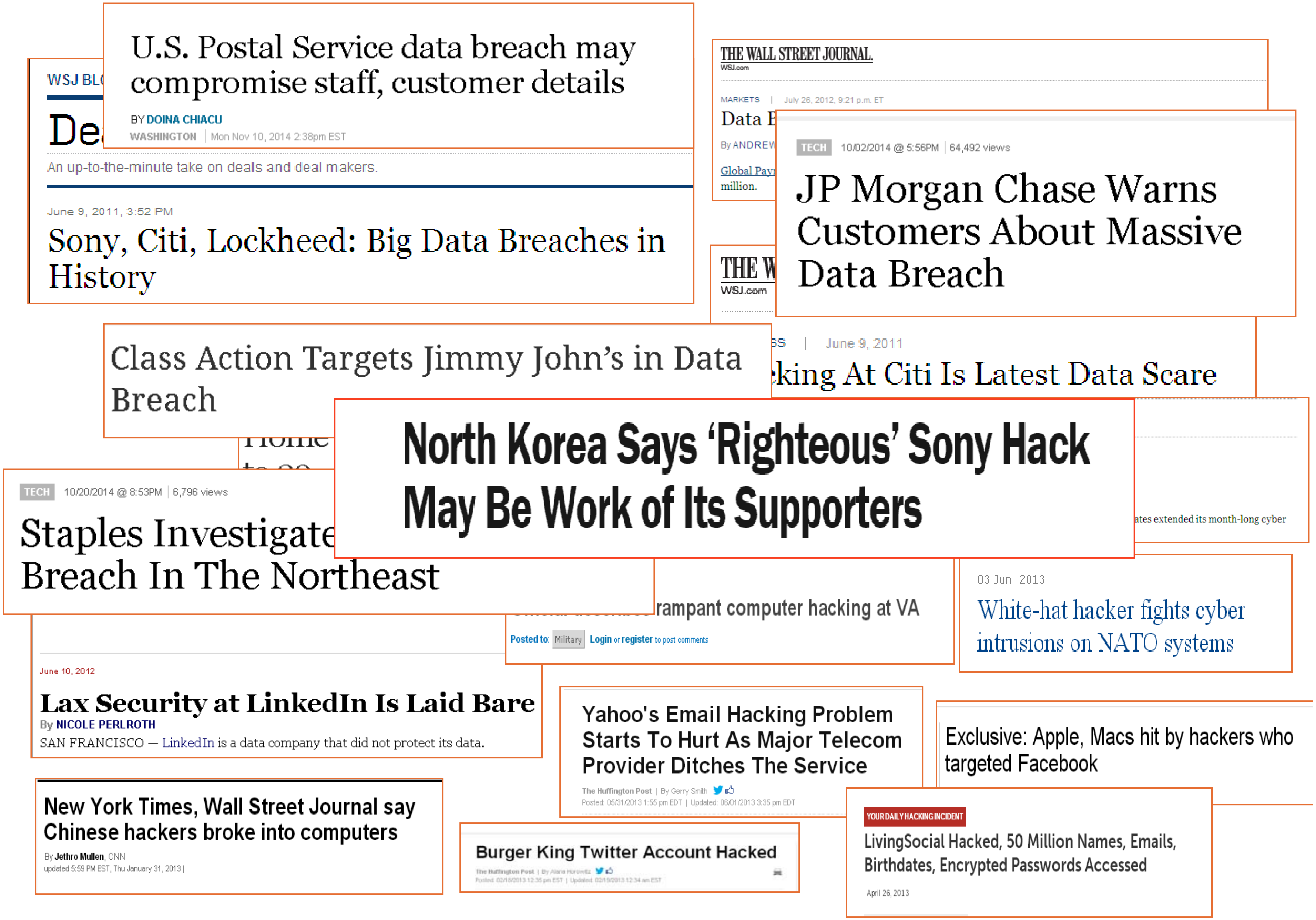
Understanding Cyber Risks and Security Options



WSJ BL

De

U.S. Postal Service data breach may compromise staff, customer details

BY DOINA CHIACU

WASHINGTON | Mon Nov 10, 2014 2:38pm EST

An up-to-the-minute take on deals and deal makers.

June 9, 2011, 3:52 PM

Sony, Citi, Lockheed: Big Data Breaches in History

THE WALL STREET JOURNAL.
WSJ.com

MARKETS | July 26, 2012, 9:21 p.m. ET

Data B

By ANDREW

Global Pay
million.

TECH 10/02/2014 @ 5:56PM | 64,492 views

JP Morgan Chase Warns Customers About Massive Data Breach

THE W
WSJ.com

ss | June 9, 2011

king At Citi Is Latest Data Scare

Class Action Targets Jimmy John's in Data Breach

Home

North Korea Says 'Righteous' Sony Hack May Be Work of Its Supporters

ates extended its month-long cyber

TECH 10/20/2014 @ 8:53PM | 6,796 views

Staples Investigate
Breach In The Northeast

rampant computer hacking at VA

Posted to: Military Login or register to post comments

03 Jun. 2013

White-hat hacker fights cyber intrusions on NATO systems

June 10, 2012

Lax Security at LinkedIn Is Laid Bare

By NICOLE PERLROTH

SAN FRANCISCO — LinkedIn is a data company that did not protect its data.

Yahoo's Email Hacking Problem Starts To Hurt As Major Telecom Provider Ditches The Service

The Huffington Post | By Gerry Smith

Posted: 05/31/2013 1:55 pm EDT | Updated: 06/01/2013 3:35 pm EDT

Exclusive: Apple, Macs hit by hackers who targeted Facebook

New York Times, Wall Street Journal say Chinese hackers broke into computers

By Jethro Mullen, CNN

updated 5:59 PM EST, Thu January 31, 2013 |

Burger King Twitter Account Hacked

The Huffington Post | By Alana Horowitz

Posted: 02/18/2013 12:35 pm EST | Updated: 02/19/2013 12:34 am EST

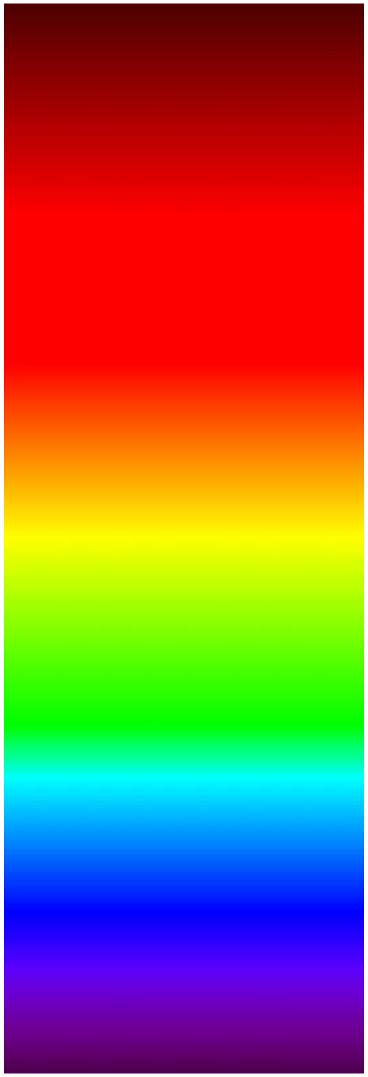
YOUR DAILY HACKING INCIDENT

LivingSocial Hacked, 50 Million Names, Emails, Birthdates, Encrypted Passwords Accessed

April 26, 2013

The Spectrum of Cyber Attacks

- Advanced Persistent Threats (“APT”)
- Cybercriminals, Exploits and Malware
- Denial of Service attacks (“DDoS”)
- Domain name hijacking
- Corporate impersonation and Phishing
- Employee mobility and disgruntled employees
- Lost or stolen laptops and mobile devices
- Inadequate security and systems: third-party vendors



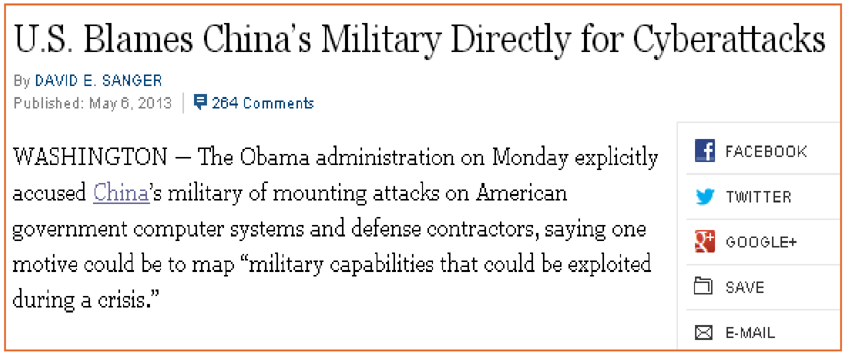
Advanced Persistent Threats

- targeted, persistent, evasive and advanced
- nation state sponsored

P.L.A. Unit 61398
“Comment Crew”

Advanced Persistent Threats

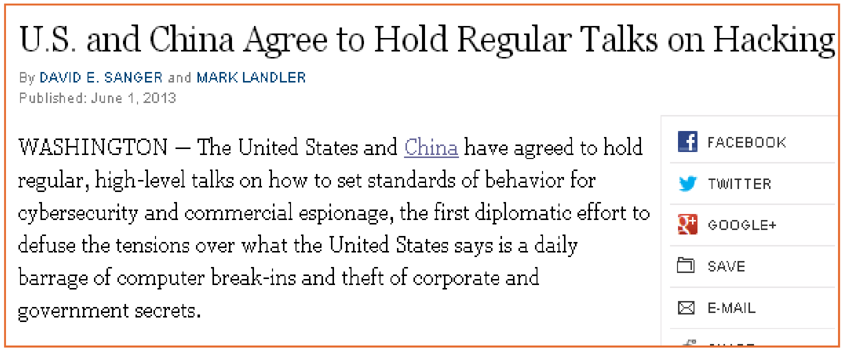
- United States Cyber Command and director of the National Security Agency, Gen. Keith B. Alexander, has said the attacks have resulted in the “greatest transfer of wealth in history.”



U.S. Blames China’s Military Directly for Cyberattacks

By DAVID E. SANGER
Published: May 6, 2013 | 264 Comments

WASHINGTON — The Obama administration on Monday explicitly accused China’s military of mounting attacks on American government computer systems and defense contractors, saying one motive could be to map “military capabilities that could be exploited during a crisis.”



U.S. and China Agree to Hold Regular Talks on Hacking

By DAVID E. SANGER and MARK LANDLER
Published: June 1, 2013

WASHINGTON — The United States and China have agreed to hold regular, high-level talks on how to set standards of behavior for cybersecurity and commercial espionage, the first diplomatic effort to defuse the tensions over what the United States says is a daily barrage of computer break-ins and theft of corporate and government secrets.

Source: New York Times, June 1, 2013.

Advanced Persistent Threats

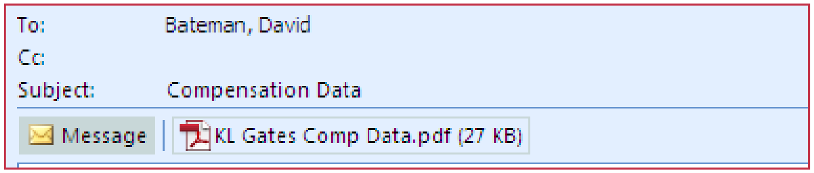
- Penetration:
  - – 67% of organizations admit that their current security activities are insufficient to stop a targeted attack.*
- Duration:
  - – average = 356 days**
- Discovery: External Alerts
  - – 55 percent are not even aware of intrusions*

**Source: Mandiant, "APT1, Exposing One of China's Cyber Espionage Units"

*Source: Trend Micro, USA. http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/index.html

Advanced Persistent Threats: Penetration

- Spear Phishing



To: Bateman, David

Cc:

Subject: Compensation Data

KL Gates Comp Data.pdf (27 KB)

- Watering Hole Attack

  rely on insecurity of frequently visited websites

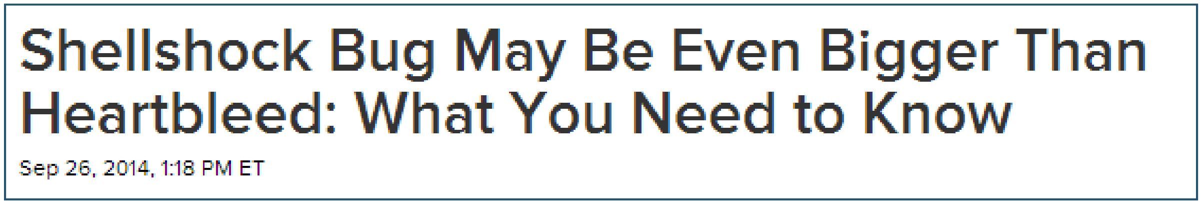
- Infected Thumb Drive

**Source: Mandiant, “APT1, Exposing One of China’s Cyber Espionage Units”

*Source: Trend Micro, USA. http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/index.html

Advanced Persistent Threats: Penetration

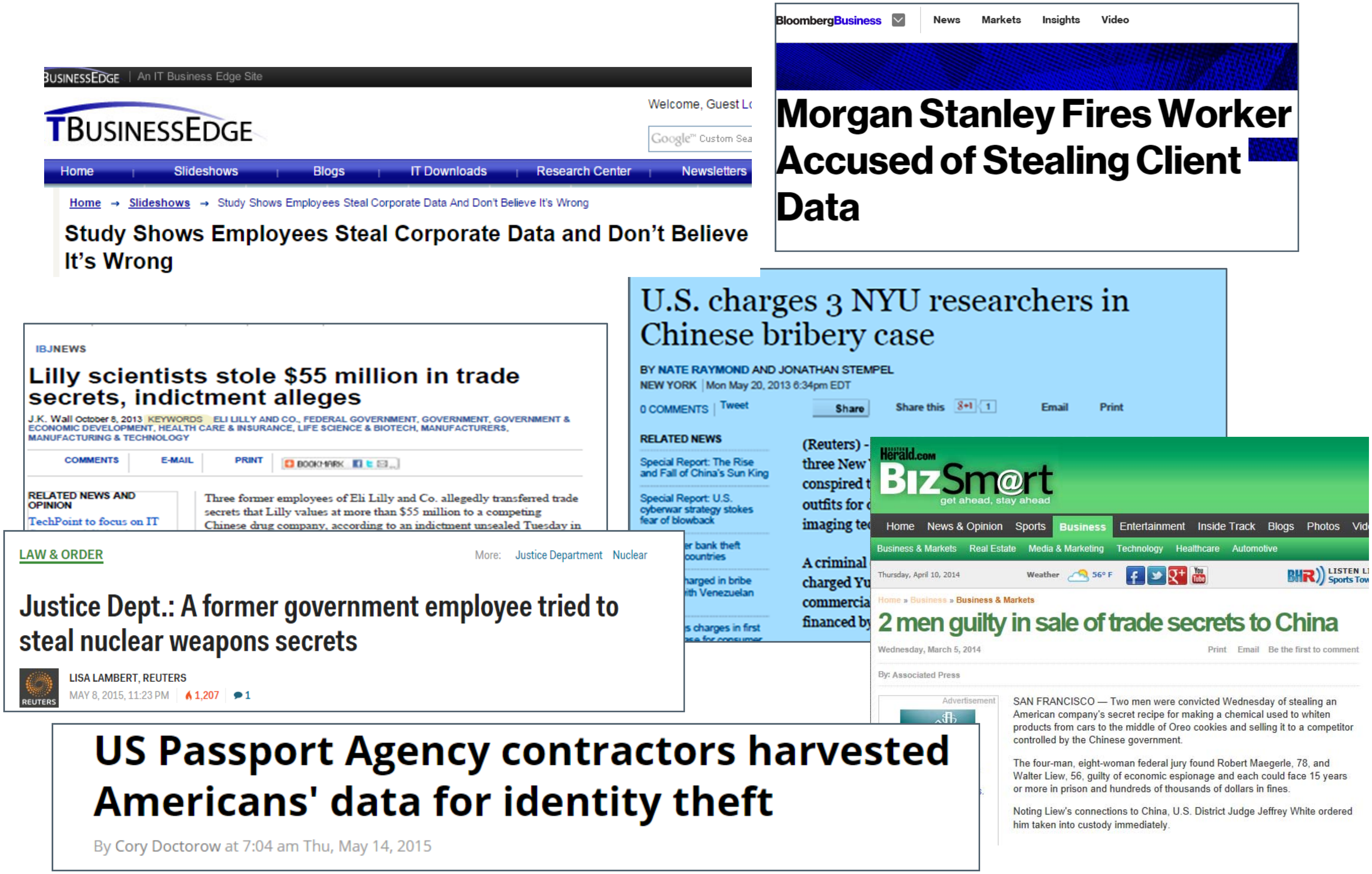
- 60,000 known software vulnerabilities
- 23 new zero-day exploits in 2014



Shellshock Bug May Be Even Bigger Than Heartbleed: What You Need to Know

Sep 26, 2014, 1:18 PM ET

Employee Theft



BUSINESSEDGE | An IT Business Edge Site
ITBUSINESSEDGE
Welcome, Guest L
Google™ Custom Sea
Home | Slideshows | Blogs | IT Downloads | Research Center | Newsletters

Home → Slideshows → Study Shows Employees Steal Corporate Data And Don't Believe It's Wrong

Study Shows Employees Steal Corporate Data and Don't Believe It's Wrong

BloombergBusiness
News
Markets
Insights
Video

Morgan Stanley Fires Worker Accused of Stealing Client Data

Lilly scientists stole $55 million in trade secrets, indictment alleges

J.K. Wall October 8, 2013 KEYWORDS ELI LILLY AND CO., FEDERAL GOVERNMENT, GOVERNMENT, GOVERNMENT & ECONOMIC DEVELOPMENT, HEALTH CARE & INSURANCE, LIFE SCIENCE & BIOTECH, MANUFACTURERS, MANUFACTURING & TECHNOLOGY

RELATED NEWS AND OPINION

TechPoint to focus on IT

Three former employees of Eli Lilly and Co. allegedly transferred trade secrets that Lilly values at more than $55 million to a competing Chinese drug company, according to an indictment unsealed Tuesday in

U.S. charges 3 NYU researchers in Chinese bribery case

BY NATE RAYMOND AND JONATHAN STEMPEL
NEW YORK | Mon May 20, 2013 6:34pm EDT

RELATED NEWS

Special Report: The Rise and Fall of China's Sun King

Special Report: U.S. cyberwar strategy stokes fear of blowback

er bank theft countries

harged in bribe ith Venezuelan

s charges in first ase for consumer

(Reuters) -
three New
conspired t
outfits for c
imaging tec

A criminal
charged Yu
commercia
financed by

Justice Dept.: A former government employee tried to steal nuclear weapons secrets

LISA LAMBERT, REUTERS
MAY 8, 2015, 11:23 PM 1,207 1

REUTERS
Herald.com
BizSm@rt
get ahead, stay ahead
Home | News & Opinion | Sports | Business | Entertainment | Inside Track | Blogs | Photos | Vid
Business & Markets | Real Estate | Media & Marketing | Technology | Healthcare | Automotive
Thursday, April 10, 2014
Weather 56° F
BHR LISTEN LI Sports Tow
Home » Business » Business & Markets

2 men guilty in sale of trade secrets to China

Wednesday, March 5, 2014

By: Associated Press

SAN FRANCISCO — Two men were convicted Wednesday of stealing an American company's secret recipe for making a chemical used to whiten products from cars to the middle of Oreo cookies and selling it to a competitor controlled by the Chinese government.

The four-man, eight-woman federal jury found Robert Maegerle, 78, and Walter Liew, 56, guilty of economic espionage and each could face 15 years or more in prison and hundreds of thousands of dollars in fines.

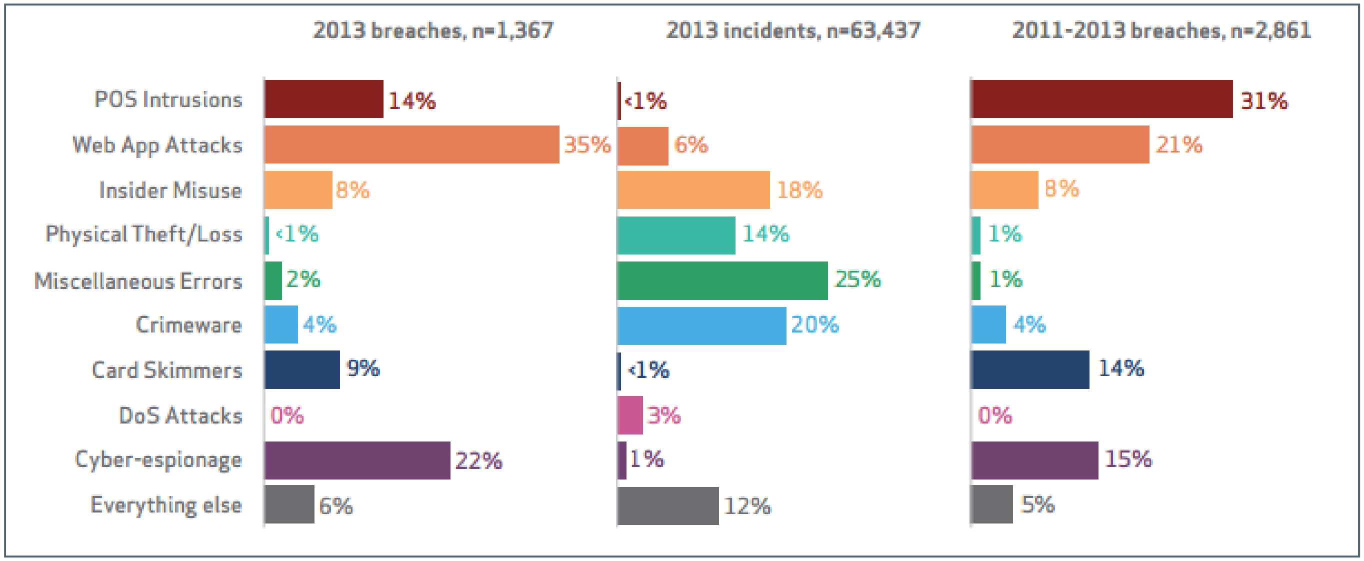
Noting Liew's connections to China, U.S. District Judge Jeffrey White ordered him taken into custody immediately.

US Passport Agency contractors harvested Americans' data for identity theft

By Cory Doctorow at 7:04 am Thu, May 14, 2015

Inadequate security and systems: third-party vendors

- Vendors with client data
- Vendors with password access
- Vendors with direct system integration
  - Point-of-sale



Cloud Computing Risks

- Exporting security function and control
- Geographical uncertainty creates exposure to civil and criminal legal standards
- Risk of collateral damage

Rising Mobile Device Risks

- 52% of mobile users **store sensitive files online**
- 24% of mobile users store work and personal info in the same account
- 21% of mobile users **share logins** with families
- Mobile malware: apps
- Insufficient mobile platform security

K&L GATES