

Thomas J. Schlagel

Chief Information Officer, BNL



- PhD in Nuclear Physics from the University of Illinois at Urbana-Champaign in 1990
- Joined BNL in 1990 as a Postdoctoral Associate in the Nuclear Theory Program
- Moved to the Computing & Communications Division (CCD) in 1994, supporting a wide range of information technology and management activities
- Held IT roles at Jupiter Media Metrix and NSLIJ from 2000 – 2003
- Returned to BNL in 2003 as Director, Information Technology Division
- In 2010, took on the new role of Chief Information Officer – senior manager accountable for cyber protections
- Resident of Setauket since 1996

The Cybersecurity Challenge

*Presented to the Community Advisory Committee
May 9, 2013*

*Thomas J Schlagel
Chief Information Officer*





The Information Technology Division runs the systems that keep the lab running


- Annual budget of \$36M and 150 employees, responsible for:
 - Communications systems – voice and data networks, video/teleconferencing, email, collaboration services
 - Research Library
 - Business systems to support HR, Finance, Procurement, Facilities, ES&H
 - Centralized Service Desk for Customer Support
 - Cyber security protections against external and internal threats





IT extends into every part of the scientific discovery process

- Control systems that monitor the power/cooling infrastructure
- Computerized controls of the systems that run the
- accelerators – magnets, cryogenics, beam steering
- Online data acquisition systems that monitor and collect
- data from experiments
- High performance computing facilities to store and
- process experimental data
- Supercomputing resources to test theories and run simulations

- 
- An aerial photograph showing a large, circular building under construction in a campus setting. The building has a prominent circular structure with a central area and several radial paths leading to the outer edge. The surrounding area includes various campus buildings, parking lots, and green spaces. The image is used as a background for a list of bullet points.
- 20 Gbps connectivity to the Internet
 - > 10,000 devices
 - Close to 0.8 Petaflops (1,000 billion floating point operations per second) of BlueGene compute cycles
 - Fundamental science research with 1000's of worldwide collaborators
 - Proprietary research – for example, energy research



bnl.gov

Eight Charged With Debit Card Cyber-Crime Targeting Banks

By Christie Smythe - May 9, 2013 1:52 PM ET



0 COMMENTS

+ QUEUE



Eight [New York](#) residents were charged in what U.S. prosecutors said was a \$45 million global debit card cyber-attack scheme targeting banks based in the United Arab Emirates and Oman.

The defendants are accused in a four-count indictment unsealed today in federal court in [Brooklyn](#), New York, of participating in two worldwide attacks. They used stolen account information for prepaid MasterCard-branded [debit cards](#) to withdraw millions of dollars from ATM machines from October 2012 to April 2013, prosecutors said.

The targeted banks were [National Bank of Ras Al-Khaimah PSC](#), based in the United Arab Emirates, and Bank Muscat SAOG, Oman's biggest bank by assets, according to the U.S. Attorney's Office in Brooklyn.

Members of the scheme hacked into credit card processors to steal the card data and eliminate withdrawal limits, prosecutors said. They took out cash in coordinated efforts "reminiscent of the casino heist in Ocean's 11," Brooklyn U.S. Attorney Loretta Lynch said today in a news conference.

AP Twitter hack causes panic on Wall Street and sends Dow plunging

Market recovers after hackers tweeted from the official AP feed that two explosions had hit the White House

Heidi Moore in New York and Dan Roberts in Washington
guardian.co.uk, Tuesday 23 April 2013 15.41 EDT

 Jump to comments (62)



The panic, however brief, demonstrates how tightly intertwined Wall Street has become with Twitter. Photograph: Spencer Platt/Getty Images

Wall Street collided with [social media](#) on Tuesday, when a false tweet from a trusted news organization sent the US stock market into freefall.

The 143-point fall in the [Dow Jones](#) industrial average came after hackers sent a message from the Twitter feed of the [Associated Press](#), saying the White House had been hit by two explosions and that Barack Obama was injured. The fake tweet, which was immediately corrected by Associated Press employees, caused a sensation on Twitter and in the stock market.

Department of Labor website reportedly compromised to target nuclear weapons workers

By Dieter Bohn on May 3, 2013 10:24 pm [Email](#) [@backlon](#)

DON'T MISS ANY STORIES *FOLLOW THE VERGE*

[Like](#)

118k

[Follow](#)

216K followers



[71](#)

[Like](#)

134

[Tweet](#)

13

[+1](#)

6

[Share](#)

Two computer security software firms are reporting that a US Department of Labor website was compromised with malware designed to target employees in the Department of Energy — likely nuclear researchers. [According to Invincea](#), a zero-day exploit targeting Internet Explorer 8 was discovered on the DoL's "Site Exposure Matrix Database," a site meant to provide information on the health risks associated with exposure to radioactive materials. That site contained a redirect which secretly installed malware that could communicate with a remote server, according to [Alien Vault](#).

The strategy of using a website your intended targets are likely to visit is known as a "watering hole," and you may recall that a [similar tactic was used to target Apple, Facebook, and Twitter developers](#). With this current hack, the method used to communicate with the command-and-control server "matches with a backdoor used by a known chinese [sic] actor called DeepPanda," Alien Vault's Jaime Blasco writes, but just because the technique matches up doesn't necessarily mean that the hackers in this case are the same group.

THE LATEST HE



to watch'



LATEST MEDIA



RSA hacked, data exposed that could 'reduce the effectiveness' of SecurID tokens

By Tim Stevens posted Mar 18th, 2011 at 8:49 AM



If you've ever wondered whether two-factor authentication systems actually boost security, things that spit out pseudorandom numbers you have to enter in addition to a password, the answer is yes, yes they do. But, their effectiveness is of course dependent on the security of the systems that actually generate those funny numbers, and as of this morning those are looking a little less reliable. [RSA](#), the security division of [EMC](#) and producer of the [SecurID](#) systems used by countless corporations (and the Department of Defense), has been hacked. Yesterday it sent out messages to its clients and posted an open letter stating that it's been the victim of an "advanced" attack that "resulted in certain information being extracted from RSA's systems" -- information "specifically related to RSA's SecurID two-factor authentication products."

Yeah, yikes. The company assures that the system hasn't been *totally* compromised, but the information retrieved "could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack." RSA is recommending its customers beef up security in other ways, including a suggestion that RSA's customers "enforce strong password and pin policies." Of course, if security admins wanted to rely on those they wouldn't have made everyone carry around SecurID tokens in the first place.

FEATURED STORIES

MAY 7, 2013

3D Systems will turn your Star Trek figure for \$70, faces-on (video)

MAY 7, 2013

Vivo Xplay boasts 5.7-in screen, dedicated audio nifty single-hand mode with video)

MAY 7, 2013

Sony VAIO Fit 15 review Sony's mainstream not a makeover

MAY 6, 2013

Fitbit Flex review

MAY 4, 2013

Eyes-on with Cornell Un laser tag dunebots (video)

MAY 4, 2013

Eyes-on: University of Pennsylvania's TitanArm exoskeleton (video)

MAY 3, 2013

PlayJam's Jasper Smith

Topics ▾

News

In Depth

Reviews

Blogs ▾

Opinion

Share

Security

Application Security | **Cybercrime and Hacking** | Cyberwarfare | Data Security

Malware and Vulnerabilities | Mobile Security | Privacy

[Home](#) > [Security](#) > [Cybercrime and Hacking](#)

News

Oak Ridge National Lab shuts down Internet, email after cyberattack

DOE laboratory says it was victim of an Advanced Persistent Threat designed to steal technical data

By Jaikumar Vijayan

April 19, 2011 06:30 PM ET [3 Comments](#)[in](#) Share [Twitter](#) [+1](#) [StumbleUpon](#) [Reddit](#) [Facebook Like](#) 106 [Email](#) [More](#)

Computerworld - The Oak Ridge National Laboratory, home to one of the world's most [powerful supercomputers](#), has been forced to shut down its email systems and all Internet access for employees since late last Friday, following a sophisticated cyberattack.

The restrictions on Internet access will remain in place until those investigating the attack know for sure that it has been completely contained, said Barbara Penland, ORNL's director of communications.

The lab is expected to restore external email service sometime on Wednesday, however no attachments will be allowed for the time being.

Penland said several other national laboratories and government organizations were targeted in the same attacks, which appear to have been launched earlier this month.

Data breaches

[Systems manager arrested for hacking former employer's network](#)

[Dutch bill would give police hacking powers](#)

The measures at Oak Ridge were implemented late on Friday night after initial investigations showed that those behind the attacks were attempting to steal technical data from lab's systems and send it to an external system, Penland said.



ANNUAL REPORT TO CONGRESS

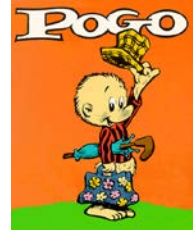
Military and Security Developments
Involving the People's Republic of China 2013

Office of the Secretary of Defense

Preparation of this report cost the Department of Defense a total of approximately \$95,000 in Fiscal Years 2012-2013.

Cyber Activities Directed Against the Department of Defense.

In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military. These intrusions were focused on exfiltrating information. China is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs.



“We have met the enemy...”

- In the 1990’s, the common information security architecture strategy was to build a barrier between “us” and “them” – Fortress BNL
- This implies a level trust between the devices on the inside
- And it works if your attackers are always on the outside...
- But once the attackers jump past your firewall you have limited visibility and protection
- “Hard on the outside with a soft, gooey center”

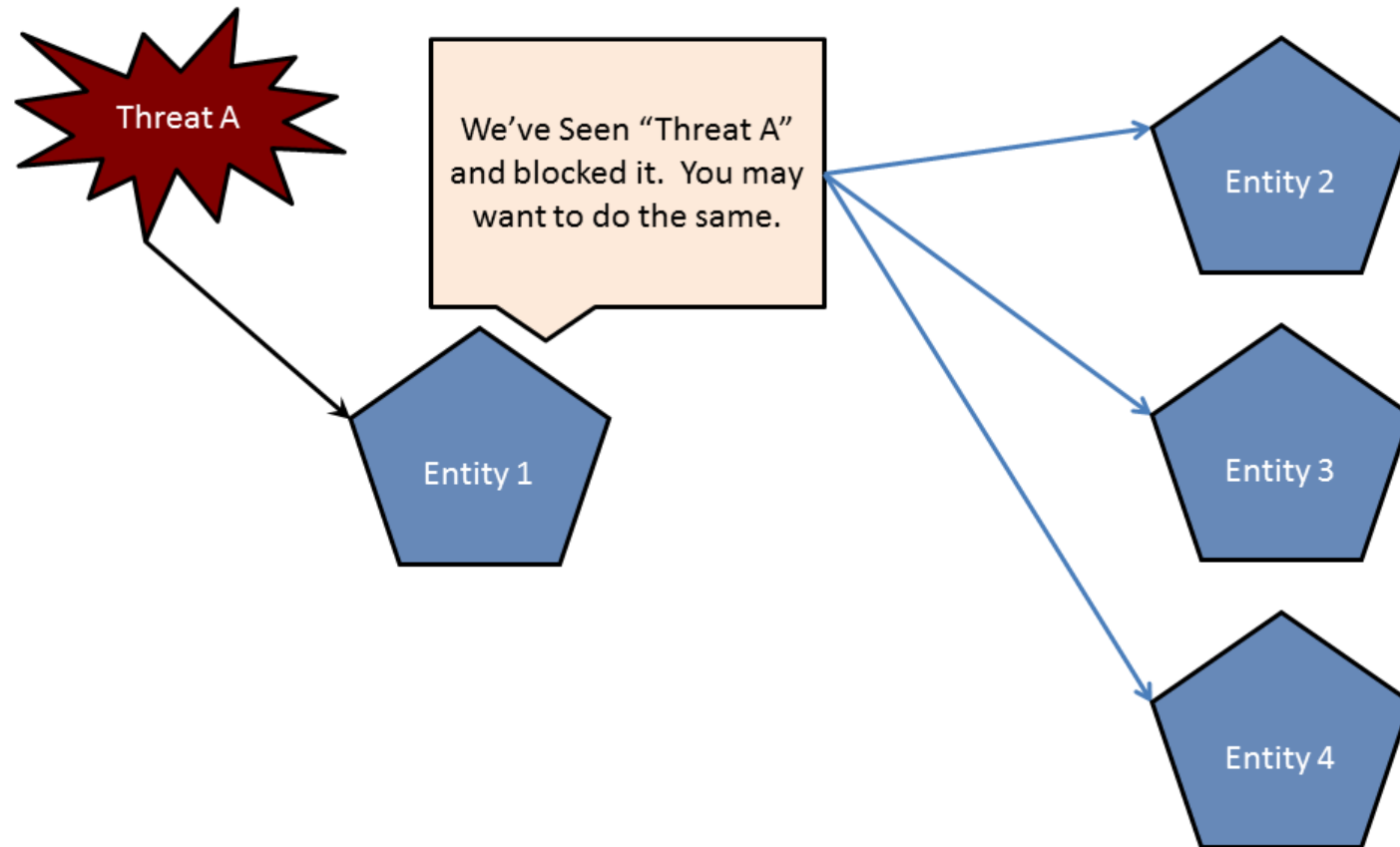
Defense in depth approach

- In a modern information security architecture, you must plan for the scenario that attackers will find ways past your external protections to attack devices on the network
- In the mid-2000's we shifted to a stronger defense in depth approach by building successive layers of protections
- In addition to external defenses, we focus our efforts on
 - Strengthening host-based protections (patching, anti-virus)
 - Grouping machines with common risk levels and adding additional network protections
 - Instrumenting the hosts and network to detect anomalous behavior and rapidly isolate them from the rest of the network

Risk Management

- We follow the Federal government requirements and standards for identifying and categorizing cyber risk and for developing controls to mitigate that risk
- When we think about information security risk, we consider
 - Confidentiality
 - Integrity
 - Availability
- Risk levels – Low, Moderate, High
- The risk levels inform the choice of controls used to mitigate the risk
- We need to balance risk mitigation with the open access required for collaborative scientific research

DOE Cybersecurity Collaboration and Information Exchange



Cybersecurity effectiveness

- We have regular internal and external assessments of our technical and program effectiveness
- These assessments show that we have effective controls in place to detect and stop attackers
- But attackers are relentless, and always have an advantage over defenders
 - Attackers are organized and use the information available on the Internet to plan their attack
 - Changing attack vectors
 - Spam > Phishing > Spear-phishing > Watering hole attacks
 - Constantly changing vulnerability landscape – 3rd party products and 0-day vulnerabilities

What can you do? Stop. Think. Connect.

- **Stop. Think. Connect.** is the Department of Homeland Security public awareness campaign to increase the understanding of cyber threats and to empower the American public to be safer and more secure online
 - <http://www.dhs.gov/stopthinkconnect>
- Resources for
 - Students, Parents and Educators, Young Professionals, Older Americans
 - Government, Industry, Small Business, Law Enforcement

Stop

- Stop hackers from accessing your accounts - set secure passwords
- Stop sharing too much information - keep your personal information personal
- Stop - trust your gut – if something doesn't feel right, stop what you are doing
- Stop and think about who can see the information you post online
- Stop any questionable online behavior. Only do and say things online that you would do in real life

Stop. Think.

- Think about the information you want to share before you share it
- Think how your online actions can affect offline life
- Think before you act – don't automatically click on links
- Think about why you are sharing information online. Is it going to be safe?
- Think about why you're going to a site. Did you get it from someone you trust?
- Think about who you are talking to online. Do you really know who they are?

Stop. Think. Connect.

- Connect over secure networks
- Connect with people you know
- Connect with care and be on the lookout for potential threats
- Connect safely and show your friends and family how to behave online
- Connect with people and sites you trust when you're online

QUESTIONS?