

The Role of Private Industry and Government in Critical Infrastructure Assurance

Anup K. Ghosh
Reliable Software Technologies
21515 Ridgetop Circle, #250
Sterling, VA 20166
anup.ghosh@computer.org
www.rstcorp.com

Michael J. Del Rosso
Infrastructure Defense
6100 Lincolnia Road
Alexandria, VA 22312
mdelrosso@iddefense.com
www.iddefense.com

1 Introduction

The national critical infrastructure is composed of systems whose incapacity could have devastating consequences to the economy or defense of the nation. The critical infrastructures are commonly understood to be telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, and government and emergency services. At the heart of the national critical infrastructure is software and information. The information age has transformed these basic infrastructures into a highly interconnected and inter-dependent system. The information infrastructure makes the interconnections possible and software is the driver of all information communication. Software is also the most fragile piece of the infrastructure, making the foundation of our infrastructure frail and vulnerable to both attack and simple failures.

Both the dependency on software and the pervasive extent of software in controlling the infrastructure have made the critical infrastructure more like a house of cards than a rock-solid foundation. For example, a software “glitch” in AT&T’s nationwide frame relay network in April of 1998 caused disruption in a number of commercial sectors including ATM banking machines, transactions involving credit cards, bank accounts, travel reservations, and retail [3]. Operations Eligible Receiver and Solar Sunrise in 1997 and 1998, respectively, have shown the vulnerability of the U.S. DoD’s networks to concerted attacks. Operation Eligible Receiver was an exercise run by the military’s Joint Chiefs of Staff to test the military’s resistance to cyber attack. A Red Team from the NSA using only laptops and the Internet, with no advanced intelligence, was able to break into the National Military Command Center and obtain root access [1].

In February of 1998, the U.S. DoD detected coordinated probes and intrusions during the Gulf War buildup. Operation Solar Sunrise was created to track and capture the perpetrators of the attack against the Pentagon. The perpetrators turned out to be two teenagers from Cloverdale, CA who exploited a common software

vulnerability to break into DoD systems where they installed backdoors and password sniffers. Clearly, our nation’s systems are vulnerable to both simple failures and to malicious attack — even from teenagers.

2 Private Industry Must Lead the Way

In this position paper, we argue for the role of private industry in providing critical infrastructure assurance as well as a role for the government in participating. The U.S. government has a vital interest in the viability of commercial infrastructures — namely 95% of all government communications are performed over commercial infrastructures. Furthermore, almost all government procurement of systems is from the commercial market. For instance, the armed services are now standardizing on commercial operating systems such as the Windows 32-bit (Win32) platform for mission-critical applications [4]. The recent failure of a ship propulsion system aboard a U.S. Aegis class cruiser shows the vulnerability of critical systems to failures in commercial software, such as the Windows NT platform [2].

The government must be a partner with commercial industry in developing more robust infrastructures; however, the solution is not for the government to dictate, monitor, regulate or dictate to the infrastructures. The most innovative and efficient solutions to infrastructure assurance and defense will come from the private sector. The government is ill-equipped to solve alone the problems in the infrastructures on which it is so dependent. The commercial sector is better positioned to provide critical infrastructure assurance for the following reasons.

1. The commercial sector largely owns the critical infrastructure.
2. The commercial sector is heavily vested in the robustness and viability of the critical infrastructures.
3. The commercial sector is quick to respond to real commercial needs.
4. The commercial sector is the source of innovation.

It is important to underscore the fact that private industry owns the critical infrastructures. While the government has a vested interest in robust and survivable infrastructures (as does private industry), it cannot dictate the development and maintenance of these infrastructures. In addition, private industry is loathe to trust the government with its sensitive corporate information. As a result, private industry is not willing to sign off on any solution where the government controls the infrastructures and the important data that is part and parcel to the infrastructures.

Even though the commercial sector must lead critical infrastructure assurance, the government has a role to play in driving forward work in this area. As a large consumer of the services provided by the critical infrastructures, the government has a large stake in the robustness of the critical infrastructures to failures and attack. Where the government cannot proscribe good solutions, it can provide necessary market pull for more robust infrastructures. More importantly, the government has a wealth of vulnerability knowledge about the infrastructures. As having the dubious honor of being the #1 target of malicious hacks so far, government agencies possess a large amount of vulnerability data that needs to be shared with all stakeholders of the critical infrastructures.

In spite of the mutual interests between commercial and government agencies in assuring the critical infrastructures against simple failures and malicious attacks, the two entities are working largely independently on this problem. Mistrust and lack of communication between government and industry account for the large gap between their respective efforts in critical infrastructure assurance.

3 The Role of Trusted Third Parties

The key to providing critical infrastructure assurance is to provide trusted third parties that can collect and disseminate vulnerability information in a trusted manner. Commercial entities do not readily share their vulnerability data with the government and other commercial entities for fear of competitive disadvantage as well as possible legal liability. One solution for which a business case can be made is the establishment of trusted third parties from the commercial sector. Since the commercial sector owns the critical infrastructures and is fearful of more government regulation, a trusted third party from the private sector can serve the role of vulnerability data collection, sanitation, and distribution. One model espoused by Presidential Decision Directive 63 (PDD-63) is the establishment of private information sharing and analysis centers (ISACs) that are trusted third party entities.

Trusted third parties in the private sector have been

used in other domains where trust between two entities that are unknown to each other is necessary. For instance, private Certification Authorities such as Verisign have been established to vouch for identities of companies and individuals used in digital certificates. The end user is able to trust that the name on the digital certificate is the true identity of the organization or individual because of trust in the third party that vouches for the identity. Similarly, trusted third parties have a role in critical infrastructure assurance. Rather than ask the private sector to trust government agencies with their vulnerability data, a trusted third party can come from private industry whose business it is to collect, sanitize, analyze, and disseminate vulnerability data to stakeholders in critical infrastructure assurance.

The goal of critical infrastructure assurance is to provide pro-active assurance services to the owners and consumers of the critical infrastructures. These services include reconnaissance and intelligence in infrastructure vulnerabilities, consulting and assessment of vulnerabilities, education and training of system maintainers, and research and development of infrastructure assurance technologies. The organizations that will use the services of the trusted third parties are organizations whose businesses depend on the critical infrastructures.

Unlike computer emergency/incident response centers, the goal of providing reconnaissance and intelligence activities is to prepare organizations for projected threats against the infrastructure as well as for identifying vulnerabilities in the infrastructures that may be exploited for malicious gain. The inter-dependencies in the different infrastructures mean that a vulnerability in one infrastructure could very well affect the performance of other infrastructures. A trusted third party, whose role it is to analyze and assess cross-domain infrastructure vulnerabilities, will be able to provide effective early warning and reconnaissance for organizations across industries.

An immediate need for critical infrastructure assurance is the need to evaluate the posture of organizations in the face of failures in the infrastructure or attacks against the infrastructure. To this end, vulnerability assessment and consulting is necessary to ensure that organizations' systems are implementing current best practices and are properly postured against failures and attacks against the infrastructure. One paradigm the authors' organizations are exploring is certification of systems for survivability to failures and attacks in the critical infrastructures. The certification will provide assurance that a given organization is meeting best practices in ensuring survivability in the face of infrastructure failures and attacks.

Education and training of system maintainers is essen-

tial for organizations to understand the vulnerabilities in the infrastructure and to continue to maintain robust and secure systems. Education and training programs will use industry experts to prepare organizations for addressing critical infrastructure vulnerabilities. Finally, research and development of infrastructure assurance technologies is necessary for developing more survivable systems and for coordinating large-scale detection and response to infrastructure vulnerabilities.

4 Conclusions

In this position paper, we have argued for the necessity of private industry to lead the way to critical infrastructure assurance. The current paradigm of responding to critical infrastructure incidents and emergencies must be shifted to where critical infrastructure assurance is provided before crises develop in order to prepare, mitigate, and effectively respond to infrastructure failures and attacks.

The gap in trust between sharing vulnerability information has to date hindered critical infrastructure assurance. However, in this gap lies the opportunity to provide trusted third party services to both private industry and government. A trusted third party can serve in the model of a private sector ISAC as established in PDD-63. Paramount to establishing successful ISACs is establishing trust between the stakeholders of critical infrastructure. The model of private trusted third parties has been successfully applied before in other domains. We believe that a successful business case can be made for private trusted third parties that serve as ISACs for critical infrastructure assurance.

We like to conclude with an analysis of what government and private industry can do to make critical infrastructure assurance a reality. First, the government needs to recognize that data sharing between private entities must occur for critical infrastructure assurance. Anti-trust laws have traditionally erected barriers to information sharing between private entities. However, recognizing that data sharing is an essential part in addressing the Year 2000 (Y2K) problem, the government has already passed legislation facilitating data sharing between private entities without risk of violating anti-trust laws. Similar legislation would facilitate data sharing for other areas of critical infrastructure assurance. Second, the government has a tremendous wealth of infrastructure vulnerability data. The government must also clear the way for sharing of this data with ISACs for the greater good of the infrastructure. Again, this information can be sanitized by trusted ISACs to prevent breaches of national security. Finally, it is important for the government to not regulate or dictate the critical infrastructure assurance industry. The private sector has a unique blend of market forces, talent, and practicality that can bring innovative and effective solutions to

this problem. If the government plays a heavy hand in regulating this industry, *e.g.*, by pigeon-holing ISACs narrowly, then the end result will be less than optimal and may miss the mark all together.

The private sector must also respond to the threats against the critical infrastructure. The increasing dependence on software and information communications has made businesses more vulnerable to infrastructure failures and attacks. Thus, the private sector has a vested interest in the robustness and survivability of the infrastructure. Because the private sector owns the infrastructure, it is the only sector that can effectively address the problems in the infrastructure and provide assurance of survivability. The private sector can provide trusted third parties to facilitate data sharing, analysis, and distribution.

A variety of different ISACs will be necessary to cater to the myriad requirements in critical infrastructure assurance. For instance, ISACs will be necessary to provide different services such as information security consulting, data collection and sanitizing, training and education, certification, and research. Also, the organizations which will use and benefit from ISACs will have disparate needs and interests, requiring different types of ISAC functions. For instance, ISACs will need to be established for Federal, state, and municipal governments as well as for different sectors of private industry, large and small. As the trusted third party sector grows, interrelationships between ISACs will need to grow in order to facilitate trusted information exchange.

In conclusion, where there are currently lots of problems to address in critical infrastructure assurance, we see lots of opportunities for the private sector to bring innovative solutions.

REFERENCES

- [1] J. Adams. A private-sector solution to cybercrime vulnerabilities. In *Proceedings of the 1998 Conference on Defending Cyberspace*, Bethesda, MD, September 23-25 1998. CardTech/SecurTech.
- [2] M. Binderberger. Re: Navy turns to off-the-shelf PCs to power ships (risks-19.75). *RISKS Digest*, 19(76), May 25 1998.
- [3] Edupage Editors. AT&T network failure takes a toll on commerce. *RISKS Digest*, 19(68), April 16 1998. Online at <http://catless.ncl.ac.uk/Risks/19.68.html>.
- [4] G. Slabodkin. Software glitches leave Navy smart ship dead in the water, July 13 1998. Available online: www.gcn.com/gcn/1998/July13/cov2.htm.