Donn's Corner

ISSA JOURNAL

By Donn Parker – ISSA Distinguished Fellow, Silicon Valley, USA Chapter

Information Security Maxims

This column in the ISSA Journal presented and briefly explained my sometimes controversial information security maxims (general rules, principles, or truths) for your edification. The topics I address start with cybercrime followed by information security solutions, advice for information security management, cybercrime predictions, and security future. A caveat is in order: for every maxim, there is an exception. Donn's Corner ran monthly in the ISSA Journal from February 2014 through August 2015.

Number 1 – The Golden age of Cybercrime

1. We are in the golden age of cybercrime between disaster and annihilation.

Number 2 – Cybercrime

2. Computers and devices using computers play just four roles in crime: Object, subject, tool, and symbol.
3. A cybercrime is an abuse or misuse where a computer or device containing a computer is the object, subject, tool, or symbol, and the perpetrator intentionally made or could have made gain.
4. Fragile computers as objects of great importance have been shot, blown up, kicked, shaken, drowned, electrocuted, fried, baked, burned, urinated upon, dropped, stolen, held for ransom, lost, irradiated, and sat on.
5. If it came from a computer, it must surely be correct, true, and significant.

Number 3 – Automated Crime

6. For the first time in criminal history, it is possible to possess a crime and execute it repeatedly as an app; not just do a crime one up.
7. Automated cybercrime provides the makings of perfect crime.

Number 4 – Errors and Omissions

8. Enterprises probably lose more from errors and omissions than they do from intentional acts.
9. Computers don't make errors or omissions; people do.
10. Assume loss incidents are intentional before accepting them as accidental.
11. It is better to concentrate first on preventing and mitigating intentional wrongdoings.
12. It is difficult at times to tell the difference between intentional and accidental wrongdoings.
13. Some intentional acts are derived from observed accidents.

Number 5 – Tabulating Cybercrimes

14. There are no known valid representative tabulations or cross tabulations of cybercrime.
15. The partial and biased tabulations that we have may be used for proof-of-existence.
16. The annual breach reports are excellent sources of "lower bound" tabulations of cybercrimes (known but more are unknown).
17. Viruses, worms, hacker intrusions, point of sale frauds, phishing, and software piracy are not risks; they are likely certainties.
18. Hackers and hacker attacks haven't gone away.

Number 6 – Checklists

19. At the right level of abstraction, detail, and comprehensiveness, security checklists are valuable aids, but only aids.
20. Remember, your adversaries use different checklists than yours.
21. Never assume a checklist is complete.

Number 7 – Cybercriminals

22. Employers don't hire crooks; people become trust violators in the course of their work.
23. Computers don't commit crimes; people do.
24. Cybercriminals think they are too smart to get caught.
25. Wrongdoers often become the equivalent of trusted people to execute their crimes.
26. Wrongdoers find computers are attractive targets; they don't show anguish, cry, or hit back.
27. Information security professionals are expert and highly trusted and, therefore, potentially highly dangerous.
28. Collusion should be suspected in complex cybercrimes.
29. One cybercrime attracts more cybercrimes. Cybercriminals are frequent copycats.
30. Restitution for harm done rarely occurs and is more difficult and dangerous.
31. Cybercriminals routinely lie and deceive.

32. Cybercriminals may be more dangerous in prison than out by educating other prisoners.
33. Recidivism is unlikely among amateur trust violators that are motivated by personal problems.
34. Violation of trust deceptively called "insider crime" is probably more frequent than reported.
35. Perpetrators are more likely to engage in crimes in familiar work environments.
36. Publicly revealing too much about an enterprise's security, vulnerabilities, and adversities is a grave danger.
37. Put your choice here.

Number 8 – Cybercrime Methods and Tactics

38. "How much electronic money, information, or software should I steal, modify, use, hide for extortion, plagiarize, or destroy?" Since the effort is the same for any amount.
39. Perpetrators will gravitate to the simplest and safest methods first.
40. The salami technique of taking many small slices of the whole asset that goes unnoticed or ignored is profitable with computers.
41. The infamous accounting fraud of accumulating fractions of pennies after multiplication and division round-down is purely fictional.
42. Enterprise security policies, standards, and guides are excellent resources for planning cybercrimes.
43. Copy-cat cybercrimes abound: if done once, it will be done many times.
44. Attacks are plentiful and easy; defenses are limited and difficult.
45. We can't win for losing. Cybercrime happens.
46. Phishing (social engineering) is ultimately successful.
47. For perpetrators, one bug in their work and they go to jail.
48. A successful adversary must know the environment of his crime perfectly and completely.
49. Endangerment is an often overlooked but common cybercrime.
50. A clever form of sabotage is to blindly "work to rule" when exceptions occur.
51. Computers and networks free adversaries from geographic proximity to and real-time observation of their wrongdoings.

Number 9 – Classification of Enterprise Information

52. Two-level classification of information with applicable security labels is good enough except where multilevel is required by contract, law, or regulation.
53. Never use "confidential," "secret," and "top secret" labels except for government purposes.
54. Protect public information from plagiarism and unintended modification.

Number 10 – Limitations of the Need-to-Know

55. The need-to-know rule: Entrust only needed information.
56. The need-to-withhold rule: Withhold only specified information.
57. If more information is sharable than not, then need-to-withhold may be the better rule.

Number 11 – Ethical Conflicts

58. Seek informed consent of stakeholders to avoid unethical conduct.
59. People engaged in unethical acts often rationalize that they are solving a problem by causing the least harm to the least number of people.
60. Perpetrators act rationally from their perspectives but irrationally from victims' perspectives.
61. What is the security officer of a criminal enterprise to do (Enron for instance)?

Number 12 – Some Advice for Information Security Management

62. The enterprise's overall security effectiveness is only as strong as its unknown weakest link.
63. It is the nature of security that the best that security staffs can do is to go unnoticed.
64. CSOs may seem to become obsolete and their positions at stake when they are successful and adversities become infrequent. This is called "working your way out of a job."
65. Good security is when nothing very bad happens. And when nothing very bad happens, who needs security? Security seeks a "natural" lowest level. Periodic revitalization is necessary.
66. Security failures may be depicted as amusing but produce great personal anguish and suffering.
67. Even seemingly good security solutions may introduce unanticipated new vulnerabilities. For example, universal use of cryptographic protection in laptops in a large bank significantly increased the loss of laptops, because users assumed reduced need to protect them.
68. The security imperative: CSOs get only one chance to recommend security solutions to organizations because if they aren't accepted or effective, the organization stakeholders will use the failure as an excuse to preclude use of more security solutions. CSOs must be right the first time.
69. Diligent enterprise information security should be based on:
    a. A cooperative and understanding enterprise culture,
    b. Traditional controls and practices and loss experience,

c. Compliance with requirements,
d. Others' good practices, experience, and experimentation under similar circumstances,
e. Standards, audit reports, and contracts,
f. Cautiously used vendor advice and experimentation,
g. Acceptance by management and stakeholders,
h. Cost, and
i. Cautious, proven, and selective use of current professional trade and research literature and news media.

70. Risk assessment dangerously provides management the opportunity and reason to accept risks and preclude acceptance of otherwise good security solutions.
71. Decisions by higher management fiat should be obtained when solution disagreements or intractable trade-offs occur.
72. Explicit information security compliance should be required in job descriptions and performance evaluations of all stakeholders.
73. The security of the information about the security of an enterprise is critically important and sensitive.

Number 13 – Cybercrime Predictions

74. We are approaching the total automation of crimes. For the first time in criminal history it is now possible to produce, package, possess, buy, and sell a crime, not just do a crime. This may be accomplished by selecting victims, perpetration, conversion to irreversible gain, and erasure of all evidence within a single uninterrupted software application that may be bought, sold, and improved upon by experts.
75. Automation will facilitate achieving the perfect crime where perpetrators know little or nothing about the crimes they execute and the identity of the victims, gains are untraceable and irreversible, and no evidence remains of the event except the loss.
76. Many cybercrimes or aspects of them are unobservable at computer speeds far exceeding the time scale of human capability to mitigate them. This requires totally automated security without human intervention.
77. Many cybercrimes are now carried out as formal business ventures. They involve the use of packaged crime tools that are subject to continuing improvement and for which there is now an active and expanding market. The market is created by otherwise unqualified perpetrators willing to purchase and use them.
78. Older characteristics of past cybercrimes and adversaries such as malicious hackers and their games don't become obsolete. All types of criminals and their methods remain active and accumulate.
79. Much that is deducible from news or trade media reports of cybercrime is at most that something interesting may have happened.
80. Cybercrime is rapidly outpacing security and occupies the leading edge of information technology where criminal payoff is the greatest.

Number 14 – Limitations of Information Security

81. Try to remove an asset from the need for protection before protecting it.
82. Information security should include protection of possession (control), authenticity, and utility of information as well as confidentiality, integrity, and availability (CIA).
83. Information security is an unbounded and never complete art and practice.
84. Information security is a psychological discipline.
85. There always are more untreated vulnerabilities.
86. The effectiveness of security solutions is dependent on timely and sustained alertness, motivation, and commitment of trusted stakeholders.
87. Positive security motivation must be achieved with rewards for exemplary security and penalties for poor security before awareness training will be effective.
88. There are no known best security solutions.
89. Application of controls and practices add complexity and new vulnerabilities.
90. Information security ages and deteriorates and must be periodically renewed and reinvigorated.
91. With a big enough hammer you can break anything.

Number 15 – Information Security Solutions

92. Don't spend more protecting an asset than it is worth.
93. We must think like the enemy to overcome him.
94. Don't apply security solutions unless the stakeholders accept and support them.
95. Solutions and vulnerabilities are in one-to-many and many-to-one relationship.
96. The value of security solutions is usually unknown.
97. Security and the constraints impose unrecoverable costs and are universally hated.
98. The lack of quality security is primarily a "people problem."
99. Adding security solutions may reduce the value of other solutions, increase vulnerabilities, and even reduce overall security by providing a challenge to adversaries.
100. Properly used computers are often far superior anomaly detection devices than humans.
101. Attempting to forecast security risks (probabilities and impacts) of what unknown adversaries may do is fruitless and dangerous to careers when wrong.
102. Risk assessments may be achieved by providing simple and succinct expert opinion reports.

103. Segregation of duties or dual control and confidential personal advisory services for trusted people are important security solutions.
104. Multilevel classification of information in non-government enterprises ultimately deteriorates.
105. An objective of good enterprise security is at a minimum to have all appropriate accepted controls and practices in one's industry effectively in place or documented reasons why they are not in place.

Number 16 – The Trusted Persons Security Threat

106. Internal controls and catching trust violators protects trusted people.
107. Unusual efforts to gain trusted status, expertise, and special knowledge may be warning signs.
108. Security controls and practices in hiring, contracting, revealing secrets, and terminating employees should be commensurate with the degree of trust.
109. Balancing enterprise security with protection of trusted people's rights is the ultimate security control issue.
110. We are unable to anticipate sufficiently all of the unknown vulnerabilities and attacks before our increasingly intelligent and capable unknown cybercrime adversaries do.
111. Safety is a part of security.
112. Segregation of duties and dual control are sometimes effective alternatives to one another.
113. Ethics and law preclude enterprises from taking excessively vigorous security actions.
114. The security basics provide us with the equivalent of locked doors, moats, thick walls, auditors, forensics, and recovery, but with a big enough hammer and sufficiently effective deception, trusted people can break anything.
115. Deterioration and violation of controls and practices by trusted people is a constant problem and requires continued restrengthening.

Number 17 – CISO?

116. The qualified information security professional is a consultant and service provider to the enterprise.
117. The person accountable for a breach and loss is the person that could have prevented or mitigated it.
118. The title should fit the job, and the job should fit the title.
119. Chief and officer titles carry personal responsibility.
120. Policy should clearly state the security and loss responsibilities of all positions in the enterprise.

Donn Parker, CISSP, retired, and information security pioneer, donnlorna@aol.com.

Published in the ISSA Journal as a monthly column February 2014 through August 2015