One Step Behind.

The ‘catch up’ mind-set that permeates the security industry.

A white paper discussing the divergence between the efficacy of current fixed point, single use security equipment and the increasing tactical fluidity of modern threats.

Abstract

The most dangerous game of whack-a-mole is being played out in the way the security industry operates. Reactions to increasingly fluid security threats are being deployed in stunningly predictable ways. There is a failure to leverage the rapid pace of technological advancement with a seeming preference to rely on limited use, often bulky, fixed point technologies.

This paper discusses some high profile security incidents and looks at the pattern of response by those with responsibility for deploying security measures. It questions if there are inherent limitations in these responses and whether there exist opportunities to introduce more dynamic, intelligent mechanisms to greater protect the assets of governments, corporations and societies in general.

Problem Statement

While it appears that terrorism has become, at least in some variants, a more decentralized affair, all lone actors retain the lessons learned from previous atrocities. The way incidents are reported, investigated and addressed are publicized to an extent, such that only the most inattentive terrorist would remain ignorant of the countermeasures deployed in the wake of each event.

This leads to a fluid landscape where the terrorists respond with agility. Post 9/11 two of the next major transportation related incidents did not involve air travel. The 2004 Madrid bombings, and the 2005 London bombings claimed 244 lives between them and injured almost 2000. The transportation methods targeted were trains and buses. The security response to 9/11 did nothing to deter, and little to complicate the intentions of the attackers who conducted the train and bus attacks with lethal unpredictability.

Whether or not more should have been done to mitigate these specific events is not the intent of this paper. But rather we take a look at what lessons need to be learned to ensure there are no unnecessary future failures to leverage the technological resources available to the security industry today. Resources that may make the industry more adroit in matching the fluidity of the modern threat.

The predictable reaction to incidents and the unpredictable actions of malfeasant actors combine to create a chasm that security professionals have a responsibility to address. And on current evidence, many are failing.

Background

It is not just because of the scale of the devastation that 9/11 serves as a reference point for the evolution of the security industry. If indeed any real evidence of significant evolution can be found. The events of 9/11 serve as a reference point because they set the stage for the way the security industry reacts to certain high profile incidents. Predictably.

Every air traveler since 9/11 continues to proceed through security screening processes that are directly influenced by the consequences of that day. These measures should give comfort to travelers that it is now, infinitely harder to carry a box cutter on board a flight. But is that the question? How many more attempts to get a box cutter on board a plane have been made since?

As we will soon discuss, the next two air related terror incidents involved different modus operandi.

Critique

Can a valid accusation be levelled at the security industry that a lack of innovative thinking might be deemed negligent? There is a strong case to be made that it can.

Such a critique of the security industry would state that it suffers from a collectivized mind-set entrenched with reactionary thinking. A case of institutionalized barn door closing after the horses have bolted. An analysis of this might reveal some of the causal factors.

1. The limitations of specific measures

Richard Reid (aka ‘The Shoe Bomber’) tried to detonate explosives in his shoes aboard a plane, and ever since, most travelers are faced with the prospect of removing their shoes before boarding. Umar Farouk Abdulmutallab (aka ‘The Underwear Bomber’) tried to detonate explosives in his underwear aboard a plane and subsequently travelers are subjected to increasingly awkward and public experiences with bulky body scanners. The trend here is clear. A specific threat is executed or attempted and the response of the security industry is to address it with a specific countermeasure. The limitation of this approach is that terrorists tend not to repeat the same actions. It is akin to a game of infinite whack-a-mole where the mole never appears through the same hole twice.

Since 9/11 there has not been a single attempt to hijack or damage a domestic US flight[1]. It is also worth noting that both Reid and Abdulmutallab were ultimately foiled by passenger intervention and not bulky x-ray scanners.

2. Providing adequate political cover

The greater the devastation, intended or actualized, the more likely there will be a race to achieve political cover. Even accepting that there may be a very low statistical chance of an exact repeat of the methodology employed in a specific attack, no person in a position of security accountability wants to have a credible accusation of inaction being levelled against them.

This inevitably causes knees to jerk which in turn paints an unhelpful backdrop for promoting the kind of strategic problem solving processes necessary for truly effective threat minimization. Innovation will consequently be stifled in favor of more easily defensible and traditional techniques.

In most other walks of life, and especially commerce, innovation is a critical part of development. And innovation usually blossoms within empowered entrepreneurial environments. It is therefore a foremost challenge of the security industry to create room for innovation and creativity to prosper. In organizations where innovation is lacking, it may be caused by the feeling of incongruity, when a culture of ‘creativity’ may feel out of place compared to the gravity of the topic.

[1] https://www.tmtindustryinsider.com/2017/04/air-safety-do-away-with-tsa/

Threat management needs creative minds and technological savviness to bring the brightest solution to the darkest corners of the threat landscape. But the need for political cover makes this hard. A cultural shift must occur.

3. Vested and invested interests

Most traditional security solutions have highly capital intensive technologies associated with them. A single airport body scanner will run to $250,000[2]. Some simple arithmetic will reveal that the TSA has a multimillion dollar investment in this single piece of equipment alone. With this level of financial and physical commitment to the technology, and absent any catastrophic failure, then a certain dynamic must surely exist. Namely that there are multiple parties cognitively programed towards believing that the most efficacious solution is the one upon which they have already invested.

A cycle of repetition

Thinking just of one particular strand of threat, that of the terrorist attack, the game has changed remarkably in the last several years. The methods used have varied considerably since 9/11 with a focus on a more individualistic approach, frequently referred to as The Lone Wolf. There is an implication in this name. It conjures an image of a single rogue actor conducting his atrocity independently of a wider network. But this is a limiting definition. The lone wolf is also an informed wolf. His next action will be made cognizant of the responses to all previous terrorist attempts. He will therefore be searching for a tactic that neutralizes the efficacy of all known countermeasures.

The plane hijack becomes a train bombing. The train bombing morphs into a bus bombing. The bombings are replaced by armed city sieges. The city siege becomes a venue attack. And most recently, a van or car is ruthlessly and maniacally driven through concentrated pedestrianized zones.

The moderately comforting thought for those involved in the security industry might be that each iteration of devastation should be viewed as a black swan event. An unforeseeable tactical shift impossible to counter. And at a micro level there may indeed be at least some validity in this logic. But the minute these terror transformations are viewed at a macro level with even the vaguest of holistic thinking, then the pattern becomes predictable. The pattern is to avoid previous tactics and attempt something new. This is why so much fixed point, single purpose security technology proves ineffective in countering the next threat.

Following the recent preponderance of vehicular attacks, the response to these is familiar. Attempts are made to make it harder for cars to drive in and through high footfall areas at speed. Planners in many European and US cities are indeed convening to investigate ways of blending security measures into design aesthetics. And this is not to say that this approach is wrong or unnecessary, it's to say it follows the pattern of the infinite whack-a-mole. While the planners erect concrete barriers at city pinch points, the terrorists are likely already planning something entirely different.

More eyes, less vision

To greater or lesser extents, the same challenge exists within the way enforcement authorities, education institutions and corporations utilize surveillance. If the problem is the

[2] https://blogs.brown.edu/csci-1951e-s01/2015/02/03/security-of-airports-full-body-scanners-and-walk-through-metal-detectors/

need to locate and track bad actors, then the solution must surely be more fixed point cameras? Well, not necessarily. Even the widest lenses still have limited fields of view from a fixed base. Some of the most surveilled cities in the world still have dark recesses within which one can hide and corners around which a certain camera can't see. Just erecting more cameras cannot be the entire answer. Agility is lacking, and agility is the modern terrorist's power tool.

Problem summary

We will likely always live in a world where there can be no such thing as a perfect security landscape. Such is the price we pay for freedom. But the gap between current traditional security technologies and the agility and determination of those intent on destruction is negligently wide. The fluidity demonstrated by the pernicious, clashes directly with the entrenched and rigid thinking of institutionalized security professionals. And it need not be this way.

Solution plotting

In most areas of life, leisure and commerce, mobile technologies increasingly play a critical role. The development pace of processing power, application sophistication, reliability, and intelligence that can be handheld continues to accelerate.

It is past time that the security industry leveraged this effectively.

A culture shift likely needs to take place to facilitate this. There needs to be an atmosphere where serious and indeed grave topics can be handled not just with traditional thinking, but blended with the spirit of innovation and creativity that fuels so many other parts of modern life.

Specific solutions to specific threats are not enough.

Technology already exists to place more intelligence and early detection systems that cater to a broad range of threats into the hands of those responsible for keeping us, and our assets safe.

Conclusion

There is a place, a need, and an opportunity for a hybrid approach to security planning and deployment. Within this hybrid and holistic approach, traditional and proven fixed point technologies can be deployed where necessary and complemented with newer, more agile solutions, providing a more dynamic, agile and predictive solution to modern security threats.

Royal Holdings are at the cutting edge of security technology and are the inventors of SWORD, a Mobile Based Security Solution providing an IoT level of situational awareness, detection and recognition.