

[WP-021]

## Whitepaper: The Impact of Critical Infrastructure Protection and IT

A Discussion about Possible Risk Inherited from Existing Critical Infrastructure Industries

**Version 050615**

June 2005

Author: Bob Radvanovsky, [rsradvan@unixworks.com](mailto:rsradvan@unixworks.com)

*(A special thanks goes to those listed for being my “sounding board” on this project.)*

Copyright © 2005 Bob Radvanovsky. All rights reserved.



## Legal Disclaimer

---

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material. *The authors are not lawyers, and this should not be construed as legal advice, but rather as an analysis of everyday operating procedure and common sense.*

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for the purpose of discussing a possible, and/or proposed IT security issue, and is not dependent upon any specified infrastructure, architectural condition or its issue(s).

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

## Introduction

---

With the introduction of the Healthcare Information Privacy and Availability Act (HIPAA) of 1996, set the stage for a whole slew of additional compliance, mandated directives at a federal level imposed to key industrial sectors, starting (obviously) first with the healthcare industry. Though I do not have any doubt that the healthcare industry does in fact need reform in how it does its business, nor would I have any issues with some of the reforms currently underway as part of reducing (if removing) extraneous and unnecessary paperwork, as part of the legal paperwork blizzard in an effort to protect doctors and medical staff from potential financially damaging lawsuits.

No one will (no doubt) have any stipulation that faster momentum may have come about as (almost) of a direct, net effect resulting from failed institutions who “cooked their books”, improperly impeded and willingly denied access to critical and sensitive corporate information and financial data, and performed countless tasks considered highly unethical, if not illegal, by their very nature. Companies, such as Enron, Worldcom, Arthur Anderson, et. al, have forced our governments, both at state and federal levels, to re-evaluate whether Corporate America is as honest as they have stated that they have been. People have made statements blaming former-CEO Bernie Ebbers from the failed Worldcom (now MCI) as part of our national economic swift and maintained downturn, even so much so that the President of the United States has made comments specific to the course of events resulting from the Worldcom investigations and court hearings.



Resulting from a prior presidential legacy, former President Clinton introduced Presidential Decision Direction NSC-63 (PDD-63) on May 22, 1998 introducing the terms “critical infrastructure” and “critical infrastructure protection” to our nation. These were initial steps made by the federal government to initiate forward momentum in justifiably protecting our nation’s critical infrastructures, of which, both the healthcare and financial/banking industries were listed as key industries considered “critical” to the survival and maintained operability of our nation. Following the tragedies that occurred on September 11, 2001, President Bush issued a series of directives, starting with the Homeland Security Presidential Directive (HSPD)-1, which introduced the Homeland Security Council, separate from the National Security Council, as a protectionist method of safeguarding our national resources and infrastructures. Later, HSPD-7, identified as the “*Critical Infrastructure Identification, Privatization and Protection*” directive issued on December 17, 2003, outlined and elaborated more in detail on the term (specifically) “*critical infrastructure protection*”.

## What is “critical infrastructure”?

---

The term “critical infrastructure” refers to assets of physical and computer-based systems that are essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separated systems that had little interdependence, at least, until 9/11. As a result, advances in information technology and with efforts performed to improve efficiencies in these systems, infrastructures have become increasingly automated and more interlinked. These improvements have created new vulnerabilities to equipment failure, human error, weather and other natural causes, as well as physical and computer-related attacks. Addressing these vulnerabilities necessitate flexibility, a massive evolutionary approach that spans both public and private sectors, protecting both domestic and international interests.

Every department and agency of federal, state and local governments are responsible for protecting their own infrastructure; each department and agency should have measures to assure that information is valid and accurate, protecting that information as if it were considered an asset. Part of the assurance process is through consistent testing and evaluation of their infrastructures, performing vulnerability assessments periodically against physical and computer-based systems, and obtaining expedient and valid authorities to validate those systems. This applies to both public and private sectors.<sup>1</sup>

---

<sup>1</sup> [http://www.usfa.fema.gov/subjects/emr-isac/what\\_is.shtm](http://www.usfa.fema.gov/subjects/emr-isac/what_is.shtm).



## So what then, is “critical infrastructure protection”?

---

The term “*critical infrastructure protection*” (CIP) pertains to the activities for protecting critical infrastructures. This includes people, physical assets, and communication (cyber) systems that are indispensably necessary for national, state and urban security, economic stability, and public safety. CIP methods and resources deter or mitigate attacks against critical infrastructures caused by people (e.g., terrorists, other criminals, hackers, etc.), by nature (e.g., hurricanes, tornadoes, earthquakes, floods, etc.), and by hazardous materials (HAZMAT) accidents involving nuclear, radiological, biological, or chemical substances. Quite simply put, CIP is about protecting assets considered invaluable to society that promote social well-being.<sup>2</sup>

What U.S. policy makers consider to be “*critical infrastructure*” has been evolving and is often ambiguous. Twenty years ago, the word “*infrastructure*” was defined primarily with respect to the adequacy of the nation’s public works. In the mid-1990’s, however, the growing threat of international terrorism led policy makers to reconsider the definition of “*infrastructure*” in the context of national security. Successive federal government reports, laws, and executive orders have refined, and generally expanded, the number of infrastructure sectors and the types of assets considered to be “critical” for purposes of homeland security.<sup>3</sup>

This definition was adopted, by reference, in the Homeland Security Act of 2002 (*P.L. 107-296, Sec. 2.4*) establishing the Department of Homeland Security (DHS). The National Strategy also adopts the definition of “*critical infrastructure*” in P.L. 107-56, and provides the following list of specific infrastructure sectors (and its assets) falling under that definition:

- ***Information technology.***
- Telecommunications.
- Chemical and petroleum-chemical.
- Transportation systems.
- Emergency services (includes first responder services).
- Postal and shipping services.
- Agriculture and food (include preparation, delivery and retail).
- Public health and healthcare.
- Drinking water / water treatment.
- Energy (both generation as well as transmission).
- Banking and finance.
- National monuments and icons.
- Defense industrial base.
- Key industry / technology sites.
- Large gathering sites.

---

<sup>2</sup> [http://www.usfa.fema.gov/subjects/emr-isac/what\\_is.shtm](http://www.usfa.fema.gov/subjects/emr-isac/what_is.shtm).

<sup>3</sup> The Library of Congress, CRS Report for Congress, Guarding America: Security Guards and U.S. Critical Infrastructure Protection, CRS- RL32670 (November, 2004).



## What could impact “critical infrastructure”?

---

For starters, there are loosely-defined directives not directly tied with or to each other, either within or between different industrial sectors. Secondly, many industrial sectors utilize and employ the services of a much older technology referred to as “SCADA” (or “*System Control and Data Acquisition systems*”). SCADA represents something called “control systems” that may/may not be connected to a controlling computational device and/or may/may not directly be connected to a network, or in many cases, the Internet. SCADA systems are currently being revitalized and renovated in an effort to bring those systems more up-to-date, more current, and (specifically) enable them to be more secure. Most people are unaware of the importance of SCADA-controlled devices esp. with how debilitating their impact could be if affected resulting from either natural or manmade causes.

Essentially, “*control systems*” are computer-based systems that are used by many infrastructures and industries to monitor and control sensitive processes and physical functions. Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. In the electric power industry they can manage and control the transmission and delivery of electric power, for example, by opening and closing circuit breakers and setting thresholds for preventive shutdowns. Within certain industries such as chemical and power generation, safety systems are typically implemented to mitigate a disastrous event if control and other systems fail. In addition, to guard against both physical attack and system failure, organizations may establish back-up control centers that include uninterruptible power supplies and backup generators.<sup>6</sup>

To the best of my knowledge, there are no governing compliance bodies of authority that regulate, control and dictate coordinately any form of interoperability between each other, let alone between industrial sectors. Each industry (supposedly) self-regulates itself, but there appears to be any (if not) little communications between interest groups and their representative organizations. This, to me, poses a serious issue insofar as to the vast amount of control systems which exist throughout the United States, within more than one industrial sector, and the lack of any coordination between each sector. Technically, SCADA is a form of IT, though many IT departments would vehemently deny that control systems are part of their core responsibilities, at least, from traditional operations of IT.

Much of the news media’s and government’s attention has focused primarily on the Internet and implementing redundancies in duplicated networking paths for the Internet, though the Internet (as a whole) is (supposedly) self-healing and self-replicating in its path discovery mechanisms esp. on Tier 0 and Tier 1 backbones -- which what makes up the Internet.

*The need for such elaboration is such that Information Technology is listed as 1 of 15 key critical infrastructures outlined by President Bush within HSPD-7; thus, IT (in effect) is a part of “critical infrastructure protection”. For that matter, so is SCADA.*

---

<sup>6</sup> The Library of Congress, CRS Report for Congress: “Critical Infrastructure: Control Systems and the Terrorist Threat”, CRS-RL31534 (February 21, 2003).



## How does CIP relate to (say) SOX?

---

SOX, GLBA and HIPAA all have their compliance issues respective to their industries, and from a slightly different perspective, represent (perhaps) only one aspect of that industry. Case in point, HIPAA represents privacy enforcement – plain and simple -- it does not correlate to paperwork reduction, efficiencies in information or documentation flow, nor the securification methods which must be implemented in general. Whatever security methods have been implemented, were driven by the privacy enforcement aspect of HIPAA, not simply because it makes good business sense. In today's always-connected world, the Internet is playing an increasingly more important role in transaction-based data interchanges. Secured transactions, patient information, and personal records – all are being moved across the Internet, most of it encrypted.

The problem is systemic in that each industrial sector has compliance issuances and directives for either the entire industry, or (such as the case with HIPAA) simply one aspect of it. In any case, the compliance directives offer little correlation to each other, and in some cases, might pose a conflicting, if not legal, risk. What are the chances that there could (though remote) that a scenario could pose itself involving two (or more) conflicts between differing compliance governances, say SOX requiring that financial data be disclosed, but would be a violation of HIPAA in doing so? Again, though it may seem remote, the possibility of something similar to this scenario occurring will happen eventually. This will have a debilitating impact on how IT operates.

How is it that IT would be impacted? With one compliance governance, would require that IT provide ALL representative information and disclose it accordingly; however, another might require the limitation (if not removal) of specific representative information, thus being in conflict with each other. IT would be smack dab right in the middle of a classic quagmire, neither going forward, but at the same, not reversing its direction, and not being able to stand in place.

Additionally, this places a tremendous amount of legal pressure against IT. Why? Some of the governances now implicates that IT is (now) the enforcement arm of the compliance governance(s) within the corporation. This is something that IT is not supposed to, let alone, unwilling to perform. The traditional role of providing data warehouses for data mining, transaction interchanges, Internet browsing, financial reporting, et. al – how does IT become now a law enforcement group?

This places too much undue burden upon IT and IT organizations. How would each corporate legal department like to be inclusive for each and every compliance violation? The forced collusion between IT and legal departments would (simply put) be an invitation for disastrous results.



## Why can't we all get along?

The problem that I foresee is confusion between compliance governance groups, organizations and their affiliations with one another. Secondly, with the introduction of CIP conceptually, has introduced multiple layers of control between the actual organizing body and those who would implement and regulate their solution.

As one colleague has pointed out, the left hand doesn't know what the right hand is doing, and in most cases, the left hand's index finger is unaware of the existence of the left hand's thumb versus the right hand's index finger and thumb accordingly. The issue isn't so much about compliance and governance is that it is more about coordinated compliance and governance. The problem will be effective and coordinated communications between all interested governing bodies and their affiliated organizations.

Unless this happens, and soon, our nation is in for some interesting circumstances, of which not only will there be some "victims", but "victim corporations" who will be held responsible for their actions, from all counts.

## CIP and compliance

The self-regulating aspect is notable for each representative industrial sector. But what happens when industries crossover within their same sector, or (more importantly) with other industrial sectors? Confusion and uncoordinated activities could result in lawsuits, and more companies, due to imposed compliance governances, would fall.

I foresee the need of a centralized governance body or board that regulates (for sake of better terms) – *everything*. Each compliance governance body belongs to its respective industrial sector: SOX and GLBA report to the banking and financial sector, HIPAA to the healthcare sector, etc. Each body reports to its industrial sector headquarters, the headquarters reports to a centralized body, which (more than likely) be controlled (entirely) by the federal government. The process is immense and conceptually, would take years to implement. However, the outcomes would be significant in a much more managed, more communicative, more coordinated efforts within, throughout and between each industrial sector.

Additionally, IT and its role would be removed from the responsibilities of each sector, reporting directly to the centralized governance body. Thus, this would allow IT to do its job, and at the same time, provide methodologies and levels of enforcement to the centralized governance body. This body would have a separate enforcement arm, containing IT and financial auditors, policy managers, compliance and authority specialists, forensics investigators, and (of course) law enforcers. Thus, the requirement that the federal government having a representative at each corporate level -- would be fulfilled. This, to me, isn't something that can be stopped – this is inevitability in that the federal government would regulate how "honest" a corporate entity is. Though this is not mandated (as of this writing), it may be representative of an eventuality that could be on the "ground floor" as to how far we could shape better business practices for the future.

