

MGT405: Critical Infrastructure Protection

2-Day Program • Thu, 10 Sept - Fri, 11 Sept 2009 • 9:00am - 5:00pm • 12 CPE Credits • Instructor: Marcus Sachs

The critical infrastructure of a nation is the system of highly complex and interdependent physical and cyber-based assets essential to the minimum operations of a nation's economy and government. It includes, but is not limited to, communications, energy, banking and finance, transportation, water supply, and emergency services. It could be owned and operated by the government or the private sector, or both. Historically most national critical infrastructure was physically and logically separated; they were systems that had little interdependence. But as a result of advances in information technology over the past several decades and the necessity of improved efficiency, these systems and assets have become increasingly automated and interlinked. Unfortunately these same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities requires flexible and evolutionary approaches that span both the public and private sectors and protect both domestic and international security.

Because of imbalances in military strengths, future enemies – including nations, groups, or individuals – may seek to cause harm in non-traditional ways, including domestic attacks against critical infrastructures. Because our global economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on infrastructure and information systems may be capable of significantly harming both a nation's military power and economy. This new threat is visible in the terrorist attacks on the World Trade Center in 1993 and 2001, growing numbers of cyber espionage attacks against the military, civil government, and the private sector, and even natural events such as earthquakes, typhoons, and solar flares.

This course begins by examining in depth the events of the past 20 years, including the lessons learned about the interdependencies of the critical infrastructures following various terrorist attacks and what the United States learned in the aftermath of hurricanes Katrina and Rita in the summer of 2005. While there are many cross-sector interdependencies to consider, we will focus on the dependence of the various infrastructure sectors on the Internet and the impact of highly complex computer controlled systems. We will also discuss the creation of the US Department of Homeland Security and its role in protecting a national critical infrastructure from cyber intrusions.

Authored and presented by a leading expert on critical infrastructure protection and cyber warfare, this course will offer detailed explanations of specific pervasive Internet technical problems and conduct in-depth examinations of the types of attacks that might do the most harm to your organization and your infrastructure sector. We will take a comprehensive look at the current Internet governance model, and you will learn how to develop business continuity and disaster recovery plans to counter current cyber threats and threat actors that take advantage of this model. You will also gain knowledge about the new directions being taken by criminals, terrorists, spies, and nation states and what nations are planning to do for the defense of their critical infrastructure against these new threats. Finally, you will learn how to protect your networks from the dangers lurking in cyberspace while developing a full understanding of emerging techniques used to detect and contain outbreaks of malicious activity on the Internet.

Who Should Attend:

- Managers, supervisors, senior engineers, or other professionals with a strong working knowledge of plant operations
- Government officials with responsibilities for CIP policy development

Note: Due to the sensitivity of the course subject and the focus on protecting national critical infrastructures, this course is only available to citizens of the United States, Canada, Australia, New Zealand, and the United Kingdom currently living and working in those countries. Proof of eligibility will be required when checking in at the training event as well as when entering the classroom.

Register at www.sans.org/canberra09_2