn B. Parker, "A Diligence-Based Idealized Security Review," *ISSA Journal*, January 2008, and Donn B. Parker, *Fighting Computer Crime, a New Framework for Protecting Information* (John Wiley & Son, 1998).

ting risk from the New Model, you should not attempt to rely on risk cost-effectiveness justification. Think of security as a necessary overhead cost of doing business just as are facilities management, legal, audit, human resources, payroll, and accounting, and like the other overheads, it does not produce a return on investment (The return of savings from expenditures for security is unknown since the incidents that would have caused the savings did not occur.) I suggest that you gradually limit the extent of your risk assessments and reporting to meet only the minimum requirements of the law and regulations and remove the word "risk" from your writings, job titles, and job descriptions.

My simple little model lies at the heart of the definition of information security. Like any art it is open-ended and may be surrounded by many kinds and levels of add-ons such as IT forensics, criminal justice, the law, IT (the tail wagging the dog), industrial security, privacy, reliability, ethics, and so on. While these may vary, the important definitional heart of the art should be well-defined, permanent, and understood by all security professionals. My New Model meets this goal.

Some take-away suggestions

- Always start the solution of a security problem by attempting to avoid it.
- If a security problem cannot be avoided, the next attempt should be to deter potential wrongdoers from causing the problem.
- Treat the security constraints imposed on stakeholders as among the most reviled requirements of job performance and use of information and information systems.
- Motivation to support security must come before security awareness. Motivation is stimulated by rewards for exemplary security and penalties for poor security carried out consistently by example and enforced in policies, contracts, job descriptions, and job performance reviews.
- Never make a security change without the full support of the people affected by it. Otherwise, they will make it ineffective and overcome your efforts at every opportunity to their advantage.
- Avoid the danger of putting assets in harm's way unnecessarily. It is one of the most common and overlooked potential threats to information and systems. This becomes an even greater threat with the increasing distribution of information in mobile and cloud computing. It is also a common violation that security practitioners perpetrate when they publicly reveal sensitive security information.
- Treat the security of security with great importance. Information about the security protecting the most sensitive information that an organization possesses is recursively the most sensitive information it possesses.
- Unintended observation of confidential information is a violation at least as serious as disclosure and requires quite different controls and practices.
- To achieve confidentiality, the need-to-withhold rule may be just as important as the need-to-know rule.
- Repudiation is a violation only when false or harmful and is equally as serious as its inverse, deception. Both are within the meaning of misrepresentation that violates authenticity.
- One of the most common ways to sabotage information and systems is to follow instructions exactly as stated for all circumstances.
- Failure to engage in misuse or abuse of information or information systems when legitimately instructed or required to do so may be a security violation.
- Recognize the six security states of information: confidentiality and possession, integrity and authenticity, availability and utility.
- Perpetrators merely finding the existence or location of sensitive information whether stolen or not may be a significant loss.
- Risk assessment introduces negative, unnecessary uncertainty into the art of information security and intimidates management. Security risk is managed by and under the control of unknown potential perpetrators.
- How much you could lose from incidents need not necessarily be related to how much you spend for security. Security should be treated as a cost of doing business diligently.

Resources

Additional writings by the author supporting this article:

—*Fighting Computer Crime, a New Framework for Protecting Information* (John Wiley & Sons, 1998)

—"Making the Case for Replacing Risk-Based Security," (*ISSA Journal*, May 2006)

—"A Diligence-Based Idealized Security Review," (*ISSA Journal*, January 2008)

—"The Great Debate: Security Spending," (*ISSA Journal*, April 2008)

—"Positive and Negative Security Methods," (*ISSA Journal*, December 2009)

The definitions of security states are quoted from *Webster's Third New International Dictionary.*

About the Author

Donn Parker, CISSP, (Retired), has been a SRI International consultant and researcher on information security and computer crime for 35 of his 50 years in the computer field. He has written numerous books, papers, articles, and reports in his specialty, based on interviews of more than 200 computer criminals and security 250 reviews of large corporations. Readers may contact Parker about this article and his lecture services at donnlorna@aol.com.