eCommerce, Terrorism, and Security

Chair:

John R. Harrald
Professor & Director

Panel members:

The Survival of eCommerce Systems after the World Trade Center Attacks

John R. Harrald¹, YounHee Kim²
¹Professor, ²PhD Student
Department of Engineering Management and Systems Engineering, The George Washington University, United States

Protecting eCommerce Against the Unknown and Unseen Enemy

Theresa Jefferson¹, Julie C.H. Ryan²
¹Professor, ²Professor
Institute for Crisis, Disaster, and Risk Management, The George Washington University, United States

Examining the Process for Developing Security Standards

Dennis "Mike" Egan
Director
Homeland Security Intermodal Transportation, Systems Planning Corporation, United States

eCommerce and Maritime Security

Disaster and Risk Management: Slovenia’s Perspective

Iztok Podbregar
Director & Assistant Professor
Slovenian Intelligence and Security Agency, Government of the Republic of Slovenia & Faculty of Organizational Sciences, University of Maribor, Slovenia

Andrej Sotlar
Lecturer & Deputy Head
Department of Security, College of Police and Security Studies, University of Ljubljana, Slovenia
Although the immediate impact of terrorism is highly visible death, injury, and destruction, the terrorists have made no secret that their primary target is the economic power of America and the developed world. “[W]e will target the keys of your economy until you stop your transgression or one of us dies.” (Osama bin Laden, October, 2002). The purpose of this panel is to describe the impacts on eCommerce of past attacks, to discuss current vulnerabilities, and identify potential risk reduction interventions.

The Survival of eCommerce Systems after the World Trade Center Attacks

John R. Harrald, Professor
Youn Hee Kim, Doctoral Candidate
Engineering Management and Systems Engineering
The George Washington University

The attacks on the World Trade Center produced $77 Billion in insured losses, and seemingly devastated major businesses. This paper is a description of preliminary results of a National Science Foundation funded study of the financial impacts of the attacks on large publicly held corporations. A group of 20 companies is examined in detail and their financial performance compared to their industry is compared for 18 months prior to and after the 9-11 attacks. The rapid recovery of most of these corporations is described, and reasons for this financial recovery are discussed. One of the primary reasons for the recovery of many corporations was the robustness of their eCommerce systems. Many of these systems were operating from remote sites within 24 hours of the destruction of the towers and most were fully operational prior to the re-opening of the New York Stock exchange seven days after the attack. The factors that provided for this system resilience are identified and describe.

Protecting eCommerce Against the Unknown and Unseen Enemy

Theresa Jefferson, Ph.D.
Assistant Professor of Engineering Management and Systems Eng.
The George Washington University
Julie, C. H. Ryan, Ph.D.
Assistant Professor of Engineering Management and Systems Engineering
The George Washington University

Protecting eCommerce systems from abuse and misuse is a never-ending challenge. Vulnerabilities in software applications and operating systems combined with readily available hacking tools have resulted in numerous accounts of online attacks. The media frequently contains details of computer worms, denial of service attacks, viruses, and compromised systems. The hackers responsible for these crimes are generally motivated by malicious and senseless purposes. However, there are many breaches of security that are never reported. The hacker that goes undetected by security administrators is often a much more dangerous enemy. His attacks do not cause visible damage. This enemy’s intent is to steal secrets and corporate data, and his success lies in remaining unnoticed. The skills and resources needed to protect ecommerce systems against electronic espionage are difficult to obtain and even harder to implement.
Examining the Process for Developing Security Standards for eCommerce and Maritime Security

Dennis “Mike” Egan, Director  
Homeland Security and Intermodal Transportation  
Systems Planning Corporation

Maritime transportation is critical to the global economy, it is also a unique source of vulnerability to terrorism. Approximately 95% by volume of the non North American U.S. foreign trade is dependent upon shipping, according to the Department of Transportation (DOT, 1999). Specially designed container ships transport over 6 million of container carrying high value cargoes into U.S. container ports each year. Less than 2% of these containers are physically inspected. The complex, interdependent, decentralized operations of a typical U.S. port are extremely vulnerable to the terrorist threat. International initiatives and U.S. programs such as the Container Security Initiative are attempting to provide a more rigorous system of identifying and tracking containers and their contents. This paper describes the role of the eCommerce component of maritime trade in reducing the uncertainty that must be resolved by security officials, and the economic costs of increased security that will be borne by shippers, shipping companies, and ports. The key will be in reducing the number of indeterminate cases that require expensive investigation only to determine that no threat exists through more complete and accurate electronic transfer of information between public and private sectors.