THE FUTURE OF CYBER SECURITY RISK?
WAKE UP, YOU'RE THERE!

Session 5106 | Tuesday, Sept 26 11am

- Rachelle Loyear, CISM, MBCP, PMP
- Tim McCreight, CPP, CISSP, CISA
- John Petruzzi, CPP, CISM, CBCP
RESTRICTED
UNDER 17 REQUIRES ACCOMPANYING PARENT OR ADULT GUARDIAN

The following seminar contains coarse language, violent situations, personal opinions, and partial speaker nudity.

Viewer discretion is advised.
WELCOME TO THE FUTURE...

ARTIFICIAL INTELLIGENCE: THE FUTURE OF BUSINESS

How artificial intelligence and robotics will amplify people, products, and business.

MACHINE LEARNING

Data mining

Artificial intelligence

Statistics

Prediction

Analysis

INTERNET OF THINGS

Connected City

REMOTE HOME CONTROL

ECO MODE

22°C

NORMAL

OFF

securityexpo.org
Welcome to the future…

HBO Hackers Demand Ransom After Leaking 'GoT' Stars' Phone Numbers

TL;DR
DC security robot quits job by drowning itself in a fountain

The trouble with smart homes

Toyota joins forces with Intel and five other companies to develop a self-driving car 'ecosystem'

Cyberterrorism: A look into the future
WAKE UP CALL #1
YES, YOU ARE A TARGET

There is no industry that hackers won’t target as long as they have something to gain from it. And any personally identifiable information has some value to someone on the Dark Web, whether it will be used for identity theft purposes, for an advanced targeted attack or for something else. Cyber criminals work tirelessly to breach systems in a variety of verticals, and it shows. In 2015, the Identity Theft Resource Center tallied over 760 data breaches, amounting to the exposure of more than 169 million records.

Health care
Depending on the source, or the manner in which a study was conducted, there will be some variation in what comes out as the most highly targeted industry. Regardless of minor discrepancies, health care will always fall toward the top of the list, if not at the top of the list. According to Trend Micro’s comprehensive analysis of data breaches that took place between 2005 and 2015, health care came out ahead, representing the most highly targeted industry for data breaches. Given the recent flurry of reports of health care breaches, this isn’t necessarily surprising.

Education
Interestingly, number two on Trend Micro’s list of most-brecked industries was education. In this case, educational records were the sought-after loot, especially at the college and university levels. Trend Micro notes that many educational records contain personally identifiable information including contact information, Social Security numbers, and more.
WAKE UP CALL #2
YES, YOU ARE ALREADY COMPROMISED

Assume your network has been hacked, says Cisco

Howard Solomon @howarditwc
Published: January 16th, 2014

Why it seems like everyone's being hacked

German and US leaders aren't the only ones worried about hacking. The past fortnight has seen several countries, companies and celebrities affected by data breaches. And the hackers have picked some unusual targets.

US: North Korea's been hacking everyone since 2009

The state-sanctioned attacks reportedly include the WannaCry ransomware.
WAKE UP CALL #3
NO, YOU CANNOT KEEP THEM OUT

You Can’t Keep the Crooks Off Your Network, So Now What?

Adair Lashinsky
Jan 22, 2017

Good morning.

Due to late nights and early mornings, I’m going to save my wrap-up from Cannes for one more day and point you instead to the new cover story in Fortune, entitled simply, “Hacked.” It’s a package comprising an overview of the state of play for corporations in defending themselves against cybercriminals as well as an intriguing look by Robert Hackett at Google’s (GOOGL, $GOOGL) cyber bounty hunting project.
NOW WHAT?

Tactical Response

- Educate Your Users
- Implement Tactical Response Program
- Harden Critical Protections

Enterprise Security Risk Management (ESRM)

- Continual Awareness and Monitoring
- Mitigate Intolerable Risks
- Educate Business Leaders
- Identify Critical Assets
WHAT IS ESRM?

- ESRM is a cyclical, iterative approach to managing all security risk across an enterprise using established risk-management principles.

WHAT ESRM IS NOT...

- ESRM is not “convergence”. A converged security team integrates traditional and IT related security functions under one command structure. The degree of integration identifies the degree of convergence.

- ESRM is not Enterprise Risk Management (ERM). ERM is a program to manage all company risks, which may also include security risks. ESRM is a management philosophy that uses similar risk principles to manage security risks.

* From the forthcoming book: *Enterprise Security Risk Management: Concepts and Applications*
HOW DOES ESRM PREPARE YOU FOR THE FUTURE OF CYBER RISK?

• Executives understand the current state of risk
• Continual scanning keeps you thinking ahead
• Focus on “The Family Jewels”
• Planning = Preparedness
HOW DO YOU GET THERE?

- ESRM is a journey that will not occur overnight. An iterative improvement model for ESRM focuses on first embracing the ideas of ESRM and rolling the approach into the security approach from ad hoc to optimized over time.
HOW CAN ASIS HELP?

- Coming Soon... ESRM Tool / Application
HOW CAN ASIS HELP?

• Coming Soon... ESRM Tool / Application
CONTACTS

- Rachelle Loyear
  - rachelle.loyear@usa.g4s.com
- Tim McCreight
  - tim.mccreight@hitachi-systems-security.com
- John Petruzzi
  - john.petruzzi@usa.g4s.com