INVITED TALK 3

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

A NEW FRAMEWORK FOR INFORMATION SECURITY TO AVOID INFORMATION ANARCHY

Donn B. Parker

SRI International, 333 Ravenswood Ave., Menlo Park, CA 94025

1. INTRODUCTION

The purpose of information security that most infosec specialists identify is to preserve the three elements of confidentiality, integrity, and availability of information. The 1991 paper, *Restating the Foundation of Information Security*[1], argues that this is a dangerously oversimplified definition of infosec. The preservation of these three elements does not include many kinds of information losses that infosec should prevent. My intent is to demonstrate in more rigorous fashion that the preservation of these elements must be expanded for infosec to be sufficiently comprehensive to protect information appropriately in all of its security aspects.

Accordingly, I have added authenticity, utility, and possession of information as other elements that must be included. I discovered the last element, possession of information, in dealing with the theft of small computers, wherein the loss of the exclusive possession of the information content of the stolen computers is often greater in value than the loss of the computers. Yet the thieves may not even be aware of the information and therefore do not violate either the possible confidentiality or availability of it when the victim still possesses a backup copy. The victims have lost exclusive possession of the information in these cases but not its confidentiality, availability, utility, integrity, or authenticity. The victims might suffer a loss from extortion, for example, in which none of these other elements are violated.

My intent here is to rigorously demonstrate the need for all six of the above elements of information security preservation. The stated pairing and order of these six required elements—and the resultant deeper understanding of infosec—also have some logic and practical value, as will be seen. First, I will demonstrate the need for these elements through scenarios of infosec loss in which each loss is explicitly covered by one and only one of the elements. Therefore, if a loss scenario is accepted as a subject for infosec attention, then the element covering the loss in that scenario must be attributed as an element of infosec. In addition, I suggest some controls that are needed specifically to protect the information from each loss. Some of these controls might be overlooked if any one of the six elements has not been explicitly included.

The possibility exists that more elements of information security than the six presented here may be needed to cover additional types of losses. This could happen as information technology advances, criminals become more innovative, or the concept of infosec changes is extended.

I claim that if the elements of infosec are not rigorously, comprehensively, and logically stated and addressed, using the correct English language meaning of each word, infosec will remain the incomplete and flawed folk art it is today. (Integrity has been abused in this regard by defining it incorrectly to include the meaning of authenticity—see the appendix for the dictionary definitions of the elements.) With such inexactitude, infosec and its practitioners will ultimately lose the confidence of society, and the perpetrators of information loss will continue to successfully take advantage of infosec shortcomings both in practice and under the law.

For example, all infosec specialists should understand that protecting the possession of information as intellectual property is an obvious requirement under common, copyright, trade secret, and patent law. Yet possession cannot be included within the meaning of the original three elements of preserving confidentiality, integrity, and availability. To illustrate, possession but not confidentiality can be lost if the victim encrypted the information before it was stolen. In addition, by definition, integrity cannot be lost or changed in this example because it is an intrinsic property of information content and is not associated with the extrinsic property of possession that does not affect the content. Finally, possession but not availability can be lost if, for example, the new possessor makes the stolen information available for sale to the owner, such as in a case of extortion. Exclusive possession can also be lost but availability preserved if only a copy of the information is stolen. In contrast to the theft of tangible objects when the objects are copies, not authentic originals, loss of exclusive possession is unique to information. Infosec must recognize that two or more people can possess the very same, authentic information simultaneously.

Possession is an extrinsic property of information similar to confidentiality. The information may or may not be possessed, but this has no effect on the information itself. Examination of the information does not necessarily identify who possesses the information or if anyone possesses it. In addition, the information may contain the ownership identity but not the identity of the current possessor. For infosec purposes, ownership should be considered to be a form of possession. Under law, one party may possess information but another may own it. Stealing information may be different than stealing the ownership of information.

I believe that possession has not been fully considered as a unique element of infosec because government—which considers possession and confidentiality as synonymous—has dominated the development of infosec. Treating possession and confidentiality separately reveals a profound underlying difference in the security needs of business and democratic government and makes clear why democratic government security does not apply identically to business. In a democratic government, information is owned by all the people governed; it is public information, and the only constraint is whether it should be kept confidential. Otherwise, at least in the United States, the Freedom of Information Act requires that the information be shared with the public. A democratic government holds no exclusive copyright, patent, or trade secret right to it. Government does not buy, sell, barter, or trade information, except in some cases to cover costs of publication or to offset costs of other services.

In business, information is a commodity or facilitates a service that is bought, sold, bartered, and traded to make a profit, and the primary purpose of infosec is to protect such business information as an asset or property. When government information is stolen, the fear is only for loss of confidentiality; when business information is stolen, possession or exclusive possession is lost. Loss of confidentiality is only a consequence in some cases after loss of possession. For example, the huge problem of software piracy is the loss of possession—including control over software use—and confidentiality is rarely an issue. Business does have a small amount of high-value information for which loss of confidentiality rather than loss of exclusive possession is the greatest concern, and the consequential loss of confidentiality is most often profits. A similar loss in government would result in very different consequences, primarily loss of military or diplomatic advantage.

We must conclude that business and government infosec have some of the same confidentiality concerns, but business infosec has the additional possession element that government does not have. Taking most kinds of information from the government is not stealing and no loss is incurred. Taking most kinds of information from a business is stealing and loss of possession or at least exclusive possession is extremely serious. Espionage against government and business that causes a loss of confidentiality of some information is most serious.

These differences make clear why employee clearances, the principle of need-to-know, mandatory access control, classification of information, and cryptography are typically most important government controls, whereas the owner, custodian, user accountability principle of need-to-withhold; discretionary access control; copyright and patent; and digital signatures are typically most important business controls.

Now consider the value of the expanded and more comprehensive elements of infosec for the purpose of identifying threats. If the security elements are separated into the more distinct six parts, more actions that adversaries may take can be conceived of in a threat analysis than the typically stated modification, destruction, disclosure, and use. For example, I am led to derive a far more "comprehensive threat list for information security." The following list—derived by considering all six elements as well as from collecting and studying more than 3,500 computer abuse cases since 1958—is a far more complete list of abusive actions against information:

- Threats to availability and usefulness
  - Destroy, damage, or contaminate
  - Deny, prolong, or delay use or access
- Threats to integrity and authenticity
  - Enter, use, or produce false data
  - Modify, replace, or reorder
  - Misrepresent
  - Repudiate (reject as untrue)
  - Misuse or fail to use as required

- Threats to confidentiality and possession
  - Access
  - Disclose
  - Observe or monitor
  - Copy
  - Steal
- Exposure to threats—Endanger by exposure to any of the above threats.

The last item, exposure to threats, was added as a separate category to deal with the human failing, and sometimes crime, of negligence on the part of managers, owners, custodians, users, and infosec specialists. The best solution to this problem is meeting a standard of due diligence by using infosec controls that are easily available or known and that are used by others under similar circumstances. Holding people accountable for their duties and responsibilities, as well as motivation and awareness programs for employees and managers, are also very important.

2. FORMAL DEMONSTRATION

I claim that the following six scenarios of information losses derived from real cases are well within the range of above-listed threats that information security should protect against. Following each scenario is an analysis of why each of the six proposed elements does or does not address the loss scenario. Because one and only one element of information security covers each scenario, that element must be included as a stated part of information security.

2.1 Loss Scenario I: Availability

Scenario I discusses the significance of the element of availability in a computer file theft. In an act of sabotage, the name of a data file is removed from the file directories in a computer possessed by the victim. Users of the computer and the data file no longer have the file available to them because the computer operating system recognizes the existence of information for users only if it is named in the file directories. The other information security elements do not address this loss because the utility, integrity, authenticity, confidentiality, and possession of the unavailable information have not been changed in the scenario as stated. Therefore, since availability is prevented as a result of this loss, preservation of availability must be accepted as a purpose of infosec.

Several controls are used to preserve or restore availability of data files in computers. These controls include having a backup directory with erased file names and pointers until the files are purged by overwriting with new files, good backup practices, good access controls to computers and specific data files, use of more than one name to identify and find a file, availability of utility programs to search for files by their content, and shadow or mirror file storage.

The severity of availability loss can vary considerably. For instance, all copies of a data file can be totally destroyed with no means of recovery; a data file can be partly usable with delayed recovery at moderate cost; or the user may have inconvenient access to the file with timely full recovery.

2.2 Loss Scenario II: Utility

In this scenario, an error occurred when the only copy of valuable information was routinely encrypted in a computer and the encryption key was accidentally erased or changed. The usefulness of the information was therefore lost and in this case could only be restored if cryptanalysis could be successfully accomplished.

Although this scenario could be described as a loss of availability or authenticity of the key that was lost or changed, the loss focuses on the usefulness of the information, not on the key. The only purpose of the key was to facilitate the encryption but not to provide the usefulness of the information that was encrypted. The loss concerned the information and its loss of utility. The loss of the key would be a loss of a different information asset.

The information in this scenario is available but in a form that is not useful. The integrity, authenticity, and possession are unaffected. Confidentiality is greatly improved if changed at all.

To preserve utility of information, four controls are suggested. These include internal application controls such as verification of data before and after transactions, security walk-throughs during application development to limit unresponsive forms of information at times and places of use, minimization of adverse effects of security on information use, and control of access that may allow unauthorized persons to reduce the usefulness of information.

The loss of utility can vary in severity. The most severe case would be the total loss of usefulness of the information with no recovery. Less severe cases could range from somewhat useful with full usefulness of data restored at moderate cost to less-than-perfect usefulness with timely full recovery.

2.3 Loss Scenario III: Integrity

A software company under pressure to meet a delivery date provided an accounts payable application program to a client without including an important control. The master copy held by the software company contained the control that functioned according to specifications. The omission was not discovered because no known violations of the control occurred. An accountant in the client company, however, discovered that the control was missing and that the program had failed to check for duplicate payments. The accountant took advantage of the omission and engaged in a large accounts-payable embezzlement. The client company sued the software supplier for negligence.

The software application performed as intended except that the duplicate billing control was missing. Because the program was incomplete, however, the product lacked integrity. The meaning of "integrity" is limited to "a state of completeness, wholeness, soundness, and adherence to a code of conduct."

Availability and utility were not violated in that the program was in use and was useful for its intended purpose so far as it went. Having come from the correct supplier, the program was authentic and performed correctly as far as it went. Its failure to perform the duplicate billing control meant that the program performed incorrectly under some circumstances, not because the control was incorrectly programmed but because it was missing. If the control were present but failed to conform to specifications, the program would lack authenticity; however, conforming to specifications was not relevant since the control was missing. The software company's failure was omitting the control in the program delivered, not the failure of the program (to the extent that it could perform) to conform to specifications. It was also a genuine program from the software company. Thus, the program lacked integrity, not authenticity. Confidentiality and possession are not affected and not at issue in the scenario.

Several controls can be used to prevent loss of integrity of information. These controls include using and checking sequence numbers and check sums or hash totals for series of ordered items that would ensure completeness and wholeness; doing reasonableness checks on types of information in designated fields; performing manual and automatic text checks on presence of records, subprograms, paragraphs, or titles; checking for unexecutable code and mismatched conditional transfers in computer programs; and promoting adherence to codes of ethics (to achieve integrity of people).

The severity of integrity loss can vary. Significant parts of the information can be contaminated or misordered but be short of total unavailability, with no recovery possible. Or, with delay, a few parts of the data in that condition can be restored at moderate cost. Alternatively, small amounts of contaminated information can be recovered in a more timely way at low cost.

2.4 Loss Scenario IV: Authenticity

A book distributor obtained the text of a book on a disk from an obscure publisher. The distributor changed the name of the publisher on the disk to a well-known one, had the book printed, and—unknown to either publisher—distributed it successfully in a foreign country.

The book was misrepresented as published by a well-known publisher. Therefore, it did not conform to reality and was not an authentic book from that publisher.

Availability and utility are not at issue in this case. The book also had integrity because it was complete and sound. The publisher lacked integrity since it didn't conform to ethical practice, but that is not the subject of the scenario. The correct owner also possessed the book even though it was deceptively represented as having come from the popular publisher. Although the distributor would have attempted to keep its actions secret from the popular publisher (and probably the obscure publisher), confidentiality of the content of the book was not at issue.

A number of controls can be applied to ensure authenticity of information. These include confirming account balances, transactions, correct names, deliveries, and addresses; checking on genuineness of products; segregating duties or dual performance of activities; using double entry bookkeeping; checking for out-of-range values; and using passwords, digital signatures, and tokens to authenticate users at workstations and LAN servers.

The severity of authenticity loss can take several forms, including no conformance to genuineness or to fact or reality with no recovery possible. Authenticity loss can also be moderately false or deceptive with delayed recovery at moderate cost, or information can be mostly factual.

2.5 Loss Scenario V: Confidentiality

An individual inserted a radio transmitter into an ATM that received signals from the touch-screen CRT used for inputting customers' PINs and conveying account balances. The device then broadcast the information to a receiver that recorded the PINs and account balances on a VCR for retrieval.

The secrecy of the customers' PINs and account balances were violated. Hence, their privacy was invaded.

Availability, utility, integrity, and authenticity are unaffected in the confidentiality violation. The customers' and the bank's exclusive possession of the account balances information was lost but not possession per se because they still held and owned the information.

Controls to maintain confidentiality include using cryptography, training employees to resist deceptive social engineering attacks designed to obtain their technical knowledge, physically controlling location and movement of mobile computers and disks, and controlling access to computers and networks. Security also requires ensuring that resources for protection should not exceed the value of what may be lost, especially with low incidence. For example, protection against radio frequency emanations in ATMs (such as in the scenario described above) is probably not advisable considering the cost of shielding and access control, the paucity of such high-tech attacks, and the limited monetary losses possible.

The severity of loss of confidentiality could vary. The loss in the worst circumstance would be disclosure of information to the most harmful party with permanent effect. Information could also be known to several moderately harmful parties with a moderate-term effect or be known to one harmless, unauthorized party with short-term effect.

2.6 Loss Scenario VI: Possession

A gang of burglars aided by the disgruntled and recently fired operations supervisor break into a computer center and steal all copies of a company's master files on tapes and disks. They also raid the backup facility and steal all backup copies of the files. They hold the materials for ransom in an extortion attempt.

The burglary resulted in temporary lost possession of all copies but not loss of legal ownership of the master files and media on which they were stored. Loss of ownership and permanent loss of possession would be accomplished if the materials were never returned and the victims were to stop trying to recover them.

Availability is delayed in this scenario but could be accomplished by paying the ransom or using legal force to recover the materials. Utility, integrity, and authenticity are not an issue. Confidentiality would not be violated unless the files were read or disclosed.

Several controls should be used to protect the possession of information. These include using copyright, patent, and trade secret laws; implementing physical and logical access limitation methods; preserving and examining computer audit logs for evidence of stealing; using file labels; inventorying tangible and intangible assets; etching identification on computer equipment; using distinctive colors and labels on disk jackets; and assigning ownership to organizational information assets.

The severity of loss of possession varies with the nature of the offense. In a worst-case scenario, the most harmful party would take the information along with any and all copies with no recovery possible. Or a moderately harmful party could take it for a moderate period of time before it would be recovered at moderate cost. In the least harmful case, a harmless party would possess one copy of the information with timely recovery possible.

3. CONCLUSION

Some scenarios of losses that infosec should address require the use of all six elements of preservation to specify the security to be applied. The six elements are independent of one another by having unique definitions, with one exception. The only possible definition of an element included within the definition of another is when loss of confidentiality results when loss of possession occurs, because a violation of confidentiality always results in at least a violation of loss of exclusive possession. Loss of exclusive or nonexclusive possession, however, does not necessarily result in loss of confidentiality, as seen in the above scenario of stealing information without examining it or when the information stolen is not confidential.

All six elements of infosec presented here must be used. This is essential if infosec is to be complete and accurately described. Moreover, to adequately reduce or eliminate vulnerabilities and threats, the use of all six elements is critical to ensure that nothing is overlooked in applying appropriate controls, such as those identified above. These elements also aid in identifying abusive actions that adversaries could take before the actions are realized. As technology advances, adversaries become more sophisticated, and as the concept and scope of infosec changes, more changes or additions to the six elements may be required.

All six elements can be paired into three double elements for simplification and ease of reference, and the order of presentation should have some meaning as well. Availability and utility fit together as the first element. Controls common to them include secure location, appropriate form for secure use, and accessibility of backup copies. Integrity and authenticity fit together—one concerned with internal structure and the other with value conformance with external facts or reality. Controls for both include double entry, reasonableness checks, use of sequence numbers and check sums or hash totals, and comparison testing. Control of change applies to both. Finally, confidentiality and possession go together since they are only partially independent, as previously stated. Commonly applied controls include copyright protection, cryptography, digital signatures, escrow, and secure storage. The order used here is logical since integrity and authenticity generally have value only if the information is available and useful, and confidentiality and possession have material meaning if the value of the information is sufficient because it has integrity and authenticity.

A summary of the complete framework of infosec is provided in Figure 1. It includes the six elements of purpose, an abbreviated list of abusive acts, nine functions, and four goals.

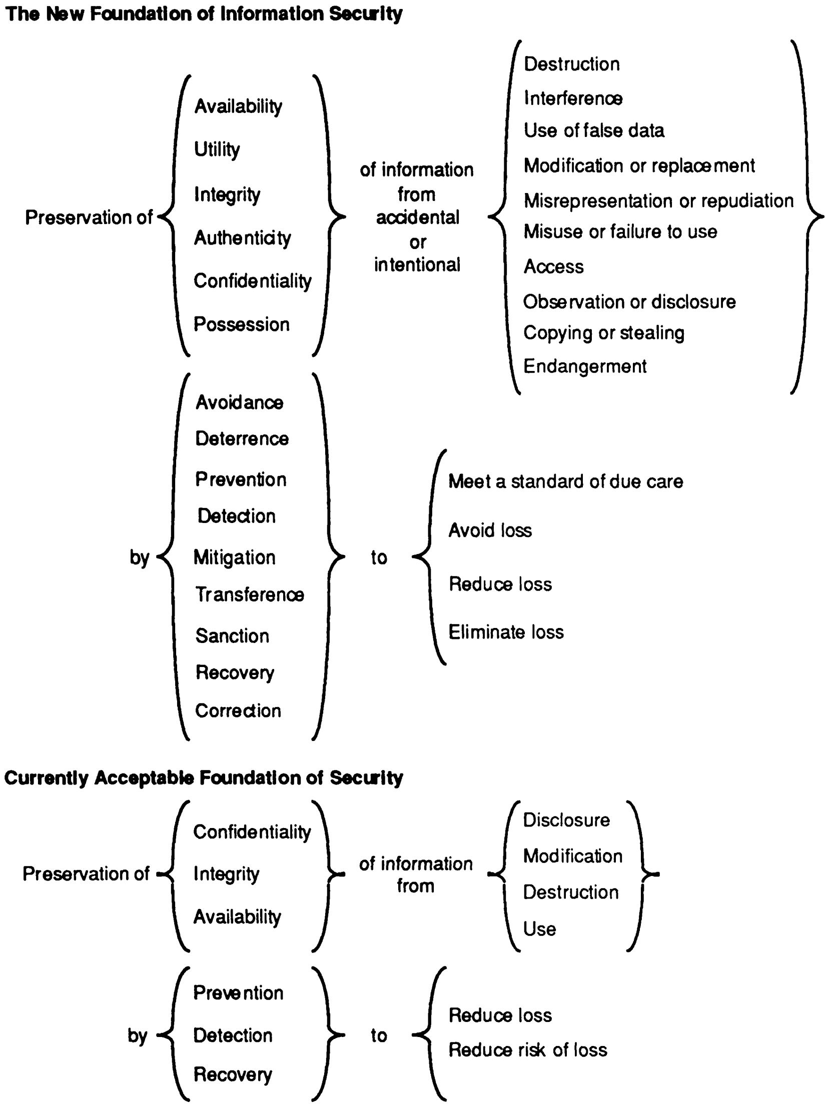

Figure 1. Information security framework

REFERENCE

1. Parker D., 1991, Proceedings of the 14th Natl. Comp. Sec. Conf.

APPENDIX

The following definitions are the relevant abstractions taken from *Webster's Third New International Dictionary.*

Security: Freedom from danger, fear, anxiety, care, uncertainty, doubt; basis for confidence; measures taken to ensure against surprise attack, espionage, observation, sabotage; protection against economic vicissitudes (old age guarantees); penal custody; resistance of a cryptogram to cryptanalysis usually measured by the time and effort needed to solve it.

Availability: Capable of use for the accomplishment of a purpose, immediately utilizable, accessible, may be obtained.

Utility: Useful, fitness for some purpose, capacity to satisfy human wants or desires.

Integrity: Unimpaired or unmarred condition; soundness; adherence to a code of moral, artistic or other values; the quality or state of being complete or undivided; material wholeness.

Authenticity: Quality of being authoritative, valid, true, real, genuine, worthy of acceptance or belief by reason of conformity to fact and reality.

Confidentiality: Quality or state of being private or secret; known only to a limited few.

Possession: Act or condition 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.