

# New Threats

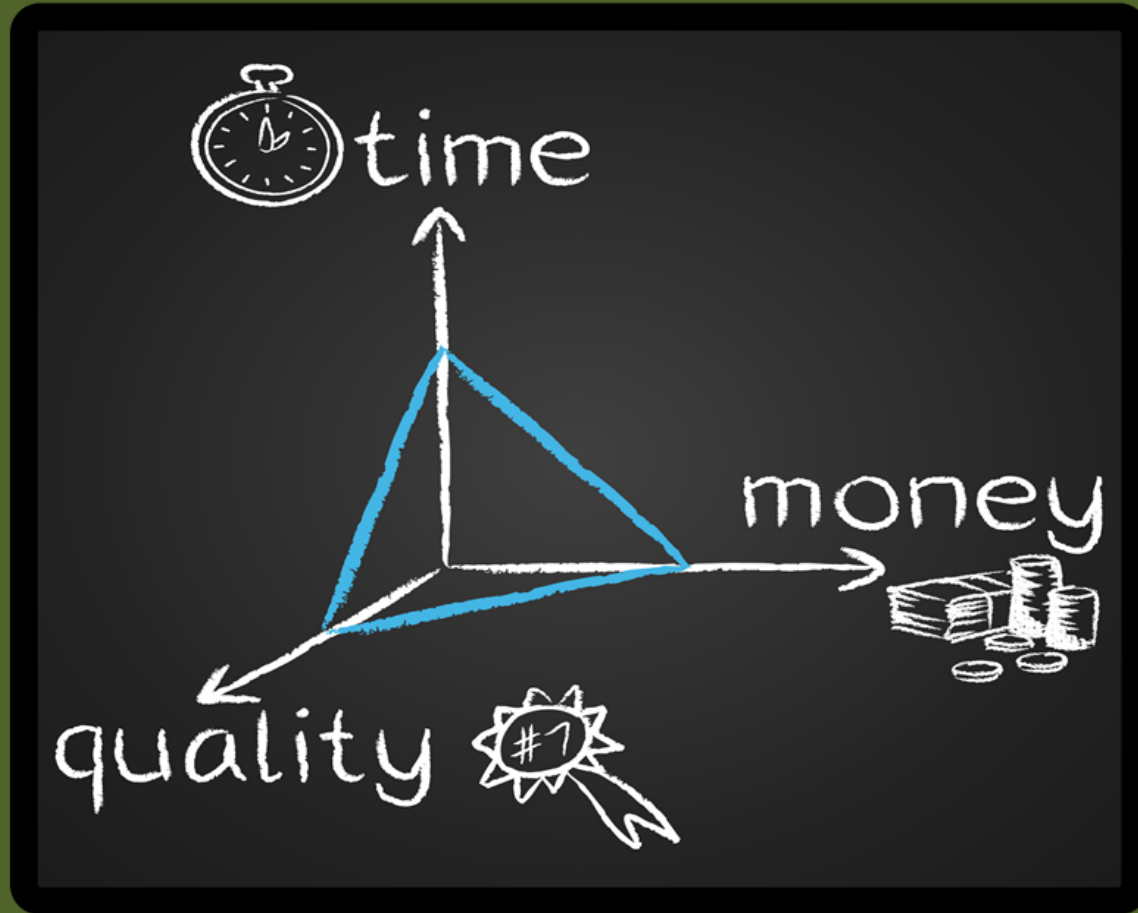
Motivation: What are the new threats?

- Risks.
- Hacktivism.
- Denial-of-Service and Botnets.
- Social Networks and Open Source
- Cloud.



**Prof Bill Buchanan,**  
Edinburgh Napier University

# New Threats?



## Risk

Understanding it ... and communicating

## Understanding Risk



What is ... a threat ... a risk ... a vulnerability ... the motivation?

- Wide range of threats to organisations.
- Organisations now highly dependent on their information infrastructure.
- Real-time threat analysis needed to cope with threats.

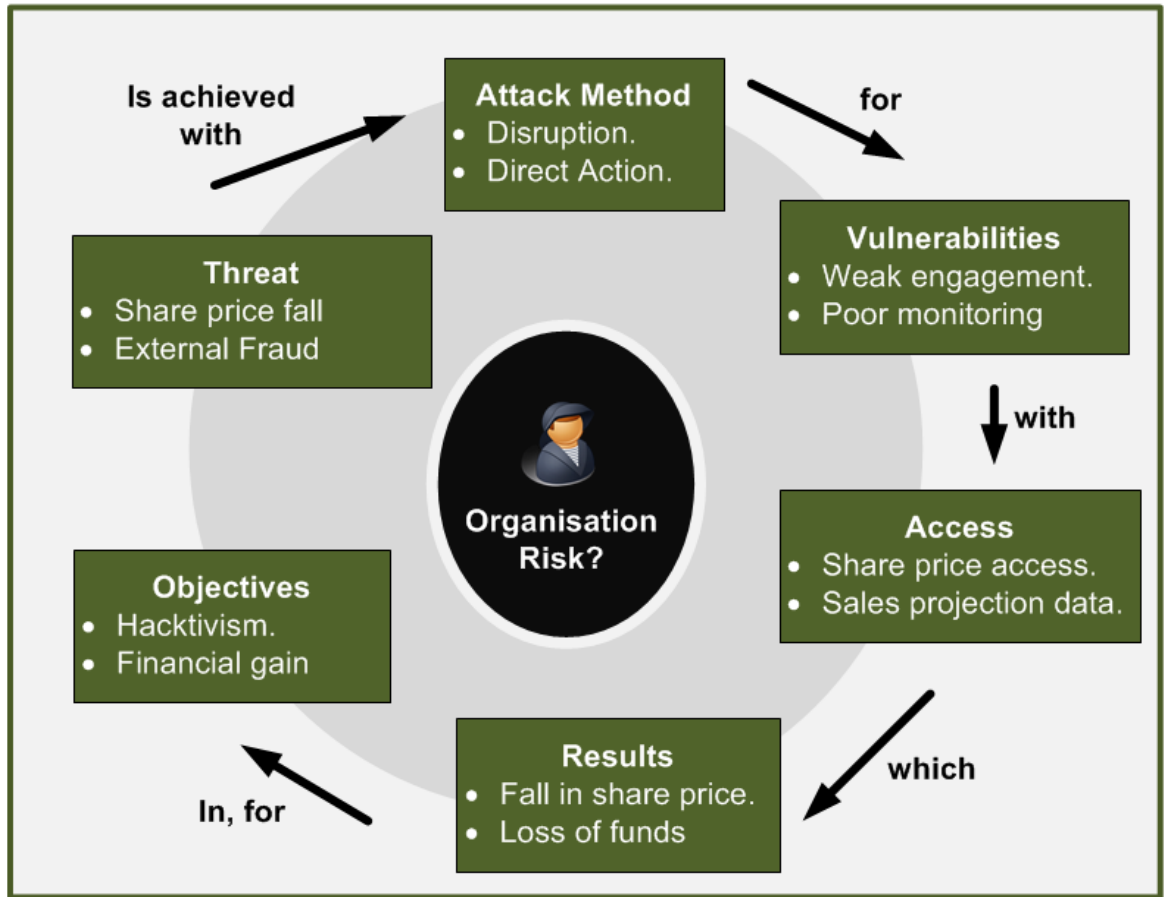


## Understanding Risk

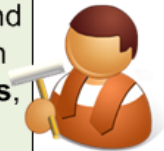


What is ... a threat ... a risk ... a vulnerability ... the motivation?

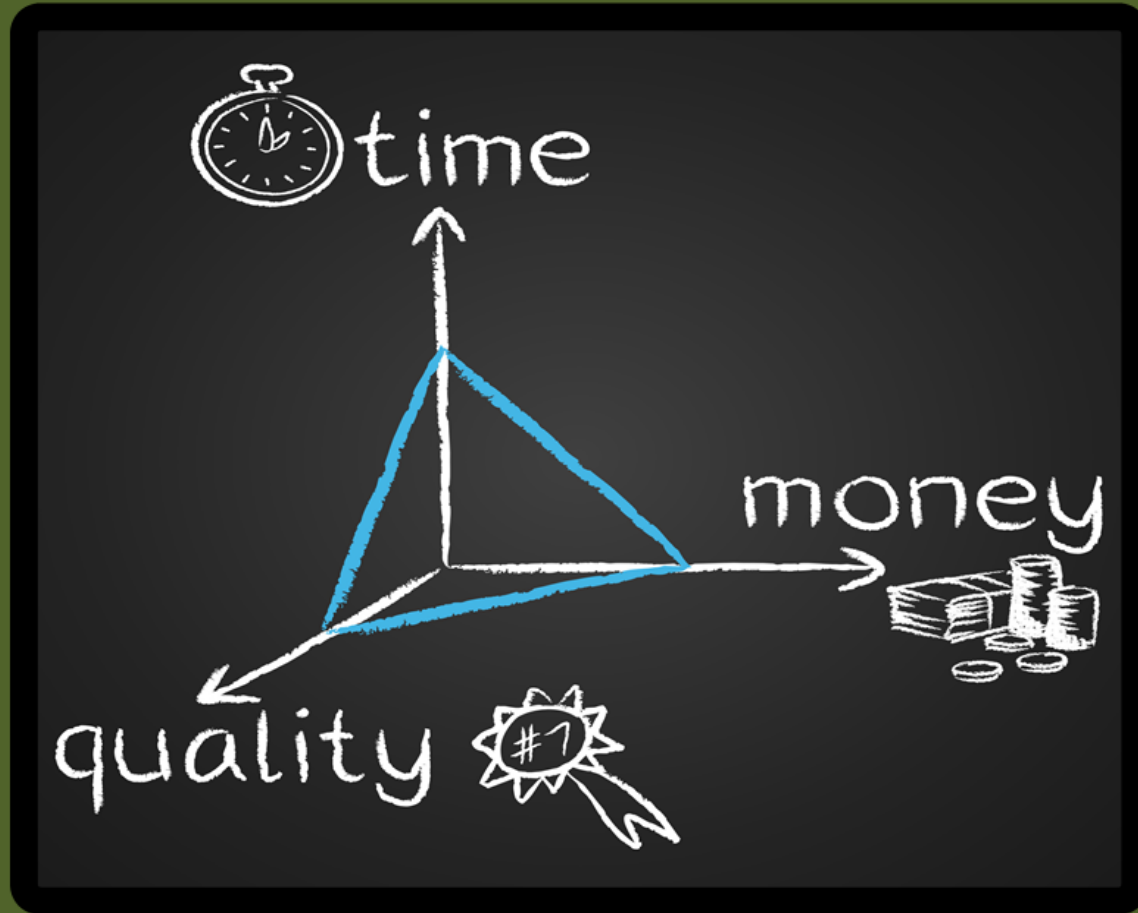
- Risk Taxonomy/Ontology required within the organisation.
- Business and Technical staff struggle to communicate on risk.



Get two risk management experts in a room, one financial and the other IT, and they will NOT be able to discuss risk. Each has **different context ... different vocabularies, definitions, metrics, processes and standards** (Woloch, 2006)



# New Threats?



## Hacktivism

A Threat to Society and Organisations

### A cause or a fight?



Who? ... Why? ...  
Where? ... When?

- One person's freedom fighter is another's terrorist.
- One person's cause is another person's fight.

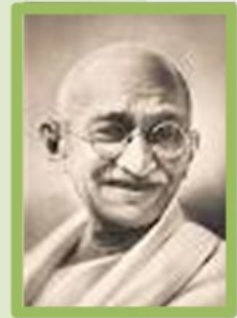
Martin Luther King



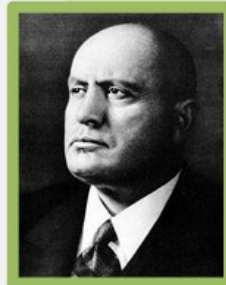
Che Guevara



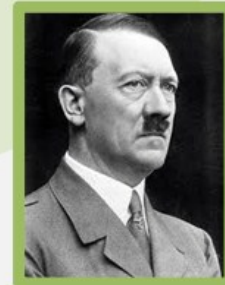
Dalai Lama



Mahatma Gandhi



Benito Mussolini



Adolf Hitler

# Hacktivism



Who? ... Why? ...  
Where? ... When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?

## 2012

- Anonymous focus on India on censorship.
- Virgin Broadband over PirateBay block.
- SOCA (Serious and Organised Crime Agency) over arrests, also Norwegian Lottery and Bild.
- Home Office sites over Gary McKinnon case.

## 2010, Mastercard and Visa

- Why: Decision to stop processing payments to the whistle-blowing site Wikileaks,
- Result: DDoS attacks on Visa, Mastercard, om.nl and politie.nl

## 2011, Tunisian government websites

- Why: Censorship of the Wikileaks documents
- Result: DDoS attacks against sites. Some Tunisians assisting in these attacks.

## 2009. Climate Research Unit of East Anglia University

Why: Emails published showed conspiracy to suppress data that contradicted their conclusions on global warming (Russian FTP server)

## 2011, HBGary

Why: HBGary were going after Anonymous  
Reward: Emails published, Web site defaced.

## 2010, Australian Government.

Why: Australian Government's attempt to filter the Internet.

## 2012. Department of Justice and the FBI.

Denial of service attack

## 2011. Sony's PlayStation Network.

- Why: Sony were suing Geohotz, who jailbroke the PlayStation 3.
- Result: Afterwards, a group of hackers claimed to have 2.2 million credit card numbers from PSN users for sale





# Hacktivism



Who? ... Why? ...  
Where? ... When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?

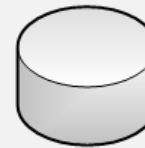


**HBGary Federal CEO  
Aaron Barr to unmasked  
Anonymous with a list  
HBGary contacts with NSA,  
Interpol, McAfee, and many  
others**



**Hbgaryfederal used CMS  
and comprised by:**

<http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27>



**Username, passwords  
(stored as hash values),  
email database**



**"ranger12"**

**"martin12"**



**CEO Aaron Barr and COO Ted  
Vera had weak passwords (six  
characters and two numbers) –  
which were easily broken**

**Passwords broken by  
Rainbow tables**



**Passwords found for CEO and COO**



# Hacktivism



Who? ... Why? ...  
Where? ... When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?



“ranger12”  
“martin12”

CEO Aaron Barr and COO Ted Vera used the same password for a range of systems: Twitter, email, Linked in, and so on.



Support.hbgary.com



Remote login to support.hbgary.com from Ted Vera's account



Flaw exploited in system to escalate privilege



Gigabytes of research and backup data

Aaron was a System Administrator for their Gmail Apps Hbgary account



Complete control of company email

# Hacktivism



Who? ... Why? ...  
Where? ... When?

- Use strong passwords.
- Never re-use passwords (30% of users do).
- Patch systems.
- Watch out for social engineering.
- Beware of unchecked Web sites.
- Get an SLA from your Cloud provider.
- Don't store emails in the Cloud.
- Restrict access from outside.



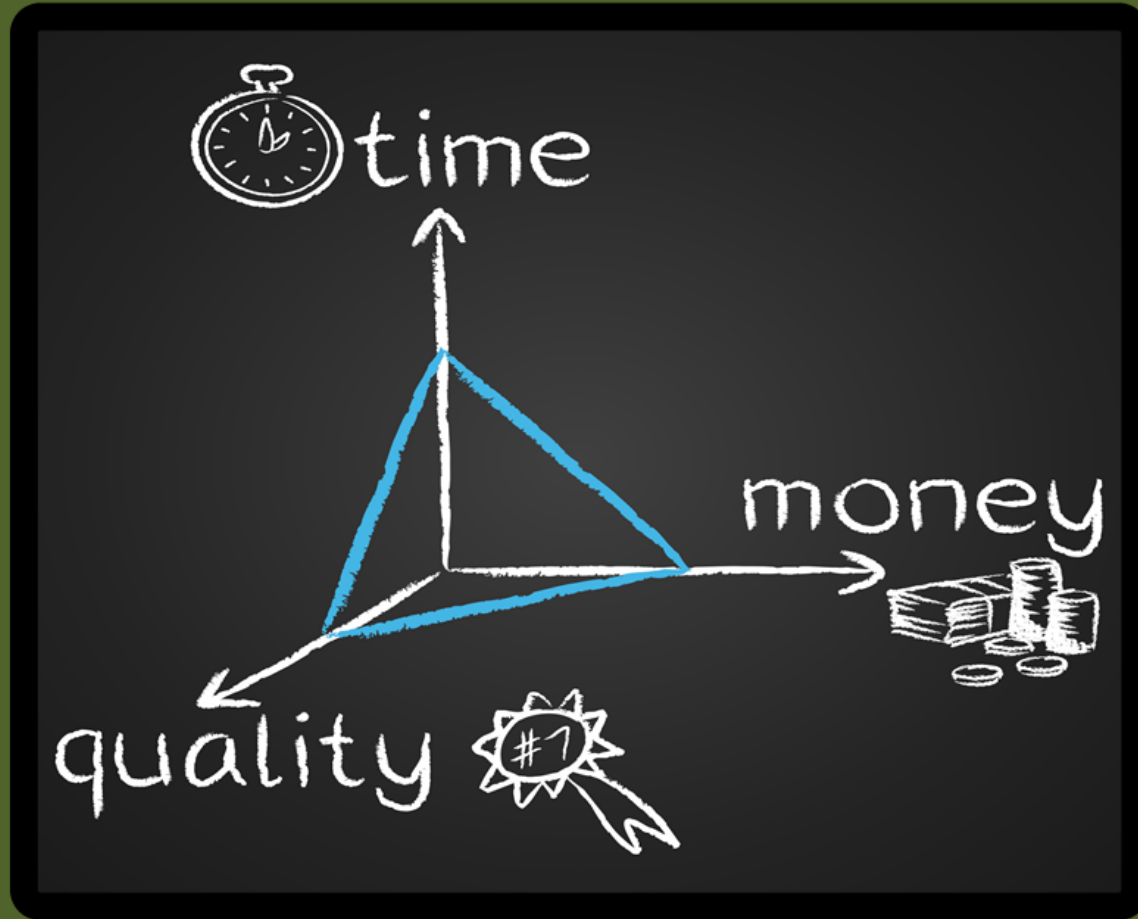
Now for another site owned by Greg Hoglund, owner of HBGary

Social Engineering ... to gain root password for Greg's site



Web site taken offline and user registration database published

# New Threats?



## Denial-of-Service and Botnets

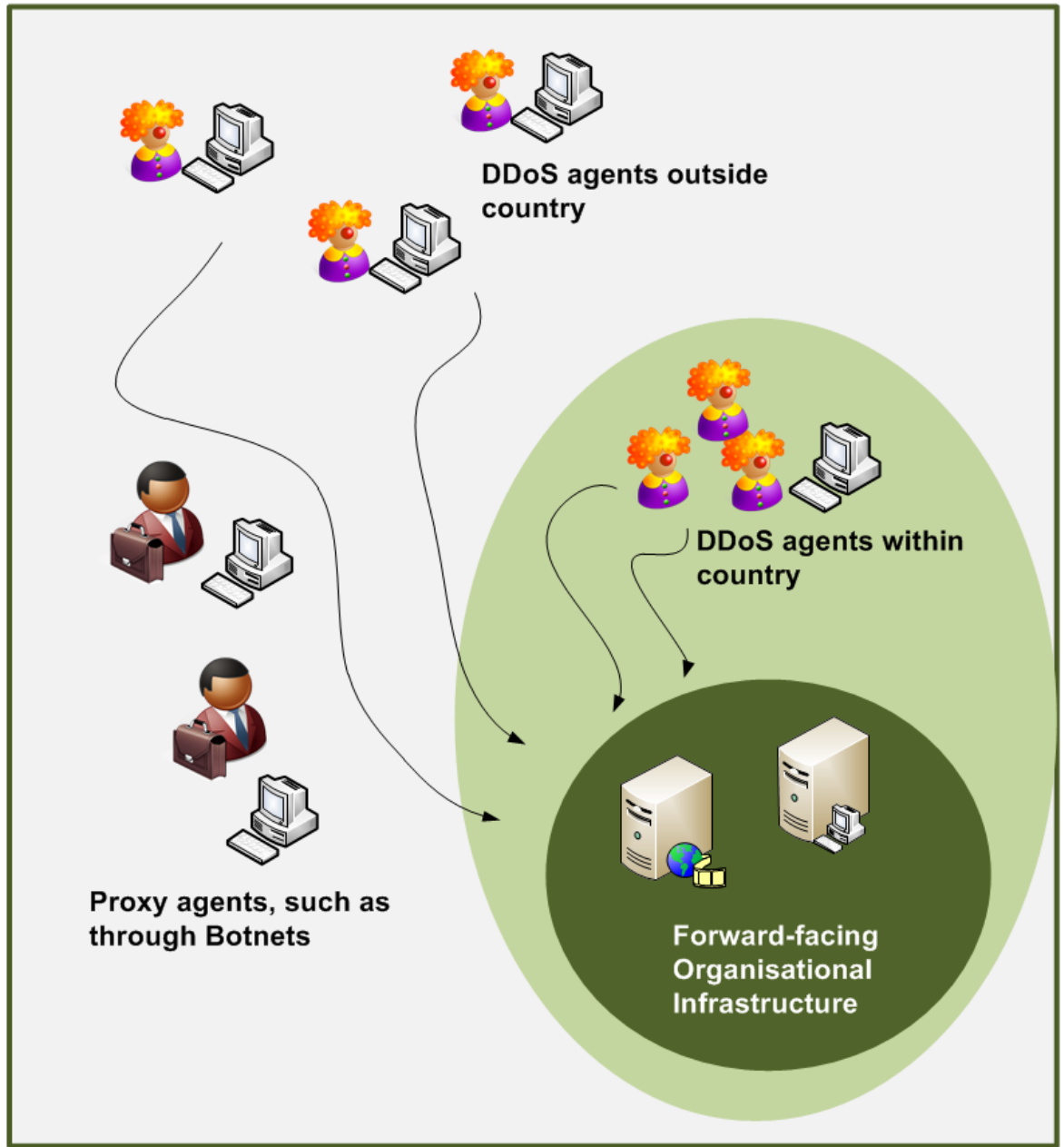
Distributed Threats

### Denial of Service



Who? ... Why? ...  
Where? ... When?

- DDoS is difficult to defend against.
- Agents often exist outside the country.
- Agents often use proxy agents to perform attack.



# Botnet



The army of evil

A study of Torpig over 10 days found:

- 180,000 infections and gathered over 70 GB of data.
- More than 1.2 million IP addresses which contacted the command and control server.
- 8,310 accounts at 410 different institutions, included 1,770 PayPal account, with 1,660 unique credit and debit card numbers.

Control by proxy

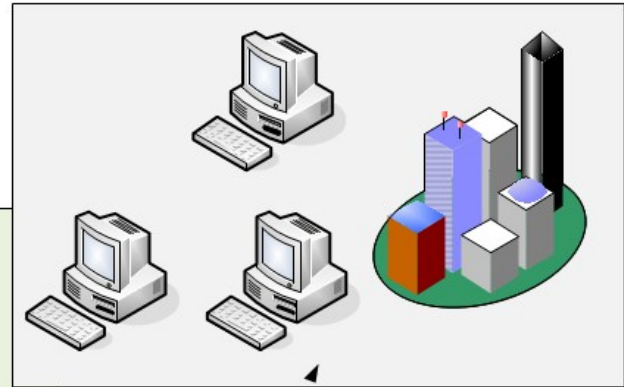
Botnet

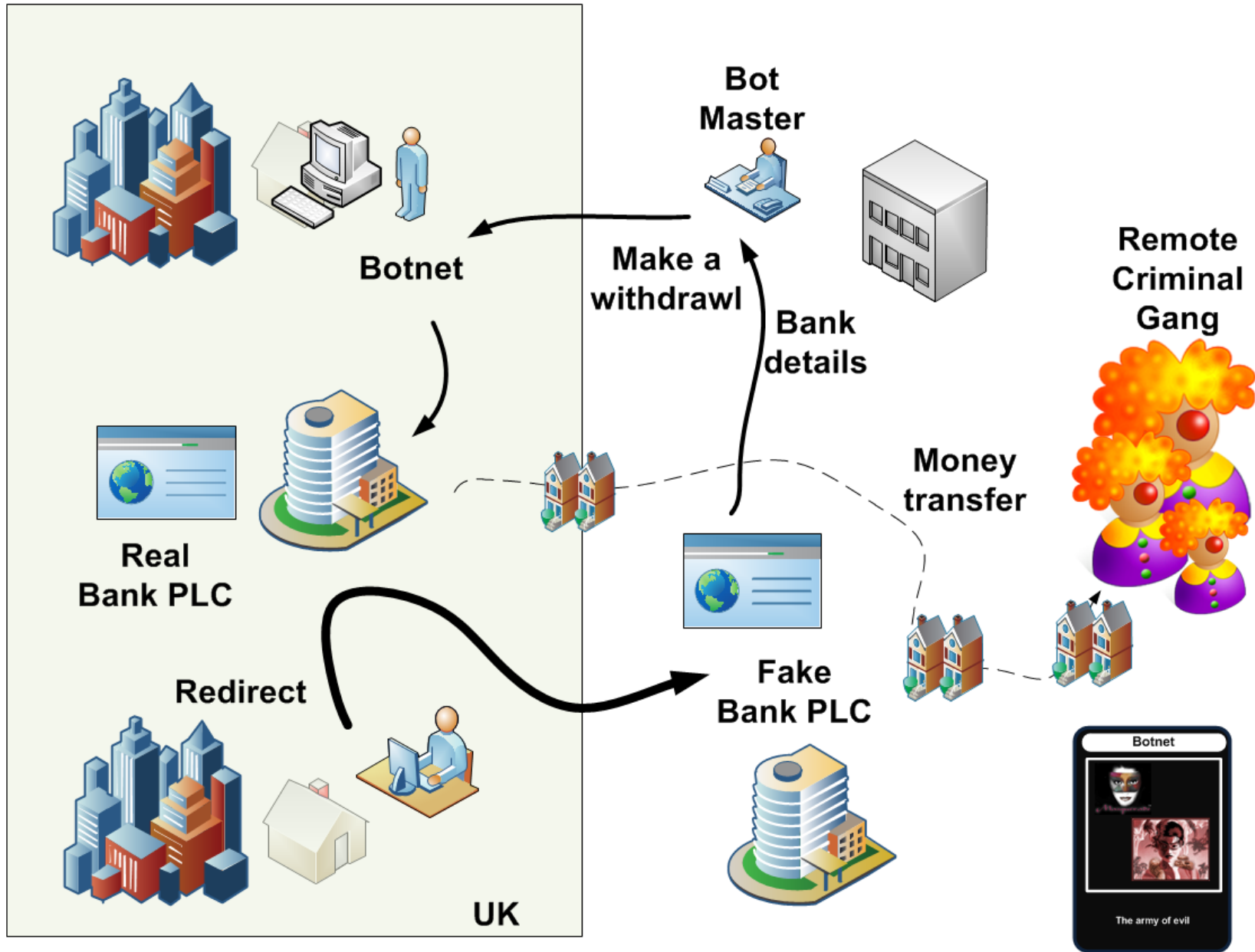


Botnet access

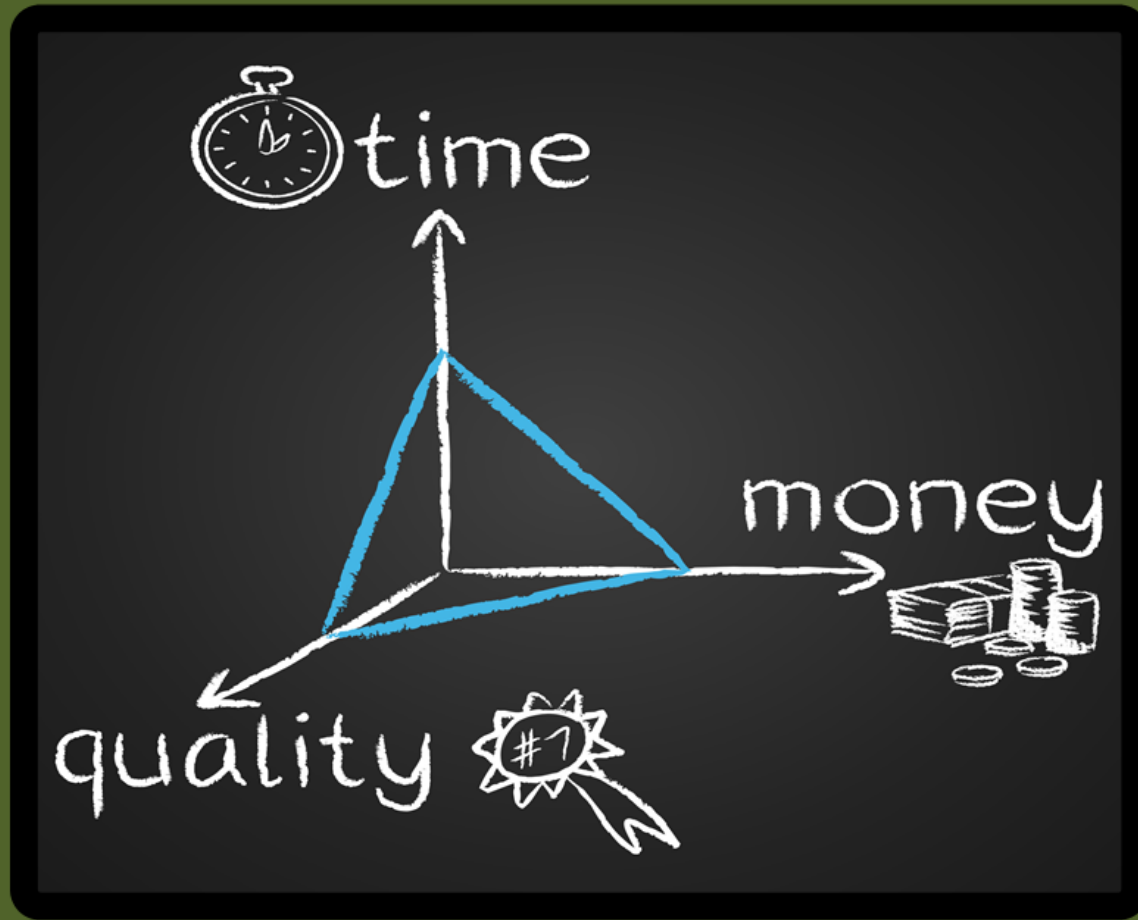
Botnet command

Bot Master





# New Threats?



**Social Networks and Open Source**  
A Real-time Threat



## Social Networks



Data Leakage ... and what are people saying about us?

- Open Source Information can often lead to IP Theft.
- Threats against brands and organisations can occur within short time intervals.

### Twitter and Facebook

- Company profile.
- IP Leakage.



### “XYZ Sucks” Sites

- Bad reputation.
- IP Leakage.

### Blogging

- Bad sentiment against brands and organisations.



Organisation Risk?

### Poor Affiliate Selling

- Bad reputation.
- Fraud.

### Google Hacks

- IP Theft.
- Company Documents.

### Rallying Calls

- Fast rallying against brands/organisations.



... increasing **brand awareness** and **improving brand reputation** are often the two main objectives for social media marketing .. So beware of the flip-side ... negative sentiment.



## D: e-Perception

- Twitter activity.
- Semantics of external activity.
- Bulletin board activity.
- Blogging activity.
- Geographical presence analysis.

### Analysis:

- Twitter Feed rate.
- Semantic Analysis (+2 – foreclosure, loss, attack. fraud ☹; +1 – bad/won't, -1 – good, help, kind -2 - ☺).
- Retweeting activity.
- Geographical Analysis.
- Weighing factors for key domain players (eg BBC).



**Huffington Post** @HuffingtonPost  
Bank of America returns foreclosed home to mother with disabled daughter [huff.to/LyHGU1](http://huff.to/LyHGU1)

Expand

6h



**Bank of America** @BofA\_News  
#BofA passes 10 mln #mobilebanking customers, marking growth of nearly 3 mln active users in the past year: [go.bofa.com/38u5](http://go.bofa.com/38u5)

Expand

23 May




**CNBC** @CNBC  
BayernLB sues Bank of America over losses on hundreds of millions of dollars of countrywide mortgage debt it bought. --Court Filings

Expand

22 May

**Respected sources**

**Black list**



**The Onion** @TheOnion  
NEWSWIRE: Man Who Just Received Complimentary Daffy Duck Checks Can't Stay Mad At Bank Of America [onion.com/MCDntN](http://onion.com/MCDntN)

Expand

25 May



**ThinkProgress** @thinkprogress  
Occupy protesters help Los Angeles woman + disabled daughter save their home from Bank Of America [thkpr.gs/Jsecvu](http://thkpr.gs/Jsecvu)

Expand Reply Retweet Favorite

25 May



**Adryan** @Adryan711  
Bank Of America is the worst bank ever!

Expand

24 May



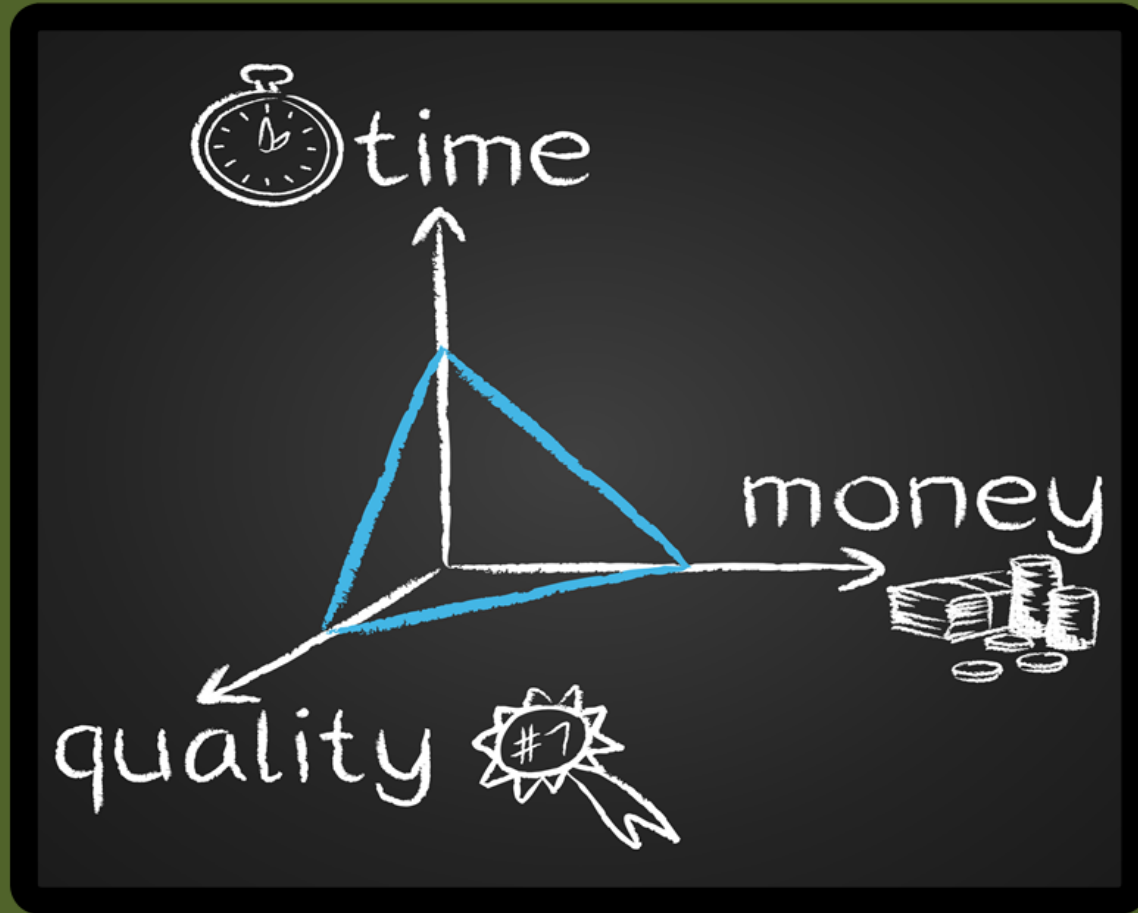
**Action** @BoneKnightmare  
Bank Of America Apparently Doesn't Want Credit Card Customers Who Pay Their Cards Off [bit.ly/KgYRuu](http://bit.ly/KgYRuu)

Expand

19 May

**Other sources**

# New Threats?



## Cloud and Data Leakage

Where's my Documents?

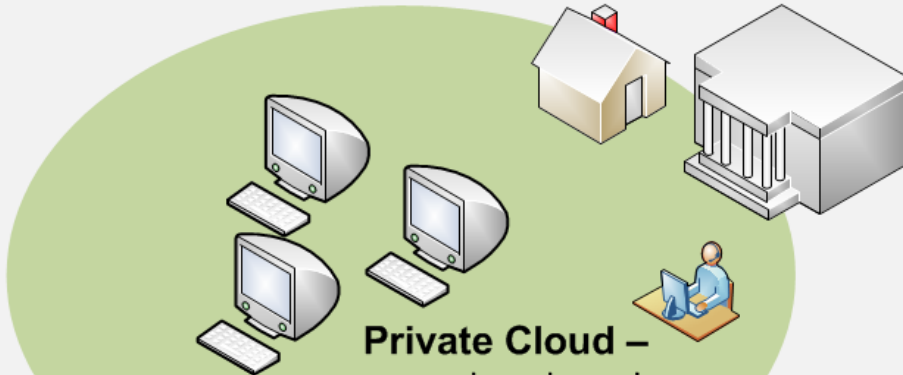
## Clouds

RISK

Where is my data?  
Where is my servers?  
Where are my people?

Can I be compliant with statutory and regulatory requirements?

- Where is my data stored?
- Who handles breach notifications?
- How long is my data stored for?
- How is eDiscovery handled?



**Private Cloud** – owned and run by an organisation



**Public Cloud** – owned by an organisation selling a cloud infrastructure



Dropbox



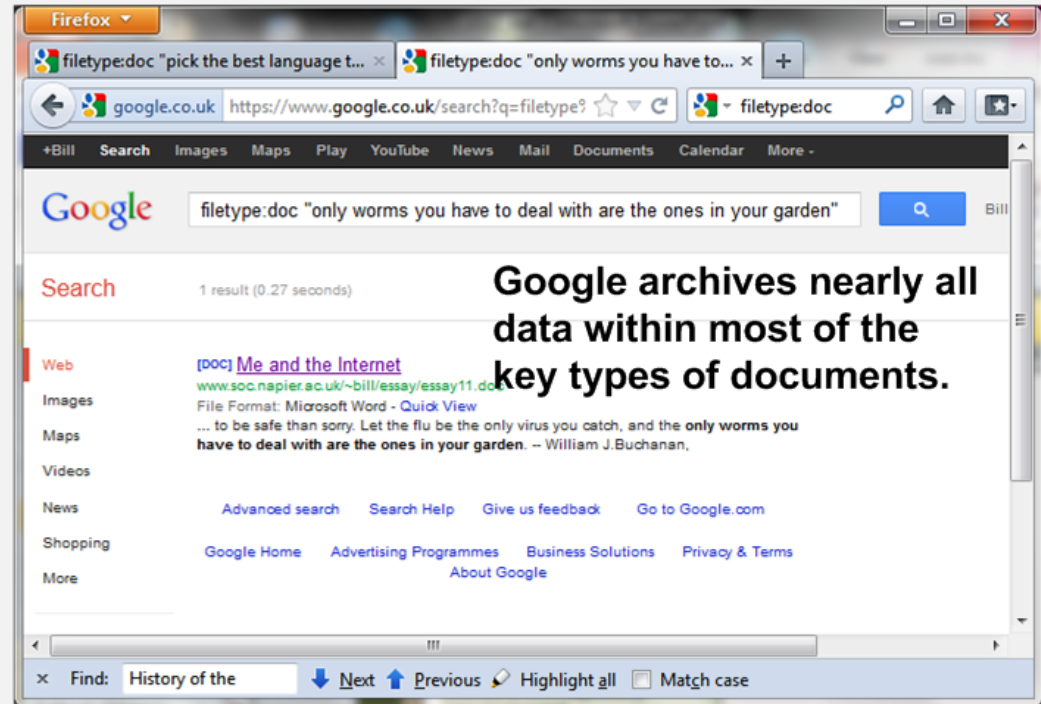
**Sharing Applications**

## Clouds

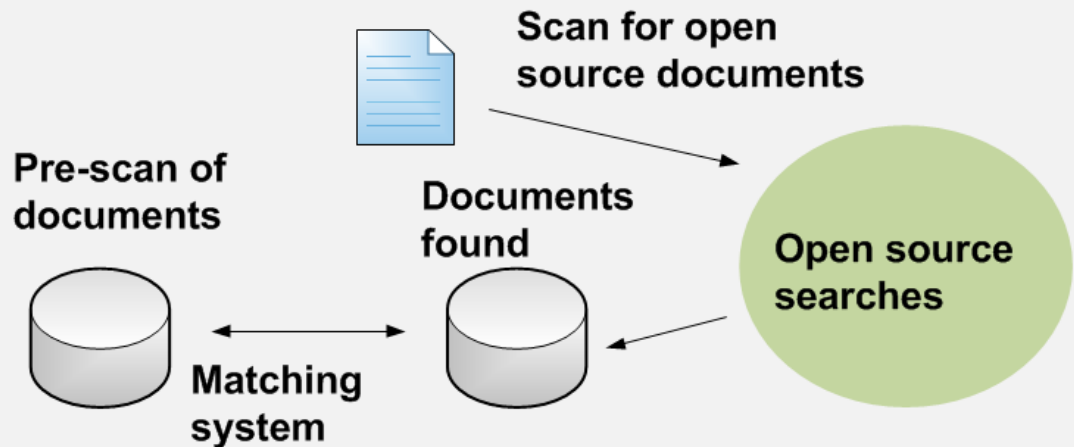
**RISK**

Where is my data?  
Where is my servers?  
Where are my people?

- Document markings are important.
- Proactive methods required for scanning open source.
- Watermarking required.
- Scanning of on-site documents required to match and documents found.



**Google archives nearly all data within most of the key types of documents.**



# New Threats

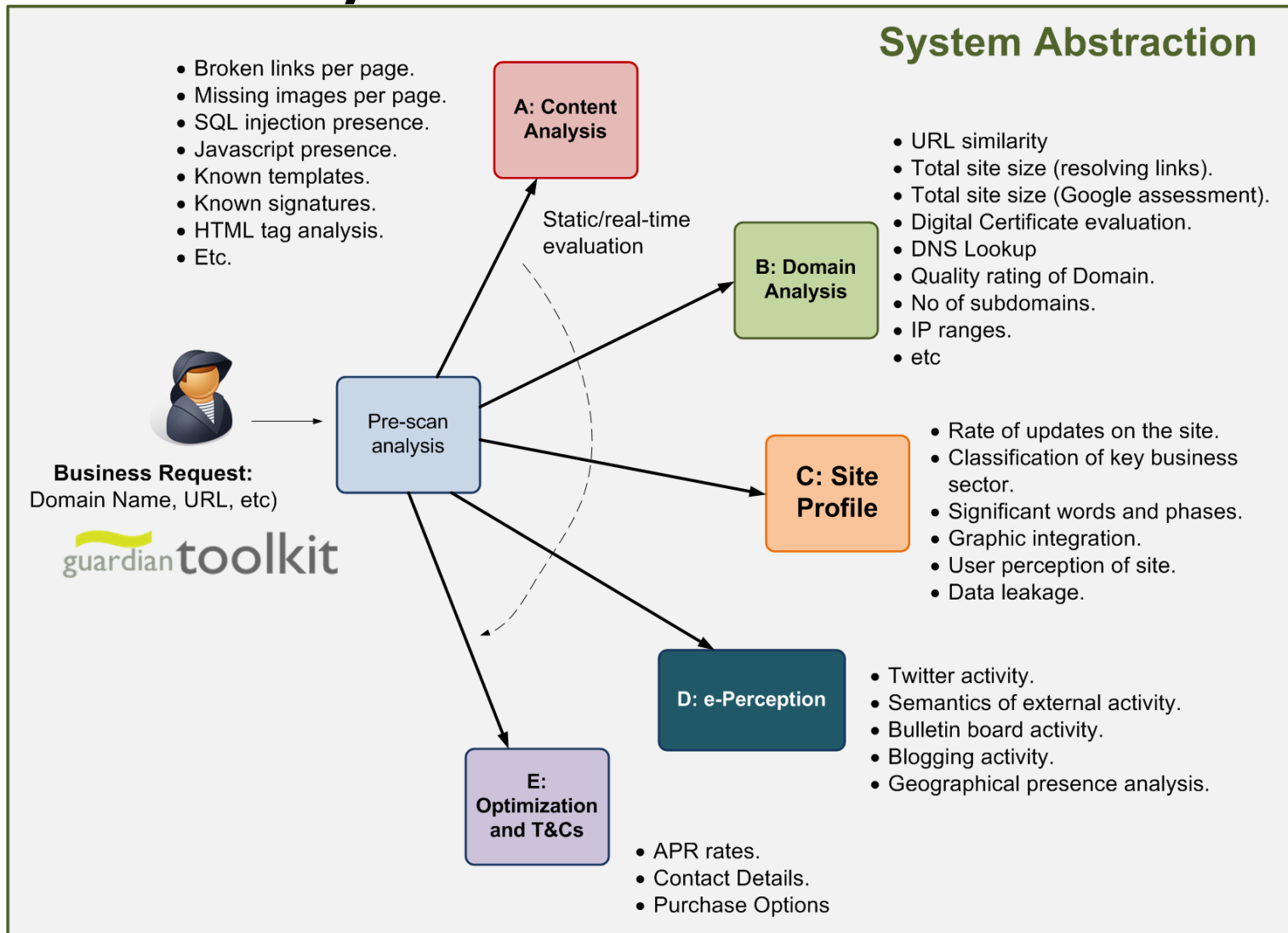
Motivation: What are the new threats?

- Risks.
- Hacktivism.
- Denial-of-Service and Botnets.
- Social Networks and Brand Awareness.
- Cloud.



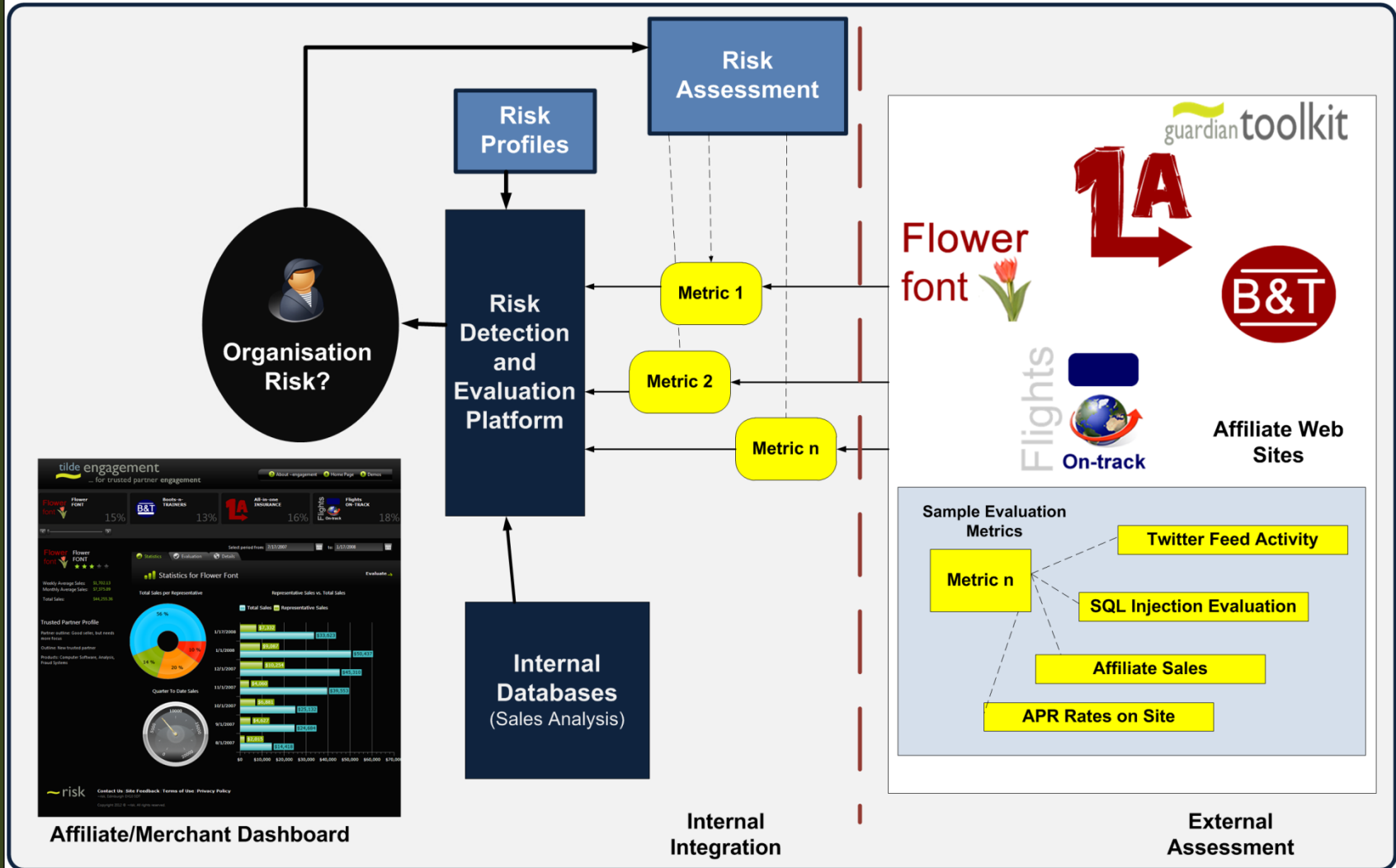
**Prof Bill Buchanan,**  
Edinburgh Napier University

# System Abstraction





# System Overview



# Our Risk Model

