

Critical Infrastructure

Part I: Trains and Transit Systems

Authors:

Will Gragido CISSP CISA NSA-IAM/IEM

John Pirc, CEH | NSA-IAM | SANS Security Thought Leader

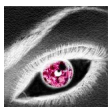
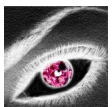


Table of Contents

Part I: Trains and Transit Systems	1
Introduction	3
Assessing the Risk.....	4
The Persistence of Time.....	4
Trains and Transit Systems: Hypothetical Situation	5
Historical Examples of Trains and Transit System Exploitation	6
Transport Command and Control Systems At-a-Glance.....	7
Conclusion.....	8
About the Authors:.....	9



Introduction

We live in a complex world, built upon complex standards. Our systems of commerce and trade today are evolving at a pace that constantly eclipse and redefine themselves. Some reflect humanity's eldest traditions while others defining new ones. Our theological and philosophical systems are no different, in fact in many respects they also are eclipsing and redefining themselves (at times in parallel with), systems of trade utilizing technology in order to provide a better tomorrow. Our world is a world in which the balance of power hangs precariously by a thread. A thread that today is heavily dependent upon information technology in order to remain intact. Often times this balance is threatened than most would appreciate or wish to acknowledge however, this does not change the fact that the threats are real and so are the needs to mitigate them.

Ours is a world in which diversity is celebrated and at times, sadly finds itself intolerant of the diversity, which we hold dear the world over. As a result, checks and balances have become of overt importance. They are necessary and non-negotiable in the pursuit of ensuring order. The order of which we speak is, of course, the balance of life upon which all human beings depend as was mentioned previously. This balance includes the infrastructure. Here in the United States, Homeland Security Presidential Directive (HSPD-7) designates responsible agencies as Sector Specific Agencies (SSA), responsible for one or more of these infrastructural elements. HSPD-7 defines the following Critical Infrastructure/Key Resource (CI/KR):

- Information technology
- Telecommunications
- Chemicals
- Transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems
- Emergency services
- Postal and shipping services
- Agriculture, food (meat, poultry, egg products)
- Public health, health care, and food (other than meat, poultry, egg products)
- Drinking water and waste water treatment systems
- Energy, including the production refining, storage, and distribution of oil and gas, and electric power
- Banking and finance
- National monuments and icons
- Defense industrial base



Assessing the Risk

In short, all life depends upon its ability to define an acceptable level of risk. In order to arrive at this state, the need to define threats, vulnerabilities in addition to the probability of exploitation is of paramount importance. In our world – in developed and undeveloped nations alike, critical infrastructure and key resources remain under heavy scrutiny in various states of maturity from a risk perspective. Were anything to occur to these critical infrastructure (CI) / key resources (KR), in simulated or non-simulated modes, the need to quickly and succinctly define the impact to humanity in terms of risk in every sense of the word, would become a priority to say the very least. The need to define in no uncertain terms the qualitative and quantitative impact (taking into consideration the data gained in the event that previously conducted assessments), would be without question integral in this process.

The information and data yielded because of these efforts in many respects could and likely would influence life, as we know it on planet Earth. As a result, the ability to assess and measure risk in a comprehensive manner is vital to our critical infrastructure just as it is in all aspects of life. In essence, it is essential to our very survival and could be argued that it has always been since time immemorial, woven into the tapestry of our lives and history. Some would argue it is the result of Darwinian evolution and adaptation, others that it is the result of Creational design. Regardless it is integral to all human beings; arguing against this desire to mitigate risk in order to ensure the least amount of potential negative impact is therefore inappropriate and simply stated illogical.

The Persistence of Time

Tempus Fugit, time flees. Yet though it flees or as some conventionally and erroneously translate this as “flies”, one cannot argue that time is not persistent. As a result, the failure to act swiftly or at all does nothing to impact the persistent march of time. With this in mind, imagine if you will, a world in which time continues its march while the inhabitants revisit and by virtue of some cataclysmic event (which may or may not have been avoided had proper measures been taken), reacclimatized and acquainted with hardships not seen in decades or perhaps centuries. In a world where some terrible event has occurred in one or more elements of critical infrastructure or key resources, and humanity have been forced – against its will into the annals of time would circumstance be benevolent? Would it sit as judge, jury and executioner?

Imagine a world in which communications systems and electricity were magic, the stuff of the gods; where transportation systems – motor scooters, motorcycles, automobiles, trucks, trains, planes, and ships were strangely familiar but mythical. A world where modern conveniences such as running water, indoor heat and working sewage systems were simply a dream. In absence of proper preparation, this world – as extreme and distant as it may sound, could very well be tomorrow’s reality. To begin with, we, as human beings would have a much different view of the world were this the case.



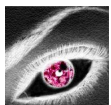
Consider the view which humans during the Roman Empire had versus that which existed prior to and directly afterward – you'll note in doing so a defined difference in how these people lived and co-existed with one another. Additionally, you will note their dependency upon their infrastructure, which either existed via nature or as the result of the efforts of humanity. Regardless of how they came into being, the impact of their infrastructure (in addition to the insight and vision of using it), was profound and irrefutable. If this world was our world than our world as we know it would have ceased to exist in a disturbing manner. It would be foreign; alien to us though it had just changed. Perhaps as alien as the bottom of the sea, the surface of the moon or the rings of Saturn all very real yet all terribly different from anything any human would call home. It would be a world challenged with redefining itself; driven by its need to maintain order; balancing precariously, rules and principles, which may no longer be relevant, or seen as such.

Trains and Transit Systems: Hypothetical Situation

If an event or events of interest occurred, which caused critical infrastructure (CI) or key resources (KR) to fail without warning would the shock and impact be more than we are individually or collectively prepared for? What if it were only to affect a smaller subsection of the spider-web that makes up the tapestry of our worlds existence – say the national railway system. What impact would that have upon how we live? What if only the systems related to railway transportation and shipping systems were to vanish, up in smoke – literally or figuratively. What would be the net effect? How would affect our children? Our neighbors? Our governments? Our commodities exchanges – local and national; perhaps even international? What impact would the loss of these systems or a strategic surgical strike against key resources introduce to our nation and world at large? Our assertion is that the impact would be devastating and paralyzing; grandiose and horrifying and at the same time impossible to accurately predict without enough historical data from which to draw a conclusion from. It would be the culmination of all fear, the fear seen in the attacks brought to US soil on 9/11, delivered straight into the intravenous system of America's heartland depending on the scope, severity and order of magnitude involved. Railway and transportation systems like play key roles as we have discussed previously. Consider the impact of a disastrous event occurring within the rail system knowing the following functions that it provides us on a daily basis:

- Transportation of people – our most priceless and precious assets
- Transportation of raw materials for the use in the production of goods
- Transportation of partially manufactured goods used in the production of other goods
- Transportation of completed goods ready for market
- Transportation of food and necessities
- Transportation of fuel
- Transportation of biological / chemically hazardous materials (ever seen what happens when a train carrying chlorine gas derails and there is a leak? Not good)

Their role is beyond important to our way of life; their significance epic. This is not a complete or comprehensive list. It merely outlines and articulates some of the interplay that railway transportation systems have in our lives. The argument could be made that were some event of interest to occur there would be alternate ways to transport goods and people, but what are the costs in doing so?



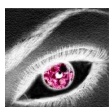
Would these alternate means be able to accommodate the load, as a result become greater targets of opportunity for exploitation, and compromise yielding greater devastation? These are not simple question to ask or to answer. However, we need to ask ourselves as professionals and representatives of our industry the difficult questions in order properly gauge our readiness in dealing with threats introduced into these environments. As previously discussed in the section dealing with risk, were we to possess all of the necessary data points we would be able to establish risk relevant data sets from which estimates and assertions having to do with risk could be arrived at. We would be prepared or enabled to estimate the costs associated with collateral action and activity in these scenarios while also being able to manipulate the data in complex ways to gain a better understanding of real and potential impact indices.

For example, suppose that all the train and transit lines in your major geographic locale were redirected in such a way that they all arrived at a central location / destination – passenger trains and freight alike, carrying with them compromised loads (physical and logical), with the intention being death, destruction and pandemonium – the calling cards and hallmarks of terrorist acts. What if these trains contained high explosives (placed there purposefully or as part of the cargo load -- fertilizer for example), or caustic gases such as chlorine which when released is quite deadly. What new degree of threat and risk might be introduced within our culture? Our neighborhoods? Our cities? Our nation? What degree of confidence would exist in the system that manages these transit lines – perhaps a SCADA based system—which in fact permeate most of these environments today, were it compromised and undermined?

Historical Examples of Trains and Transit System Exploitation

History has provided many examples that describe and chronicle the use of trains in acts of violence and terror the world over. In 1995, the Aum Shinrikyo cult of Japan, released Sarin gas into the Tokyo subway system with the intention of killing thousands if not hundreds of thousands of commuting Tokyo natives and visitors. Upon investigation of the cult and its head quarters, Japanese authorities found enough Sarin gas to kill approximately 4.5 million people. Additionally, the cult was in possession of nerve gases (VX, Tabun, and Soban), chemical agents such as Mustard Gas and Sodium Cyanide. Furthermore, the cult possessed a sizeable cache of biological warfare agents including Ebola, Anthrax, Q-Fever (which is highly contagious) as well as large sums of psychedelic and hallucinogenic drugs. All of which were intended to make their way into the general populace in the easiest and most efficient manner possible, the mass transit system. One need only imagine what the impact might have been had these terrorists succeeded in their mission.

Between 1998 and 2005 for example, approximately 183 attacks succeeded on rail system target. The results of these attacks were the deaths of approximately 630 people with thousands of others injured as a result. One attack in particular that was not predominantly cyber based but deadly nonetheless, took place March 11, 2004 in Madrid, Spain. The attackers utilized backpack bombs; improvised explosive devices (IEDs) and took the lives of 191 people while seriously injuring another 2050. The devices in question were comprised of a mixture of Goma-2 ECO, a high explosive chiefly manufactured and used in mining operations weighing approximately 10kg (22lb) with 1kg (2.2lb) of nails and screws packed around the explosive to be used as shrapnel.



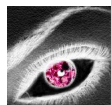
The IED was remotely triggered using a cell phone. Richard Clarke, Cyber security special advisor to President Bush was quoted saying, "Osama Bin Laden is not going to come for you on the Internet". Perhaps that statement was true at some point in time but the fact is, they can reach out and touch someone via cell phone and with the reported active in critical infrastructure, the statement does not hold true today. Initially responsibility for the attacks was uncertain however later it was established that the Euskadi Ta Askatasuna or ETA or a Basque nationalist and separatist organization. Authorities in Spain are still investigating the incident and those involved.

In 2008, a Polish teen allegedly hacked the City of Lodz' tram system using a modified TV remote control. The teenagers' actions described as a 'prank' led to a state of chaos culminating in the derailing of four vehicles. Twelve people were injured because of his actions. Though he meant no harm, his actions could have easily resulted in much more serious consequence for himself and others. According to authorities, the device he created was capable of controlling all the junctions on the line. The teenager took copious notes with respect to the best junctions for manipulation, their location, and what signals were easiest most lucrative to change. According to officials, transport command and control systems are designed by engineers with little to no exposure or knowledge of or about security. They use commodity (e.g. readily had and available), electronics and basic skills to complete their tasks. This incident however successfully caused transit authorities the world over to reconsider their designs. Given the ease of exploit seen and demonstrated in this example, imagine what the impact might have been had an Islamic fundamentalist group rather than a 14-year Polish boy had control of the tram or a series of trams and railways in many cities, remotely accessible via the touch of a button or key stroke?



Transport Command and Control Systems At-a-Glance

Unbelievably, you can actually control critical transit systems in the palm of your hand. Now, according to the vendor documentation it is as easy as using an 802.11b enabled handheld device with encryption of course. The main point of debate is that the transport command and control system network could be compromised through the wireless infrastructure if not properly secured. The nefarious cyber actor is going to take advantage of any low hanging fruit available to her and wireless is always a ripe target for exploitation. One must ask, is transportation system security any different from SCADA security? No, they are both considered critical infrastructure. We know that the possibility of exploitation on a grand scale is real and that as recently as April of 2009 the United States power grid was compromised thusly proving that the vulnerabilities are real and that the potential for further, more severe exploitation is greater still. The following article, "Spies hacked into U.S. electricity grid" http://news.cnet.com/8301-11128_3-10214898-54.html, relates in detail the events surrounding this. So should we ignore other pieces of critical infrastructure such as transportation? Is it possible that our transportation systems have been compromised or likely to be compromised? It is the opinion of the authors that this is in the realm of possibilities. Let us step beyond the hype and into the realm of the proactive.



Taking proactive measures in securing transportation control systems is not optional. It is occurring today within the Electric and Utilities industry in the U.S. through NERC CIP and needs to occur throughout other aspects of our national infrastructure we deem critical. The NERC CIP standard defines the criteria necessary for assuring a guaranteed level of security deemed minimal in protecting the power grid. Where are the standards for transportation in terms of Cyber Security? Furthermore, the compensating controls to secure critical infrastructure often leave out technologies that would address advanced malicious code and content in addition to advanced attack threat vectors such as advanced persistent threats (APTs) which we will be discussing in a forthcoming paper. In researching standards and law's that are applicable to cyber, security in the transportation/rail industry can be found at the following sites:

- THE 9/11 COMMISSION ACT OF 2007 Public Law 110-53 addresses the need for IT infrastructure security for the transportation industry: <http://www.surfacetransportationisac.org/SupDocs/HR1Summary.pdf>
- Public safety communications community and other narrowband private land mobile radio users of interoperable multi-vendor equipment implementing the Project 25 Standard APCO PROJECT 25 STATEMENT OF REQUIREMENTS: <http://www.apcointl.org/frequency/project25/documents/SOR-2009.pdf>
- NIST Special Publication 800-53 Rev 3: Recommended Security Controls for Federal Information Systems and Organizations: <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf>

With any standards or law, they are left to interpretation and should not be treated as a checkbox. As we move to a more interconnected World, we need to treat our critical infrastructures with kid gloves and push for standards that go beyond to insure and educate the masses on the importance of IT security.

Conclusion

In closing, the authors would like to make the following statement regarding the potential for attacks of this sort: they are real and not beyond the scope of those, whose intent it is to achieve a goal by any means necessary to and including the loss or "sacrifice" of human lives. As information security and risk management professionals we owe it to ourselves, our loved ones, our colleagues, our customers, our clients, our neighbors and fellow citizens to ensure that the same level of due diligence seen within the assessment of critical infrastructures such as transit systems be carried out as it is within other environments. To not do so would be both irresponsible and portray ignorance with respect to our understanding of the evolving threat landscape.



About the Authors:

Will Gragido – An information security and risk management professional with over 15 year's professional industry experience, Will Gragido brings a wealth of knowledge and experience to bear. Working in a variety of roles, Will has deep expertise and knowledge in operations, analysis, management, professional services & consultancy, pre-sales / architecture and business development within the information security industry. Will is a long-standing member of the ISC2, ISACA, and ISSA. Mr.Gragido holds the CISSP and CISA certifications, as well as accreditations in the National Security Agency's Information Security Assessment Methodology (IAM) and Information Security Evaluation Methodology (IEM). He resides in the Chicagoland area, is a graduate of DePaul University and is currently preparing for business school. You can follow Will on Twitter: <http://twitter.com/wgragido>

John Pirc - John has more than 10+ years of security experience in security research, worldwide product management/development, security IV&V testing, forensics, APT's, Critical Infrastructure and architecting/deploying enterprise wide security solutions for both public and private organizations worldwide. John has worked for the US Intelligence Community, small private security consulting firm and large global vendors. In addition to a BBA in Information Systems from the University of Texas, John also holds the NSA Information Assurance Methodology and Certified Ethical Hacker certifications. John was recently named security thought leader from SANS Institute and advisory board member of SANS Execubytes publication. You can follow John on Twitter: <http://twitter.com/jopirc>

