Creating an All Employee Security Culture
Re-thinking Security

Business ebbs and flows depending on market demand, a product that is hot today may be a bust tomorrow. In the security industry the ebbs and flows are driven primarily by fear of the unknown. Big spending after a well publicized incident or threat will trigger an emotional response and drive up sales. It isn't unusual to see talking heads on TV talking about connecting the dots, security "experts" explaining that with good intelligence lone wolf actors could have been stopped, or that there is some repository of information that will lead authorities to preventing the next attack. And of course, if we only spent more on prevention then it would be ok…that some magic widget is going to prevent bad things from happening.

Unfortunately, none of this really exists. Yes, there is intelligence collection and yes, governments store lots of data but at the end of the day it is up to individuals to know when something is wrong and know to take action. Some analyst sitting in a closed up room outside of Washington, DC does not have the context to understand what might be vulnerable to an attack so it's unrealistic to think they can connect sketchy information about a threat to a specific vulnerability. Hence the predictable statement after almost every shooting or terror attack "there was no specific and credible threat." There is always a credible threat; we have the threat of lone actors inspired by an ideology, terror groups that want to eliminate our way of life, fired workers that shoot up their former place of employment, domestic disputes that result in workplace violence.

It's time to start thinking about managing risk instead of managing security. People are taught from a young age to think about safety. Take the small child on a bike; in today's world they are probably wearing a helmet. This is based on a risk assessment by the parent, hopefully concluding that the cost of a helmet is worth it to mitigate the risk of a fall becoming a traumatic brain injury. We avoid dangerous neighborhoods because they are "unsafe" because of shootings, etc. but when a shooting happens somewhere we believe it should be safe we talk about enhancing security. It's time to apply the lessons of life safety when we think about security. They really are the same thing, but because they tend to be served by two different industries we have been conditioned to think of them separately.

Most people readily accept responsibility for safety, we put smoke detectors in our houses, wear seat belts, ride a bike with a helmet, lock up hazardous materials, etc. We manage risks. We need to transition this culture of managing our own risks to what has become a multi-billion dollar industry based largely on fear of the unknown. Yesterday a bomb was blow up in a Bangkok shrine and this morning BBC News showed CCTV footage of the suspect before and after placing the bomb. I've written about cameras before and think they play a valuable role in managing risk but next time someone says "we need more cameras to prevent attacks" you might want to think hard about what budget that should be in…prevention or investigation and prosecution. The latter is a critical function and maybe the cost is justified, but make that decision based on fact and consider whether there are other ways to prevent assaults, bombings, shootings, other acts of violence. If people take responsibility for their security related risks the same way they do safety risks they will be far safer. Had a bystander in Bangkok sounded the

alert when the backpack was placed (odds are somebody saw it) the outcome might not have been 20 dead and 120 injured.

Security professionals are critical to most organizations because they can help define the risk. Someone who knows how vulnerability may be exploited and can make recommendations to mitigate those vulnerabilities is important to an overall risk management system. They can train and inform other employees, watch for trends and indicators of increased risk. The challenge for an effective risk management system is to get the rest of the employees to "own" security.

Using modern communications tools such as Smartphones and tablets provides an opportunity to change how people think and behave when it comes to security in a wide range of settings. In school and university environments most employees are not actively engaged in incident management and response. While some training programs do encourage participation, programs do not enable non-security staff to communicate into an incident command system during an event. The fact that almost every adult in the US is carrying a powerful computer and communication system (a smart phone) is overlooked in most security plans. Suspicious activity reporting, incident status reporting, receiving incident alerts and situational updates, and participating in planning are all areas the Smartphone enables. Crowdsourcing provides live, thinking sensors (people) that understand context, know what is vulnerable, know what a threat looks like and can be pro-active. I See Crime is a Smartphone solution for suspicious activity reporting, I'm Safe for Schools provides teachers the ability to communicate critical information via a Smartphone before and during a crisis and I'm Safe Abroad provides a simple tool for travelers to check in or request assistance when needed. The key distinction of these tools is that they are designed to be in the hands of all employees, not just a handful of security staff.

All employees currently embrace the fact that safety is everyone's role, but when asked who is responsible for security they will normally indicate someone else. This new approach changes that culture, creating an efficient and sustainable way of managing security as part of an overall risk management process.