



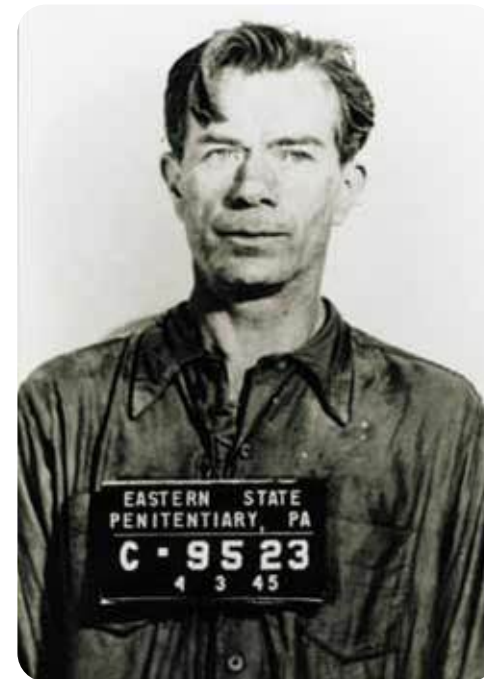
# AT&T Security Consulting *"The Dark Web"*

Scott Sweren, Sr. Consultant  
October 2017

## Willie Sutton....bank robber...author

“Why do you rob banks?”

*“Because that’s where the money is”*





EPOCH  
TIMES

China Alleged to Have Hacked Three Medical Device  
Companies



CNN

Money

Cybercrime Costs the Average U.S. Firm \$15 Million a  
Year



TechRepublic®

63% of SMBs Increased Security Spending, but More  
Than Half Still Experienced Breaches



REUTERS

Russia Hacked Hundreds of Western Asian Companies:  
Security Firm



DARKReading

Ransomware Sales on the Dark Web Spike 2,502% in 2017

# 10 Worst Data Breaches of All Time



**10. US Govt. Agency, 2008:** 76 million records

**9. Russian Internet Portal, 2014:** 98 million accounts

**8. Entertainment and Electronics Co., 2011:** 102 million records

**7. US Retailer, 2013:** 110 million records

**6. Payment Processor, 2008-2009:** 130 million records

**5. Credit Agency, 2017:** 143 million accounts

**4. Professional Social Network, 2012:** 165 million accounts

**3. Personal Professional Network, unknown:** 360 million accounts

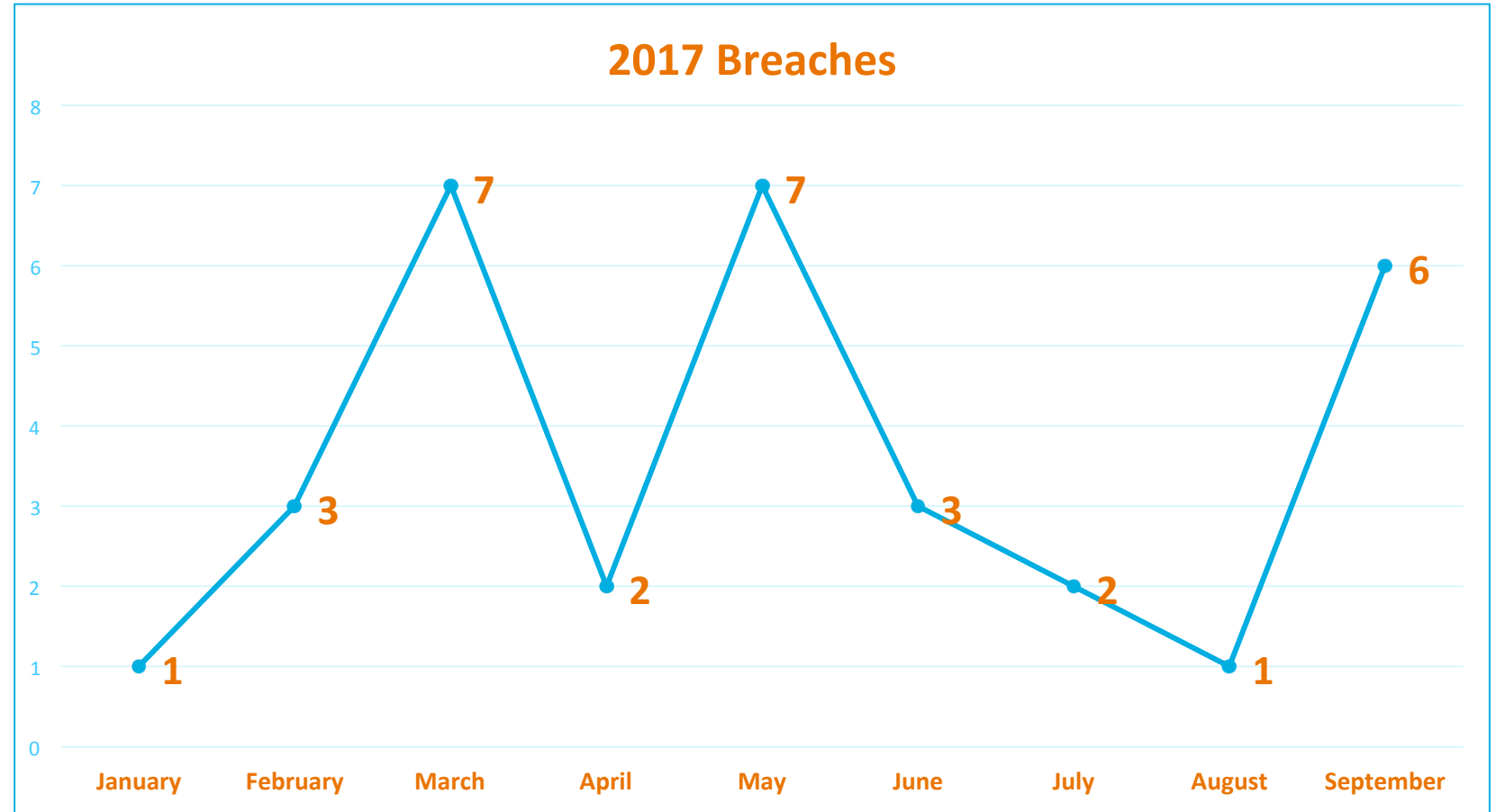
**2. Social Network, 2016:** 412 million accounts

**1. Internet Portal, 2013 & 2016:** 1.5 billion accounts combined

Elizabeth Palermo & Paul Wagenseil Sep 8, 2017 [HTTPS://WWW.TOMSGUIDE.COM/US/PICTURES-STORY/872-WORST-DATA-BREACHES.HTML#S2](https://www.tomsguide.com/us/pictures-story/872-worst-data-breaches.html#S2)

# 2017 Breaches

**32 Breaches  
To Date**



Heidi Daitch Sep 26, 2017 [HTTPS://WWW.IDENTITYFORCE.COM/BLOG/2017-DATA-BREACHES](https://www.identityforce.com/blog/2017-data-breaches)

## Insider Threats

- Spear phishing email
- Plugging in a thumb drive that hasn't been security screened
- Social engineering
- Lack of employee training, awareness around security

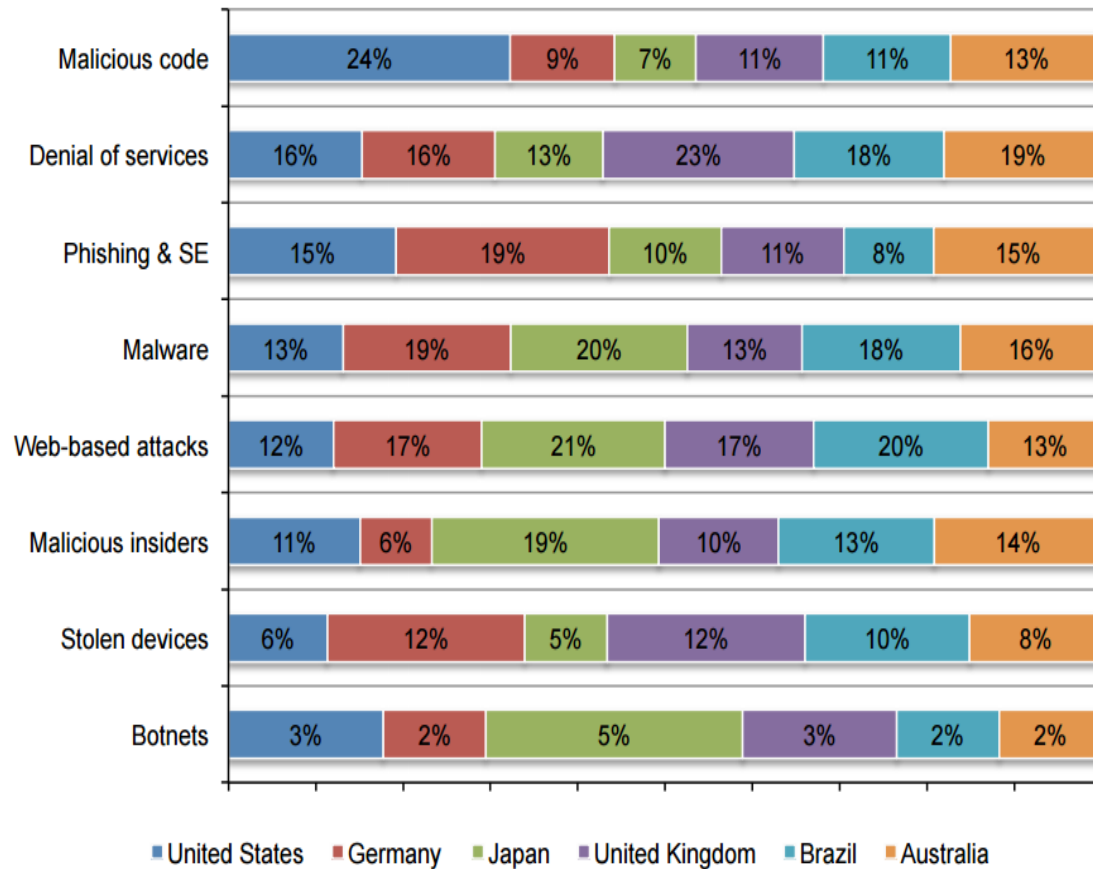
## Malicious Insider Risks

- Revenge
- Money
- Whistleblowers
- Hacktivism
- Espionage
- Business Advantage

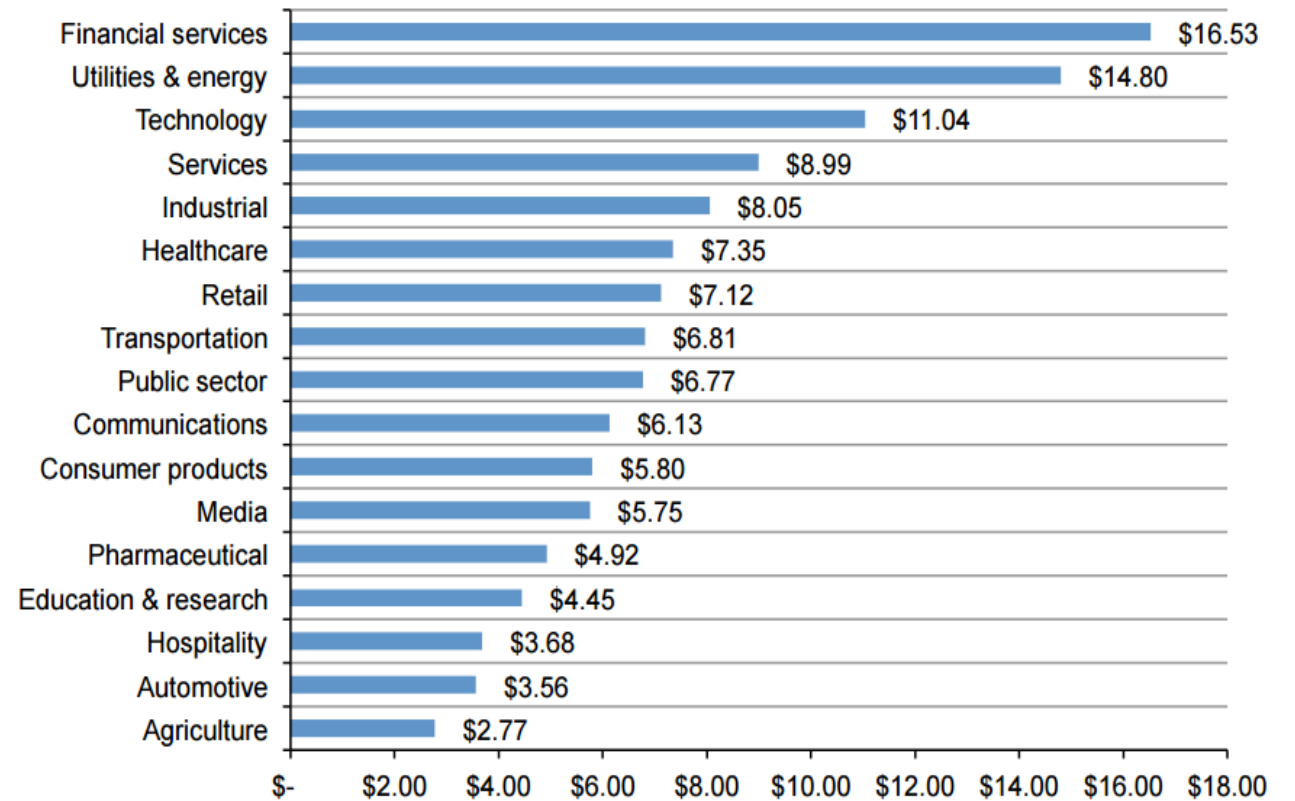
Source: AT&T Cybersecurity Insights Report – Decoding the Adversary Volume <https://www.business.att.com/cybersecurity/docs/decodingtheadversary.pdf>

# Some Stats...

**Figure 6. Percentage annualized cyber crime cost by attack type**  
n = 237 separate companies



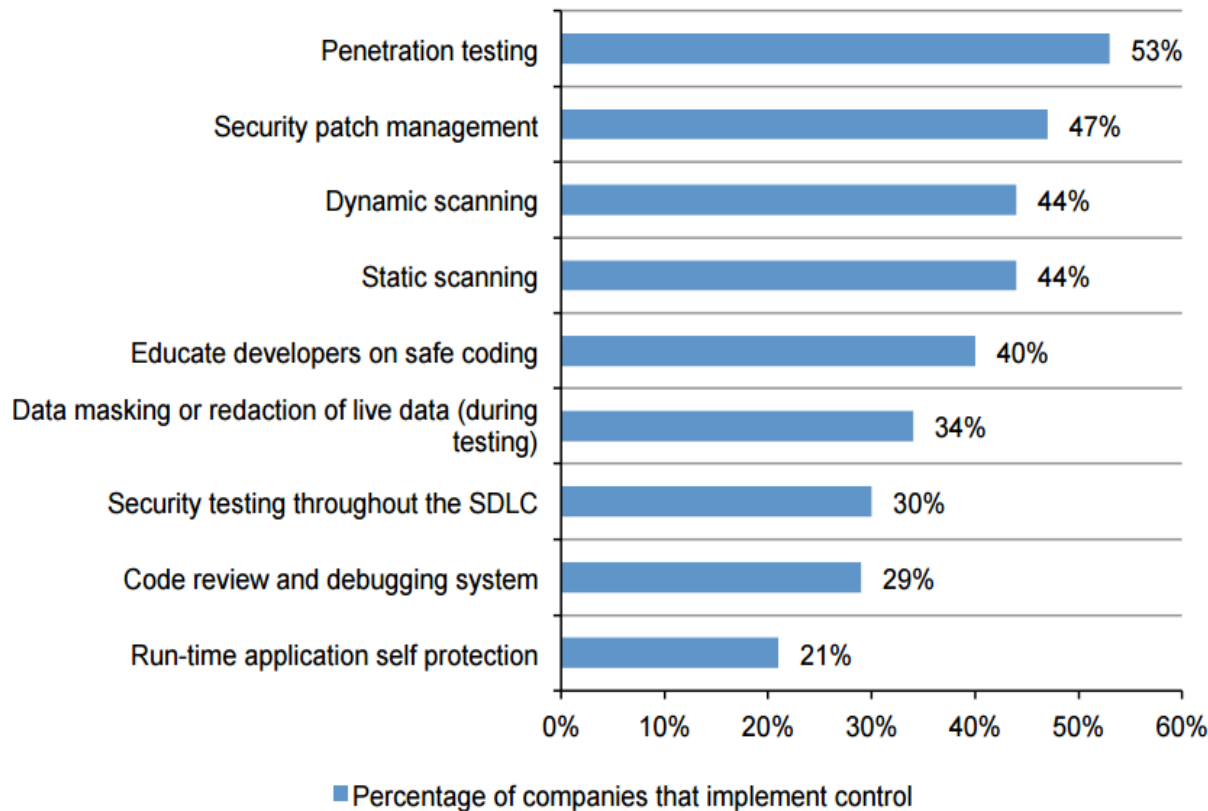
**Figure 4. Average annualized cost by industry sector**  
US\$ millions, n = 237 separate companies



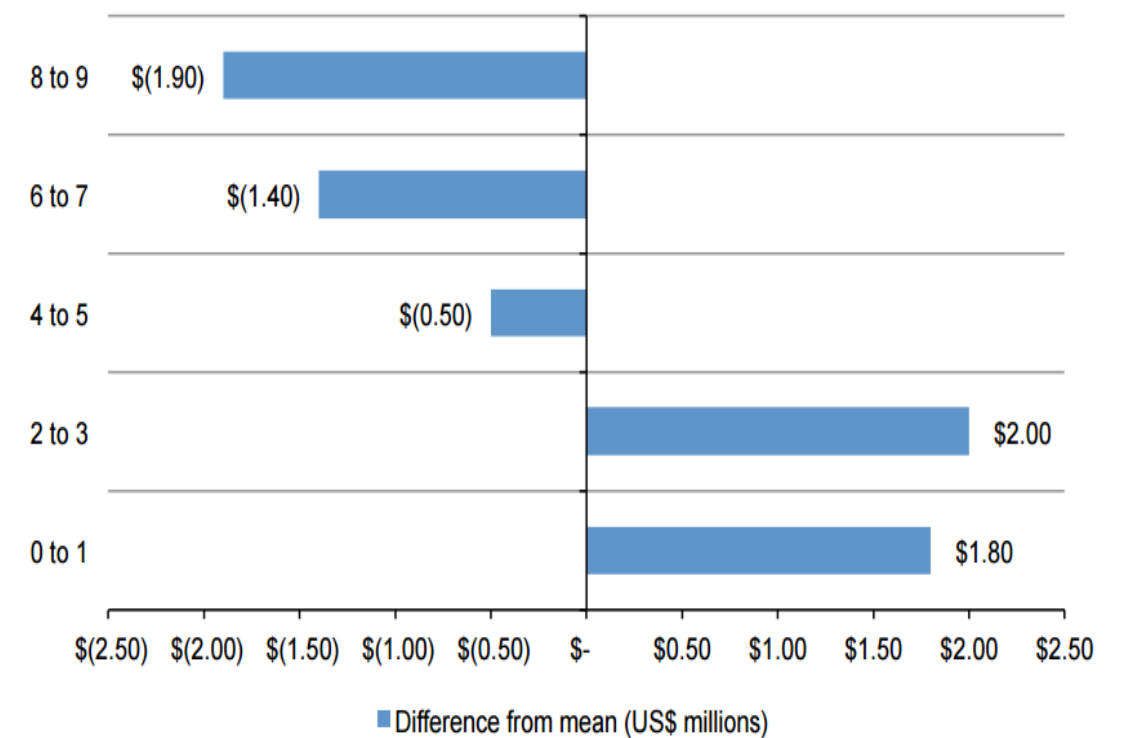
Source: Ponemon Institute 2016 Cost of Data Breach Study: Global Analysis

# Application Security Stats ...

**Figure 21. Percentage use of nine application security controls**  
n = 237 separate companies



**Figure 22. Cost differentials for the persistent use of application security controls**  
US\$ millions, n = 237 separate companies



Source: Ponemon Institute 2016 Cost of Data Breach Study: Global Analysis





## It is about more than Payment Card Data

### Financial

Driven primarily by stealing data that can be *monetized* (BOA, MAZAFKA, RBN)

### Hacktivism

Wish to make a *political or social statement* with attacks (Anonymous, LulzSec, FSA)

### CyberEspionage

State sponsored *IP theft to benefit state*

Primarily China, and Russia although other countries take part

## Motivated to Steal Intellectual Property, corporate secrets

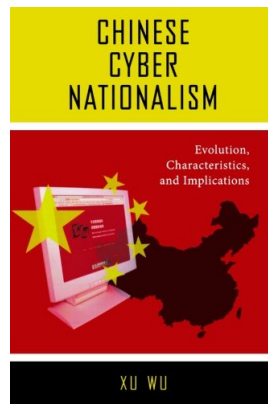
Chinese, Russian, and other governments sponsor

“Patriot Hackers” take up cause

Companies performing research – private,  
government, aerospace, IP, etc.

Advanced Persistent Threat...”Low and Slow”

\$300,000,000,000 per year cost to US



*“The United States is Under Attack...The Communist Chinese Government has defined us as the enemy. It is buying, building and stealing whatever it takes to contain and destroy us. Again, the Chinese Government has defined us as the enemy.”*

Source: Dana Rohrbacher, US Congressional Subcommittee on Oversight and Investigations , April 15, 2011

# A New Battlefield (APT)



## North Korea

- 50K servers, South Korean financial system (2013)
- Sony Pictures, "The Interview" (Nov 2014)

Image Source: krebsonsecurity.com



## China

- RSA/EMC phishing email, 0-day Flash Vuln (2011)
- Lockheed Martin VPN/2FA attack, F35 (2011)
- OPM 21M records including clearances (July 2015)

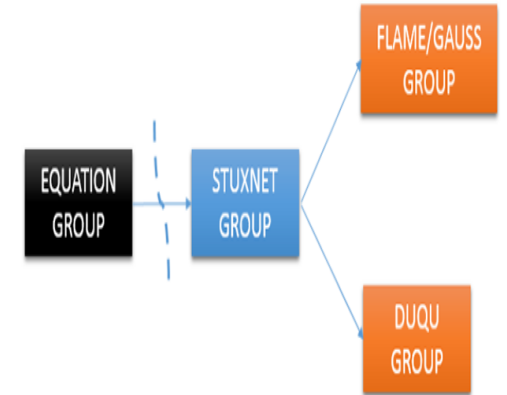
Image Source: CNN.com



## Russia

- Pentagon JCS email hack (Aug 2015)
- WH email (Apr 2015)

Image Source: CNN.com



## US (with support from Israel)

- Iran Stuxnet/Duku enrichment facilities hack (2010)
- Equation Group revealed by Kaspersky (2015)

## Victims -WorldBank, Stratfor, SONY, etc.

Shut down sites with DDOS attacks, steal data to “make a political or social statement”

- Anonymous & LulzSec, Free Syrian Army
- Entertainment, New Media, Internet Portals, etc.



“SABU”

*“One man’s freedom fighter is another man’s terrorist. So let them call us terrorists,” he added moments later: “I’ll still bomb their buildings.”*  
*Jeremy Hammond*



## **Dmitry Ivanovich Golubov “Script” (ARRESTED)**

- Alleged to be a major cyberthief
  - Founder of CarderPlanet
  - Ran for Ukrainian Senate
  - Heads political party
- 



## **Max Ray Butler “IceMan” (convicted)**

- Founder of CardersMarket
  - Recovered 1.3 million accounts on laptop
- 



## **Steven Watt (Convicted)**

- Created Trojan responsible for major retail breaches
- Graduated college at 19
- Worked at Morgan Stanley at time of breach

# “Internet Party of Ukraine” – Dmitry Gulubov (Script)

**ІНТЕРНЕТ ПАРТІЯ УКРАЇНИ**

ГОЛОВНА | ЗМІ ПРО НАС | ЧЛЕНИ ПАРТІЇ | БЛОГИ | ВСТУПИТИ ДО ПАРТІЇ

Наша команда | Програма партії | Символка | Бібліотека | Політ. гумор | Медіа | Форум

**НОВИНИ**

**Генетическая Афера**  
31 Травень, 2009 - 08:25 — Гость

Не так давно мне довелось общаться с одним пожилым канадским фермером. Он с горечью рассказывал, что никакой свободы для работающего эффективного собственника не пахнет и близко. Но не только это огорчало потомственного трудягу-фермера. Его до глубины души возмущало то (цитирую его почти дословно), что он теперь полностью, абсолютно зависим от некоей корпорации, контролируемой людьми, которые в жизни никогда на земле не...

рейтинг материалу +1 » докладець » 2 коментарів »

**112 тисяч безробітних не получат компенсації**  
29 Травень, 2009 - 15:05 — Павел

Українці, узаповнені по согласию сторон в период действия нормы, согласно которой социальная помощь по безработице выплачивается на 91-й...

**АКТИВИСТИ**

Pawel	7886
grandzk	6793
	1268



**ІНТЕРНЕТ ПАРТИЯ УКРАЇНИ** | Нас 11 мил.

**ЧЕЛОВЕК СЛОВА**  
ИНТЕРНЕТ ПАРТИЯ УКРАИНЫ

**СТЕПАН ЧУБАККА**

Главная | Поиск

Задать вопрос | **29** сентября 2013 | информация на сегодняшний день

Вступить в партию | Войти

Партия | Главная новость | В Одессе начали выполнять указ | Лидер партии

# The Most Prolific Gang in Cyber History?



**Albert Gonzalez**  
**"soupnazi" (convicted)**

- Large-scale retail breaches
- Most while on payroll with SS \$75k/yr
- Serving 20 year term



**Humza Zaman,**  
**laundering (convicted)**

- Internal bad actor, worked on-staff at global bank as network security manager
- Money mule, ATMs (FedEx portion to Gonzalez)



**Jonathan James**

**Christopher Scott**      **No Image**

**Christopher Scott & Jonathan James**  
**(convicted)**

- US-1 war driving specialists



**Maksym Yastremskiy**  
**"Maksik" (convicted)**

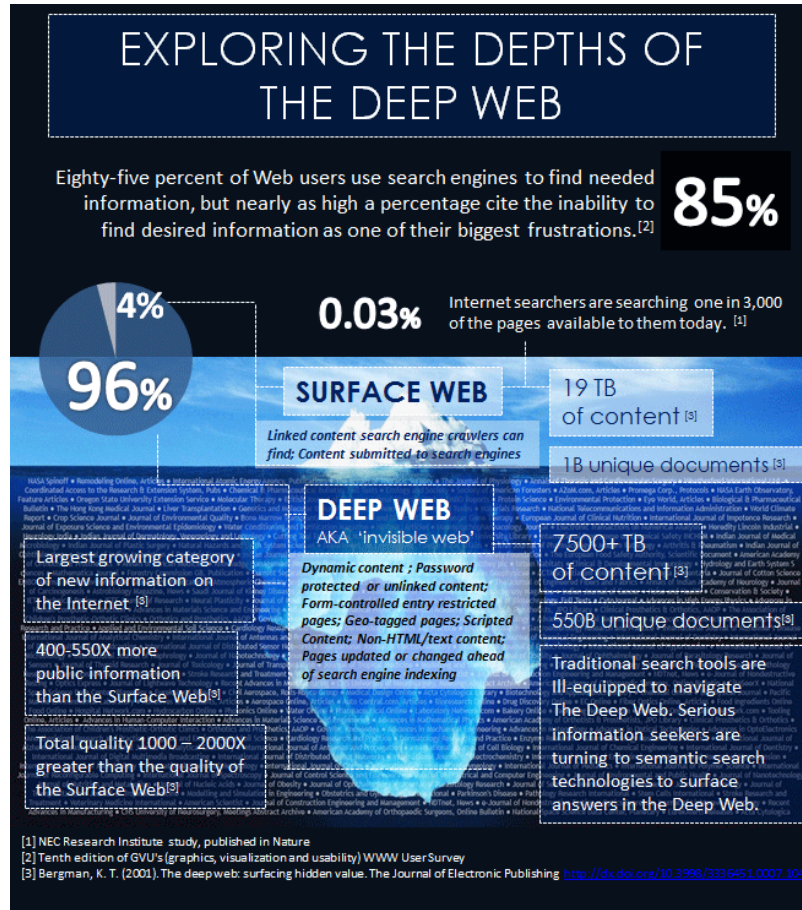
- Greatest profiteer \$11M as carder



# How it is Done







<http://inventionmachine.com/DeepWeb>

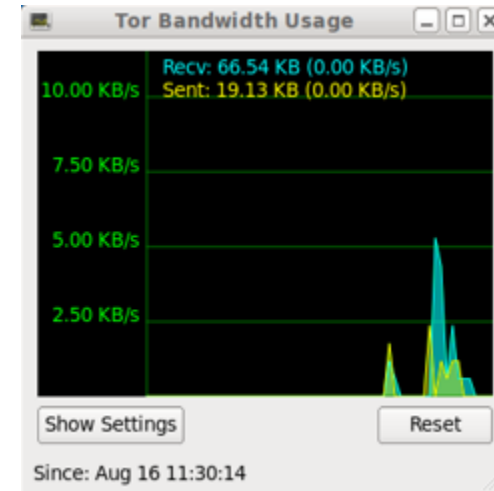


Source: Charlie Abrahams, MarkMonitor

Surface web (clear web) accounts for 4% of content...19TB of content (1 billion unique documents)

Deepweb accounts for 96% of content or 7,500+ TB (550 billion unique documents) Deepweb has an estimated 1,000 – 2,000 more information than clear web

Used by spies, journalists, dissidents, activists, those in restricted countries...and criminals.



[http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main\\_Page](http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page)

## Financial Services

Currencies, banks, money markets, clearing houses, exchangers.

- [The Green Machine!](#) Forum type marketplace with some of the oldest and most experienced vendors around. Get your paypals, CCs, etc, here!
- [The PaypalCenter](#) Live Paypal accounts with good balances - buy some, and fix your financial situation for awhile.
- [Skimmed Cards](#) Oldest seller on old HW. Fresh stock. 99.9% safe. Worldwide cashout! |EXPRESS SHIPPING| |ESCROW|
- [GreenNotes Counter](#) Highest Quality USD and EUR Counterfeits on the market. Trusted and reputable vendor.
- [Fake Real Plastic](#) - Credit Card vendor sharing my work for a reasonable price.
- [Wiki Cards](#) Top Quality Credit Cards, worldwide shipping
- [Prepaid Paradise](#) - No Risk Pre-Paid Debit Cards for sale
- [Bitcoin Blender](#) - Bitcoin Laundry (mixing) service and safe Wallet.
- [Fish Squad](#) Paypal phisher group. Buy some phished accounts online, grab yourself some money.
- [Wall Street](#) - Paypal accounts, credit cards, we have everything!!
- [StolenPal](#) Long-time, trusted PayPal account vendor site, if you need money fast. Sells stolen PayPal accounts
- [BitMix](#) High volume Bitcoin mixer. Anonymize your bitcoins and make them untraceable.
- [MMM Euro Counterfeits](#) 100, 50 and 20 euro counterfeits. We are a trusted vendor with safe shipping.
- [SafeCoins](#) Launder and buy bitcoins safe.
- [SOL's USD Counterfeits](#) High Quality 20 USD Counterfeit Notes - Trusted Service

15 Video - Movies / TV

16 Books

17 Drugs

18 Erotica

18.1 Noncommercial (E)

18.2 Commercial (E)

18.3 Under Age

18.4 Animal Related

18.5 Other

19 Uncategorized

20 Non-English

20.1 Belarussian / Белорусский

20.2 Finnish / Suomi

20.3 French / Français

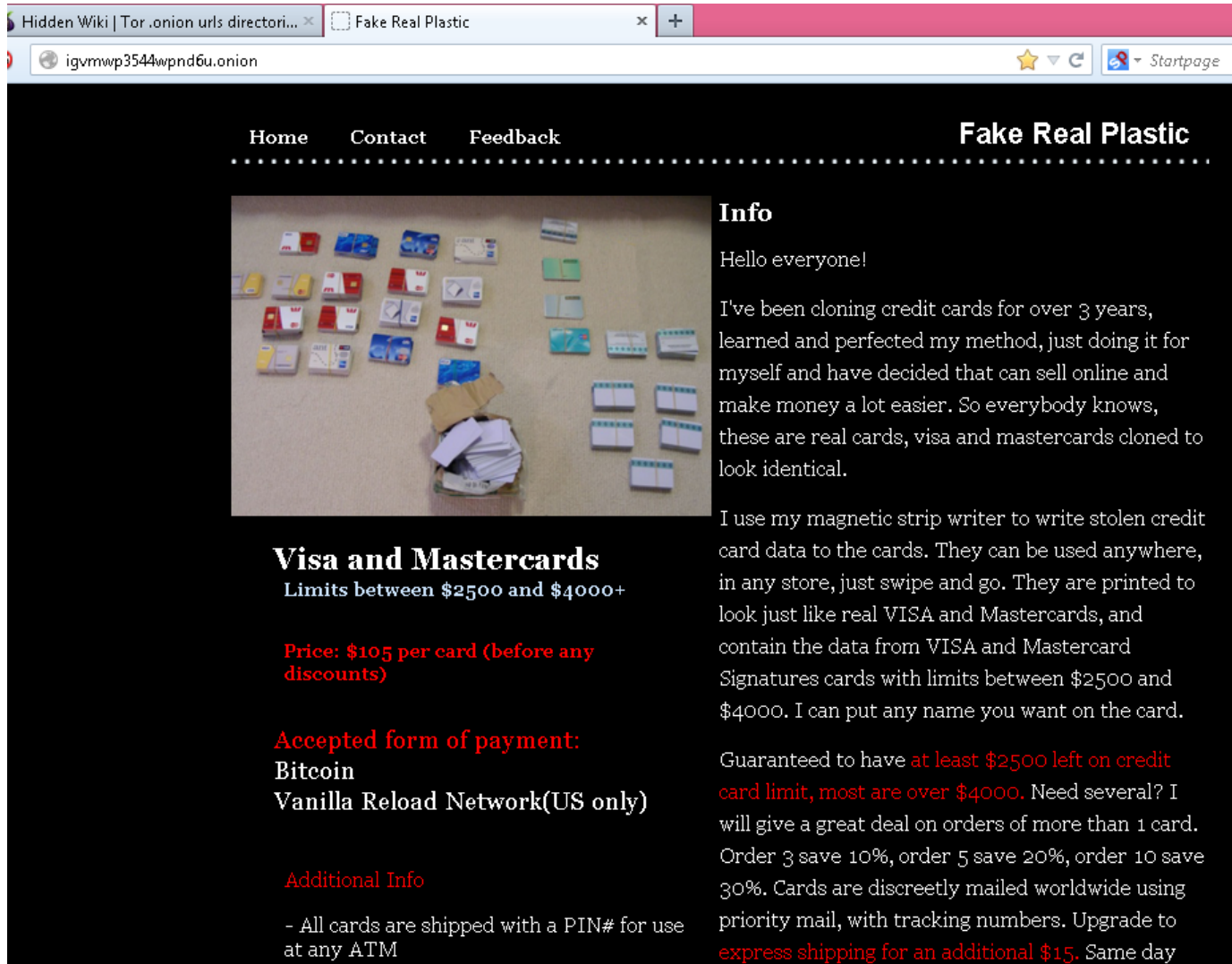
20.4 German / Deutsch

20.5 Greek / ελληνικά

20.6 Italian / Italiano


20.7 Japanese / 日本語

20.8 Korean / 한국어



The screenshot shows a Tor browser window with the address bar displaying 'igvmwp3544wpnd6u.onion'. The website has a dark background and a navigation menu with 'Home', 'Contact', and 'Feedback'. The main content area features a photograph of various credit cards and a small stack of cash. Below the photo, there is a section titled 'Visa and Mastercards' with details on limits, price, and payment methods. To the right, an 'Info' section provides a personal introduction and further details about the cloning process and shipping options.

Home Contact Feedback **Fake Real Plastic**



**Visa and Mastercards**  
Limits between \$2500 and \$4000+

**Price: \$105 per card (before any discounts)**

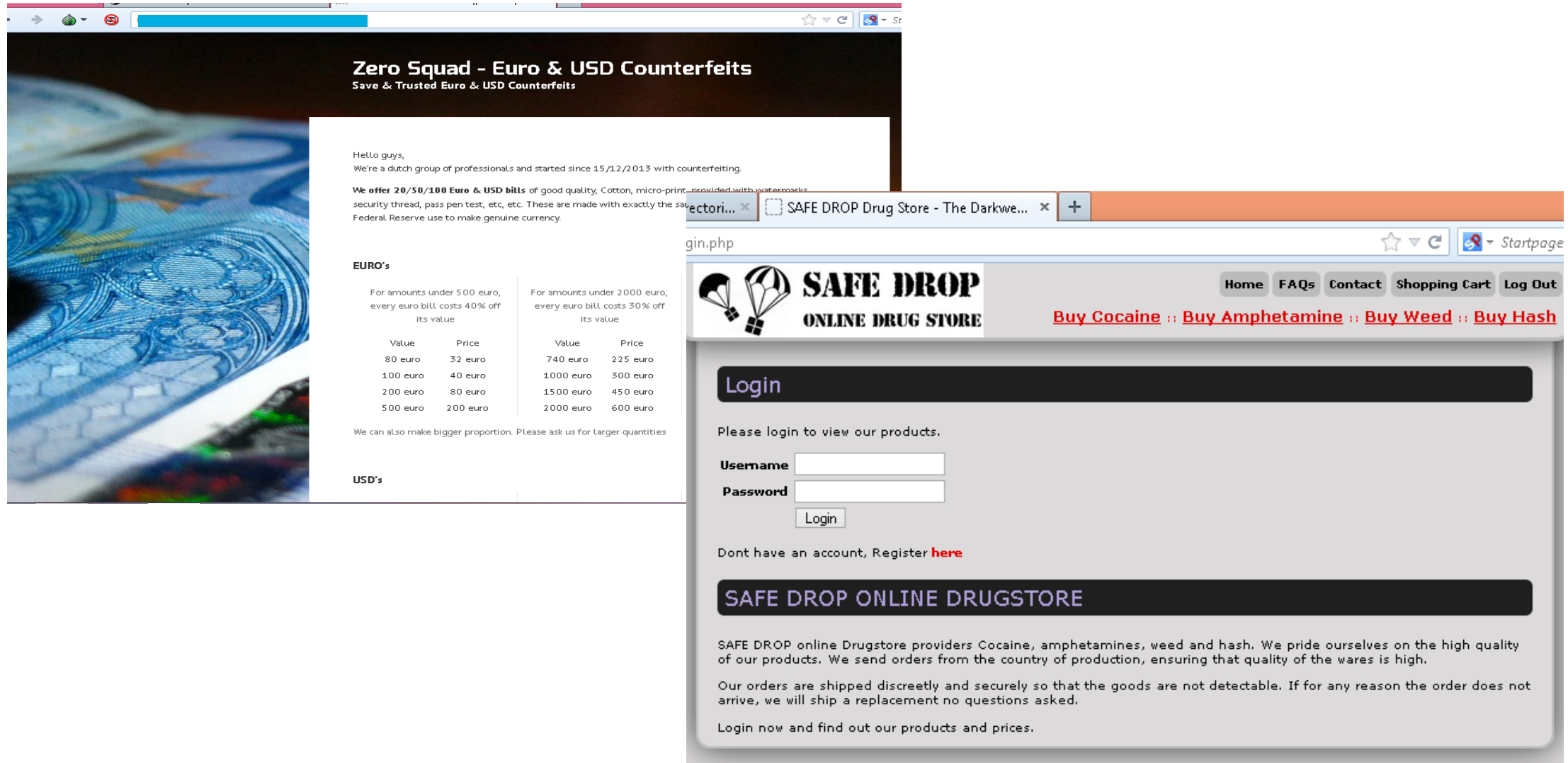
**Accepted form of payment:**  
Bitcoin  
Vanilla Reload Network(US only)

**Additional Info**

- All cards are shipped with a PIN# for use at any ATM

**Info**  
Hello everyone!  
I've been cloning credit cards for over 3 years, learned and perfected my method, just doing it for myself and have decided that can sell online and make money a lot easier. So everybody knows, these are real cards, visa and mastercards cloned to look identical.  
I use my magnetic strip writer to write stolen credit card data to the cards. They can be used anywhere, in any store, just swipe and go. They are printed to look just like real VISA and Mastercards, and contain the data from VISA and Mastercard Signatures cards with limits between \$2500 and \$4000. I can put any name you want on the card.  
Guaranteed to have **at least \$2500 left on credit card limit, most are over \$4000**. Need several? I will give a great deal on orders of more than 1 card. Order 3 save 10%, order 5 save 20%, order 10 save 30%. Cards are discreetly mailed worldwide using priority mail, with tracking numbers. Upgrade to **express shipping for an additional \$15**. Same day

# Zero Squad & Safe Drop



**Zero Squad - Euro & USD Counterfeits**  
Save & Trusted Euro & USD Counterfeits

Hello guys,  
We're a dutch group of professionals and started since 15/12/2013 with counterfeiting.

We offer **20/50/100 Euro & USD bills** of good quality, Cotton, micro-print, provided with watermarks, security thread, pass pen test, etc. These are made with exactly the same quality as the Federal Reserve use to make genuine currency.

**EURO's**

For amounts under 500 euro, every euro bill, costs 40% off its value		For amounts under 2000 euro, every euro bill, costs 30% off its value	
Value	Price	Value	Price
80 euro	32 euro	740 euro	225 euro
100 euro	40 euro	1000 euro	300 euro
200 euro	80 euro	1500 euro	450 euro
500 euro	200 euro	2000 euro	600 euro

We can also make bigger proportion. Please ask us for larger quantities

**USD's**

**SAFE DROP ONLINE DRUG STORE**

Home | FAQs | Contact | Shopping Cart | Log Out

[Buy Cocaine](#) :: [Buy Amphetamine](#) :: [Buy Weed](#) :: [Buy Hash](#)

Login

Please login to view our products.

Username

Password

Login

Dont have an account, Register [here](#)

**SAFE DROP ONLINE DRUGSTORE**

SAFE DROP online Drugstore providers Cocaine, amphetamines, weed and hash. We pride ourselves on the high quality of our products. We send orders from the country of production, ensuring that quality of the wares is high.

Our orders are shipped discreetly and securely so that the goods are not detectable. If for any reason the order does not arrive, we will ship a replacement no questions asked.

Login now and find out our products and prices.





**Cebulka**  
Forum sieci onion

[?](#) [FAQ](#) [SZUKAJ](#) [UŻYTKOWNICY](#) [GRUPY](#) [PROFIL](#) [PRYWATNE WIADOMOŚCI](#) [REJESTRUJ](#) [LOGUJ](#) [WYLOGUJ](#)

[Cebulka Strona Główna](#) » [Cebulka](#) » [English Zone](#) » [English Subforum](#) » [International Hitman Service LEGIT](#)

[Poprzedni temat](#) « [Następny temat](#)

International Hitman Service LEGIT	
Autor	Wiadomość
<b>ufs 1</b>	<p>Wysłany: - <b>International Hitman Service LEGIT</b> <span style="float: right;">[Cytuj]</span></p> <p>Posty: 1</p> <p>English only please. All info here: <a href="http://lw4ipk5choakk5ze.onion/raw/5432/">http://lw4ipk5choakk5ze.onion/raw/5432/</a></p> <p>for the case of downtime, here is the direct email adress: <a href="mailto:unfrndlysltn@safe-mail.net">unfrndlysltn@safe-mail.net</a> PGP key: -----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v2.0.21 (MingW32)</p> <pre>mQENBFIs5OkBCAC+FWC0mQllyGJu2rJC2NwslIIF0u0vBQjwT2DtSV1hrDET6R/o czhkD2Den5Y7CRJDBvEww3fW18CwxwvTcFKK72m5Ky9soM43Yz4fmGtR.SnMTafx1 28se/nNVNDeporBUVyxQDj7ZlrrOBTe7qfbKqqYm7OwWzM2lQsWyyIMVHPMV3/y 34FdhFpQSRkzpcY2s89uZTkC0fxP+eB3tdXKedM3kQj/M1cqI6b1mJQTaQdnMIGC sz2tDu9Aerz+3rSybaYduchnneNOoTI3d2C1x15IfGkzLXtJEdmQJcKNpS+M2jww dF5Mro8COqqQs4sfbGQRZRwL7SouaRpCHarDABEBAAG0L1VuZnJpZ2W5kbHlzb2x1 dGlvbiA8dW5mcm5kbHlzbHRuQHhZmUtBWFpbC5uZXQ+IQE5BBBMBAGAjBQJSLOTp AhsDBwsJCAcDAgEGFQgCCQoLBBYCAwECHgECF4AACgkQfsZepm5QL5KFxAf8D7ST +2HL+Tho6p/0KoxuFcpM+Q0tEH2WAb8OMnxVuVHp+uvu+PuZ3u64e2wq3x9aa8sh qCD9xLgdJkqH1CAZ6XamPz8bkMp3R6ZF6XhPTY8feCpl5qAjBhIwcHaw57u85SdY RRW+m+UTxTFEfpG8cDSNgSf0H3ovCV58UoTr2JFvird7lI2EchTEvgd0mdBQwVFD +TAV7ZaQ95yvfGfKlgGPUOrMkgNXJcQTI+gQyDfinmgEQAzx2M8aqKe7jivZj209 Vl5nhyhSh44r9rwbzrFN7RghQL5vC+q01gpvpbbzoiyFL0/Bz0VHEvGHI688ZxGw 9PQHbz9yglal0LF1Qe7kBDQRSLOTPAQgAu79z8F127BL09YeeJYcyO/5Nv06x9LNI oJ2lecpEDkBBHG30Ckut5iDZayhPGzFJA2T1hjx81QzIHUyd19kz8M2o0RPv4Omz xof7WoNnxU8/q9wFzow2a4/YeCD3S7qsB63TyptO+MOTFJILkiubvYX/+QqAdv DBHEhTKI2Xckz92eM3kGsW3+P×2aaKaGrTPd9JunyTVkpT/YV4A7IokuJWFezHY+</pre>

# The Challenge of Defining Security

# What do we mean when we say “Security”?

Denotation? Connotation? Some commonly used phrases to describe security:

“Personal, private or public **protection**”?

“Providing a **level of defense** for a target of high value against aggressors.”?

“LIFE, Property, Knowledge. Freedom”?

“Being prepared to lessen or eliminate the effect of unwanted events.”?

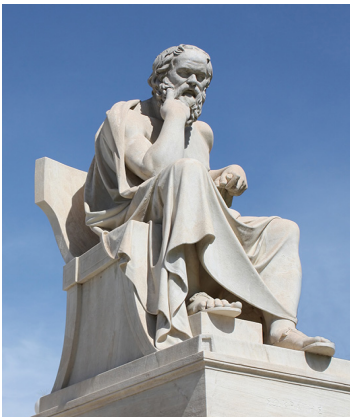
“**Protection** from vulnerabilities and actions to reduce risk of comprises.”?

“Ensure **confidentiality**, integrity and availability of systems and data”?

*“...in the absence of agreed definitions the concept of security means different things to different people in different contexts.”* Manunta, Giovanni. “What is Security?”:Security Journal. 1999 Pg. 57-66

What is “F-Ness”? If you don’t know then:

- You can’t know if something is or is not “F”
- Can’t describe the characteristics of “F-ness”
- Can’t tell someone how to achieve “F-ness”



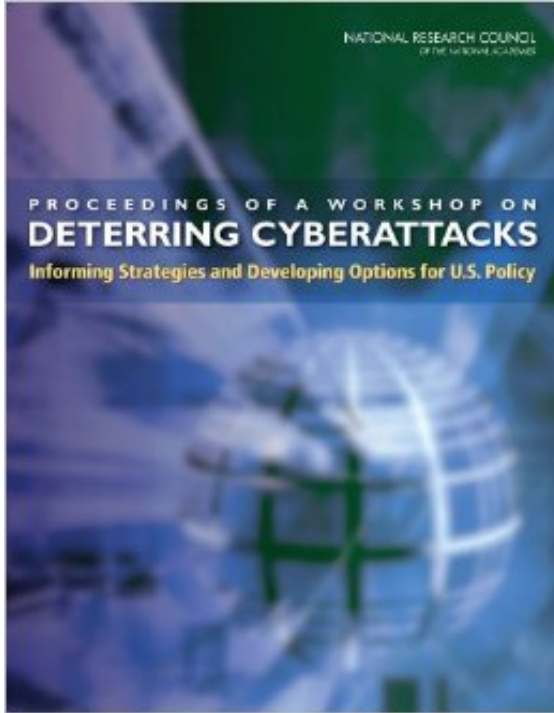
*"I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description ["hard-core pornography"]; and perhaps I could never succeed in intelligibly doing so. **But I know it when I see it**, and the motion picture involved in this case is not that."- Mr. Justice Stewart; Jacobellis v. Ohio, 378 US 184 (1964)*

# Definition Through Negation (apophasis)



*I cannot define what security is through its attributes but I can define security by describing what it is not.*

*Nobody will tell a company when they are secure but are quick to render an opinion after a breach...*



**Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy**

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council  
ISBN: 0-309-16086-3, 400 pages, 8 1/2 x 11, (2010)

*“Given the poor state of cybersecurity, compliance-driven security is at best a qualified failure.”*

– *Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council*

*PCI DSS, FISMA, HIPAA/HITECH, SB1386, NREC, FRPA, ISO27001, MPSA, PA DSS, etc., etc., etc.!*

*“Information Security Professionals”* are really “technology professionals”  
and not “security professionals”

Security is ultimately about predicting and **controlling human behavior** on two sides of a relationship...  
Security describes an Adversarial Relationship

Frequentist Probability Models are ineffective for Adaptive Threats...**Bayesian Probability is a better measure**

Security Professionals in all domains need to understand...

- Rational Actor Model
- Deterrence/Compellence theory
- Threat Adaptation
- Threat Asymmetry
- Parallax and Convergence
- Change Blindness
- Proximate Reality
- Defense in Depth
- Conditional Probability
- Etc.!!

*“..includes threats intentionally caused by humans.”* It further states that Adaptive Threats are: *“...caused by people that can change their behavior or characteristics in reaction to prevention, protection, response, and recovery measures taken.”* – DHS Lexicon, 2010

According to Pimmerman, an Asymmetric Threat must meet three criteria. These have been modified for our purposes and include:

1. It must involve an exploit, tactic or strategy that the adversary both could and would use against an organization
2. It must involve an exploit, tactic, or strategy that the organization would not employ against the adversary
3. It must involve an exploit, tactic, or strategy that, if not countered, could have serious consequences



# Is this a Valid Statement? (hint..Hindsight Bias)

 ZDNet  
VIDEOS SMART CITIES WINDOWS 10 CLOUD INNOVATION SECURITY TECH PRO MORE  
MUST READ: CYBERSECURITY AS BIG A CHALLENGE AS COUNTERTERRORISM, SAYS SPY CHIEF  

## Over 90 percent of data breaches in first half of 2014 were preventable

The Online Trust Alliance says that a high percentage of data breaches were the result of staff mistakes -- rather than external hacking.

 By Charlie Osborne for Zero Day | January 21, 2015 -- 13:15 GMT (05:15 PST) | Topic: Security

Over 90 percent of data breaches in the first half of 2014 could have been prevented if businesses rethought their risk cyberstrategies, according to the Online Trust Alliance.

The [Online Trust Alliance](#) (OTA), a non-profit geared towards enhancing online trust and assisting businesses in their best practices and risk assessment, released its 2015 Data Protection Best Practices and Risk Assessment Guides on Wednesday. The organization says that in January to June last year, only 40 percent of data breaches involving the loss of personally identifiable information (PII) were caused by external intrusions -- while 29 percent were caused either accidentally or maliciously by employees.

OTA says a lack of internal controls, lost or stolen devices and documents, as well as social engineering and fraud were to blame for almost 30 percent of data loss incidents suffered by businesses.

In OTA's Risk Assessment Guide, the organization asks questions that IT decision makers must ask themselves if they are going to assess the risk of business practices against cyberthreats. Not only does a modern-day business have to ask if its own security practices are up to scratch, but whether third-party vendors -- such as those in the supply chain or providing outsourced IT services -- constitute a threat to security.

Some of the questions corporations need to ask themselves are detailed below:

- Do you understand the international and local regulatory requirements and privacy directives related specifically to your business based on where the customer or consumer resides?

*“Felix qui potuit  
rerum cognoscere causas”*

“blessed accomplishment theirs, who can  
track the causes of things” -Virgil; 420 BC

*“...at current spending rates, companies are only addressing 68% of vulnerabilities. To achieve 95% protection, companies would need to increase spending by 700% from \$30.8 million to \$270.9 million.*”

Ponemon Institute; 2012

*“Today, the PCI process takes up to 55% of the total data security budget for retailers...”*

IHL; 2015

# Which would you rather have?



## Malicious Insiders

- **Strengthen Your Security Foundation**
  - Focus your team on the basics first
- **Make Security Everyone's Responsibility**
  - Employee training helps turn employees into a malicious insider early warning system
- **Break Down Organizational Silos**
  - Demand security teams have full access to all data and records in all departments and divisions
- **Invest in Behavioral Analytics**
  - Big Data tools can help sniff out activities by malicious insiders

## Unintentional Insiders

- **Train Your Users**
  - Offer mandatory security awareness courses
- **Share the Security Responsibility**
  - Follow ISO 27001 to create a steering group
- **Employee Buy-in for Security Starts at the Top**
  - Lead by example
- **Enforce the Rules**
  - Enforce security training efforts with prompt and highly visible enforcement of your security policies
- **Don't Ban Shadow IT, Manage It**
  - Find out why business units buy cloud services and secure them
- **Evaluate and Monitor Your Suppliers**
  - Assess their security and compliance practices before and while doing business with them

Source: AT&T Cybersecurity Insights Report – Decoding the Adversary Volume <https://www.business.att.com/cybersecurity/docs/decodingtheadversary.pdf>



**AT&T** Business