Risk Management or Risk Analysis?

- From "Risk Staging" and "Risk Management or Risk Analysis?", by Fred Cohen
  - I like these articles because they contain "semi-confrontational" statements about some of the realities with risk in cyber applications
    - http://all.net/Analyst/netsec/1998-05.html
  - This is an informal discussion about risk in the context of network security.
  - The material below is mostly directly adopted from the articles
  - I wanted to use these articles as the basis of a discussion about risk assessment in computer networks. There are those who believe it is a good thing, and those who think it cannot be done (based on issues brought up by the author).

Risk Management or Risk Analysis?

- Risk analysis
  - "at least classical risk analysis - consists of
    - (1) gathering facts, assumptions, and estimates; and
    - (2) making calculations based on that information to generate results including expected loss and the cost effectiveness of various mitigation techniques."
- Risk management
  - "at least as it is commonly practiced - consists of
    - (1) gathering facts, assumptions, and estimates; and
    - (2) making decisions about which risks to take."

Risk Management or Risk Analysis?

- Risk w.r.t. intrusion detection and response
  - theoretically, "no matter how many things we are able to detect, there will either be an infinite number of false positives, an infinite number of false negatives, or both."
  - There is a tradeoff between false positive and false negatives
    - » may be tuned

Risk Management or Risk Analysis?

- Prevention
  - How much does it cost, is it necessary?
  - "Unless the number of actual attacks against a system is very large, the vast majority of attack mechanisms will never be used."
  - "Thus the vast majority of the prevention is never exercised."
  - "This would not be true if we could predict which attacks were going to be used against which systems with what frequency."
  - "Probabilistic risk assessment (PRA) is based on the notion that we can do that, but in my experience, the predictive power of PRA in information protection is inadequate to change this situation."
  - "Effective prevention almost always carries high cost and unnecessary restriction."
  - "Unless you can show that prevention is more cost effective, detection and reaction will normally be the defenses of choice."

Risk Management or Risk Analysis?

- Risk as the product of dependencies, vulnerabilities and threats
- Three examples:
  - "If we had a highly vulnerable system and thousands of people who had good reason to attack it, but its failure had no impact on our business, there would be no risk and thus no financially justified reason to protect it."
  - "Similarly, if the system were critical to our business, had no vulnerabilities, but there were thousands of attackers anxious to attack it, there would still be no risk and thus no reason to protect it."
  - "Finally, if the system was critical to our business, was full of vulnerabilities, but there was nobody interested in attacking it, there would be no risk and thus no reason to protect it."

Risk Management or Risk Analysis?

- ROI (Return of Investment) as an argument for prevention
  - example: organization with high levels of macro viruses in email attachments
    - » tech. support spent 20% on cleanup related exercises
    - » why is there no centralized virus scanner?
      - cost is $50k + estimated $50k maintenance
    - » current cost of %20 of tech. support time is $200k

Risk Management or Risk Analysis?

- Dependencies:
  - "The systems being infected by viruses in these cases are used for normal business purposes. They facilitate communication between individuals within the organization and individuals in customer and vendor organizations. While the business can exist without these systems, they provide far greater efficiency than can be attained through other means. Timeliness is not usually critical in these systems. The dependencies have been demonstrated by actual harm."

- Vulnerabilities:
  - "These systems are vulnerable to all sorts of attacks, but the particular vulnerability here is from macro viruses. All of these systems are vulnerable and none of the vulnerabilities can be removed today without destroying the utility of the systems. The vulnerabilities have been demonstrated by exploitations against this organization."

Risk Management or Risk Analysis?

- Threats:
  - "The threats range over a wide range. Very little skill is required in order to write computer viruses and this organization is targeted and actively attacked by threats with the motivation and capability to use viruses. This has been demonstrated by actual incidents."

Risk Management or Risk Analysis?

- Standard Risk Analysis
  - expected loss L is product of
  - probability of event e, i.e., $p(e)$ and
  - loss from event e, i.e., $l(e)$
  - over all events e in E
- Mitigation strategies can be optimized by greed
- Seem quite logical, but there are challenges...

Risk Management or Risk Analysis?

- "The list of events:
  - The list of events that can cause a loss on a single system cannot be listed exhaustively.
  - This is one of the results of the undecidability issues surrounding attacks. Since there are a potentially infinite number of different attacks, listing them all is not possible.
  - People usually get around this by listing the ones they know about and ignoring the rest. But of course attackers may not go along with this strategy. They may use attacks you didn't list or attacks that didn't exist when you made your list."

Risk Management or Risk Analysis?

- "The probability of events:
  - Many, perhaps most, naturally occurring events occur in a distribution that may be modeled to within a reasonable degree of accuracy using the common methods of statistics.
    - You might, for example, use a random stochastic process model to assess a probability for earthquakes of more than magnitude 5 occurring in London.
    - But the same cannot be said for man-made phenomena, particularly in the case of human computer attackers.
    - In fact, human attackers tend to act more like step functions than Gaussian probability distributions.
  - For this reason, the basic mathematics of statistics are probably inappropriate for analyzing malicious attacks on computer systems today."

Risk Management or Risk Analysis?

- "Event Independence:
  - One of the most important bases of statistics is the independence of events.
    - For example, in assessing the risk of tornadoes, we normally assume that they are independent of things such as earthquakes. The likelihood of having both during the same time period is then computed by multiplying their probabilities together.
  - But attacks against computer systems often involve multiple simultaneous events. In fact, based solely on experience, it is far more likely that an attack will combine multiple techniques than it is that a single technique will be applied.
  - Trying to assess the joint probabilities of events related in an unknown manner is essentially impossible."

Risk Management or Risk Analysis?

- "Expected loss of events:
  - It turns out that even getting an agreement on the actual loss associated with an event after the event has taken place is very hard.
    - For example, the Morris Internet virus of 1988 had assessed losses ranging from under $100,000 to over $100,000,000. That's a range of more than three orders of magnitude! If we can't get within a factor of 1,000 for events after they take place, how can we expect to get accurate calculations of loss in advance?
  - There is a substantial body of knowledge on information valuation, including encyclopedic volumes on the subject from the EDP Auditor's Association and others. Depending on how you assess value, several orders of magnitude difference may be generated by an assessment."

Risk Management or Risk Analysis?

- "Mitigation techniques:
  - Just as we can't exhaustively list attacks ahead of time, we cannot exhaustively list mitigation techniques.
  - There are so many options available for risk reduction and elimination that nobody knows about all of them."

Risk Management or Risk Analysis?

- "Reduction in expected loss:
  - Even if we could list every possible risk reduction technique, in order to assess the cost effectiveness of these techniques, we need a figure for reduction in expected loss.
  - Unfortunately, nobody has ever come up with a valid way to do this."

Risk Management or Risk Analysis?

- Example: “the reduction in expected loss involved in moving from a system requiring at least 15 characters for a password to a system requiring at least 16 characters.”
- “How do we compute the effect on expected loss?
  - » It's not 26 times harder to guess a 16 character password than a 15 character password, but even if it were, the difference in password “guessability” is not the only factor involved.
  - » Passwords may have to be written down more frequently, or perhaps they are even more likely to be stored in computers that automatically contact other computers rather than remembered by the user.
  - » There will be more mistakes in password entry, thus increasing the day-to-day investment associated with the longer passwords.”

Risk Management or Risk Analysis?

- "This defense will not be effective against attackers who tap into communications or who exploit other vulnerabilities.
- And the effect is not independent of other effects from other techniques - such as using cryptography to protect the information residing within the system.
- Nobody has ever come up with a viable argument for associating a particular reduction in expected loss to a particular defensive technique."

Risk Management or Risk Analysis?

- "Sensitivity:
  - It turns out that risk analysis can be very sensitive to details.
  - For example, a small change in probability or expected loss may cause the choice of one technique over another.
  - Once that technique is selected, it might have cascading effects on subsequent decisions because of the way it changes the mitigating effects of other techniques.
  - I have not seen risk assessment done with sensitivity analysis built in, however, those who have tried using intervals instead of fixed values to address this issue have found that the analysis becomes far more complex."

Risk Management or Risk Analysis?

- Exponentiate for networks:
  - All of these issues in risk assessment apply to individual systems, but when we go to networks, things get far more complex.
  - Each computer in a computer network might contain or process different information with different value, might be subjected to different attacks, and might have different defenses.
  - If we assume they are independent, we miss catastrophic events that impact the entire network, but if we try to calculate all combinations of events and their impacts on all combinations of computers, we run into a substantial combinatorics problem.
  - Furthermore, networking introduces new classes of events, different sorts of losses, may dramatically change the expected loss reduction associated with different mitigation techniques, and that's just the beginning.