



2009 Event Calendar

- April 27-29, 2009
Critical Infrastructure and Security Risk Vulnerability Workshop
Vancouver, BC, Canada
[Click here](#)
- May 12-14, 2009
APWG Spring Counter-eCrime Operations Summit
Barcelona, Spain
[Click here](#)
- May 20, 2009
GeoSpatial Summit
Schenectady, NY, USA
[Click here](#)
- June 3-4, 2009
12th Annual New York State Cyber security Conference
Albany, NY, USA
[Click here](#)
- June 9-11, 2009
Kestenberg Siegal Lipkus LLP Anti-Counterfeiting Training Conference
Vancouver, BC Canada
[Click here](#)
- June 18-19, 2009
Tri-Lateral Security Conference
Calgary, AB, Canada
[Click here](#)
- July 10-12, 2009
Video Game Cultures and Future of Interactive Entertainment Conference
Mansfield College, Oxford, UK
[Click here](#)



HEADLINE NEWS — April 21, 2009

What's New on the Frontline!

Conference Supports Global Anti-Counterfeiting Efforts

By Kathy Macdonald

An annual conference in Vancouver, B.C., will highlight the newest and most innovative techniques to combat Internet counterfeiting and piracy as well as the latest products being counterfeited or pirated and the global efforts being taken to confront this epidemic. It's the 31st Kestenberg, Siegal, Lipkus LLP Anti-Counterfeiting Training Conference, to be held June 9-11, 2009.

Lorne Lipkus and his team have more than 20 years experience in the field of anti-counterfeiting including the serving of more than 8,000 Anton Piller Orders. In addition, they have coordinated numerous investigations and attended on behalf of their clients at several laws enforcement operations as a resource and/or witness. They regularly coordinate this training, which is free of charge to law enforcement across Canada.

Lorne is the chair of training and education for the Canadian Anti-Counterfeiting Network (CACN) and he is also the chair of the Canadian Intellectual Property Council. He remarked recently that, "we offer the most complete training tools available to deal with anti-counterfeiting cases. This includes educating investigators about copyright and trademark infringement. We offer ideas on what laws cover the incident and then we work in partnership with police and private investigators from the time of the first sighting of the suspected counterfeit products to preserving evidence for the search warrant, processing the evidence, advising on the charges and, then, presenting the evidence for trial."

Experts working in this field, on a daily basis, often attend the conference. They present on the socio-economic implications of the crime, the profile of the persons engaged in this crime and the modus operandi often associated with this kind of crime including organized crime, tax evaders, welfare fraudsters and trans-shipments criminals.

Along with the hundreds of counterfeit items they have on display, the conference offers an opportunity to network with law enforcement and others in numerous jurisdictions across Canada, the United States, Mexico and other locations globally. It is a very worthwhile event from the standpoint of networking education and cost. Check out the calendar in this webletter for the contact website.

Welcome to E-Telligence

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

UNDERSTANDING CYBERCRIME IN THE NEW AGE OF VIRTUAL CRIME

By Magda Marczak, M.A., Crime Analyst, Delta Police Criminal Intelligence
Part Two of Two



During the 2008 Canadian Law Enforcement Cyber Crime conference hosted in Toronto, Canadian law enforcement officials, along with the RCMP, launched a partnership with Microsoft to receive training on the latest technologies and threats in order to tackle cybercrime.

Previously, cybercrime training was not available to law enforcement because there were so few cybercrime investigators. In reality, law enforcement representatives are not trained in high tech computer crime, which makes it more challenging to keep up the evolution of cybercrime.

According to Det. Mark Fenton of the Internet Investigative Unit, Vancouver Police Department, cybercrime investigators are responsible for creating their own training courses, which ultimately interferes with the investigations. Although many municipalities have set up their own cybercrime unit (i.e., Vancouver Police Department, Calgary Police Service, Ottawa Police Service and many more), police officers continue to struggle with the investigations due to rapid technological advances.

According to RCMP Sgt. Marc Moreau, cell phone technology has been taken to the next level of sophistication in the past couple of years. About 10 to 15 years ago, cell phones did not have the current capabilities and were not as popular but, today, almost every investigation requires the seizure and analysis of cell phones by trained investigators and analysts.

Another challenge that law enforcement agencies are struggling with is the current legislation to obtain Part IV wiretaps. All organized crime groups are now using cell phones, Blackberries, and various other electronic devices. The current standards to obtain a Part IV wiretap are too onerous on the law enforcement agencies, thus making it challenging to be granted in court. The threshold to obtain a Part IV wiretap must be amended to aid law enforcement agents in their cybercrime and other investigations.

Given that there is so little research done on cybercrime in BC, Simon Fraser University is now developing a new cybercrime studies program. In July 2008, Simon Fraser University opened the new International Center for Cybercrime Research which is supported by both the Government of British Columbia and the Society for the Policing of Cyber Space (POLCYB). POLCYB is a not-for-profit society operating in BC since 1999. POLCYB operates on international levels and its objectives are "to enhance and develop global partnerships to prevent, detect, and combat cybercrime." In some ways, this approach is a response to Global Centre for Securing Cyberspace which was implemented in 2007. The GCSC facility will house international law enforcement agencies and computer experts. Its mandate is to help achieve cyberspace safety and security with the objective of finding new ways to prosecute cyber criminals.

Canadian Association of Police Board (CAPB) Survey Results

The 2008 CAPB survey was designed to shed light on the magnitude of the cybercrime problem in Canada. The survey was conducted by Deloitte LLP and was comprised of three components: an Ipsos Reid market research survey of 587 Canadians, an extensive interview process with 63 key contacts throughout law enforcement, prosecutions, government, academia, and an analysis of survey data.

The key findings of the survey suggest that:

- 70 percent of cybercrime victims do not report the crime as they are not sure who they should report to.
- 89 percent of the respondents believe that cybercrime prevention should be the governments and law enforcement agencies priority.
- 49 percent of the respondents have been victims of cybercrime which include: computer viruses, banking and personal information being lost or stolen through the Internet, children being bullied or sexually abused through online contact, identity theft, and interference with critical infrastructures such as power grids and phone services.
- 95 percent of the respondents believe that they are being targeted for cybercrime (identity theft, financial fraud, and computer viruses).

The CABP report offered numerous recommendations to address the continuous problem of cybercrime including the following:

- Establish a dedicated center where law enforcement, government, the private sector, and academia can co-ordinate the fight against cybercrime.
- Implement the proposed August 2002 legislation with respect to the lawful access provisions of the criminal code. Changes to the existing legislation that would enable information sharing with law enforcement with lower judicial standards than those now applied to search and seizure warrants.
- Implement new legislation making spamming an offence and adopt the recommendations made by the Spam Task Force 2005. According to Richard Simpson, the director general for the electronic branch of Industry Canada "Canada is currently the only G8 country without anti-spam legislation."
- Change the Canada Evidence Act that would improve on the existing Mutual Legal Assistance treaty's ability to enable the admission of documents held in the normal course of business in another country.
- Increase resourcing and funding for law enforcement and crown prosecutors related to cybercrime investigations and prosecutions.
- Create a central mechanism for the mandatory reporting of designated cyber security incidents to enable quantification of the potential damage to the Canadian economy.
- Implement mandatory reporting requirements for child pornography.
- Increase cybercrime awareness and prevention programs in school curriculums to educate children on the issues of cybercrime.

Cybercrime has become a serious threat to the economic integrity of Canada, especially during the current worldwide economic crisis.

Worldwide, law enforcement agencies are becoming more aware that organized groups are behind malicious attacks. These groups have learned that cybercrime generates high profits with a low risk of being caught.

Cybercrime is a challenge for law enforcement agencies since national coordination between the government, law enforcement, and the private sector is lacking.

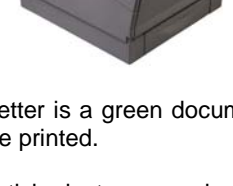
Websites You Should Visit

McAfee Threat Center
www.mcafee.com/us/threat_center/default.asp

Cyberbullying Course and Tips
<http://www.cyberbullying.ca/>

eBay Security Center
<http://pages.ebay.com/securitycenter/>

If you need to print...



The E-Telligence newsletter is a green document and is not designed to be printed.

If you wish to print an article, just copy and paste the information into a Word document and print in the normal manner. The environment thanks you!

Forum Review: Security on eBay and PayPal

By Kathy Macdonald, GCSC



Last week (April 9), Jack Christin, senior regulatory council for eBay, and Mike Rou, senior security investigator for PayPal, ventured to Calgary from San Jose, California, to speak to a packed room of 120 police and security professionals. GCSC was pleased to host this event and present a forum for Jack and Mike to talk about securing the people behind the more than 113 million listings posted on eBay worldwide.

eBay was founded in 1995 and has grown into a multi-billion-dollar company with 15,000 employees and a global reach. Currently, eBay sells \$2,000 worth of merchandise every second while PayPal transacts about \$2,056 in total payment volume every second. Both companies work in a symbiotic relationship based on eBay selling thousands of catalogued items and PayPal supporting the payments between buyers and sellers in 19 currencies around the world. PayPal's total payment volume for 2008 and the total value of transactions was \$60 billion dollars, up 27% over the previous year.

There are opportunities for crime on eBay and PayPal sites, mainly because criminals like to follow the money. Police, loss prevention and security professionals are regularly involved in investigations on both of these platforms. They examine everything from organized retail theft rings selling shoplifted razor blades and hot water tanks, to fraudsters selling non-existent antique vehicles or concert tickets to organized crime selling counterfeit designer goods and more. It is a tough job to keep up considering that at any given time, there are more than 113 million listings on eBay worldwide and approximately 7.9 million listings added each day.

Interestingly, eBay has had their share of weird items offered for sale. In fact, they have a section on the site called "Weird Stuff." Jack and Mike talked about items like the Virgin Mary grilled cheese sandwich, a 10-year-old frozen sandwich that sold for \$28,000 to an online casino. This item caused a stir at the company and 'VMGC' was an acronym used around the water cooler and in emails on a regular basis. Then, a young entrepreneur down on his luck started a bid of \$15,000 to sell his own will. To lure interested buyers, he posted a photograph of himself smoking cigarettes, trying to attract buyers by saying he had quite a smoking habit and didn't know how long he would live. The eBay lawyers were tested on this one and decided that wills could not be sold on eBay, neither could concepts, ideas or body parts or 58 other catalogue items including prescription drugs.

How does eBay keep track of all of these items and how do they ensure safety and security for its more than 86.3 active registered users worldwide? Jack and Mike talked candidly about security and the global effort and resources eBay and PayPal invests in security and working with law enforcement. eBay incorporates advanced search techniques, visualization and mapping programs and an ongoing law enforcement and security program to equip buyers, sellers, police, loss prevention and security professionals with knowledge, tools and contact numbers to create a proactive investigative process. eBay and PayPal work on a global basis and partner with many other organizations to help make an impact on crime. Jack and Mike are part of a global law enforcement team working to deter, investigate and educate others and their commitment to this effort is significant. To read more about the eBay Global Law Enforcement Operations Police Blotter visit http://pages.ebay.com/securitycenter/law_case_study.html

What You Need to Know to Report Cyberbullying

"Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others."

—Bill Belsey

To report cyberbullying, it's really important to save as much information as you can for investigative use. The more you have saved, the easier it will be to track down the people involved. Here's what to save or look for from emails:

- E-mail address
- Date and time received
- Copies of any relevant e-mails with full e-mail headers

From groups or social networking communities, save the following:

- URL of offending MSN group site
- Nickname of offending person
- E-mail address of offending person
- Date you saw it happen

Save the following from profiles you see on the web:

- URL of profile
- Nickname of offending person
- E-mail address of offending person
- Date you viewed this profile

Save the following from chatrooms:

- Date and time of chat
- Name and URL of chat room you were in
- Nickname of offending person
- E-mail address of offending person
- Screenshot of chatroom

If you receive e-mail from cyberbullies, you can report it to your ISP with the full headers displayed. The full header shows every stage of an e-mail's journey. Forwarding e-mail with the full header displayed will let the support team track down where it came from.

If somebody has stolen or "hacked" your account and changed all the login details, you will need to get in touch with a support team to get it back.

You don't have to put up with abuse in chat, and the companies that run chatrooms don't want abusive people using their service. To ignore the chatter, highlight the abuser's name and then use the ignore button to stop all conversation with that person. Then, take a screenshot of the abuse. Note the time, date and chatroom name. Report this information to the chatroom moderator and service operator.

If you are the victim of a cyberbully, speak to a parent or a teacher. Students should know that it isn't their fault that there are some very strange people in the world. Students should not be ashamed to tell somebody about any disturbing, threatening, weird or frightening behaviour they encounter. People aren't anonymous online and, with the right info saved, they can be traced by the police and dealt with.

Bill Belsey is the creator and facilitator of www.bullyingcourse.com, an innovative website that offers online courses and webinars (web-based seminars) about the issues of bullying and cyberbullying. For more information about Bullying.org, please visit: http://www.cyberbullying.ca/pdf/Bullying_org_Canada_Overview.pdf



» You'll Be Interested in This «

Jay Pushes for Security Against Cyber Terrorism

Charleston Gazette (WV) (04/15/09) ; Eyre, Eric

Sen. Jay Rockefeller (D-W.Va.) has introduced legislation to improve cybersecurity, which he said recently is "the No. 1 security threat to the safety of Americans." Under the legislation, known as the Cyber Security Act of 2009, a new Office of the National Cybersecurity Advisor would be created. The legislation calls for the office to report to the president on cybersecurity issues.

In addition, the legislation would provide financial assistance to those who want to pursue careers in cybersecurity, establish a system to license cyber terrorism professionals, and protect small and medium-sized businesses from cyber crimes. Finally, the legislation would create a panel that would monitor the program and review security risk management reports.

In his remarks Tuesday at a science and technology research forum in Charleston, W.Va., Rockefeller said it is important to take steps to protect the nation from cyber terrorists, who already have the ability to cripple the nation's banks, utilities, and other infrastructure systems. "They can pick whatever they want to do and shut it down," Rockefeller said. "They could bring America to a halt by shutting down the economy. When you're talking about cybersecurity, you're fighting an uphill battle."

[Click here](#)

Computer Attackers Target Popular Sites for Profit

Investors.com (04/14/09) P. A4 ; Howell, Donna

According to a study by the security vendor Symantec, the number of new types of malware rose 265 per cent between 2007 and 2008.

Many of these new types of malware are being used by hackers to break into legitimate websites through flaws in their underlying code. For example, the microblogging site Twitter was recently hit by a worm that took advantage of a cross-site scripting flaw to infect users' profile pages and send out short messages that contained a link to a competing site.

The antivirus firm F-Secure said that the motive of the attack was to steal Twitter users and get them to join the competing site, StalkDaily.com.

Other new types of malware are being used to commit fraud and theft, says Dean Turner with Symantec's global intelligence network unit. For instance, the Conficker worm displays pop-ups and warnings on infected computers to try to convince victims to pay \$49.95 for fake antivirus software. Meanwhile, cybercriminals are still using phishing attacks and data-theft Trojans in an effort to try to steal victims' online banking log-in information.

[Click here](#)

The Global Centre for Securing Cyberspace provides 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.org for our website.

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