

## INVITATION TO PROFESSIONAL DEVELOPMENT SYMPOSIUM ON CYBER INSURANCE



Cyber insurance is no longer debatable for small to medium-size business owners and CFOs. The steady increase in data breaches and cybercrime, extortion attempts, and emerging threats make cyber insurance important. Standard general liability policies are not intended to cover these types of losses. Your company's financial health and reputation could be on the line-and you can't transfer responsibility.

Join us for an informative symposium moderated by risk management expert Austin Morris Jr. that will address questions such as:

- What is new in the cyber liability marketplace
- Facts you should know
- How to protect your company's financial health and reputation
- How to save money with favorable underwriting

The event features panelists **Holly L. Meyers, RN, FACHE**, Senior Vice President, Quality and Risk Management for St. Joseph Health System (SJHS) in Bryan, TX (which recently experienced a [major data breach](#)) and Beazley Group cyber insurance underwriter and expert, **Nick Economidis**.

**Date:** Wednesday, June 25, 2014

**Time:** 12:00 - 1:30 p.m.

**Location:**

The Auerbach and Berger Families Cyber Security Laboratory  
3401 Market Street, Suite 300, Philadelphia, PA

*Note:* This is a brown bag event-attendees are encouraged to bring their own lunch.

**RSVP online at:** <http://cci.drexel.edu/events/RSVP.aspx?id=432626>

**For any questions, please contact Norm Balchunas at** [DUcyberPI@drexel.edu](mailto:DUcyberPI@drexel.edu)

**About the Moderator:**

Austin Morris Jr. is the founder of Morris Risk Management LLC. MRM provides sophisticated products from leading insurers and advanced risk management solutions to businesses and nonprofits dependent on information and technology and/or producing information and technology. Security and privacy (cyber liability) insurance and technology errors & omissions insurance are our specialties. Morris Risk Management combines diverse professional experience in software, the Internet, media, technology, e-commerce, mobile, cybersecurity, and insurance. For more information, please visit [www.morrisrisk.com](http://www.morrisrisk.com).

## UPCOMING INSTITUTE EVENTS

### Affiliates Meeting of the Drexel Cybersecurity Institute

The Affiliates Meeting of the Drexel Cybersecurity Institute scheduled for June 18 has been postponed for a later date. As a result, there is more time for you to share how your expertise and interests align with the mission of the Cybersecurity Institute.

The names and interests of affiliated faculty will be featured on the Drexel Cybersecurity Institute website and these faculty will be invited to participate in the first affiliates meeting of the Institute. The meeting will focus on the creation of a strategic plan for the Institute complete with education, research and service goals and metrics.

**Date:** TBD

**Location:**

The Auerbach and Berger Families Cyber Security Laboratory  
3401 Market Street, Suite 300, Philadelphia, PA

For more information and to express your interest in affiliating with the Institute contact Norm Balchunas at [DUcyberPI@drexel.edu](mailto:DUcyberPI@drexel.edu)

## CYBERSECURITY SNIPPET: A Multi-National Effort to Disrupt the Gameover Zeus Botnet

### Background

The Gameover Zeus Botnet is a world-wide network of infected computers used by cyber criminals to steal personal and financial information. This Botnet operation has resulted in the loss of over \$100 million. The estimated number of compromised computers ranges from 500,000 to 1 million computers. Consumers are not even aware that their computers are compromised and that their computers are being used as part of the Botnet operation.

Additionally, part of this Botnet operation includes the use of ransomware which consists of cyber criminals encrypting consumers' files and then demanding payment from consumers to decrypt the files.



### Collaborative Effort to Disrupt the Botnet Operation

The effort to disrupt the Gameover Zeus Botnet consists of a multi-organization and multi-national effort. The collaborative efforts involved legal, technical, and law enforcement experts from government agencies and industry partners spanning more than 10 countries. The U.S. Department of Justice lead the collaborative efforts and has been helping consumers regain control of their compromised computers.

### Additional Information

U.S. Leads Action Against Gameover Zeus Botnet  
U.S. CERT Information on Gameover Zeus Malware

**Norm Balchunas, Col., USAF (Ret.)**  
Interim Director,  
Drexel University Cybersecurity Institute  
[njb67@drexel.edu](mailto:njb67@drexel.edu)

<http://cci.drexel.edu/cybersecurity>

\*If you wish to unsubscribe from this newsletter, please reply directly to the email.