Risks, Threats & Vulnerabilities: Snowball Lessons

Rebecca Herold, CISSP, CISA, CISM, FLMI

Final Draft for March 2007 CSI Alert

In January I posted this topic in my blog, and I received such good feedback about it that I wanted to discuss it here with the hope that it will help with awareness efforts and understanding within your organization for the differences between vulnerabilities, threats and risks, as well as how to discuss these issues with your business leaders in more appropriate ways than as mathematical equations.

Understanding Can Come Early In Life

I have some of the greatest and most illuminating information security and privacy discussions with my 7- and 9-year old sons. Their inquisitiveness and curiosity is unlimited. Their minds are open and ready to soak up everything around them, and to openly question those things that they do not understand, or challenge concepts with which they do not agree. Important qualities for dealing with information security and privacy issues.

My sons are very interested in what I do, and since I have the opportunity and fortune to do most of my work in my home office I am thankful to be able to spend a great amount of time with them. They each have their own notebook computers and have been working on computers since they were two years old without my urging. Children are great emulators of their parents, so it seems most of what I do they also want to do and learn about.

I allow my sons to participate in a couple of online virtual reality sites I've checked thoroughly and approved. I always look at the information security and privacy policies and other related information at these sites with my sons. I love doing analysis with them; they are great at doing "what if" scenarios. Something that intrigues them is how some of the sites discuss or reference "risks," "threats" and "vulnerabilities." Many of the sites use these terms incorrectly, which has led to some confusion for my sons, and so we've had good discussions about these terms and how they relate to their everyday life.

Jared = Threat

A good opportunity presented itself in January. We had around a foot or so of snow on the ground. At the end of the day the kids will often wait for 5 to 10 minutes outside the schoolhouse to be picked up. One day when my son, Heath, got home he was upset. He was waiting outside, probably around 25 - 35 feet from the building, apart from the other kids, looking across the field because he thought he saw some deer in the woods. All of a sudden, WHAP! A snowball hit him in the face. He looked up, and further down the hill from where he was from the school building he saw, through long wet lashes and foggy vision, the resident ornery kid in his school, Jared. Laughing. Patting another snowball together. Looking at my son. Jared threw another snowball at Heath. Heath saw it coming and dodged it. When Heath got home he told me was upset. He didn't know Jared well, and he didn't understand why he would throw a snowball at him. We had a long discussion about this, and eventually it led to a very good discussion about dealing with threats, vulnerabilities and the resulting risks at school. We analyzed the

© 2007 Rebecca Herold, CISSP, CISM, CISA, FLMI. All rights reserved.

situation, which also helped them understand the vulnerabilities, threats and risks within their online communities.

Here is some of the analysis by my sons:

- The primary **threat** Heath faced while waiting to be picked up after school was Jared, the snowball-throwing maniac. Of course there were other threats in waiting to be picked up outside the schoolhouse, but this was the most preeminent threat they identified.
- The **vulnerabilities** involved with the snowball-wielding Jared threat included those situations allowing Jared to exploit his snowball-throwing finesse to smack a kid in the face with a stinging frozen snowy fastball, including:
  1. standing outside the building instead of staying inside;
  2. standing away from the crowd of other kids while outside;
  3. being too far from the teacher;
  4. not paying attention to where Jared was at;
  5. becoming so engrossed and focused upon one thing (deer in the woods) and not knowing what else was going on around you.
- The **risks** of getting hit in the face with a snowball were a result of considering the likelihood of the threat exploiting one of these vulnerabilities:
  1. being outside created more risk than staying inside, because that's where the snow was, and after all, snow was the material used for the weapon;
  2. being away from a group of the kids increased the risk, because it left Heath as a more clear target;
  3. being away from a teacher increased the risk even more, because then rascal Jared would have very little fear of getting caught, or accidentally hitting the teacher;
  4. not knowing where the threat (Jared) was, or even knowing the threat existed, increased the risk further; and
  5. not being aware of the surroundings made the risk most grave since unawareness of surroundings and environment opens you up to almost anything bad possible happening.

Risk Is Not Precisely Quantifiable

Can we assign a precise probability to these risks? While we can scale the likelihood when taking into account the different vulnerabilities/threat scenarios, there is no way we can assign an accurate probability; there are too many other variables, constantly changing, that will impact and change the risks on a day-to-day, and even hour-to-hour, basis. However, knowing the threat and the various related vulnerabilities, Heath decided he will be able to help avoid (reduce the risk of) a snowball in the face again by taking some simple measures. Staying inside the schoolhouse would virtually eliminate the threat; but that would not be as fun as being outside. So, he was willing to take some risk to enjoy the outdoors and being with other friends. When outside, Heath could stay close to the teacher, or within a group of other children, to keep him from being an easy target. And in any situation, it would be good to know where Jared was at, since now he knows he is a threat and he needs to keep his eye on him!

These issues parallel the scenarios information security and privacy folks go through during their daily business decision-making processes.

© 2007 Rebecca Herold, CISSP, CISM, CISA, FLMI. All rights reserved.

Describe Risk In Business Terms Not Math Equations
A recurring problem is that many business leaders, along with too many information security folks, want to know exact probabilities for the risks resulting from identified threats and vulnerabilities. I certainly understand their desire for such numbers; business leaders are used to working with numbers (revenue projections, employee expenses, budgets, and so on) and they want to be able to quantify information security risks in the same way; it seems logical and comfortable to them. Unfortunately their common lack of understanding of threats, vulnerabilities and risks leaves them thinking risks can be accurately and consistently quantified.

Another problem is that too many information security folks go straight to the Risk = Threat x Vulnerability x Value formula when discussing information security risks with business leaders. This formula can certainly be helpful within the information security and IT areas to help prioritize activities, such as deciding when to apply certain patches and so on. However, by trying to explain to CEOs, CFOs and other CxOs, with no information security background or perspective, the fundamentals of information security vulnerabilities, threats and resulting risks only by referencing this, or a similar, formula, immediately presents information security risk as numerical calculated terms. If the CxO does not first understand these concepts, he or she is first being shown a mathematical equation, setting the stage for the CxO to now believe that information security risks can all be looked at in terms of numbers, probabilities and formulas.

Instead, first cultivate a good understanding of what vulnerabilities exist within your organization by providing ongoing awareness and training. Cultivate a good understanding of what threats exist to information and processing resources. Discuss how threats and vulnerabilities combine to create the information security risks that exist within the business on an ongoing basis at every opportunity. Use scenarios and examples that your business leaders have experienced, understand, and can relate to. Too many information security folks use terminology that might as well be Greek to your CxOs. Always communicate from the perspective of your audience and according to their responsibilities and expertise.

Use Real Life Situations For Better Understanding
Too many folks fret and worry about these communications, take too long to create communications, and then end up putting out something incomprehensible, confusing, or end up doing nothing at all because just trying to create the communications made their head hurt too much. Remember, all communications do not need to be formal. Of course you need your documented, formally delivered communications, and need to follow a well-planned awareness and training program. However, also take a minute here and two minutes there to bring up a topic and discuss how it impacts your company when you see your business leaders in the elevator, in the cafeteria, in the gym, waiting for a meeting to start, in the lounge, walking to the building...whenever!

Be creative and think outside the box. Consider the interests of your business. Describe how recently publicized incidents relate to your organization and how you would handle similar incidents, or if you are even prepared at all. Describe how recent product recalls were handled and how parallels can be made with privacy breaches.

© 2007 Rebecca Herold, CISSP, CISM, CISA, FLMI. All rights reserved.

Describe how negative publicity surrounding publicized business mistakes has impacted organizations, and what your organization must do to prevent similar mistakes. Describe how the decisions made in the Super Bowl impacted the outcome of the game, and how parallel decisions made within your organization impact the security of the information within your business. Describe how a schoolyard incident relates to your business.

After discussing snowball risks, a day or two later my sons and I were at their desks and talking about the security-related information on the various sites they go to, and if it was accurate or missing some information. In the middle of this, there was a pause while looking at a "cool neo-pet." "So viruses are threats," Noah reflected. "And that's why we need anti-virus software, because we...er, our computers...are vulnerable without it while we're on these sites, and the software helps to reduce the risks of having the viruses do bad things to our computers." Correctimundo!! Very good! I wish some concepts were soaked up and internalized as easily in some adults.

Rebecca Herold, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. Her latest publications are Say What You Do (Shaser-Vartan) and The Privacy Management Toolkit (Information Shield). She can be reached at rebeccaherold@rebeccaherold.com or http://www.rebeccaherold.com.

© 2007 Rebecca Herold, CISSP, CISM, CISA, FLMI. All rights reserved.