



2008 Calendar

Sept. 15-18, 2008
ASIS International 54th Annual Seminar/Exhibits
 Atlanta, Georgia, USA
[Click here](#)

Sept. 29-30, 2008
Cyber's Annual Cyberinfrastructure Summit
 Banff, Alberta, Canada
[Click here](#)

Oct. 1-3, 2008
6th Annual Conference on Privacy, Security and Trust
 Fredericton, NB Canada
[Click here](#)

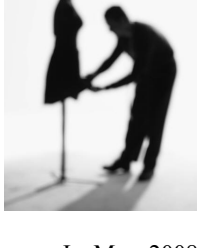
October 16-18, 2008
Canadian First Responders Conference (CBRNE)
 Calgary, AB
 More information in a future issue.

Nov. 15-21, 2008
2008 CSI Conference
 National Harbor, MD, USA
[Click here](#)



HEADLINE NEWS — August 6, 2008

Counterfeit Products: Borderless Crime on the Internet



In May 2008, the Canadian Association of Police Boards released a Canada-wide study indicating that the "borderless nature of the Internet, the relatively low risk of detection and high rewards, helps organized crime groups undertake international crimes."

Recent law suits have also brought media attention to the fact that organized crime is using the borderless-based services of the Internet to sell counterfeit goods including prescription drugs, computer software, toys, baby formula and of course designer clothes, purses and watches.

A recent law suit in France has drawn attention to the common practice of selling designer goods through eBay. The case against eBay in a commercial court in Paris was brought jointly by six brands accusing eBay of "negligence" in allowing illegal copies of their goods to be sold in online auctions.

According to the judgment, eBay must pay 19.28m euros in damages to Luis Vuitton Malletier, 17.3m to Christian Dior Couture and 3.25m to the perfume brands. Those in the know believe the ruling is seen as a landmark, because it could oblige eBay to rethink its business model.

In Canada, a B.C. Supreme Court Justice recently awarded Louis Vuitton \$980,000 in damages (plus court costs which are estimated at about \$50,000) surpassing a judgment of \$700,000 that Microsoft Corporation received from a Quebec court last year after its software was pirated and sold by another company.

Lorne Lipkus, chair of the CACN Education and Training Committee and a partner with Kestenberg Siegal Lipkus LLP, a leading anti-counterfeiting law

firm, states that "purchasing counterfeit goods supports organized crime no matter what the product is or the manner in which it is sold."

As an example Lipkus said phony drugs are becoming so popular that counterfeiters are using other goods to sneak in pills. "Pharmaceuticals are a huge, huge issue and a growing one. I am being advised of luxury counterfeit purses with the pills stuffed inside," he says.

Lipkus adds, "if there is a silver lining here, it is the evidence that Canadians will refrain from buying counterfeit goods when they know about the involvement of organized crime. This tells us that, if we pass the right laws, empower our police forces, provide them with the appropriate resources and educate our citizens, then we can solve this problem."

The RCMP Border Integrity investigators consistently note the following characteristics of the counterfeit products they encounter:

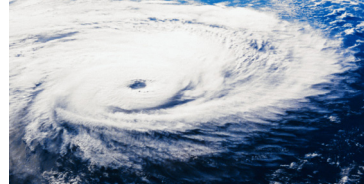
- Always cheaply made;
- Often unsafe;
- Generate huge profits for organized crime;
- People involved in trafficking counterfeit products don't care about the health and safety of the people, who knowingly or unknowingly, buy the product.

For more information, please visit www.cacn.ca. The Canadian Anti-Counterfeiting Network (CACN) is a coalition of individuals, companies, firms and associations that have joined together in the fight against product counterfeiting and copyright piracy in Canada and internationally.

Welcome to E-Telligence

Twice a month, we'll be profiling guest writers, cyber crime news and important events to keep you informed.

Predicting the Perfect Cyber Storm



Second of a two-part series on managing the risk of cyber threats by David McMahon.

"All physical events have a cyber echo. All cyber events have a physical effect."

What would happen if the matrix crashed? Simulation and models based on real threat metrics show that the prognosis is not good. The modeling of the perfect storm predicts that the current level of cyber attacks is several orders of magnitude beyond most organization's ability to sustain. If this storm was to be released from the cloud, it would cascade through critical infrastructures, along risk conductors and interdependency vectors. Those relying on telecommunications most would be affected first, and would propagate ruinous effects to other sectors. The catastrophic impacts would ricochet recursively throughout the fabric of the economy at velocities faster than a human's ability to intercede. The government would fail in the first few minutes, financial markets and energy grids would collapse by noon and the remainder of sectors would see the end of business by early afternoon. Look no further than Estonia for a poignant example.

The notion of a "perfect storm" is a deep dive exploration of complex dark forces converging in cyber space and the information war in which critical infrastructure operators find themselves decisively engaged. The perfection of the storm is shaped by phenomena like:

- Critical infrastructure interdependencies and risk conductors
- Disruptive technologies
- Convergence of IP, threat actors, applications and content
- Globalization
- Economic drivers
- Commercialization
- Criminalization
- Commoditization
- Evolution of attacks
- Virtualization of processing, storage and environments emergence

The larger the system the more profoundly influenced it will be by these macro phenomena. No information communication technology system on Earth can escape these effects. Superpowers have experimented with the concept of controlling weather as a weapon. Prophetically, the cyber-atmosphere is manipulated by sophisticated tradecraft spawned from state-sponsored espionage, adopted and commoditized by trans-national crime syndicates, and the wetware hacking perfected by terrorist organizations.

Risk management in the storm must similarly evolve well beyond paper Almanac exercises towards real time advanced hyper-realistic modeling, applied universal system theory, and supercomputing grids fed by vast sensor arrays, along the lines of modern weather forecasting.

Risk typically has a negative connotation, but there are also positive opportunities arising from risk-taking. Innovation and risk co-exist frequently. Today's compliance and legal systems will hold executives responsible for ensuring prudent risk management; this not only includes showing wise risk mitigation but demonstrating appropriate risk taking in pursuing opportunities, and ensuring safety in a proactive manner. In risk analysis, exposures owing to inaction are tabled as losses or negative impacts. Integrated risk management is a continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective. It is about making strategic decisions that contribute to the achievement of an organization's overall corporate objectives.

"Cyberspace is the nervous system that binds all critical sectors."

Risk methodology for critical infrastructures must be based upon a solid and incontrovertible theoretical foundation, notably the synthesis of Critical Infrastructure Protection (CIP) and sophisticated risk analytics with the Universal Systems Theory that addresses the complex dynamic emergent behaviour of open systems. We must understand that the pragmatics of real infrastructures is influenced by examining contagion-borne interdependences and the phenomena that contribute to perfect storm conditions. Qualitative statistical findings from a thorough consultation with critical infrastructure owners, needs to be validated and contrasted with comprehensive quantitative (empirical) metrics from primary indicators: communications, financial and geospatial data. The analyst will need to apply mature analytical processes like hypo-deductive reasoning, formal and inductive (fuzzy) logic, critical and alternative analytics, within an integrated risk management framework. The intended outcome is an adaptive model of high-fidelity and predictive accuracy, at least as good as weather forecasting today.

This thesis represents an essential departure from relying on anecdote, doctrine and security policy as the common means of managing risk. Time to invest in cyber weather satellites, operating in the cloud and less in woolly worms living underground, on the basis of managing risk.

NOTES:

The Universal Systems Theory is a multi-perspectival domain, synthesizing principles and concepts from computational epistemology, ontology, engineering, cybernetics, morphological analysis, statistical thermodynamics (entropy), self-organization, catastrophe, chaos, uncertainty and complexity theory.

The universal systems theory is a means of modeling infrastructure risk with a high-degree of precision and deterministic uncertainty, when tuned by pragmatics and empirical metrics from the network.

Critical infrastructure risk methodology talks about building a high-fidelity model to accurately represent risk conductance and convergence in a cyber connected ecosystem of critical sectors, and most precisely establish the calculation of metrics for an integrated risk management framework for critical infrastructure protection.

David McMahon has an honours degree in computer engineering from the Royal Military College of Canada and has spent the last 25 years working with the military, intelligence and security communities, both in the public and private sectors.

David has been engaged in the spectrum of operations from special forces, drug interdiction, counter-terrorism, information warfare, counter-espionage, and foreign intelligence.

He was also one of the founding members of the interdepartmental committee on Information Warfare. Today, he is the National Security Advisor for Bell Canada.

Websites you should visit...

www.cisac.ucalgary.ca

www.zebracentre.ca

www.antiphishing.com

www.cacn.ca

www.interpol.int

www.wiesenthal.com

www.ceop.gov.uk



Tip of the Week

Joining an organization or network with similar goals can be a mutually-beneficial experience for both companies and individuals. Here's a look at one that might be of interest.

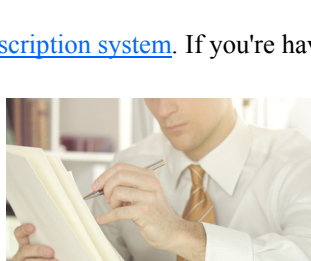
The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defenses against and responses to cyber attacks across the nation.

Joining the National Cyber Alert System can provide a number of services and benefits. Four products in the National Cyber Alert System offer a variety of information for users with varied technical expertise. Those with more technical interest can read the Technical Cyber Security Alerts or the Cyber Security Bulletins. Users looking for more general interest pieces can read the Cyber Security Alerts and Cyber Security Tips. All past issues of the following products are available:

- [Technical Cyber Security Alerts](#) provide timely information about current security issues, vulnerabilities and exploits.
- [Cyber Security Bulletins](#) provide weekly summaries of new vulnerabilities. Patch information is provided when available.
- [Cyber Security Alerts](#) provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate computer users can take to protect themselves from attack.
- [Cyber Security Tips](#) provide advice about common security issues for the general public.

A subscription to any or all of the National Cyber Alert System products ensures that you have access to timely information about security topics and threats.

To learn more or to subscribe, visit the [subscription system](#). If you're having trouble subscribing, read the [FAQ](#).



You'll be interested in this...

Carnegie Mellon Launches New Research Center to Grow Mobile Device Technologies and Services

Carnegie Mellon News (07/11/08) ; Swaney, Chris

The CyLab at Carnegie Mellon University recently launched the Mobility Research Center, which is dedicated to studying business, organizational, and technical issues surrounding mobility in managing systems in cell phones, home appliances, and building infrastructures. The new center will develop underlying technologies that will ensure privacy, security, and the reliability of sensitive and valuable information. CMU's Information Networking Institute has launched a new master's degree program in mobility to complement the new research center and to educate and train students. The ubiquity of handheld devices has made demand for new technologies to manage data and streamline connections extremely high, and the Mobility Research Center will focus on improving hardware and software technology for mobile devices, including studies on how people work, play, shop, and collaborate on mobile devices, and how new applications and services can change their lives, according to CyLab founding director Pradeep K. Khosla. Several mobile device manufacturers, including Motorola and Nokia, will work with the center. ([go to web site](#))

China Forms Anti-Phishing Alliance

People's Daily (China) (07/28/08)

In order to combat phishing activities employing .cn domain names and to maintain Internet safety, the Anti-phishing Alliance of China (APAC) was started on July 18. Its founding members include Chinese banks, securities firms, e-commerce businesses, CNNIC, .cn registrars, and scholars. CNNIC, .cn's registry, was named the APAC's secretary. CNNIC is allowed to accept reportings concerning phishing sites, to create phishing site identification, and to cease its DNS resolution after a phishing site utilizing a .cn domain name is uncovered. APAC is one of the first industry coalitions to combat phishing activities in China. Established by groups that are worried about the harm phishing causes, APAC will work to reduce this threat on the domain name level and to build a dependable Web space. APAC's efforts will first concentrate on phishing activities within groups that have close associations with public interest, such as securities firms, financial entities, e-commerce businesses, and Internet payment systems. Current APAC members include the Industrial and Commerce Bank of China, Milky Galaxy Securities, and .cn registrar HiChina ZhiCheng Technology. ([go to web site](#))

Games Bring Olympic-Sized Security Breaches

ITnews Australia (08/04/08)

Australian consumers reported losing over \$40,000 to a phony online Olympic ticketing scam. Most people who reported the fraud to an hotline launched by the New South Wales Trading Office said they were fooled by the U.S.-based site Beijingticketing.com, which is listed higher than the official Chinese site in a Google search. Security software vendor Symantec is advising consumers to be careful when accessing any Olympic-themed Web sites or emails. Symantec discovered the proliferation in Olympic-related scam attacks, in which a victim would get an email claiming that he or she has won an Olympic lottery and asking that he or she reply in order to redeem the gift. Symantec is also urging anyone traveling to Beijing to keep an eye on their computers, encrypt important information, update security software, and be careful when using internet cafes and kiosks, where entering any personal data could be risky. ([go to web site](#))

The Global Centre for Securing Cyberspace will provide a collaborative environment that will directly impact present and future criminality on the Internet. It's a cooperative centre concept dedicated to preventing, reducing and eliminating the criminal advantage of cyberspace. Bookmark www.gcsc.ca today!

Please email us if you have questions, special events, story ideas or experiences you would like to share. We hope you've enjoyed reading this webletter and we look forward to bringing you E-Telligence again soon.

If you wish to unsubscribe, please contact: kathy.macdonald@gcsc.ca