Evolving Risk Resilience

Every day many of us hop in our cars and make the commute to work. We get into our cars, strap on the seatbelt, and adjust the mirror. Along the way, we might pass a school, encountering a crossing guard and children taking the hands of adults, who remind them to "look both ways before crossing the street." Perhaps we're dropping a kiddo off for daycare and thus have them strapped securely into their special car seat. Rarely, if ever, do we stop when we reach our destination safely and marvel at the number of risks we successfully navigated, or how resilient we've become to those everyday threats.

The simple fact of the matter is that, no matter where you are or what you're doing, you are managing risk as part of everyday existence. There is no place in life where some sort of threat or vulnerability isn't lurking, ready to twist an ankle or smash a fender. Yet, humans still manage to survive and thrive. It has become part of our DNA to process physical risks and address them accordingly; whether that be in buying a car with specific safety features, ensuring that we received enough sleep to be alert for pedestrian crosswalks, or how our visual system has evolved to rapidly detect motion in our periphery.

In the physical world we have evolved built-in capabilities to protect us from physical threats, though we rarely spend much time thinking about them. The digital world, however, has not yet evolved mechanisms that can be taken so implicitly. What risk management capabilities we do have are still generally piecemeal (a firewall here, an IDS there, testing that application, training that DLP, hardening that OS). To achieve a degree of risk resilience, we must shake off the comfort of inherent physical protections and force ourselves to acknowledge the slower pace of evolution in the digital world.

Part of the challenge in evolving our digital defenses toward the goal of achieving an optimal degree of risk resilience lies in the fact that the threat landscape is constantly changing. This reality stands in stark contrast to the physical world in which we've developed our risk resilience capabilities. Threats in the physical world have not evolved anywhere near as rapidly over the decades as digital threats have. The problem is so significant that we are not even afforded the luxury of thinking of risk resilience in the information age as being a zero-sum game (whereas physical risks, though not zero, are generally quite low, causing us to treat them as effectively zero-sum in most cases).

To make matters worse, we are often fighting an attacker who is fighting back. These attackers are dedicated, opportunistic, and highly motivated. To draw a parallel to war is perhaps an overture we hesitate to make, but the dynamics of the situation are not too dissimilar. We are oftentimes challenged in knowing our own environments well enough to provide true resiliency, and then have to factor in an enemy who is equally a mystery. Sun Tzu warns "If ignorant both of your enemy and yourself, you are certain to be in peril." Today that peril is to our businesses and our bottom lines.

Addressing this challenge is assuredly desired, but what should be our approach? First and foremost, it is imperative that risks be acknowledged and quantified as best as possible. Said Charles Tremper, "The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning." The time is long gone that denial and ignorance is an option. Instead, to achieve a resilient state in our risk management programs, we must tackle the problem head-on.

Once the first step is underway, of acknowledging and assessing those risks inherent in our environments, we can then proceed to strategizing. We know that we want a resilient environment, but what does that really mean? What is our tolerance for risk, and what is the impact on the business should an application or system be inadequately resilient to the risk environment? Strategy alone, however, will not help us out. "Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat." (Sun Tzu)

Given a strategy for achieving the desired degree of resiliency, the next step is to translate that plan into actions. Programs must be launched to implement that strategy. Otherwise, the implicit message is one of outright acceptance of whatever risks exist without any response. Try explaining the importance of a risk resilience strategy to your shareholders when nothing has been done to implement it.

Be careful to ensure that your strategy and programs are holistic and comprehensive. Risk resilience is about more than fault tolerance. It means accepting that bad things will happen (not "if" but "when"), and then planning for recovery from those events. From this perspective, resilience has an implicit degree of tenacity and perseverance. It is a steady belief that, no matter what, your organization can and will recover.

Don't, however, think that this task is easy. The digital world is far more complex than the physical world, and complexity is the nemesis of resiliency. For every software vulnerability found, there are likely dozens, if not hundreds or thousands, of other vulnerabilities still hidden within the code. Each computer represents a complex system, which, when networked with other computers, exponentially increases the complexity of a given environment. Then add in customers and partners, with whom we must establish and place trust, and the entire picture muddies quickly.

Also bear in mind that complexity is more than just a matter of vulnerabilities. It is an insidious threat that we inflict upon ourselves, much to the chagrin of those charged with implementing our strategy. The greater the complexity of a system, the more difficult it is to manage growth, enable flexibility, increase speed to market, ensure profitability, and achieve success. If your infrastructure cannot keep up with the business, then it will become an obstacle to victory. It will be both attacked from the inside for its insufficiency, as well as targeted from outside at the stress points where its weaknesses are more easily exploited. Simplifying and managing this complexity becomes a critical factor in the entire risk resilience equation.

In the end, it is incumbent upon us to embrace risk resiliency, turning it to our advantage. Great risk resilience brings business strength and sharpens competitive edge. The words of Helen Keller perhaps capture this best for us when she said "Security is mostly a superstition. It does not exist in nature, nor do the children of men as a whole experience it. Avoiding danger is no safer in the long run than outright exposure. Life is either a daring adventure or nothing." Risk is all around us, in everything we do and everywhere we go. It is our responsibility, however, to act as a catalyst to evolve our resiliency within the digital world to match our existing level of resiliency within the physical world. It is only by evolving these strategies into capabilities that we will begin to establish an edge in whatever market we compete. “Thus it is that in war the victorious strategist only seeks battle after the victory has been won, whereas he who is destined to defeat first fights and afterwards looks for victory. “ (Sun Tzu)