Some Approaches to PPP for the Protection of CI

Dr. Yunyong Teng-amnuay
Department of Computer Engineering (Retired)
Faculty of Engineering, Chulalongkorn University.
Member of the Board, Thai Network Information Center Foundation (THNIC)
Bangkok, Thailand
Yunyong.T@Chula.ac.th

Although most critical infrastructures are under government operation and control, they are mostly built by commercial enterprises. This is basically a form of partnership between public and private sectors. However, in the face of modern threats of cyber criminal and malware, and the general adverse situation on computer, network, and data security, it is imperative that the private sector has to do more than being contractors to government projects. There are a number of ways that the partnership between public and private sectors can be fruitful to the security of infrastructures.

Introduction

With the advent of software-defined everything, even for the infrastructure, and the proliferation of network connectivity, the risk of cyber attack either manually through remote hacking or automatically via the spread of malware is becoming a critical concern. In view of this escalating risk scenario the government came out with a number of law and regulation that will force the organization handling the critical infrastructure to take notice of this impending problem. However, this put the burden on the organization in term of resource, complexity, and responsibility and there are resistance to such a pressure by the government.

So instead of the government going after the organizations who handle the infrastructure there should be a more constructive cooperation between various parties. One approach to the cooperation is through the public-private partnership or PPP.

Constraints on the Critical Infrastructure

A critical infrastructure is on the one hand a business enterprise but on the other hand it is a very important public service with multiple dimensions aside from profit making and responsibility to the shareholders. The most important is the accountability of the endeavour. This can be broken down into various aspects. The infrastructure has to be secure. This is not a lightly talk. The infrastructure is usually sprawling both geographically and socially, that is why is it called infrastructure. Securing such a behemoth is not simple. It has to be reliable. This is something approaching 24/7/365 requirements where a break in the service is not likely to be tolerated. Furthermore, the quality of an infrastructure implies image of the society and country and can affect trust for the investors, the business, and the people, both in and outside the country. So it is not just the shareholders but the stakeholders that the organization handling the infrastructure has to contend with.

Software - the Achilles' Heel of Infrastructure

Engineering, the foundation of infrastructure, is based on safety through proven technologies. Actually, engineers are a very conservative breed. A piece of equipment, a design, the formula for a mix of concrete, and so on, all have to pass through rigorous test of time until they are deemed solid enough for use in complex systems like skyscrapers, airplanes, bridges, ocean liners and spaceships. This is relatively easy to accomplish when those components were purely hardware based: material and circuits. It can be physically put through a lot of stress test and any problem can be ironed out through long arduous use over lengthy period of time.

However, with the advent of software, these components become astonishingly flexible, like magic. Basic hardware can be manipulated by the software, the intelligence, that is embedded into the hardware. These intelligence are in turn concocted by software "engineers" who at most are very green to their profession due to the rapid growth of the field. Never a year gone by without some "new" prominent languages arriving on the scene. It is extremely difficult to retain experienced staff, who are well-versed on secure programming, on the software development team. Most programmers are obsolete within a few years. Moreover, the rapid pace of technology and competition means a complex piece of software is usually focused on functionality and not on security. Why bother as the software will be on the shelf for less than a year before being superseded by a newer version or a product from another company altogether. The problem with this approach is that because the software is complex, it is the habit of programmer to recycle their software for the next project, and the next and the next, as long as the functionalities are still acceptable with some minor enhancements. So the various vulnerabilities of the software will still carry into the next generations with lower priority to do anything about it.

This state of "porous" software to malicious attack is a constant in software development. Older software in ancient machines are not exempted from this problem. Even worse, older software are not subjected to patches and fixes, especially on vulnerability holes. The companies responsible may be out of business or they may have move on to greener pastures.

When connecting these porous software together with network access, may be for the convenience of remote management, they become easy preys for hackers and malware and it is very difficult to secure these software-defined systems.

The 3+1 Approaches to Public-Private Partnership

Instead of hiring a contractor to do the bidding of the government project on infrastructure, it is possible to have the private sector creatively participate in the endeavour.

There are three possible approaches to involve the private sector and one possible change in common business practice that will enhance the survivability of critical infrastructure. They are as follows.

1. High-end partnership
2. Private redundant infrastructure
3. Coordinating body
4. and Departure from lean business practice

High-End Partnership

In this PPP approach, the private firms are not just contractors to fulfill the bids laid out by the government. They act as partner in infrastructure endeavor, participating from the conceptual stage, design, through to implementation and running the infrastructure, either for profit or otherwise. This approach allows the private sector to feel like an owner of the endeavour. This encourages them to invest in technology, innovation, personnel, operation and maintenance staff, and even a portion of the funding. This is because it is a long term commitment on their part, not just a build and transfer project, with or without operation. In this day and age, it is usually the private sector who has the resource to upkeep their technology. With the long term goal and vision of the government, the combination should be effective.

Private Redundant Infrastructure

The age of privatization is upon us but this form of "outsourcing" usually results in private firms running away with the concession and becoming monopoly behemoths on those infrastructures. On the flip side, the government carries on with the public utilities and infrastructures as best they could, resulting in inadequate services and interference from officials in high places.

A form of compromise is to continue with the public service infrastructure but solicit the private sector to build a parallel, and redundant, service, albeit with partial government subsidy. The facilities may be running in parallel and disaster can result in reduce level of service, or the private facility can be a standby one. In the latter case, under normal operation, the private facility can be used to gain financial benefit for the private parties involved.

Coordinating Body

From the above consideration on public versus private infrastructures, there is a tendency to nationalize the private infrastructure under the auspice of the greater good. This is a mistake and usually results in poorer service to the public, for example, the bus service in Thailand. The back and forth tucker war results in incoherent, redundant, incomplete, and unorganized public infrastructures. This becomes severe in the light of heightened malicious activities on cyber security while infrastructures are much more interdependent.

A constructive solution is to have a "centralized" coordinating body for the long-termed and coordinated visions and design goals across industries. Also, this body can serve as a clearinghouse for incidents and fast changing technologies. Government Critical Infrastructure Computer Emergency Response Team, or GovCI-CERT, can be an arm to this body, for example, including other necessary services to the infrastructure community as a whole.

Departure From Lean Business Practice

The private business is a fearsomely efficient machine. Given necessary resource it can do wonder. However, waste is not a word in business' vocabulary. Business always strives for a leaner and more efficient operation: anything to reduce the overhead. This results in a very fragile business practice and although the company still has thousands of airplanes the American Airline, almost without warning, filed for bankruptcy in 2011.

Modern companies are not very resilient. Just-in-time or zero stock measures how good the company has become. Efficiency is the norm. This results in very fragile supply chain, either in goods delivery or maintenance parts, personnels, and equipments. Usually in an outsourcing situation, it is almost impossible to look deeper into the business practice of the outsourcing company and shortage of spare parts can lengthen the downtime. This is unacceptable in critical infrastructure especially if the outage results in society-wide chaos which can have adverse effect on maintenance and parts delivery. If only the business community as a whole veers from such extreme practice via a push through public-private partnership the situation will only worsen.

Instead of the normal lean and mean business practice, the engineering approach to infrastructure has to be the norm where, for example, there is a spare on site for most major or critical parts of the electricity generating turbine. It is not just the government who has to force the acceptable level of the spares, which of course can drive cost and hurts the bidding process, but it must be a common practice on the business end to frown on any such lean and mean practices on critical infrastructures.

Conclusion

The private sector is a fearsomely efficient machine of productivity. However, their planning horizon is quite short and limited. It is the responsibility of the public sector to lay down appropriate visions and plannings that are long-termed. Such differing approaches can only benefit society if there is a strong public-private partnership. This is more important in the light of current day heightened malicious activities in cyberspace.