

The Psychology of Risk

What Governs Risk Decisions?

An excellent [article](#) in Psychology Today covers our internal risk analysis processes and why we make the choices we do.

"Risk decisions are not about risks alone," says Slovic. "People usually take risks to get a benefit." The value placed on that benefit is inherently subjective, so decisions about them cannot be made purely "on the science." (Szalavitz, M. "10 Ways We Get the Odds Wrong". Psychology Today. January/February 2008.)

In the information security field, we tend to use formulas and cost calculations to determine risk. At the same time, humans are creating the values used in those formulas. The most common formula used for risk analysis is:

(probability of occurrence) x (impact of the occurrence happening) = risk

Probability of Occurrence

Rarely are cold, hard, researched numbers used for the probability of occurrence. People make judgments based on their experiences, which may or may not be typical. For example, I've used both cable modems and DSL. The number of port scans and attempted attacks/worms was higher when I was on cable than when I was on DSL. Does that mean that cable is riskier than DSL? Not necessarily. For my limited experience, it is, but for a larger group, cable may not be riskier than DSL if calculated by

*$X*Y > Z*Y$ (where $X > Z$)*

Part of the problem is that there is simply not enough time or money to complete the research needed, so we depend on experts to tell us that something is likely or not. Experts are still human, and are still subject to emotional responses.

Impact of Occurrence

The impact of risk occurrence is also affected by emotions. The impact can likely be measured in dollars, but the perceived impact is harder to measure. Example: Social security number (SSN) exposure. As recently as ten years ago, colleges, healthcare providers, and departments of motor vehicles all used it as a primary identification number for individuals. The public either didn't notice, didn't care, or didn't realize what was possible when an SSN is exposed. Therefore, the costs associated with an SSN exposure incident were lower. Should SSNs be exposed now, with a public fearful of identity theft, there would be higher costs associated with gaining back the public's trust. The costs of rebuilding trust are not so easy to measure.

A Perfect World

As you can see, both of the values in the risk formula are influenced by humans and our perceptions of costs, benefits, and risks. So, what if ours were a perfect world and we all had the time (and money) to get hard statistics for both of these values? As was said by Benjamin Disraeli, “Lies, damned lies, and statistics”. Even “facts” can be spun to support one argument or another, and often are, so having hard numbers doesn’t always help.

Gathering hard numbers in information security presents its own problems. Companies are sometimes loathe to report when an incident occurs because of the potential of public backlash. This doesn’t even begin to include the number of home users that are attacked or compromised – half of them wouldn’t know it if they were. So, the best data available on likelihood of occurrence is a company’s own internal statistics on attacks and attempts which is only shared if an attack is successful and public notification laws come into effect, or if companies seek the assistance of law enforcement. And this assumes that companies are keeping such statistics.

Conclusion

Coming back to the Psychology Today article – humans primarily use their emotions to judge risk. All of the equations in the world won’t help us get away from this, because human emotion judges the inputs we use.

Things tend to balance themselves out though: multiple people, all with different internal risk level are agreeing on these inputs, preventing one person’s paranoia or risk-taking from having too much influence.

Does this mean that risk analysis, assessment, and management are doomed to failure? **Not at all.** Since the same group of people usually determine multiple risks, you can get a good idea of relative risk. In other words, the experts that perform risk analysis, assessment, and management have an established baseline of risk and can determine relative increases or decreases. If risk X is riskier than risk Y, we should spend more money mitigating, transferring, or otherwise avoiding risk X than risk Y. Given that, we should always be mindful that humans and human emotion are an unavoidable part of the risk management process.

For More Information

If you have any questions about the contents of this document, or are interested in learning more about risk analysis, risk assessment, or risk management, please contact:

Peter Hesse (pmhesse@geminisecurity.com)

Laura Bowser (lbowser@geminisecurity.com)

Gemini Security Solutions, Inc.

4451 Brookfield Corporate Dr. Suite 200

Chantilly, VA 20151

703-378-5808

<http://geminisecurity.com>

About Gemini Security Solutions

Gemini Security Solutions, Inc. provides impartial information security consulting services that ensure the confidentiality, integrity, and availability of critical business information and resources. Our value is centered on our ability to deliver the right expertise and the right experience, at the right time.

Founded in 2001, and with decades of experience, our certified team of experts assists organizations to assess and deliver security solutions in compliance with business strategy, policy and regulatory requirements. Our services include risk analysis and management, regulatory compliance, identity access and management, operations security, and security software development.

Gemini Security Solutions is focused on providing big business experience with a small business approach. Working with you every step of the way, Gemini Security Solutions enables secure business operations with vigor, agility and a commitment to excellence.