

Cybersecurity Update



John Haller

Information and Infrastructure Security Analyst - CERT® Division

John Haller is an information and infrastructure security analyst with the Resilient Enterprise Management team in the CERT Program at the Software Engineering Institute, Carnegie Mellon University.

Prior to joining CERT, John served as a Special Agent for the United States Postal Service Office of the Inspector General. John also worked for the U.S. Postal Inspection Service, researching online criminal behavior, conducting internet-based investigations, and supporting the development of information systems-based products internationally.

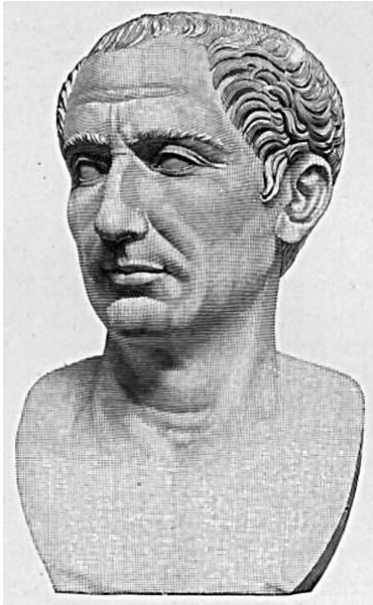
A U.S. Army veteran, John is a member of the Pennsylvania bar. He obtained his J.D. and Master of Public and International Affairs from the University of Pittsburgh.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 23 JAN 2014	2. REPORT TYPE	3. DATES COVERED 00-00-2014 to 00-00-2014			
4. TITLE AND SUBTITLE Cybersecurity Update		5a. CONTRACT NUMBER			
		5b. GRANT NUMBER			
		5c. PROGRAM ELEMENT NUMBER			
6. AUTHOR(S)		5d. PROJECT NUMBER			
		5e. TASK NUMBER			
		5f. WORK UNIT NUMBER			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213		8. PERFORMING ORGANIZATION REPORT NUMBER			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)			
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)			
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified	Same as Report (SAR)	38	



Julius Caesar
(100-44 BC)

“... If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out ...”

Suetonius, *Life of Julius Caesar* 56

“... When I started my career, in the late 80s, if there was a bank robbery, the pool of suspects was limited to the people who were in the vicinity at the time. Now when a bank is robbed the pool of suspects is limited to the number of people in the world with access to a \$500 laptop and an Internet connection...”

Shawn Henry, former FBI Executive Assistant Director

How has cybersecurity changed over the last five years?

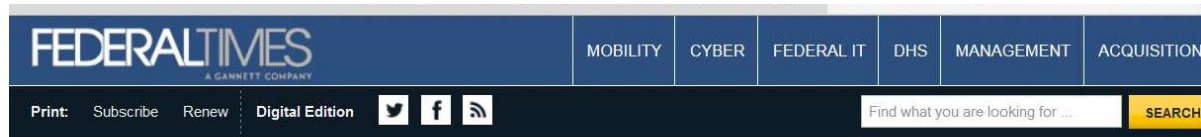
A few thoughts . . .

- I. Nation-State Involvement
- II. Complexity and Importance of External Entities
- III. Greater Dependency Every Day
- IV. Increasing Cooperation (?)



Nation-State Involvement

The involvement of governments in cybersecurity – both from a defensive and an offensive perspective – has become much more apparent.



Close look awaits NIST cybersecurity framework due next month

Jan. 15, 2014 - 06:00AM | By SEAN REILLY | Comments



The defense industrial base is among the critical infrastructure identified by the Obama administration as needing better protection from cyber threats. (Lockheed Martin)

An advertisement for a free webcast. The text reads: 'Learn How Advanced Search Can Work for the DoD Enterprise', 'FREE WEBCAST', 'On-Demand Viewing', 'CLICK HERE', 'BROUGHT TO YOU BY', 'ISR NETWORKS', and 'PRESENTED BY Google'. The background features a stylized globe and data visualization elements.

More Headlines

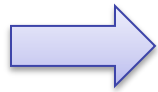
DHS awards work under \$6B cyber contract
Jan. 16, 2014



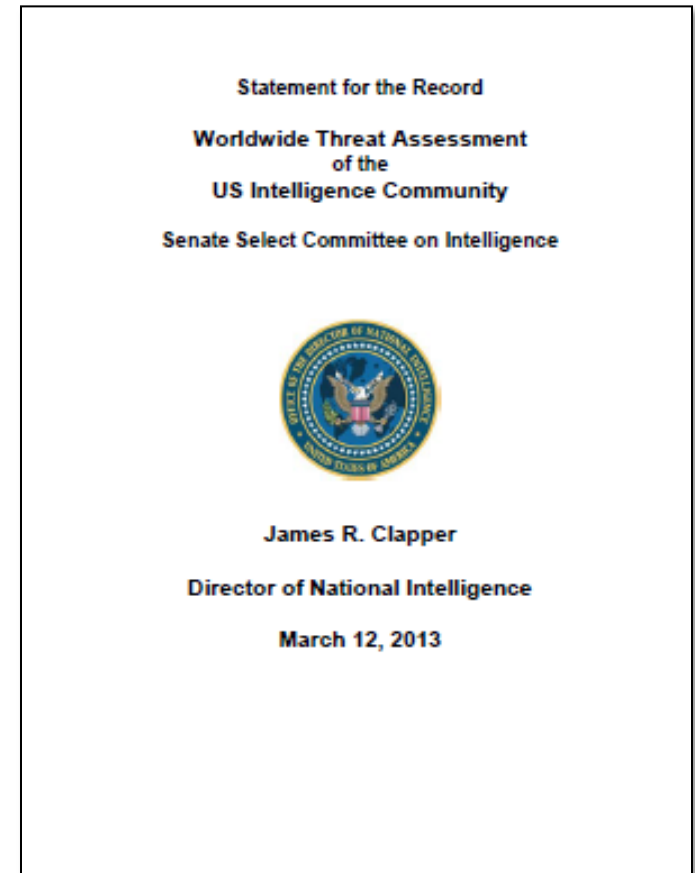
2014 spending bill funds continuous monitoring program
Jan. 14, 2014

Director of National Intelligence – March 12, 2013

U.S. Intelligence Community Worldwide Threat Categories



1. **Cyber**
2. Terrorism & transnational organized crime
3. WMD proliferation
4. Counterintelligence
5. Counterspace
6. Insecurity and competition for natural resources
7. Health and pandemic threats
8. Mass atrocities



January 31, 2013

Thursday, January 31, 2013 As of 8:28 PM EST

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Community

Home | World | U.S. | New York | **Business** | Tech | Markets | Market Data | Opinion

MEDIA & MARKETING | Updated January 31, 2013, 8:28 p.m. ET

Chinese Hackers Hit U.S. Media

Wall Street Journal, New York Times Are Breached in Campaign That Stretches Back Several Years

By SIOBHAN GORMAN, DEVLIN BARRETT and DANNY YADRON

WASHINGTON—Chinese hackers believed to have government links have been conducting wide-ranging electronic surveillance of media companies including The Wall Street Journal, apparently to spy on reporters covering China and other issues, people familiar with the incidents said.

Journal publisher Dow Jones & Co. said Thursday that the paper's computer systems had been infiltrated by Chinese hackers, apparently to monitor its China coverage.

[New York Times Co.](#) NYT +0.11% disclosed Wednesday that the newspaper also had been the victim of cyberespionage.

THE WALL STREET JOURNAL.
WSJ

The New York Times

May 23, 2013

THE WALL STREET JOURNAL

U.S. EDITION ▾ Thursday, May 23, 2013 As of 7:52 PM EDT

U.S. NEWS | Updated May 23, 2013, 7:52 p.m. ET

Iran Hacks Energy Firms, U.S. Says

Oil-and-Gas, Power Companies' Control Systems Believed to Be Infiltrated; Fear of Sabotage Potential

By SIOBHAN GORMAN and DANNY YADRON

WASHINGTON—Iranian-backed hackers have escalated a campaign of cyberassaults against U.S. corporations by launching infiltration and surveillance missions against the computer networks running energy companies, according to current and former U.S. officials.



In the latest operations, the Iranian hackers were able to gain access to control-system software that could allow them to manipulate oil or gas pipelines. They proceeded "far enough to worry people," one former official said.

But are the laws changing as needed?

Condé Nast
Traveler GOLD LIST 2014
THE WORLD'S BEST PLACES TO STAY! SEE THE 2014 GOLD LIST

SUBSCRIBE NOW!
6 MONTHS FOR \$5
Renew | Give a Gift | International

THREAT LEVEL | hacks and cracks | cybersecurity

FOLLOW THREAT LEVEL



AT&T Hacker 'Weev' Sentenced to 3.5 Years in Prison

BY KIM ZETTER 03.18.13 11:57 AM

Follow @KimZetter

Share 1,244
Tweet 194
+1 39
Pinterest



Photo: Jim Merithew/Wired.com

[Redacted]

Follow

We could all go to jail for security research at any moment, and a jury would happily convict us.

11:11 AM - 18 Mar 2013

231 RETWEETS 48 FAVORITES

Complexity and the Importance of External Entities

The protection and sustainment of assets that your organization relies on . . .

- ❑ People
- ❑ Information
- ❑ Technology
- ❑ Facilities

increasingly depends on contracted and arms-length relationships.

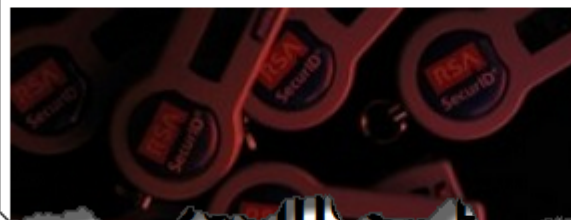
March 2011

The Washington Post Politics Opinions Local Sports National World Business Tech

Posted at 04:46 PM ET, 07/26/2011

Cyber attack on RSA cost EMC \$66 million

By [Hayley Tsukayama](#)



In its [earnings call Tuesday](#), EMC disclosed that it spent \$66 million in its second quarter to deal with a cyber attack that compromised its RSA Security division.

The New York Times

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS

Data Breach at Security Firm Linked to Attack on Lockheed

By [CHRISTOPHER DREW](#) and [JOHN MARKOFF](#)

Published: May 27, 2011

[Lockheed Martin](#), the nation's largest military contractor, has battled disruptions in its computer networks this week that might be tied to a hacking attack on a vendor that supplies coded security tokens to millions of users, security officials said on Friday.

RECO

TWITT

LINKED

Yesterday it would have looked like ...

Principles and Practice of Modern Information Security

It would have
been all about
IT and technical
controls.

A tutorial delivered at the
ACM SIGSOFT 2000 Eight International Symposium on the Foundation of Software Engineering
November 6-10, 2000, San Diego, California, USA

Jeremy

Advanced Techno
Lockheed Martin Sy
1801 Rou
Owego, N
Phone: 607-
Fax: 607-7
Email: jeremy.imt

Table of Contents

1. Preliminaries
2. Introduction to Modern Information Security
3. TCP/IP and Network Services Refresher
4. Firewalls
5. Cryptography
6. Public Key Infrastructure (PKI)
7. Smart Cards and other Mobile/Portable Security Devices
8. Virtual Private Networks (VPN)
9. Authentication
10. Intrusion Detection
11. Information Security Aspects of Software Application Development
12. Terminology/Acronyms/Glossary
13. Bibliography/References

Today it has to be about ...

Sample definition of Information Assurance:

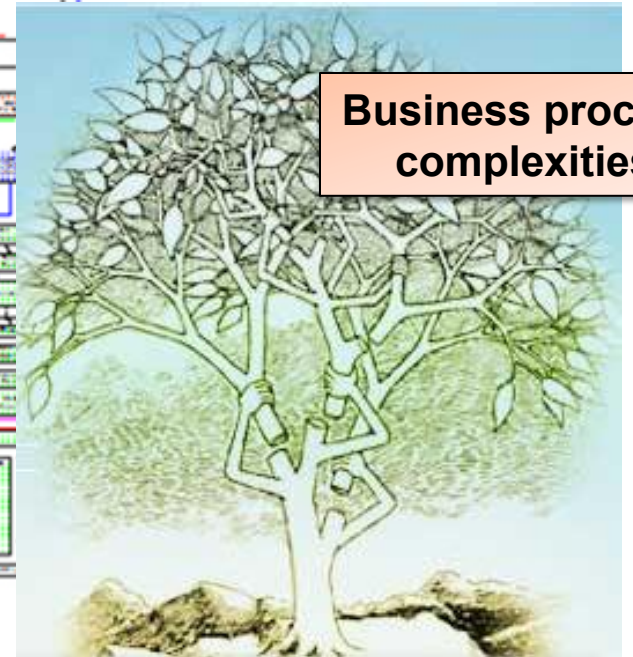
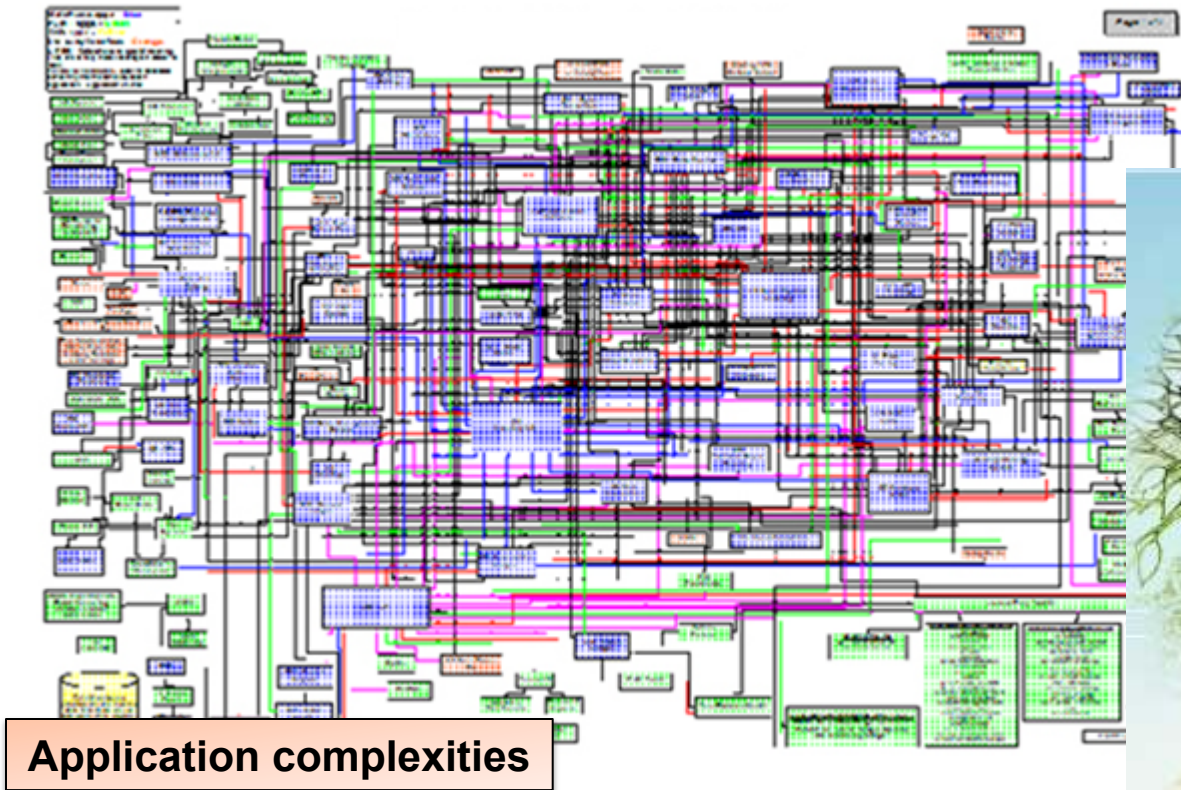
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Sample definition of Information Assurance:

Information assurance is related to the field of information security, in that it is primarily concerned with the protection of information systems and their contents. Generally considered the more broadly-focused of these two fields, IA consists more of the strategic risk management of information systems rather than the creation and application of security controls. In addition to defending against malicious hackers and code (e.g., viruses), IA practitioners consider corporate governance issues such as privacy, regulatory and standards compliance, auditing, business continuity, and disaster recovery as they relate to information systems. Further, while information security draws primarily from computer science, IA is an interdisciplinary field requiring expertise in accounting, fraud examination, forensic science, management science, systems engineering, security engineering, and criminology, in addition to

and more ...

Today it has to deal with ...



and more ...

Managing the Supply Chain for ICT Services



We realize new business opportunities, flexibility, and cost savings by outsourcing services . . .

. . . but how do we manage the *right relationships* and *mitigate the resulting risks* in a reliable way *over time*?

Greater Dependency Every Day

CYBER

We are in a major transformation because our critical infrastructures, economy, personal lives, and even basic understanding of—and interaction with—the world are becoming more intertwined with digital technologies and the internet. In some cases, the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks.

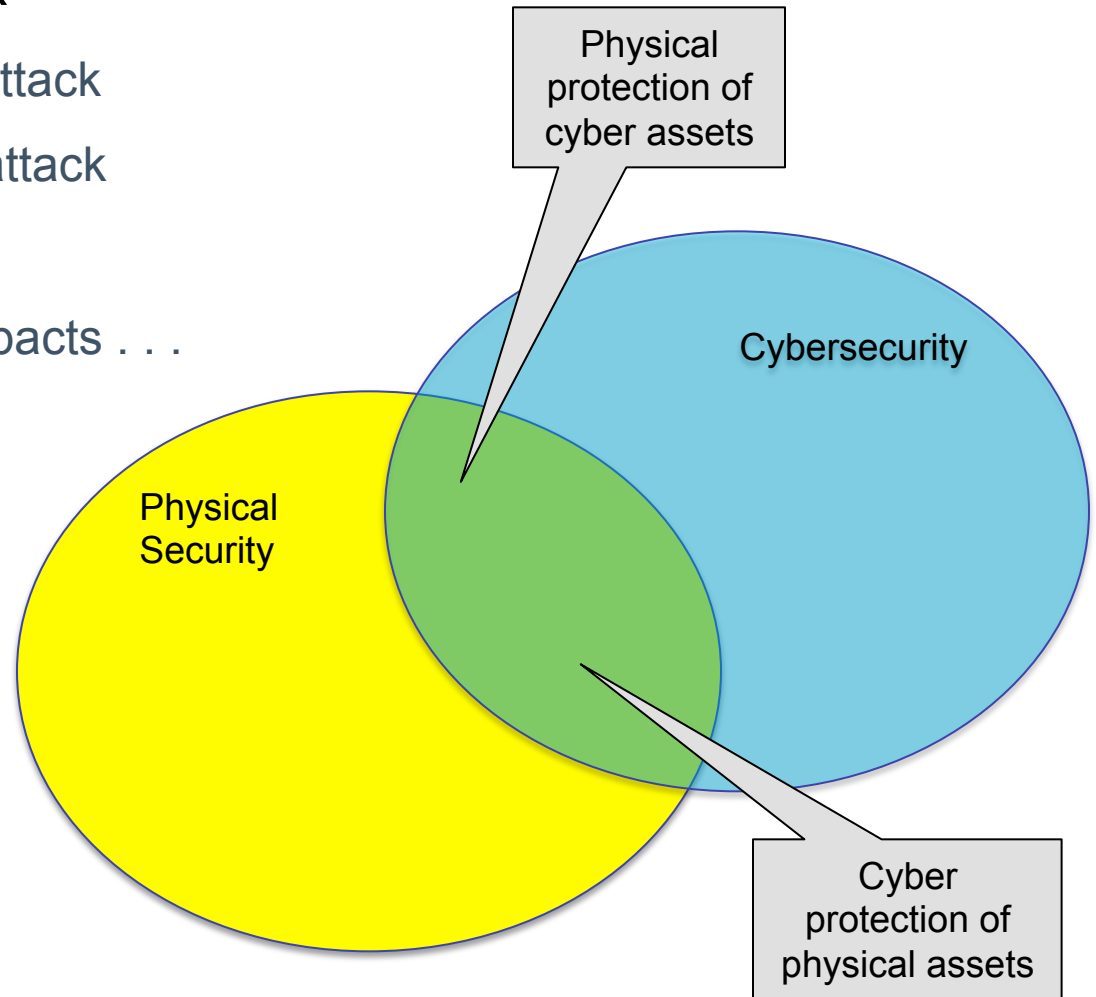
—James Clapper, Director of National Intelligence,
March 2013

Intertwining of Physical and Cyber Domains

Not only new modes of attack

- Physical-enabled cyber attack
- Cyber-enabled physical attack

But also *less predictable* impacts . . .



April 23, 2013

THE WALL STREET JOURNAL.

U.S. EDITION

Home World U.S. New York Business Tech Markets Market Data Opinion Life & Culture Real Estate Management

TECHNOLOGY | April 23, 2013, 2:19 p.m. ET

False AP Twitter Message Sparks Stock-Market Selloff

By SHIRA OVIDE

The Associated Press said Tuesday its Twitter account was compromised, resulting in a false message on the service that explosions in the White House had injured President [Barack Obama](#). The message briefly sparked selloff on U.S. stock markets.

"The Twitter account has been hacked," the AP said in a statement Tuesday. A tweet about an attack on the White House is false."

Other Twitter accounts associated with Associated Press were quick to correct the false Twitter message, which was posted just after 1 p.m. Eastern time. Afterward, the news organization's main Twitter account was suspended.



Software Engineering Institute

Carnegie Mellon University

CERT® Operational Resilience:
Manage, Protect, and Sustain

Twitter #CERTopRES

© 2013 Carnegie Mellon University

Reuters News Site Hacked

Article

Comments (7)

By SHALINI RAMACHANDRAN

Thomson Reuters Corp. said Friday that its blogging platform for Reuters News was hacked, resulting in multiple false posts to its website, including a fake interview with Syrian rebel army leader.

"Reuters did not carry out such an interview and the posting has been deleted," the international news service posted Friday on Twitter.

Reuters didn't release any details about who was responsible for the attack. "We are working to address the problem," a spokeswoman said in a statement.

According to Reuters, a false blog post attributed to one of its reporters, contained a interview with the Free Syrian Army leader Riad al-Asaad, saying that his forces were going to retreat from Aleppo, a northern Syrian province, after encountering the Syrian army. For months, the Free Syrian Army has been fighting the Syrian government for control of the country.

Reuters said the Free Syrian Army released a statement saying that the interview never took place and blamed Syrian President Bashar al-Assad's government for the false posts. Reuters said its journalists were alerted about the Syrian news site on Friday.



REUTERS

August 3 & 5, 2012



REUTERS

EDITION: U.S.

Regis

Reuters Twitter account hacked, false tweets about Syria sent

[Recommend](#) 74 recommendations. [Sign Up](#) to see what your friends recommend.

Sun Aug 5, 2012 8:19pm EDT

(Reuters) - Reuters News said one of its Twitter accounts was hacked on Sunday and false tweets were posted, mainly related to the current armed struggle in Syria.

"Earlier today @ReutersTech was hacked and changed to @ReutersME," said a spokesperson for Reuters, which is owned by Thomson Reuters CorpTO>. "The account has been suspended and is currently under investigation."

The incident follows the company's disclosure that the blogging platform of the Reuters News website was compromised on Friday and a false posting purporting to carry an interview with a Syrian rebel leader was illegally posted on a Reuters' journalist's blog.

In the latest incident a series of 22 false tweets were sent purporting to be from Reuters News. Some of the tweets also carried false reports about Syrian rebel losses suffered in battles with Syrian government forces.

The Reuters website had no immediate comment on the tweets.

[Tweet](#) 542

[Share](#)

[Share this](#)

[+1](#) 3

[Email](#)

[Print](#)

Related News

[Syrian leader Assad's plans pound vital p Aleppo](#)
Sat, Aug 4 2012

[Syrian army on rebels in Al Damascus](#)
Fri, Aug 3 2012

[Reuters blog](#)



Software Engineering Institute

Carnegie Mellon University

CERT® Operational Resilience:
Manage, Protect, and Sustain
[Twitter #CERTopRES](#)

© 2013 Carnegie Mellon University

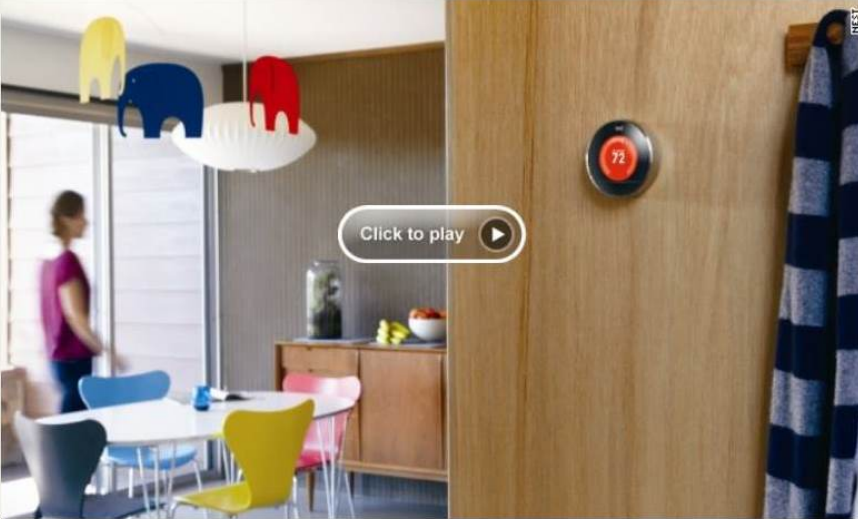
New Applications

Google's smart contact lens: what it does how it works



Video: Google is working on a smart contact lens prototype that monitors glucose levels in tears. The technology could end finger pricks for diabetics. It still needs to be tested and proved accurate and safe to win FDA approval.

By Hayley Tsukayama, Friday, January 17, 10:13 AM [E-mail the writer](#)



Google buys Nest Labs for \$3.2 billion

January 14th, 2014
09:32 AM ET

Google Steps into Home Appliances Trade

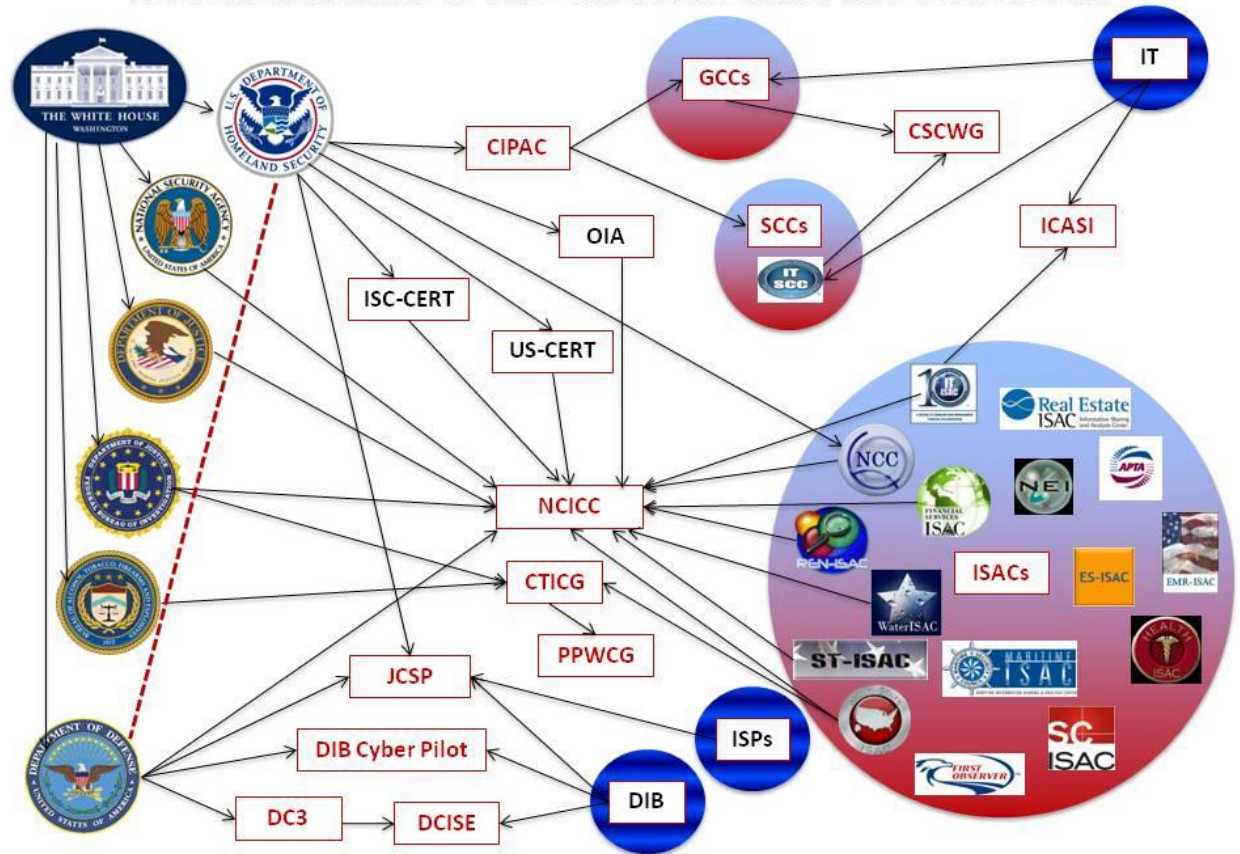
Google is making another big bet on hardware, CNN's [Christine Romans](#) reports.

The search giant announced Monday that it's buying connected device maker Nest Labs for \$3.2 billion in cash.

Cooperation (and Information Sharing)

Is it getting better?

KEY INSTITUTIONS IN THE CYBERSECURITY PPP LANDSCAPE



Financial Sector Attacks, Late 2012

DDOS attacks targeted major banks and financial institutions.

Website disruptions:

- Wells Fargo
- PNC
- USBank
- Bank of America
- JP Morgan Chase
- Citigroup
- Others



Public-Private Partnership in Action

DHS, NSA, and FBI provided on-request support to organizations that were attacked.

DHS has improved its capability to aid the attacked organizations:

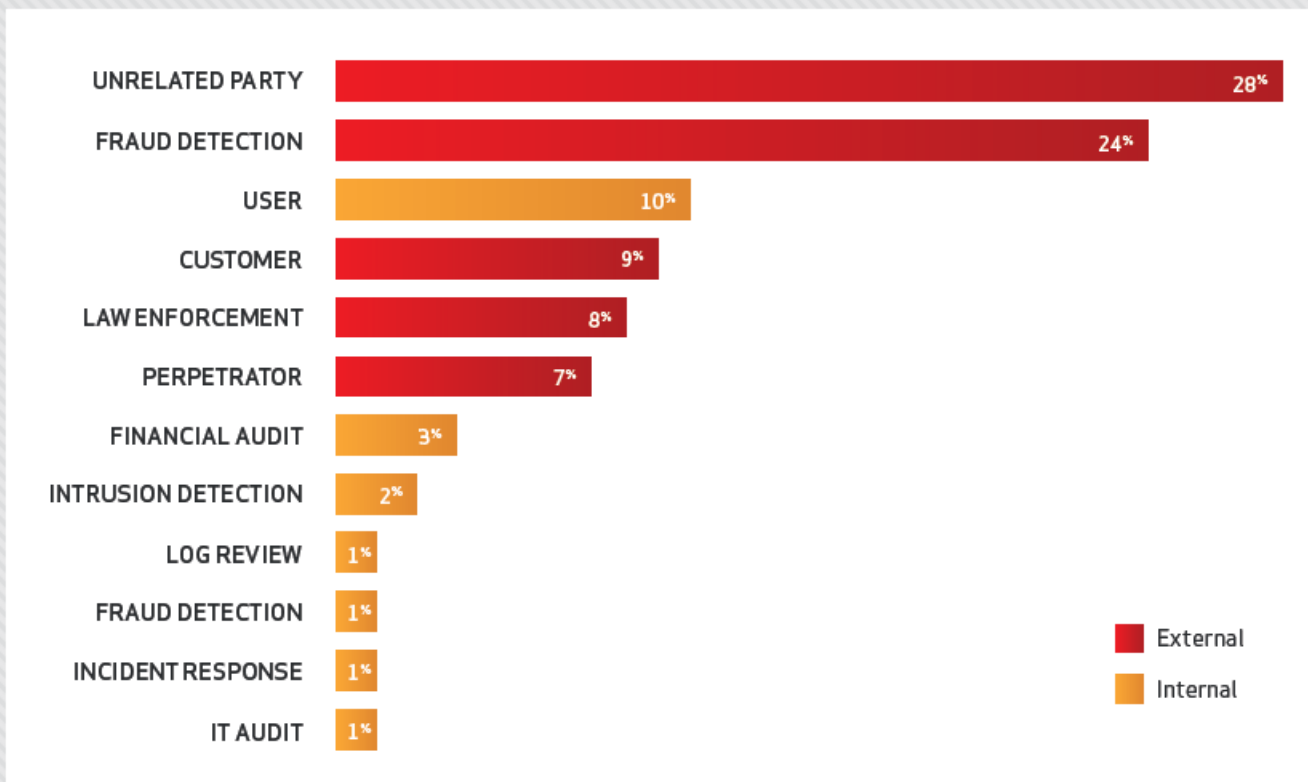
- Information gathering, analysis, and sharing
- Recommendations for mitigations
- Clarification of contact points

“A year ago, quite frankly, the capability was not there. We did not have the capacity to collaborate nearly as effectively as we do now. I won't say that it has become almost pro forma, but it's become a lot more routine for how we do this now than it was just a few months ago.”

—Mark Weatherford, DHS Deputy Undersecretary for Cybersecurity, January 2013

A Practical Case for Situational Awareness

Figure 6: Who identifies data breaches

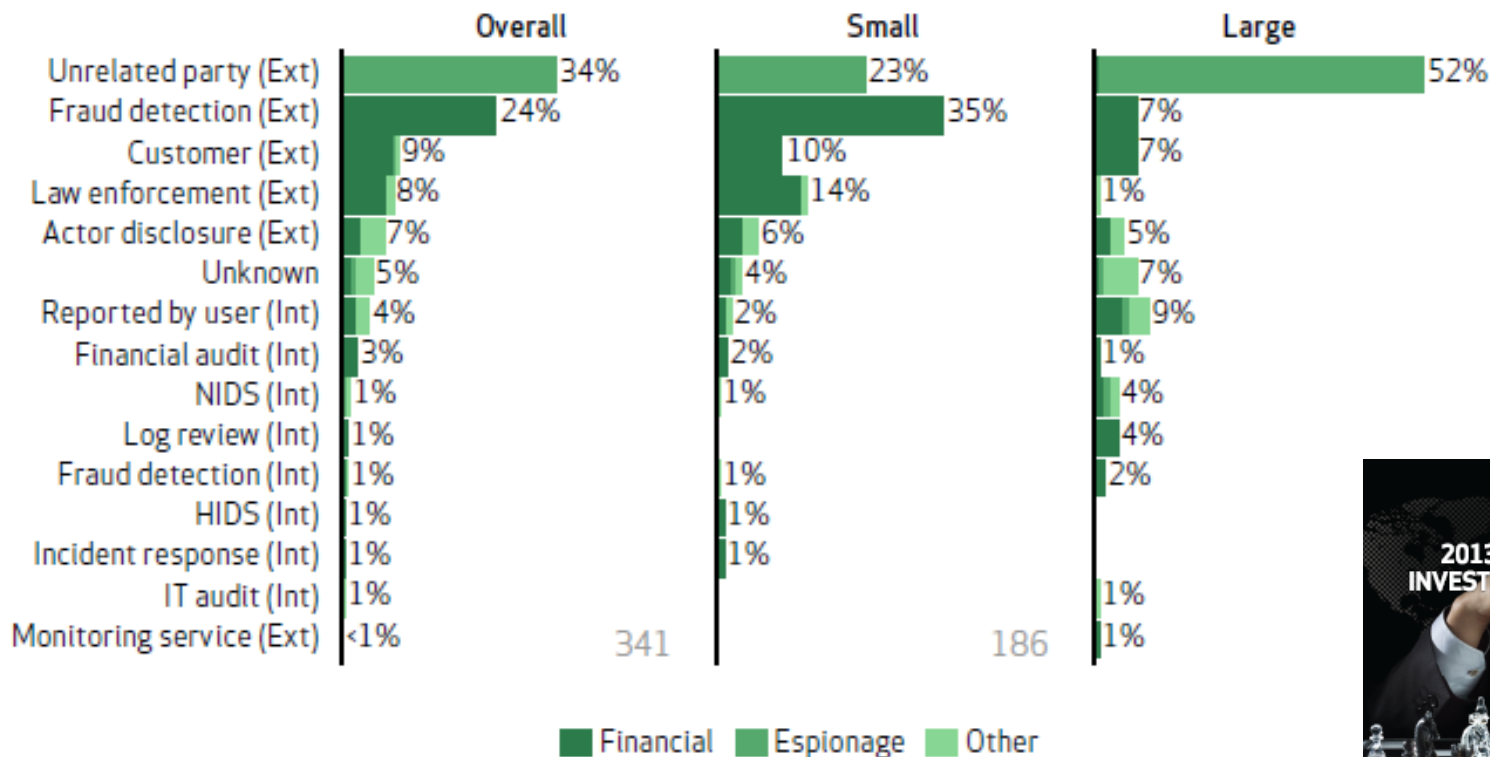


Many organizations devote a disproportionate amount of time and money to detection methods that fall below the 1% mark.



Discovery Methods vs. Size

Figure 44: Discovery methods



Recent News


USA TODAY
A GANNETT COMPANY

NEWS SPORTS LIFE **MONEY** TECH TRAVEL OPINION 47° SUBSCRIBE

JPMorgan CEO: Target breach is a wake-up call

Ken Sweet , The Associated Press 2:11 p.m. EST January 14, 2014

64 54 7



(Photo: Manuel Balce Ceneta, AP)

SHARE f 64 TWEET 54 COMMENT 7 EMAIL MORE

NEW YORK (AP) — More Target-sized security breaches will happen if banks and retail stores don't start working together to further protect customers' data, JPMorgan Chase's CEO Jamie Dimon said Tuesday.

JPMorgan has replaced 2 million credit and debit cards as a result of the Target breach, Dimon said. That number is expected to rise. JPMorgan is the world's largest issuer of credit cards.

Dimon expects that cybercrimes such as the Target breach will become more common if retailers and banks do not work on security, he said.

"This story is not over, unfortunately," Dimon said in a conference call with investors following the bank's fourth-quarter earnings announcement.

In December, Target said 40 million credit and debit card accounts — including customers' card numbers, expiration dates, debit-card PINs and the embedded code on the magnetic strip on the back of cards— were stolen in a data breach that happened between Nov. 27 and Dec. 15. Last week, the company disclosed that hackers stole an additional trove of data affecting 70 million people. That data included names and phone numbers as well as email and mailing addresses. The

3 Bureau Credit Score (FREE)
View Your Latest Credit Scores From All 3 Bureaus in 60 Seconds For \$0
CLICK HERE!
FreeScore360.com

LOOKING FOR A JOB?

Keywords

Location

Select Job Category

Find Jobs

How can a resilience view help?

Continuity of Operation
(COOP)

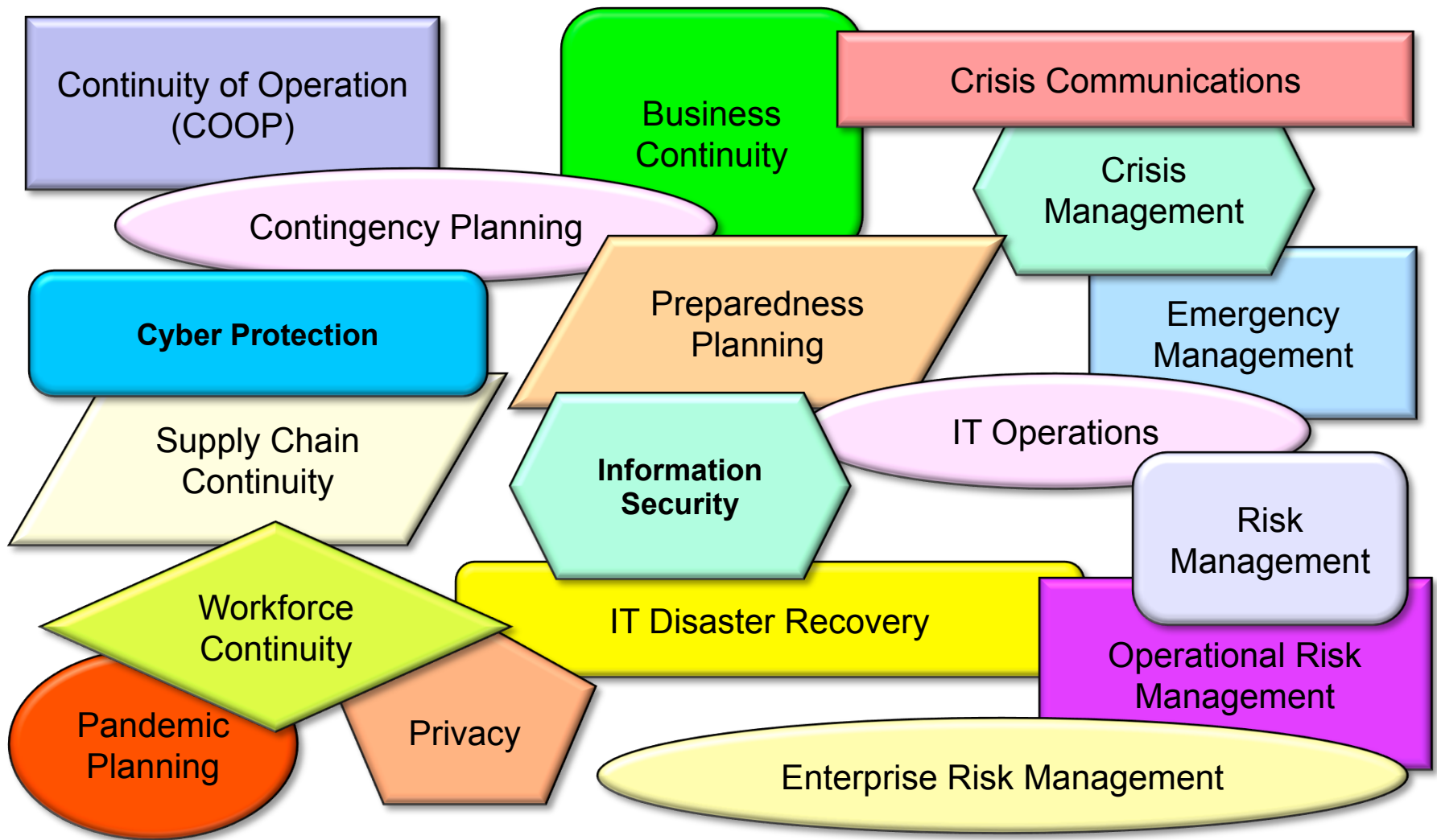
Business
Continuity

Emergency
Management

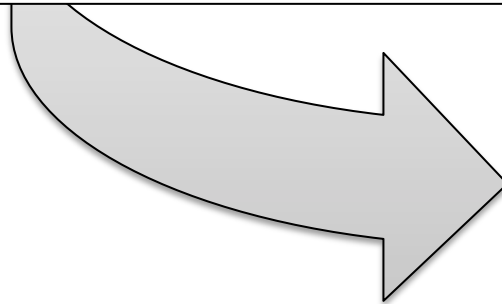
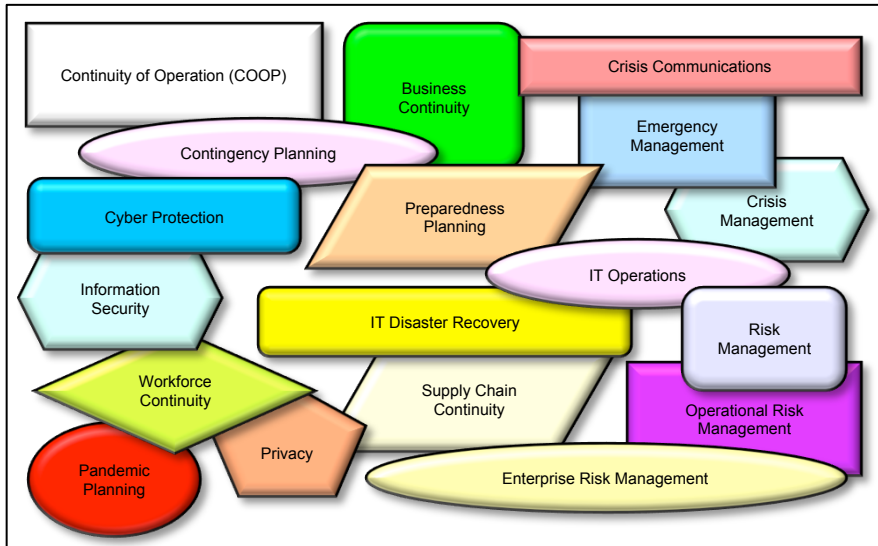
*Yesterday's Preparedness
Planning*

IT Disaster Recovery

Today's Preparedness Planning



Desired Direction



In Closing

Organizations are faced with an ever growing list of cyber security demands and complexities for a variety of reasons:

- Complex business relationships and economic pressures
- Legal uncertainty and jurisdictional issues
- Incident impacts and consequences that are difficult to predict
- . . . among many others

A system to engineer and manage enterprise cyber security activities can help.

“The oak fought the wind and was broken,
the willow bent when it must and survived.”

Robert Jordan, *The Fires of Heaven*

Q&A

SEI Training



Introduction to the CERT Resilience Management Model

February 18 - 20, 2014 (SEI, Arlington, VA)

June 17 - 19, 2014 (SEI, Pittsburgh, PA)

See Materials Widget for course document



Software Engineering Institute

Carnegie Mellon University

CERT® Operational Resilience:
Manage, Protect, and Sustain

Twitter [#CERTopRES](#)

© 2013 Carnegie Mellon University

References

1. Nader Mehravari, "Resilience Management," a course module in the CISO Executive Education and Certification Program, Heinz College, Carnegie Mellon University, 2013, <http://www.heinz.cmu.edu/school-of-information-systems-and-management/chief-information-security-officer-executive-education-and-certification-program/index.aspx>
2. Joshua Corman, "Managing Operational Threat," a presentation delivered in the CISO Executive Education and Certification Program, Heinz College, Carnegie Mellon University, March 7, 2013, <http://www.heinz.cmu.edu/school-of-information-systems-and-management/chief-information-security-officer-executive-education-and-certification-program/index.aspx>
3. Nader Mehravari, "Achieving Organizational Mission Through Resilience Management," A Discussion with CERT Experts: Constructing a Secure Cyber Future, Part of SEI Webinar Series, April 30, 2013, <https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=583853&sessionid=1&key=5E4796946B6897C34F544ADD1D1E1641&sourcepage=register>
4. Rich Pethia, "20+ Years of Cyber (in)Security," A Discussion with CERT Experts: Constructing a Secure Cyber Future, Part of SEI Webinar Series, April 30, 2013, <https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=583853&sessionid=1&key=5E4796946B6897C34F544ADD1D1E1641&sourcepage=register>
5. John Seabrook, "Network Insecurity," *The New Yorker*, May 20, 2013, pp. 64-70.
6. Lisa Daniel, "DOD Needs Industry's Help to Catch Cyber Attacks, Commander Says," American Forces Press Services, March 27, 2012, <http://www.defense.gov/news/newsarticle.aspx?id=67713>
7. Emil Protalinski, "NSA: Cybercrime Is the Greatest Transfer of Wealth in History," ZDNet, July 10, 2012, <http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598/>
8. Caralli, Richard A.; Allen, Julia H.; White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011.

References

9. “Introduction to the CERT Resilience Management Model,” Software Engineering Institute Training, <http://www.sei.cmu.edu/training/p66.cfm>
10. R.H. Zakon, “Hobbes' Internet Timeline 10.2,” <http://www.zakon.org/robert/internet/timeline/>
11. ISC Internet Host Count History, <http://www.isc.org/solutions/survey/history>
12. Verisign, “The Domain Name Industry Brief,” http://www.verisigninc.com/en_US/why-verisign/research-trends/domain-name-industry-brief/
13. Netcraft Web Server Survey, <http://news.netcraft.com/archives/category/web-server-survey/>
14. Facebook statistics, <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22>
15. ARPANET Maps, <http://som.csudh.edu/cis/lpress/history/arpamaps/> and http://mappa.mundi.net/maps/maps_001/map_0699.html
16. Joshua Corman and David Etue, “Adversary ROI: Evaluating Security from the Threat Actor’s Perspective,” RSA US Conference, 2012, <http://www.slideshare.net/DavidEtue/adversary-roi-evaluating-security-from-the-threat-actors-perspective>
17. Joshua Corman, “A Replaceability Continuum,” Cognitive Dissidents Joshua Corman Blog, October 24, 2011, <http://blog.cognitivedissidents.com/2011/10/24/a-replaceability-continuum/>
18. Verizon Security Blog, <http://www.verizonenterprise.com/security/blog/>
19. Andrew Wells, Earl Perkins, and Juergen Weiss, “Definition: Cybersecurity,” Gartner Report G00252816, June 7, 2013.
20. Lawrence Pingree and Neil MacDonald, “Best Practices for Mitigating Advanced Persistent Threats,” Gartner Report G00224682, January 18, 2012, IEEE Spectrum, February 2013.

References

21. James Clapper, "Worldwide Threat Assessment of US Intelligence Community," statement delivered to Senate Select Committee on Intelligence, March 12, 2013.
22. U.S. Government Accountability Office (GAO), "Cybersecurity – Threats Impacting the Nation," April 24, 2012.
23. Gary Stoneburner, "Toward a Unified Security/Safety Model," *Computer*, August 2006.
24. Ron Ross, "Managing Enterprise Security Risk with NIST Standards," *Computer*, August 2007.
25. Doug MacDonald, Samuel L. Clements, Scott W. Patrick, Casey Perkins, George Muller, Mary J. Lancaster, Will Hutton, "Cyber/Physical Security Vulnerability Assessment Integration," Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES, February 24-27, 2013.
26. U.S. Department of Homeland Security, "National Preparedness Report," March 30, 2013.
27. U.S. Department of Defense, "Resilient Military Systems and the Advanced Cyber Threats," DoD Defense Science Board Task Force Report, January 2013.
28. Verizon, "2013 Data Breach Investigations Report."
29. Earl Perkins, "The Impact of Critical Infrastructure Protection Standards on Security," Gartner Report G00230036, March 12, 2013.
30. U.S. Government Accountability Office (GAO), "High-Risk Series – An Update," February 2013.
31. Bradford Willke, "Securing the Nation's Critical Cyber Infrastructure," U.S. Department of Homeland Security, Paril 14, 2010.
32. David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, February 2013.
33. Roger G. Johnston, "Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities," *Journal of Physical Security* 4(2), pp. 30-34, 2010.

References

34. Steve Piper, *Definitive Guide to Next-Generation Threat Protection*, Cyberedge Press, ISBN: 978-0-9888233-0-3, 2013.
35. Siobhan Gorman, "Should Companies Be Required to Meet Certain Minimum Cybersecurity Protections?" *Wall Street Journal*, May 10, 2013.
36. "FireEye Advanced Threat Reportt – 2H 2012," FireEye, <http://www2.fireeye.com/rs/fireeye/images/fireeye-advanced-threat-report-2h2012.pdf>
37. Ponemon Institute, "2012 Cost of Cyber Crime Study," October 2012, http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf
38. Neil McDonald, "Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence," Gartner Report G00252476, May 30, 2013.

Notices

Copyright 2013 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013 and 252.227-7013 Alternate I.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon®, CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM-0000506



Software Engineering Institute

Carnegie Mellon University

CERT® Operational Resilience:
Manage, Protect, and Sustain

Twitter #CERTopRES

© 2013 Carnegie Mellon University