

# COOP CONNECTION

EMI SIG Continuity of Operations Subcommittee Newsletter



## Leadership, Staff, Facilities, and Communications

### Cyber-Crime Threat Continues

**By Tonya Petty**  
**Emergency Manager**  
**Lawrence Berkley National Laboratory**

When most of us think of continuity, we think about vital records, essential personnel, and, of course, Mission Essential Functions. Rarely is cyber security our first *forethought*. When we think about crime, most of us think about robberies, assaults, and, all too often these days, active shooters. Rarely is cyber-crime the front contender.

Many questions come to mind when thinking about cyber-crime. What constitutes cyber-crime? How is a company aware it has been a victim of cyber-crime? How are monetary losses measured for cyber-crime? It is important that we define cyber-crime so that, as continuity planners, we can better understand the risks and potential losses. The consequences of cyber-crime affect individuals and businesses alike in the following areas:

- Loss of intellectual property and sensitive business information
- Theft of financial assets
- Lost opportunity costs
- Costs for securing networks
- Recovery costs from cyberattacks
- Reputational damage to the compromised company

The Department of Energy (DOE) has been the victim of cyber-crime incidents in May of 2011, February of 2013, and July of 2013, during which, personally identifying information (PII) was compromised. Approximately 104,000 past and

#### INSIDE THIS ISSUE

Cyber-Crime Threat Continues	1
Want to Contribute to COOP Connection?	3
COOP Subcommittee Conference Calls	3
Upcoming Conferences	4
Petty Receives Award at EMI SIG Annual Meeting	4
Did You Know?	4

present federal employees' PII was leaked out in the July 2013 incident. The latest breach occurred through the Office of Personnel Management (OPM), jeopardizing the financial information of some 4 million employees.

Cyber-crime that steals someone's PII and identity for financial gain also results in an emotional cost that is not as easy to quantify. In 2013, 13.1 million people were victims of identity fraud in the United States. In fact, every two seconds, someone in America becomes the victim of identity theft, according to Javelin Strategy and Research. Recovery costs from cyberattacks associated with lost work time for victims of identity theft amounted to \$274 million.

Aside from cyber-crime on individual PII, businesses must be concerned with other information that is subject to theft and the resulting costs. When business sensitive information is hacked, the costs may not result in an emotional toll but can result in heavy implications and major damages to national economies. When cyber-crime targets businesses, the result is damage to trade, competitiveness, innovation, and global economic growth.

All companies face the risk of loss of intellectual property (IP) and confidential business information, but this is especially true for organizations in the finance, chemical, aerospace, energy, defense, and



## Cyber-Crime (continued)

Information Technology (IT) sectors. Cyber-crime is particularly damaging for organizations conducting research resulting in intellectual property (IP), which is the most costly and detrimental loss from cyber-crime. IP theft is a central problem for the information economy, costing U.S. companies \$200 to \$250 billion annually according to the U.S. Department of Commerce. The Organization for Economic Development (OECD) estimated that counterfeiting and piracy costs companies as much as \$638 billion per year. Hacking to steal IP is an outgrowth of two larger problems—the vulnerable nature of the Internet and weak protections for IP in many countries. Putting the two together creates a global problem. IP is a major source of competitive advantage for companies and for countries. The loss of IP means fewer jobs and fewer high-paying jobs in victim countries.

Valuing IP is an art form, based on estimating the future revenue IP will produce or the value that the market places on IP, which are not always the same. The actual value of IP can be quite different from the research and development costs incurred in creating it. When hackers take a company's product plans, research results, and customer lists, the company may not even realize that it has suffered loss.

The effect of cyber-crime discourages innovation globally. It reduces the ability of companies to gain the full return from their inventions causing them to turn to other activities to make a profit. The impact of IP theft is not only to shift returns away from innovators, but also to reduce the overall rate of innovation. Given the nature of IP, the damage can be almost invisible, or the consequences can be delayed due to a lag time between when IP is taken and when a competing product appears. Unlike the theft of a physical product, the company that created the IP is not prevented from making use of it after it has been taken; therefore, it cannot identify, let alone estimate, its losses.

In 2014, the United States lost an estimated 200,000 American jobs due to cyber-crime. This does not account for those individuals who are forced out of high-paying jobs and then take jobs at lower pay rates, which is common. While translating cyber-crime losses directly into job losses is not easy, the employment effect is important to the equation of risk and loss.

Most cyber-crime goes unreported. Few of the biggest cybercriminals have been caught or, in many cases, even identified. Still, monetary losses caused by cyber-crime are high, requiring significant costs for prevention and mitigation and immeasurable costs for recovery, especially when the company's reputation suffers.

Businesses' recovery costs for the customer information breach of retail chain Target in 2013 were as high as \$420 million. This recovery effort included reimbursement, the cost of reissuing millions of cards, legal fees, and credit monitoring for millions of customers. Companies also experience reduced valuation after they have been hacked, which can significantly impact stock prices anywhere between 1% and 5%. Although the decline is not permanent, it takes a quarter or two for the business to recover.

Sometimes hackers engage in cyber-crime only for the purpose of causing damage, rather than stealing money. Cybercriminals use Internet attacks to disrupt the provision of a key service. In 2012, criminals permanently erased the data from 30,000 computers at a large oil producer and launched similarly disruptive attacks against South Korean banks and media outlets. These companies and their customers experienced harm that went beyond the cost of cleanup and repair. The threat of service disruption can be part of an extortion scheme or a plot to debilitate critical infrastructure or attack a business.

The response to cyber-crime is a business decision. Companies and individuals make decisions on how to manage the potential for loss from cyber-crime by deciding how much risk they are willing to accept and how much they are willing to spend to reduce that risk. The problem with this is that if companies are unaware of their losses or underestimate their vulnerability, they will underestimate risk.

## Cyber-Crime (continued)

Cyber-crime is a problem that spans from the individual level to a global scale. The incentives in cyber-crime are classic in that they encourage attack and discourage defense. Cyber-crime produces high returns at low risk and (relatively) low cost for the hackers. Some work needs to be done at the federal level. For example, an international agreement on a standard definition of cyber-crime would improve the ability to collect consistent data. That said, even a broad definition leaves out important nonmonetary effects on innovation, national defense, and the long-term competitiveness of both countries and companies. Work by governments to improve the collection of data on the cost of cyber-crime would also make a valuable contribution to the ability to more accurately identify risk, which allows for investment and policy in cyber-crime prevention.

Studies estimate that the Internet economy annually generates between \$2 trillion and \$3 trillion, a share of the global economy that is expected to grow rapidly. McAfee estimates cyber-crime extracts between 15% and 20% of the value created by the Internet. The lack of data means that any dollar amount for the global cost of cyber-crime is an estimate based on incomplete data.

As continuity planners, we rely on strong planning, preparedness, and mitigation from IT Departments/Divisions. It is important to work with IT organizations to expand the cyber hazard to ensure effective response and recovery capabilities exist for cyber-crime among our national labs.

## References:

“A New Identity Fraud Victim Every Two Seconds.” Javelin Strategy and Research Feb. 2014. Web.

## COOP Subcommittee Conference Calls

COOP Subcommittee conference calls typically occur on the second Thursday of each month from 3-4 p.m., Eastern.

The schedule for the next four calls is below.

- October 8, 2015
- November 12, 2015
- December 10, 2015
- January 14, 2016

Agendas are sent prior to each call. If you have questions about the COOP Subcommittee conference calls, please contact Becky Bullard at [Becky.Bullard@orau.org](mailto:Becky.Bullard@orau.org) or (865) 576-9623.

## Want to Contribute to COOP Connection?

If you'd like to contribute continuity stories, calendar items, or any other news related to COOP, please send them to Becky Bullard at [Becky.Bullard@orau.org](mailto:Becky.Bullard@orau.org) or to Jeff Morrison at [morrisjl@nv.doe.gov](mailto:morrisjl@nv.doe.gov).

The deadline for submissions for the January issue is December 4, 2015.

<http://www.csoonline.com/article/2133875/malware-cyber-crime/u-s--dept--of-energy-reports-second-security-breach.html>

<http://www.federaltimes.com/story/government/cybersecurity/2015/06/05/opm-data-breach-for-you/28534883/>

## Upcoming Conferences

### [Continuity Insights](#)

Wyndham New Yorker Hotel  
New York, NY  
October 20-21, 2015

### [2015 IAEM Annual Conference](#)

63<sup>rd</sup> IAEM-USA Annual Conference & EMEX  
Clark County, Nevada  
November 13-18, 2015

## Petty Receives Award at EMI SIG Annual Meeting

Tonya Petty, COOPSC Co-Chair, Lawrence Berkeley National Laboratory, received the EMI SIG Excellence in Emergency Management Award for outstanding contribution to the emergency management profession, which includes providing valuable services to the EMI SIG, sharing useful information with EMI SIG members, and making presentations at EMI SIG meetings.



Robert Gee presents Tonya Petty of Lawrence Berkeley National Laboratory with the Excellence in Emergency Management Award.

## Did You Know?

Emergency responders now have a new tool available for their hazardous materials toolbox. [AskRail, a free phone app, provides hazardous materials information on rail-cars](#), enabling responders to quickly access important data which can affect planning and response. It is important to note that all North American Class 1 railroads use this app. It is available in the United States, Canada, and Mexico, and will be part of standard Class 1 training first responders receive. Users can:

- Enter a railcar ID to see whether the car is carrying a hazardous material;
- Look up reference materials, such as the Emergency Response Guidebook;
- Look up rail companies' emergency contact information;
- View contents of entire train.

For security reasons, AskRail is available only to qualified emergency responders. This includes those who have completed certain training as well as those who work in areas along rail routes. Interested users must review the criteria and contact the appropriate company to request access.