

Cyber Terrorism – Is it a real threat?

While at the CSI fall conference in Washington, DC, this past November, I attended the “Cyber terrorism: Are We Ready?” panel. The moderator was Richard Starnes, director of incident response for the Managed Security Operations Center. He was joined by panelists Howard Schmidt (Vice President and CISO of ebay), Ira Winkler, President of Internet Security Advisors Group, and Paul Kurtz, Executive Director of Cyber Security Industry Alliance (CSIA). I, as well as some of my colleagues in attendance were shocked at the lack of concern the panel had on the threat of cyber terrorism. We left the meeting shaking our heads that cyber terrorism was not being taken seriously.

Computers have long been used to control the functioning of equipment. A typical application is that of control systems commonly known as SCADA control systems. SCADA stands for Supervisory Control and Data Acquisition. You can think of SCADA as software that interfaces directly with the Programmable Logic Controllers (PLCs) that are attached to the equipment.

SCADA systems are used in industrial processes, utility generation (conventional and nuclear) and also water treatment plants as well as many other applications. Typically SCADA systems used to run on DOS, VMS and UNIX. But the operating environment is changing.

The British Columbia Institute of Technology (BCIT) issued a paper entitled “The Myths and Facts behind Cyber Security Risks for Industrial Control Systems.” I quote, “Process control and SCADA systems, with their reliance on proprietary networks and hardware, have long been considered immune to the network attacks that have wreaked so much havoc on corporate information systems. Unfortunately, new research indicates this complacency is misplaced – the move to open standards such as Ethernet, TCP/IP and web technologies is letting hackers take advantage of the control industry’s ignorance.” BCIT maintains an industrial cyber security incident database which shows that there has been a sharp increase in the number of events occurring around 2001.

There are three disturbing trends that should change the way we think about these systems and Cyber Terrorism. First, we are automating more and more processes. For example, if you construct a new commercial building today, all of the HVAC (Heating, Ventilation and Cooling) systems are now controlled by process computers. The second disturbing trend is that the manufactures of these systems are increasingly moving towards hosting these systems on either a Windows or Linux based operating system. And third, the people who monitor and maintain this equipment are dictating more and more that they want remote access, usually through a VPN (Virtual Private Network).

From a security perspective, all of these trends should send alarm bells ringing. Not only concern us, but also frighten us. The SQL SLAMMER worm spread quickly and affected

airlines and financial institutions through a denial of service. The Slammer worm also penetrated a private computer network (VPN) at Ohio's idled Davis-Besse nuclear plant and disabled a safety monitoring system for nearly five hours. The worm entered the plant network through an interconnected contractor's network, bypassing Davis-Besse's firewall.

Nachi (aka Blaster or Welchia) also caused havoc by generating so much traffic it immediately caused denial of service attacks. One large corporation I am aware of got the Nachi virus through a user creating a secure VPN tunnel to his work location from home. Yes it was a secure tunnel, but Nachi happily jumped right through that tunnel onto the corporate network. By allowing companies that control and monitor our equipment, our security becomes only as good as the security of the company providing the service. How good is their IT security?

Again, according to BCIT, SCADA and automation devices need to undergo security robustness design and testing prior to deployment in the field. SCADA and control protocols should be improved to include security features. Currently most devices appear to be highly vulnerable to even minor attacks and have no authentication or authorization mechanisms to prevent rogue control.

Cyber Terrorism is an increasing threat to each and every one of us. More and more we are using computers and automation devices to control a greater portion of our environment. We are using more common operating systems to host these systems on. There is a growing trend to access these process control networks from what we would typically have consider "data" or "business" networks. And most importantly SCADA and control protocols are highly vulnerable to even minor attacks.

The word Terrorism conjures up thoughts of death and destruction. In this respect, the phrase "Cyber Terrorism" implies death and destruction through Cyber means. It is therefore important to offer some thoughts of clarity around the phrase. I would like to suggest a more appropriate phrase of "Cyber Disruption". By that I mean the ability of someone or some organization to disrupt parts of our infrastructure to the point they are not usable for a period of time. We have seen examples of this through SQL SLAMMER where airlines and financial institutions (more specifically ATM's) were put out of service for a period of time. When we look to the utilities industry, what is the "worst" that can happen. It would not be unreasonable to say that control systems could be manipulated in such a way as to cause the system they are controlling to "trip" or to "shutdown". In the nuclear industry there is very much of a defense in depth strategy. When something goes wrong there are a multitude of systems that will immediately detect the unusual event and safely shut down reactor. Again, looking at worst case scenarios, water treatment plants could be manipulated to either apply more of a chemical (like chlorine) to the water or less. Again, defense in depth safety measures would catch the unusual event and shutdown the system. A well planned and well organized "Cyber Disruption" could then shutdown systems that are part of our infrastructure including power plants, water treatment plants, refineries, financial institutions and airlines. Would people die? In the authors opinion, no. That would be highly unlikely.

Let me leave you with a theoretical scenario that might put some perspective on what is possible. Vulnerabilities are discovered on a regular basis in the Windows operating system. Let us assume that someone or some organization discovers a vulnerability that allows them to gain complete access over the host they target, with the intent to use it to disrupt as much of our cyber infrastructure as possible. You or I as security experts are unaware of this vulnerability and can therefore not patch for it. Through very careful and very passive means our group quietly infiltrates and determines which networks and devices they can gain access to. If we have unwittingly attached our data and process control networks together without the appropriate defense in depth protection mechanisms (routers, firewalls, two factor authentication etc) then in our theoretical example we would have exposed ourselves. Our group now, after a lengthy planning process targets every piece of control equipment they have access to and shuts it down. Immediately after accomplishing this they unleash a worm using the hundreds of thousands, if not millions of hosts they have compromised which at a minimum causes a massive denial of service.

Cyber terrorism or more specifically Cyber disruption I believe is a real threat to each and every one of us. Let us be proactive in how we handle the security side of this emerging technology. BCIT summarized the threat perfectly when they said, "Failure to adapt to the changing threats and vulnerabilities will leave the controls world exposed to increasing cyber incidents. The result could easily be loss of reputation, environmental impacts, production and financial loss and even human injury".