

What do the Chinese Indictments for stealing US company data **mean for your business?**

PAMELA GUPTA

PRESIDENT OUTSECURE

NETCOM LEARNING INSTRUCTOR



OutSecure Inc



NetCom
LEARNING

Agenda

- ▶ Espionage
- ▶ Evolution of Cyber Threat Landscape
- ▶ The significance of the indictments for businesses
- ▶ Business state – What makes companies vulnerable (online, digital, interconnected, data, data & more data)
- ▶ Current threats
- ▶ Do you need a security strategy ?
- ▶ Beyond Protection



Nestorian Monks



Threat Landscape

- Espionage: Steal intellectual property (IP). Threats are already a huge number and the attacks are escalating.
- In 2011, McAfee, authored a report about malware that had been used by Chinese cybercriminals, many of them later revealed as linked to units in the People's Liberation Army.
- They exfiltrated data from a broad cross-section of 150 organizations over a 2-5 year period — undetected. It included the U.N., NY Times, Facebook, and numerous U.S. companies.

Nation States



- Sometimes with backing by some other entity, looking to steal money. A complete service based economy supporting their activities
- Attacks are a mix of social engineering and technical attack.

Organized Crime



- Aiming to disrupt an organization often on behalf of some cause.
- WikiLeaks
- Anonymous
- Lulzsec
- DDOS attacks

Hactivists



Kraft Foods, 1997

- ▶ A social engineer attacked Kraft Foods to learn about Kraft's rising crust pizzas
- ▶ Impact: competitor climbed from #6 to #2 by the end of 1999, thanks in part to the information gathered in 1 ½ days
 - ▶ Type of equipment in the plant
 - ▶ # of Production lines
 - ▶ Types of pizza being produced
 - ▶



U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations for Commercial Advantage

**WANTED
BY THE FBI**

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets



WANG DONG
Aliases: Jack Wang, "UglyGorilla"



SUN KAILIANG
Aliases: Sun Kai Liang, Jack Sun



WEN XINYU
Aliases: Wen Xin Yu, "WinXYHappy", "Win_XY", Lao Wen



HUANG ZHENYU
Aliases: Huang Zhen Yu, "hzy_jhxc"



GU CHUNHUI
Aliases: Gu Chun Hui, "KandyGoo"

DETAILS

On May 1, 2014, a grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army (PLA) of the People's Republic of China (PRC) for 31 criminal counts, including: conspiring to commit computer fraud; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging computers through the transmission of code and commands; aggravated identity theft; economic espionage; and theft of trade secrets.

The subjects, Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, were officers of the PRC's Third Department of the General Staff Department of the People's Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398, at some point during the investigation. The activities executed by each of these individuals allegedly involved in the conspiracy varied according to his specialties. Each provided his individual expertise to an alleged conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state-owned enterprises in China. They then used their illegal access to allegedly steal proprietary information including, for instance, e-mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs.

If you have any information concerning these individuals, please contact your local FBI office or the nearest American Embassy or Consulate.

The subjects, Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, were officers of the PRC's Third Department of the General Staff Department of the People's Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398, at some point during the investigation. The activities executed by each of these individuals allegedly involved in the conspiracy varied according to his specialties. Each provided his individual expertise to an alleged conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state-owned enterprises in China. They then used their illegal access to allegedly steal proprietary information including, for instance, e-mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs.

If you have any information concerning these individuals, please contact your local FBI office or the nearest American Embassy or Consulate.



Military Unit Cover Designator (MUCD), Unit 61398, estimated by to be staffed by hundreds, and perhaps thousands of people. China Telecom provided special fiber optic communications infrastructure*

- ▶ They have systematically stolen hundreds of terabytes of data from at least 141 organizations across 20 major industries.
- ▶ Have a well-defined attack methodology designed to steal large volumes of valuable intellectual property.
 - ▶ Technology blueprints,
 - ▶ Proprietary manufacturing processes,
 - ▶ Test results,
 - ▶ Business plans,
 - ▶ Pricing documents,
 - ▶ Partnership agreements,
 - ▶ Emails and contact lists from victim organizations' leadership.



Is your Business the next Target?

Forbes - New Posts +17 posts this hour Most Popular The WhatsApp Billionaires Lists The Business Of Nascar

2 FREE issues of Forbes

WINTER IS Here.

12 Share

70 Tweet

21 Share

0 reddit

7

8-1

0

85 Broads, Contributor
+ Follow (314)

FORBESWOMAN | 1/07/2014 @ 2:47 PM | 1,224 views

Is Your Business The Next Target?

+ Comment Now + Follow Comments

By Pamela Gupta

If a data breach is inevitable for any business, and it is – what measures do you have to take now to minimize the impact on revenue, reputation and cost involved in the aftermath?

When thieves hacked into credit and debit card data of as many as 40 million Target customers over the holidays, the breach rattled nerves and roiled Christmas shopping. In the wake of the massive data breach. Target Corp.



If you treat Security as an IT issue it can hurt your business...

- ▶ Security itself is a competitive edge
- ▶ A Strategic Security approach is critical in protecting your IP.



Find your industry or attacker— Verizon Data

Breach Report 2013

	Organized Crime	Nation State	Activists
Industry Targeted	Financial services, retail, food	Manufacturing, professional services, transportation	Information, public, services
Desired data	Payment card info, login Credentials, financial accounts	credentials, intellectual property & trade secrets, internal organization data system configuration	internal organization data, Personal information, credentials
Common methods	Physical tampering, brute-force attacks, malware (information stealer, spyware)	Malware (backdoor, information stealing, password dumper, downloader), phishing, stolen credentials, command & control activities	SQL injection, stolen credentials, hacking, backdoor malware
Targeted equipment	ATM, POS equipment, database, desktop (endpoint)	Laptop, desktop, file server, mail server, directory server	Web applications, database, mail server

Setting the Stage: The Global Economy*

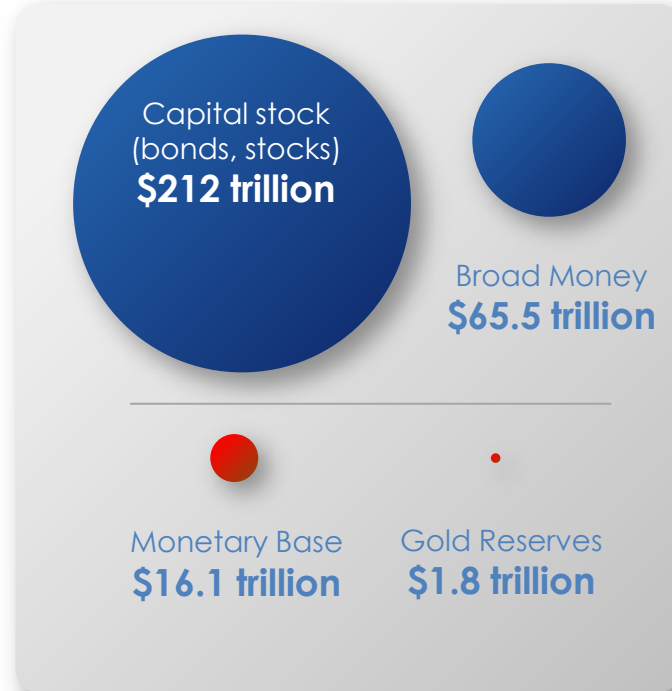
93.6%

Approximate percentage of digital currency in the global market

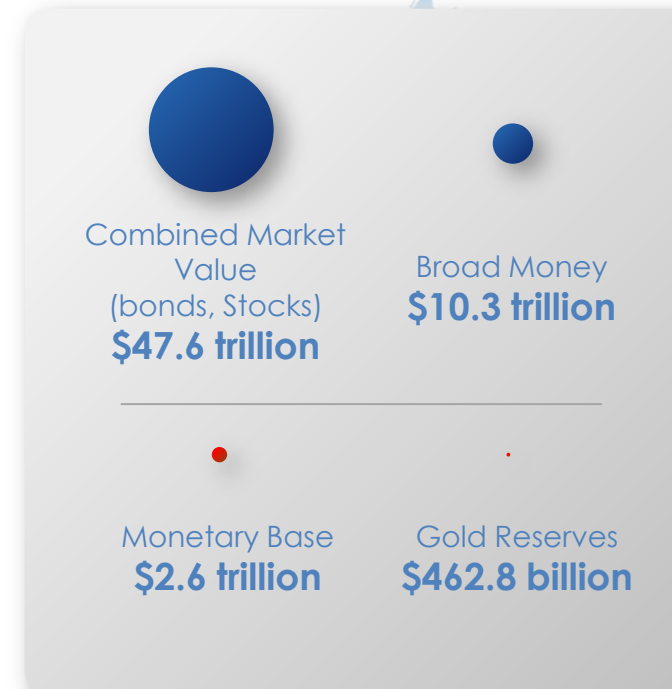
6.4%

Cash and gold available as a proportion of banking & commerce funds

Global Overview



U.S. Overview



Sources: CIA World Fact-book as of YE 2011 ; Global Capital stock est. by McKinsey

Broad money – savings, loans, deposits, money markets)

- Physical reserves (printed money, gold, etc.)
- "Digital Currency"

The Analyst's Eye: Top Fraud Threats to Watch in 2014 »

Home > Articles

Chase Breach: 465,000 Accounts Exposed

Bank Confirms Hack of Prepaid Card Servers

By Tracy Kitten, December 5, 2013. Follow Tracy @FraudBlogger

Get Daily Email Updates

Email address [Sign Up](#)

CAREERS INFO SECURITY®

Show all d



25 Data Broker Giants Hacked by ID Theft Service

SEP 13
 An identity theft service that sells Social Security numbers, birth records, credit and background reports on millions of Americans has infiltrated computers at some of America's largest consumer and business data aggregators, according to a seven-month investigation by KrebsOnSecurity.

The Web site [ssndob\[dot\]ms](#) (hereafter referred to simply as SSNDOB) has for the

New Retail Breach Among 2013's Biggest?

Fraud Linked to Harbor Freight Tools Attack is Spreading

By Tracy Kitten, August 7, 2013. Follow Tracy @FraudBlogger

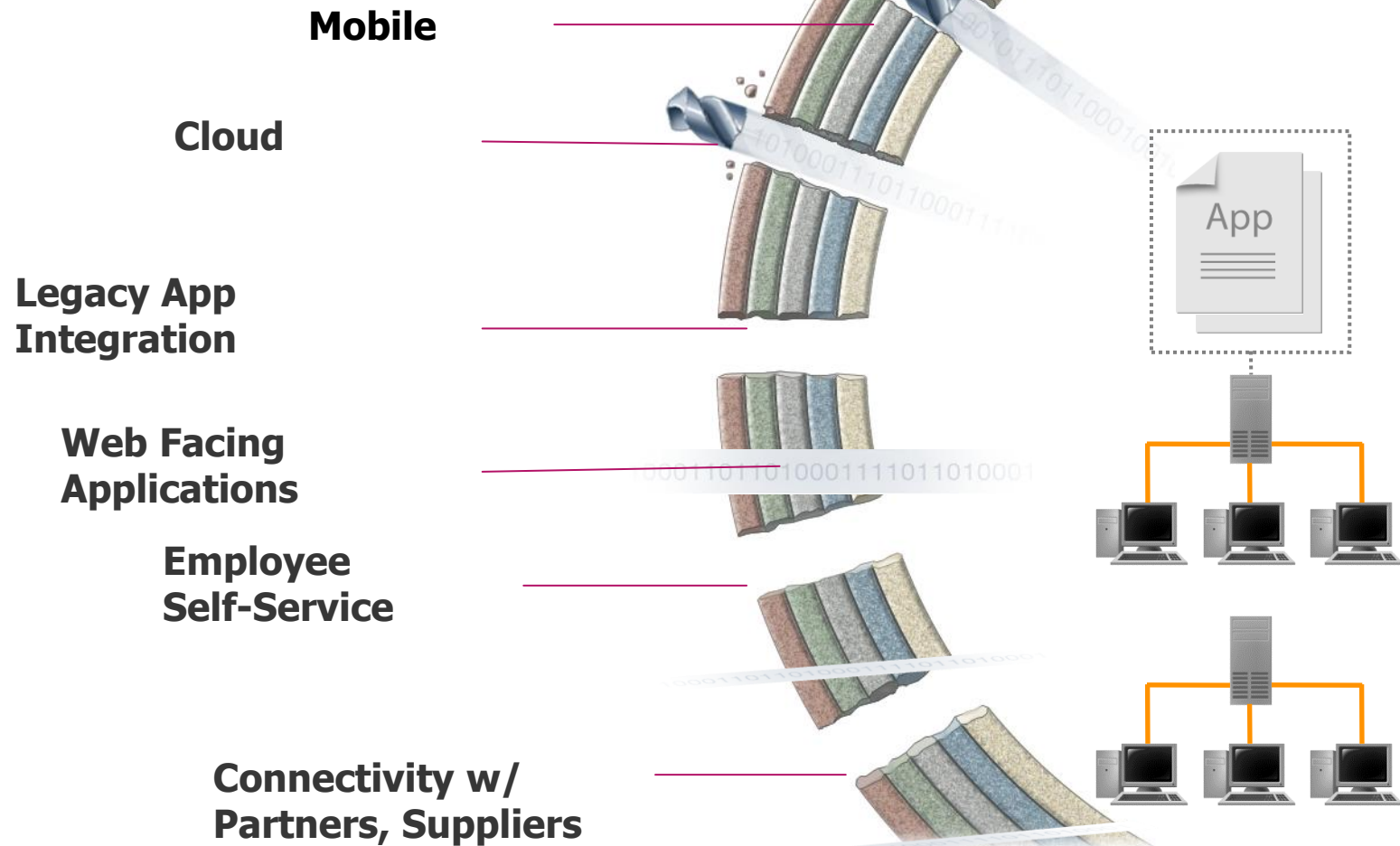
★ Credit Eligible [Email](#) [Tweet](#) [Like](#) [Share](#) [Get Permission](#)



A cyber-attack that hit [Harbor Freight Tools](#) and likely exposed card data processed at all 400 of its retail tool stores could rank among one of the biggest retail breaches this year, one card issuer says.

In fact, the issuer, who asked to remain anonymous, says compromised cards linked to the Harbor Freight attack will likely hit totals similar to those that resulted from a breach at [Schnuck](#)

The new company Perimeter



Impact on the Business

- ▶ Exposure to business and threats from operating in a interconnected global ecosystem
- ▶ Evolving threats and the changes in the adversaries skills and motivations
- ▶ Understand what to protect
- ▶ Reactive is not sustainable



A Risk based Security Program

- ▶ Identify
 - ▶ Governance
 - ▶ Risk Assessment
 - ▶ Risk Management Strategy
- ▶ Protect – Access control, awareness & training, data security & Information protection processes
- ▶ Detect
- ▶ Respond
- ▶ Recover



Its all about strategy

- ▶ Key Challenge for Boards & Senior Management
- ▶ How to strike the right balance between risk and reward

Successful Enterprise Risk Management

3 Key Differentiators

- 1. Perform a enterprise risk assessment that aligns with business strategy.** Many if not most perform it in a silo. There is no point in spending resources as its not going to be effective.
- 2. Define & communicate risk tolerance.** Many have one but its not simple, understandable or actionable.
- 3. Make risk management program nimble and adaptive – examine changing ecosystem.**



3 things to remember

1. Security is a business issue not a technology issue
2. Know what data you have worth protecting and have a structured approach to protect it
 - ▶ Not just internally, externally with your business partners as well. Do they have access to your sensitive information and if so how are they protecting it;
 - ▶ If its regulated data its easy to identify but what about your Intellectual Property (IP)? Where is it
 - ▶ What is your Proprietary Data
3. Have a data breach plan



“There are only 2 types of companies, according to FBI Director –
Those that have been hacked
& those that will be”

Thank You!



OutSecure Inc



NetCom
LEARNING



Pamela Gupta is President of OutSecure Inc. and a NetCom Learning instructor/subject matter expert.

OutSecure is a cyber-security strategy creation company that focuses on creating strategies that address risks unique to the company. The approach is unique and streamlined to produce effective strategies cost effectively and in a short period of time.

Twitter: @pamegup, @outsecure