(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

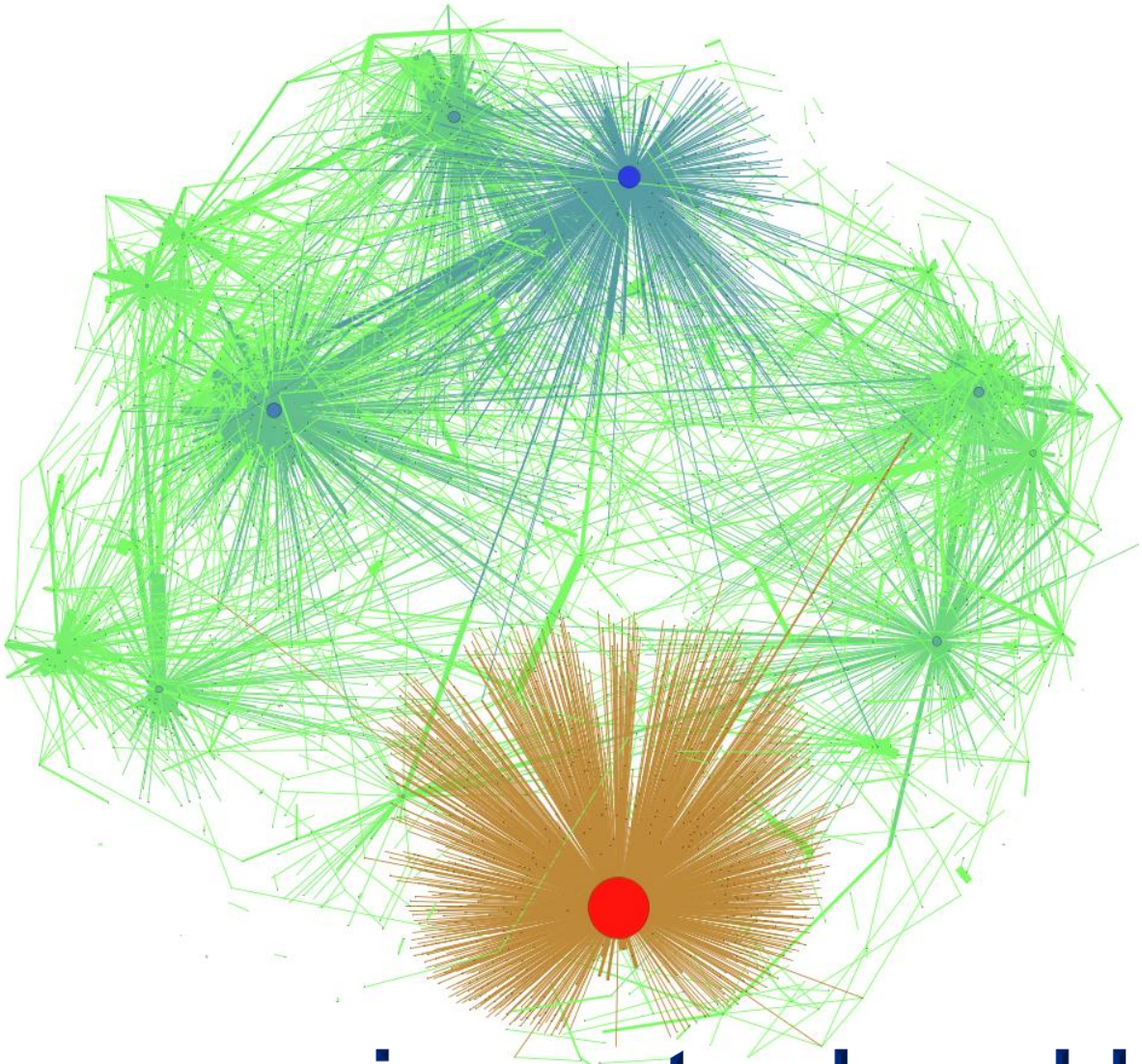
SecureNetherlands

Managing Risk in an Ever-Changing Threat Landscape

Maximum Overdrive…

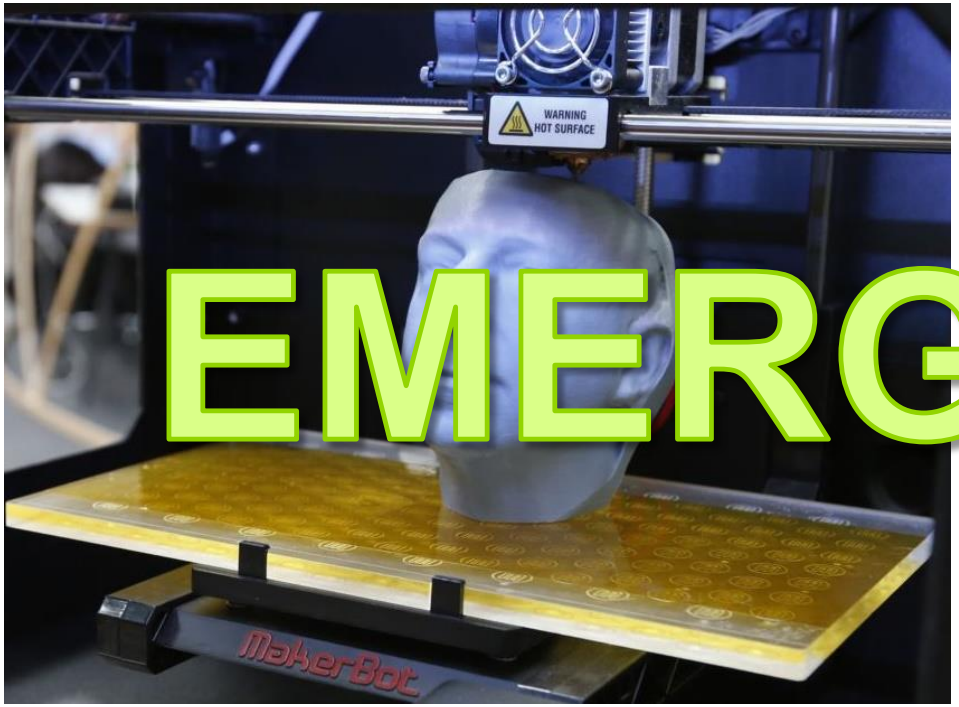
Reframing Cyber Risk in the Age of the Singularity

Pervasively interconnected…

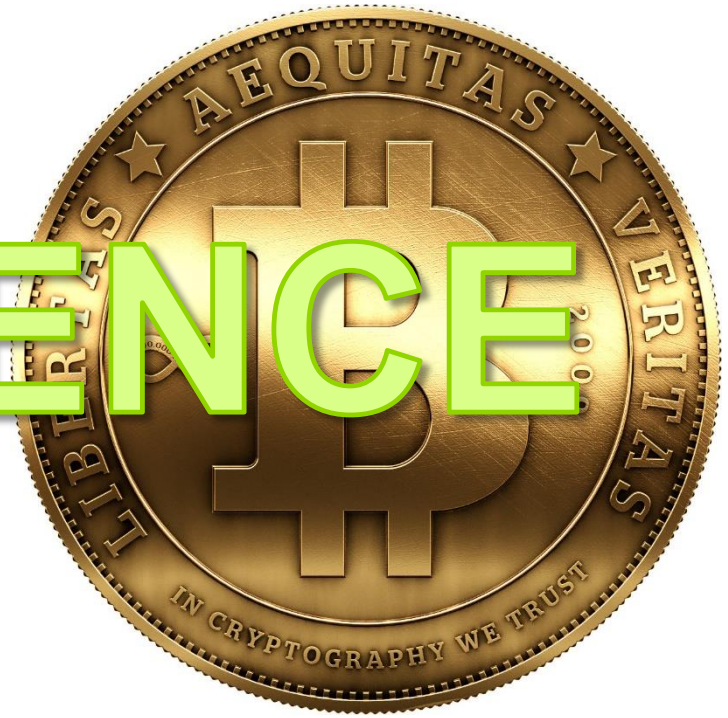


empowering, yet vulnerable.

CONVERGENCE



EMERGENCE



Expanding context and complexity

CONTEXT	THEN…
DIMENSIONALITY	Physical 3d world (Euclidian)
GEOGRAPHY	National (U.S./industrialized)
SCALE	Mainframes and home computers
SIZE	Kilobytes…
SCOPE	Specific contexts work/home
TIMEFRAME	One-off incidents
CRIMINAL NATURE	Vandalism / petty crime
INDICATORS	Intrusion (breaking and entering)
PERPITRATORS / ACTORS	Rogue users, thrill seekers, joy riders, adventurers…

Expanding context and complexity

CONTEXT	THEN…	NOW!
DIMENSIONALITY	Physical 3d world (Euclidian)	Distributed (non-Euclidian)
GEOGRAPHY	National (U.S./industrialized)	Global (interplanetary?)
SCALE	Mainframes and home computers	ALL aspects of physical, social, and economic world
SIZE	Kilobytes…	MTPS; petabyte logs
SCOPE	Specific contexts work/home	Pervasive and distributed
TIMEFRAME	One-off incidents	• Persistent threats • Staged attacks • Latent infections
CRIMINAL NATURE	Vandalism / petty crime	Negligence, extortion, organized crime, terrorism, state-sponsored espionage…
INDICATORS	Intrusion (breaking and entering)	Infection, theft, damage, replication, co-option…
PERPITRATORS / ACTORS	Rogue users, thrill seekers, joy riders, adventurers…	Script kiddies, professionals, organized crime, state actors, cyber activists, terrorists, bots…

RSAConference | Where the world talks security

RSA Conference 2015
April 20 - 24, 2015
San Francisco, CA

- 35,000 attendees
- 800 vendors
- 400 sessions

Call to arms…

RSA chief to security pros:
Stop addressing the wrong problems

RSA President Amit Yoran

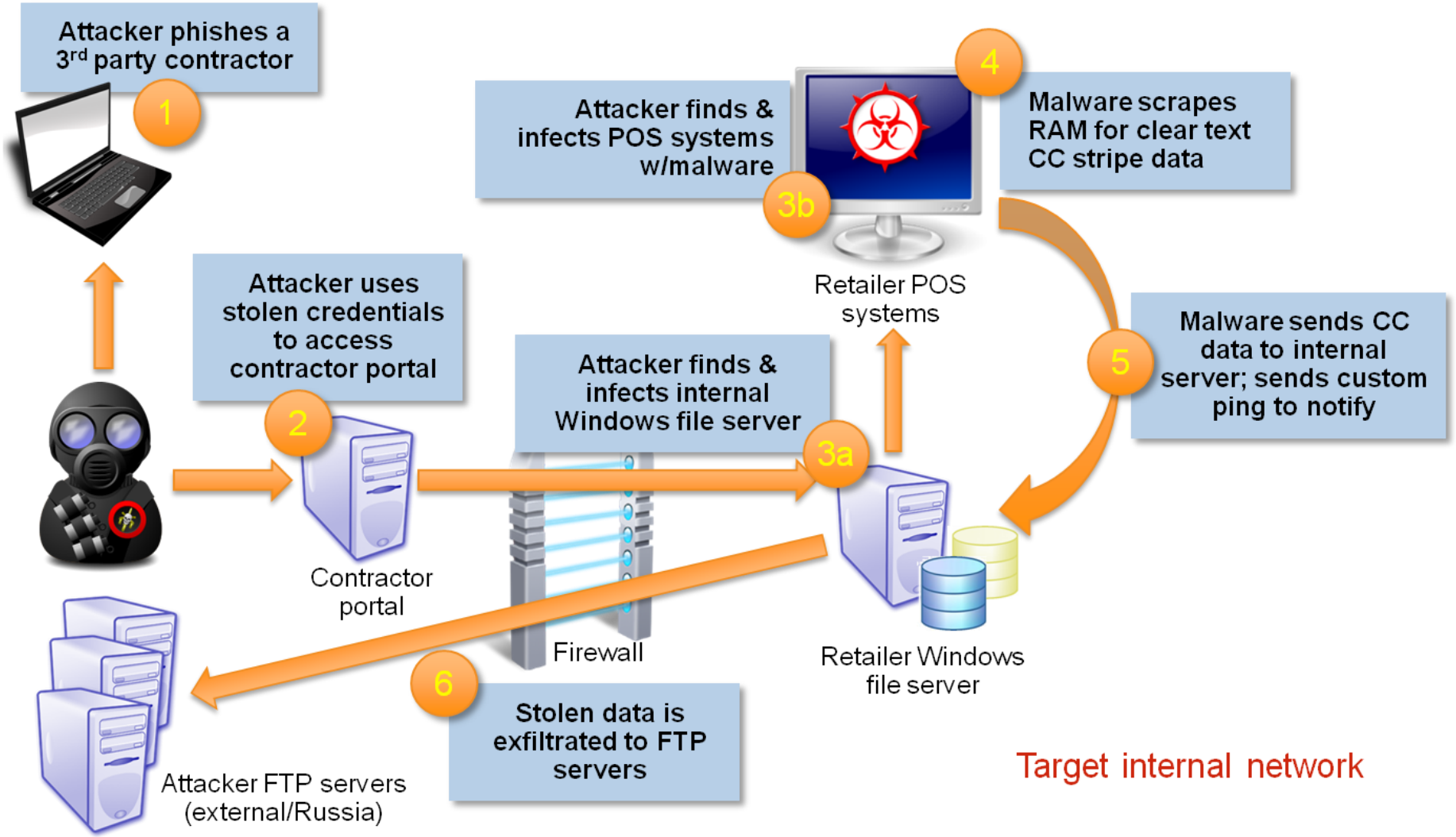
"We have sailed off the map, my friends.

Sitting here and awaiting instructions?

Not an option. And neither is what we've been doing…

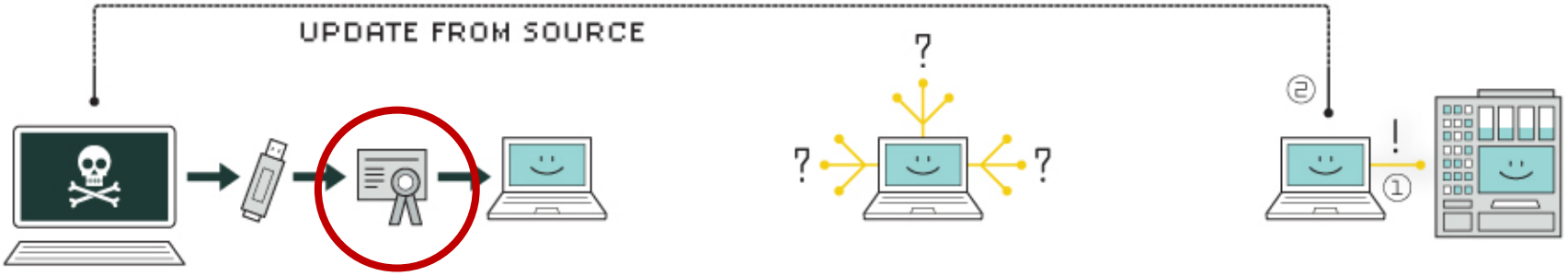
continuing to sail on with our existing maps even though the world has changed."

TARGET retailer POS breach:
Hybrid social engineering multi-layered, multi-phased attack



SOURCE: IBM Security Systems, Chris Poulin
http://www.slideshare.net/ibmsecurity/anatomy-of-an-advanced-retail-breach

STUXNET deep-incursion (+Dugu/ Flame):
State-sponsored sophisticated multi-phased worm attack



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

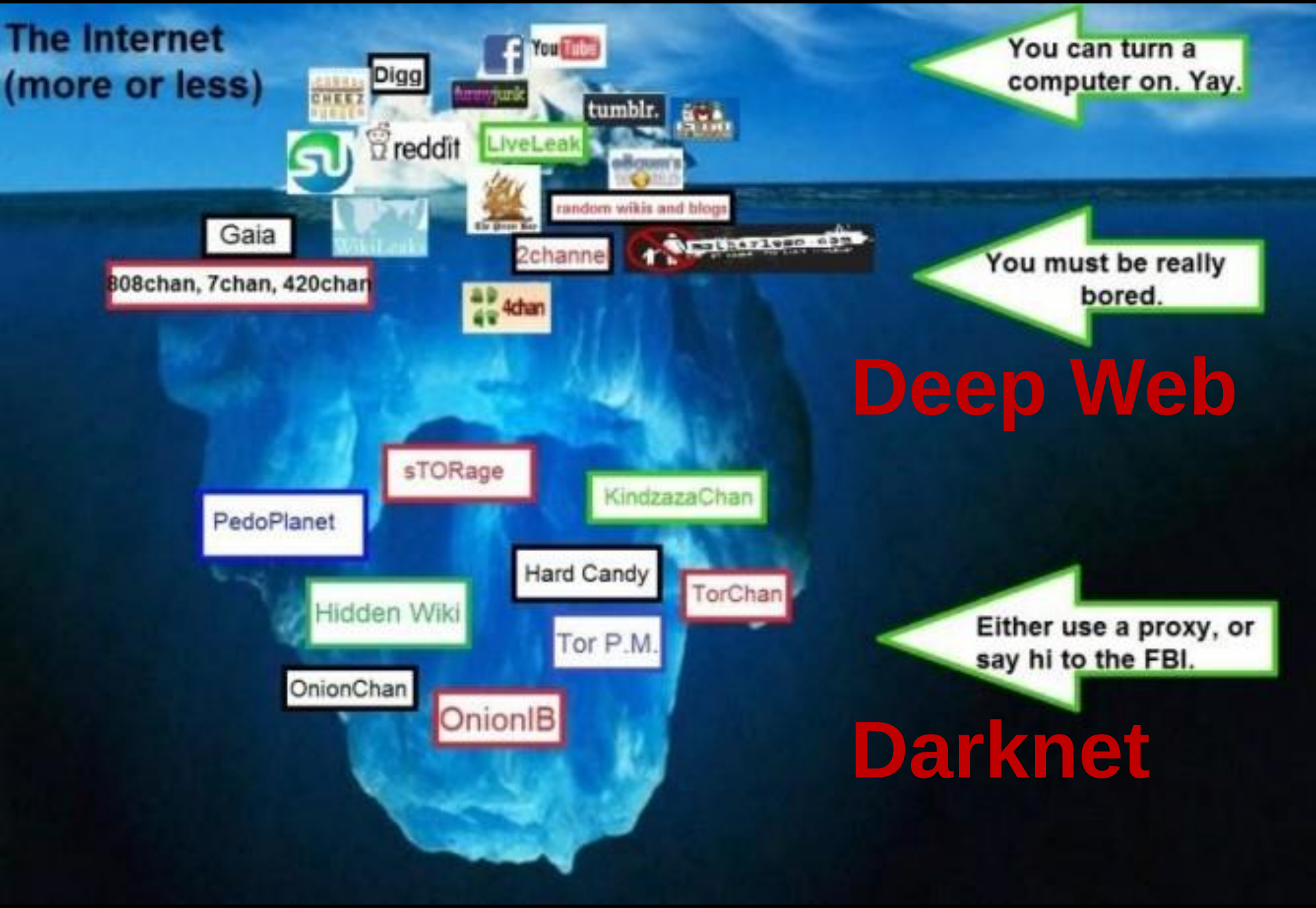
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

SOURCE: IEEE Spectrum http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet


The Internet
(more or less)
Digg
YouTube
tumblr.
reddit
LiveLeak
random wikis and blogs
Gaia
2channe
808chan, 7chan, 420chan
4chan
You can turn a computer on. Yay.
You must be really bored.
Deep Web
sTORage
KindzazaChan
PedoPlanet
Hard Candy
TorChan
Hidden Wiki
Tor P.M.
OnionChan
OnionIB
Either use a proxy, or say hi to the FBI.
Darknet

DISTRIBUTE, WHOLESALE, RESELLERS.....

CRIMEWARE TOOLKITS

Cyber Threat Professional

Anonymous markets for hacking tools (& spoils)

- Anonymous black markets for hacking tools
- Platforms to monetize results: stolen identities, financial details, passwords, etc.
- Crypto currency as enabler

NOTICE OF EXTORTION

Your business, , has been targeted for extortion. The selection process is random, and was not triggered by any event under your control.

Should you fail to pay the one-time monetary tribute, by the deadline provided below, your business will be **severely and irreparably damaged**. The following methods are commonly employed in cases of non-compliance:

- Negative Online Reviews
- BBB Complaints
- Harassing Telephone Calls
- Fraudulent Delivery Orders
- Telephone Denial-of-Service
- Bomb Threats
- Vandalism
- Mercury Contamination

Anonymous Reports of:

- Health Code Violations
- OSHA Violations
- Criminal Tax Evasion
- Money Laundering
- Illegal Drug Sales
- Marijuana Grow Operations
- Methamphetamine Production
- Terrorist Training Activity

The tribute price is only One Bitcoin (1 BTC), but must be paid by **August 15, 2014**. Payment is to be made to the Bitcoin Wallet Address listed below.

If payment is not received, our team will begin taking the actions listed above. Once engagement has begun, it can only be stopped for a tribute of Three Bitcoin (3 BTC). Because many of the actions we take are catastrophic and irreversible, is it advised to pay the tribute before the deadline is reached.

Payment Type: Bitcoin

Deadline: August 15, 2014

Amount Due: *(If paid before deadline)* 1 Bitcoin

Amount Due: *(If paid after deadline)* 3 Bitcoin

Purchase Bitcoin @
https://www.coinbase.com/

17gt1BancvtnnJwy4BA41VBUH3pfbUvzE

KIM ZETTER 05.15.15 10:14 PM

FEDS SAY THAT BANNED RESEARCHER COMMANDEERED A PLANE

GETTY IMAGES

A SECURITY RESEARCHER kicked off a United Airlines flight last month after tweeting about security vulnerabilities in its system had previously taken control of an airplane and caused it to briefly fly sideways, according to an application for a search warrant filed by an FBI agent.

Chris Roberts, a security researcher with One World Labs, told the FBI agent during an interview in February that he had hacked the in-flight entertainment system, or IFE, on an airplane and overwrote code on the plane's Thrust Management Computer while aboard the flight. He was able to issue a climb command and make the plane briefly change course, the document states.


Reactive militarization…
HEIMANN
HEIMANN

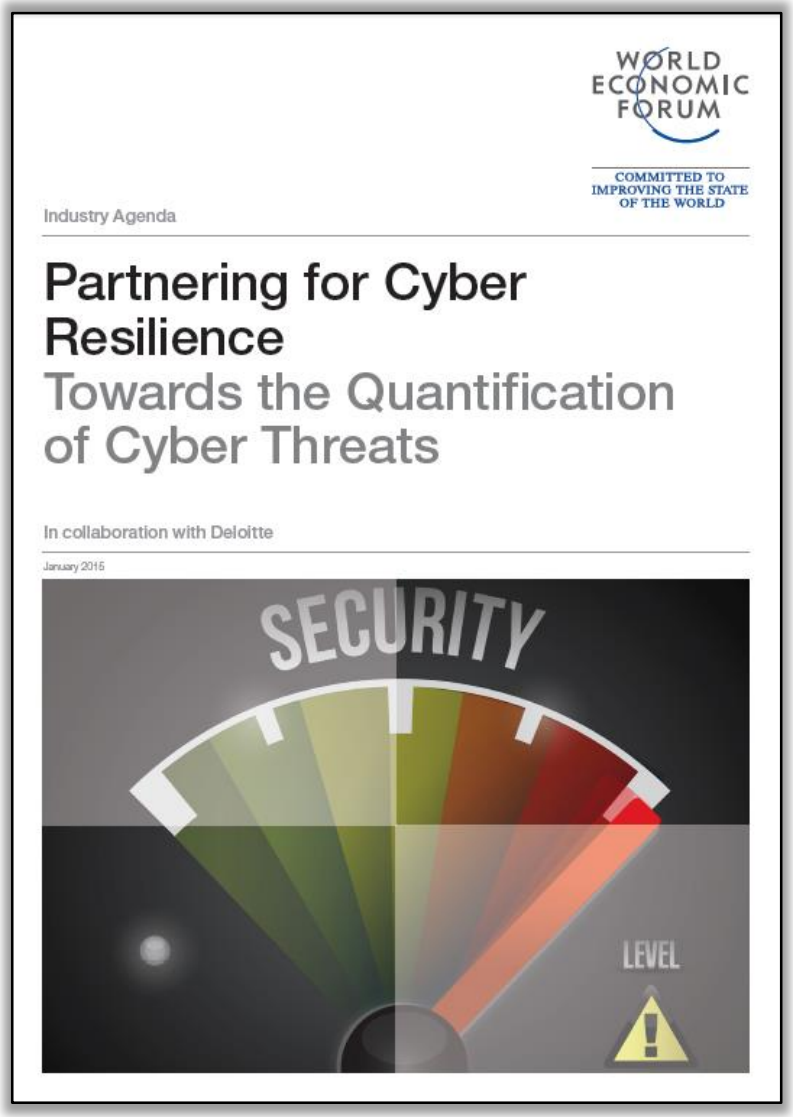
Cyber Kill Chain

- RECONNAISANCE
- WEAPONIZATION
- DELIVERY
- EXPLOIT
- INSTALLATION
- COMMAND AND CONTROL (CIC)
- ACTIONS or OBJECTIONS
  Usually Exfiltration

WHERE ARE WE GOING?

Paradigmatic reframing…

WEF: Cyber V@R



III. Technical

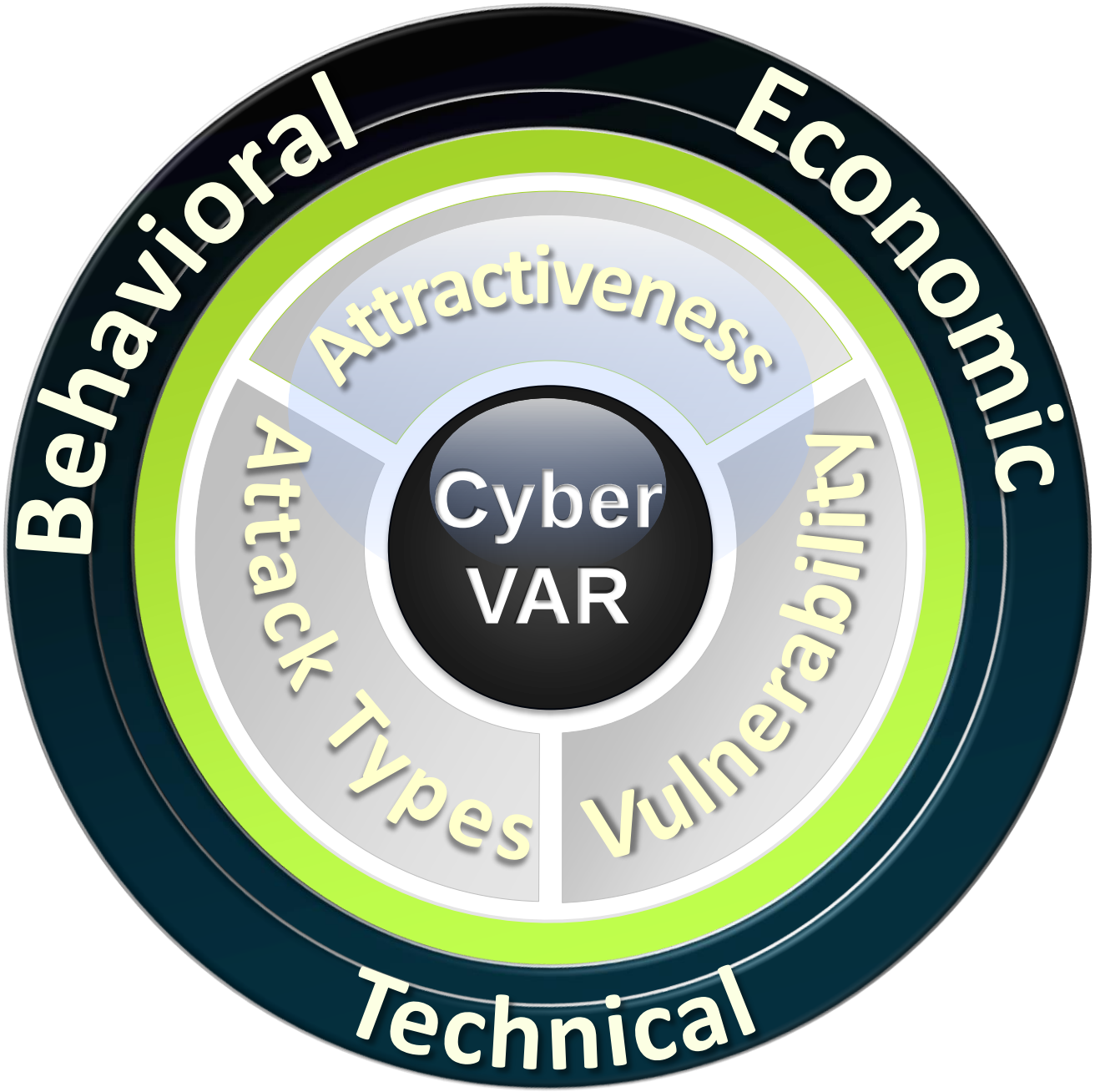
Vulnerability

II. Economic

Assets

I. Behavioral

Profile of Attacker


Behavioral
Economic
Technical
Attractiveness
Attack Types
Vulnerability
Cyber
VAR

I. BEHAVIORAL

Criminology paradigm

Cyber Threat 'criminal attractiveness'

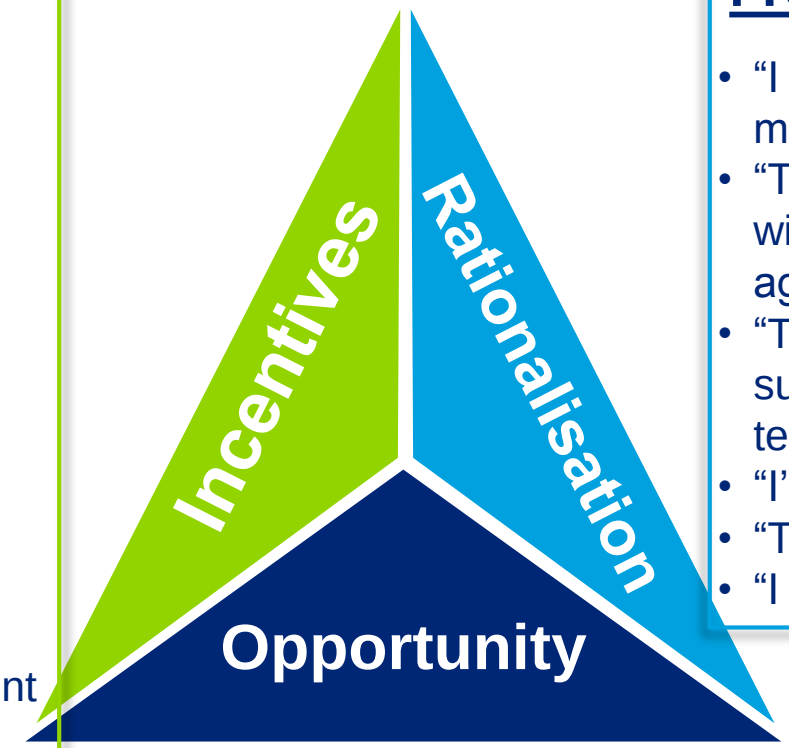
High risk of incidents when three factors align…

STRATEGIC
- National interests
- Corporate espionage / sabotage

FINANCIAL
- Fraud
- Theft (i.e. credit cards)
- Market manipulation

REPUTATIONAL
- Recognition of expertise / fame in hacker networks
- Making a political statement

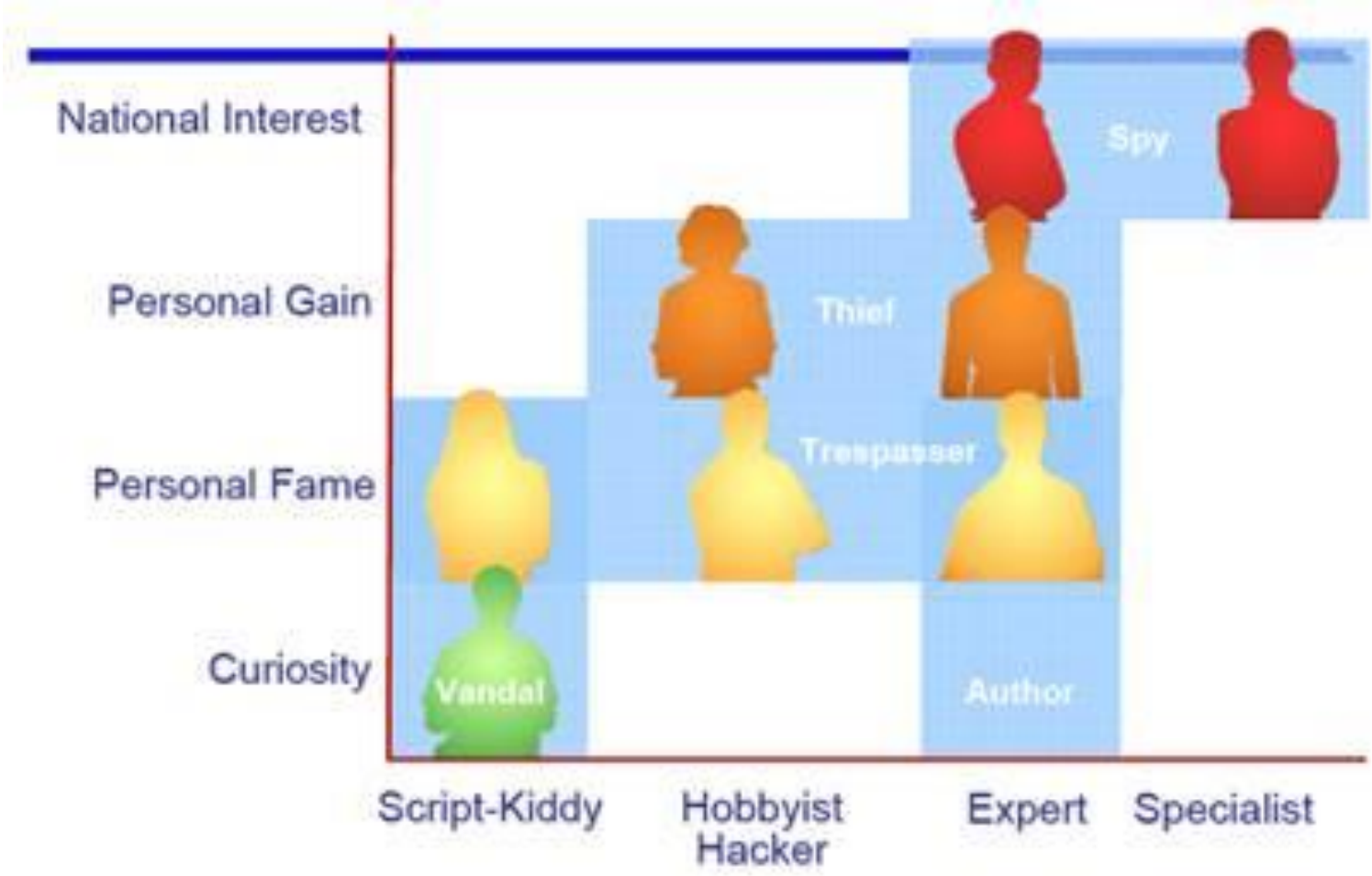
PERSONAL
- Curiousity
- Greed or revenge
- Character flaws (i.e. sociopathic disorder)



FRACTURED LOGIC
- "I need / deserve the money"
- "They are working closely with a country I do not agree with"
- "They should not have such poor security – I will teach them a lesson"
- "I'm only playing around"
- "They had it coming"
- "I am not respected"

SYSTEMIC WEAKNESSES
STRIDE susceptibility
- **Spoofing**
- **Tampering**
- **Repudiation**
- **Denial of Service**
- **Information Disclosure**
- **Elevation of Privilege**

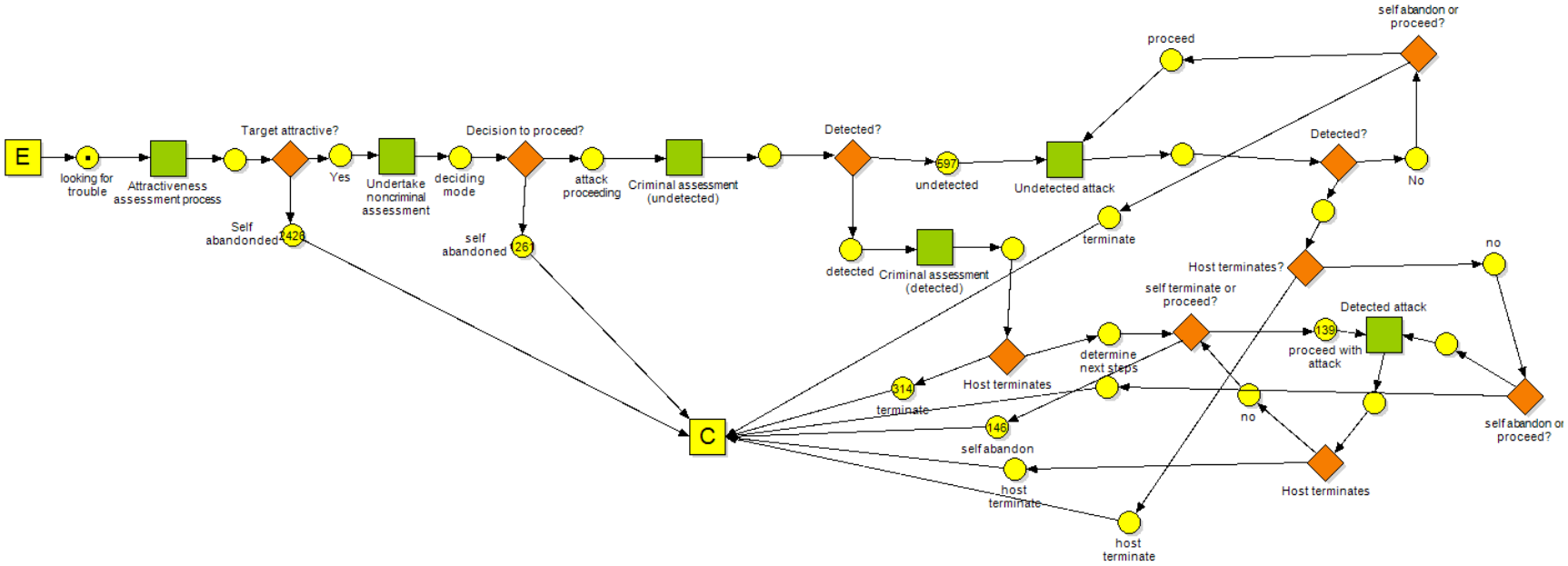
Threat Personas (Aucsmith Framework)

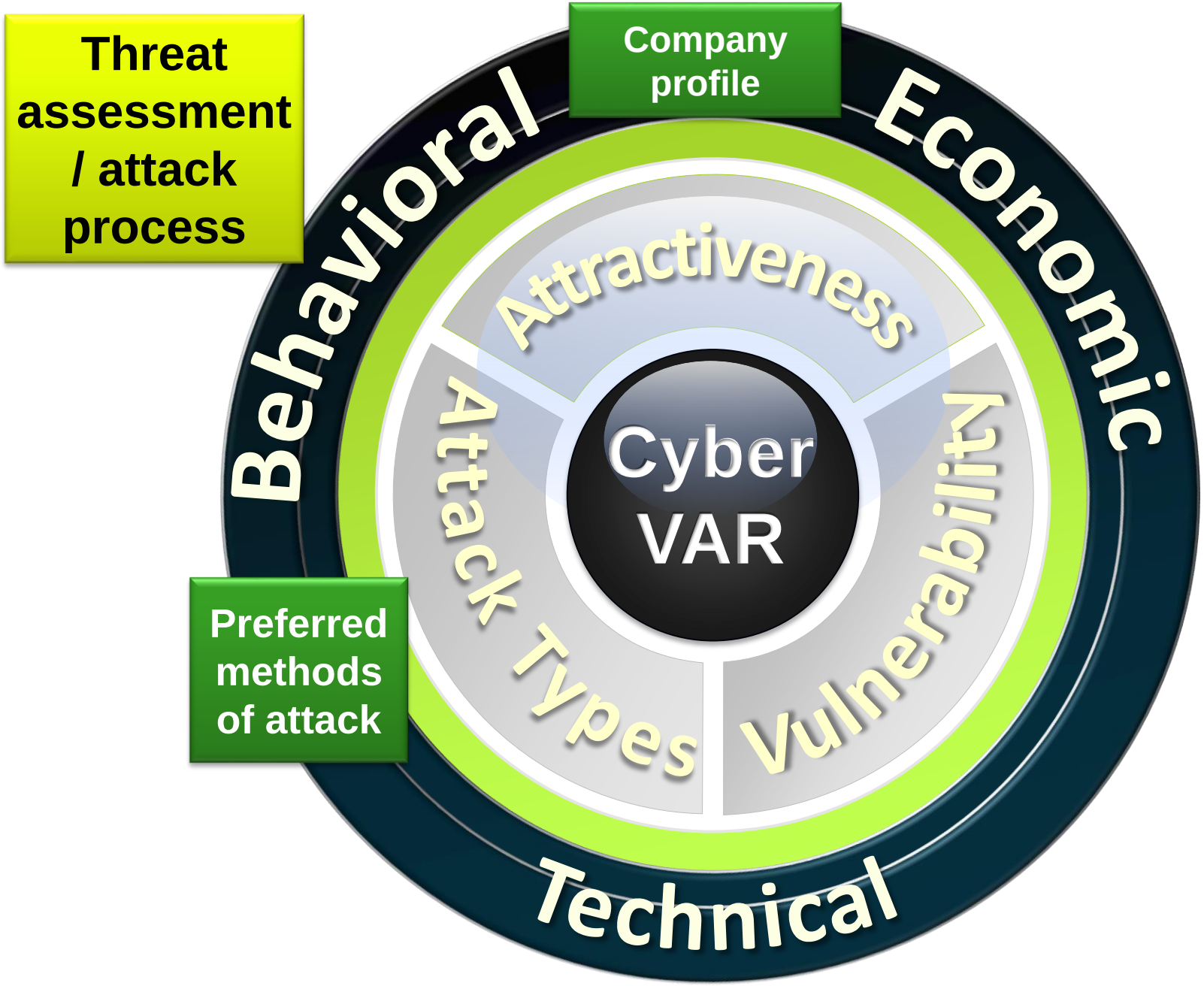


David Aucsmith (Microsoft) "Threat Personas" framework (Aucsmith, 2003).

Behavioral assessment attack simulation…

Example: Petri Net (YASPER)

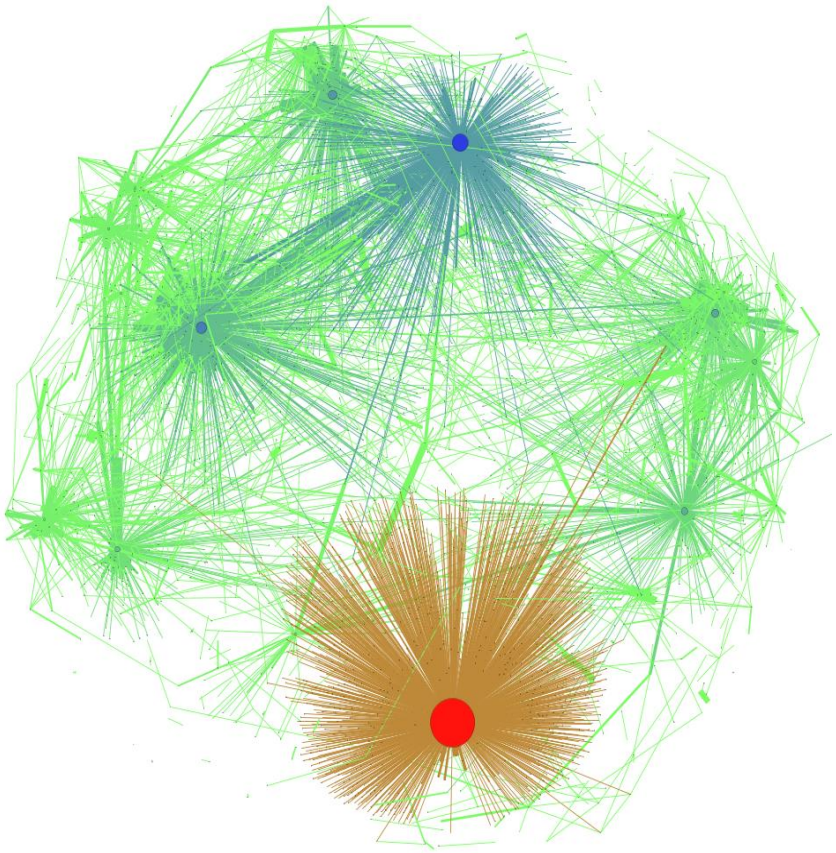



Threat assessment / attack process
Company profile
Behavioral
Economic
Technical
Attractiveness
Attack Types
Vulnerability
Cyber VAR
Preferred methods of attack

II. ECONOMIC

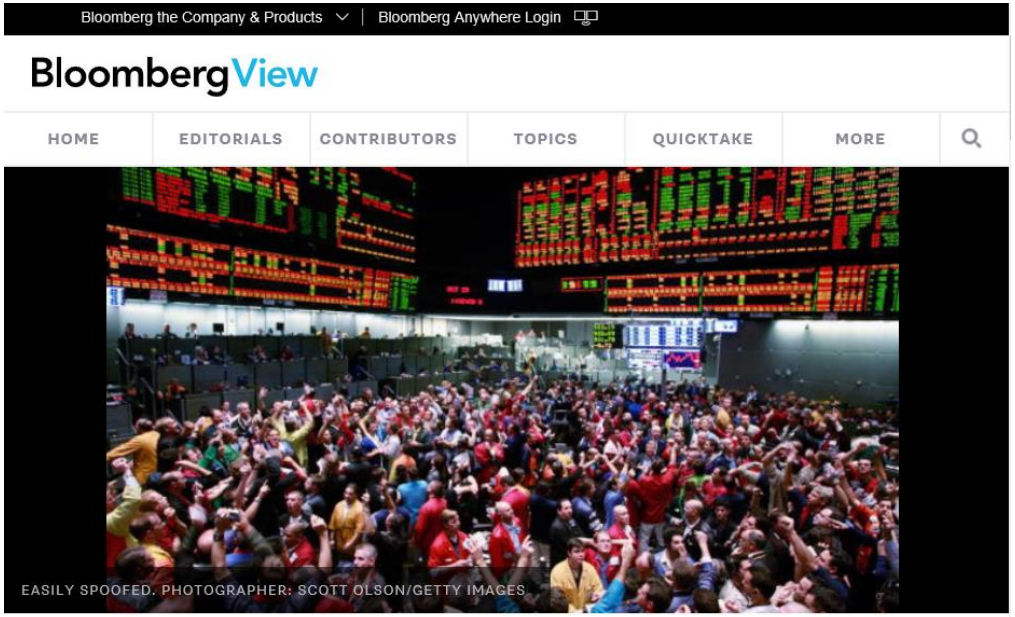
Market paradigm

Markets = networks



access ∝ risk

power ∝ vulnerability



WALL STREET 2010

Guy Trading at Home Caused the Flash Crash

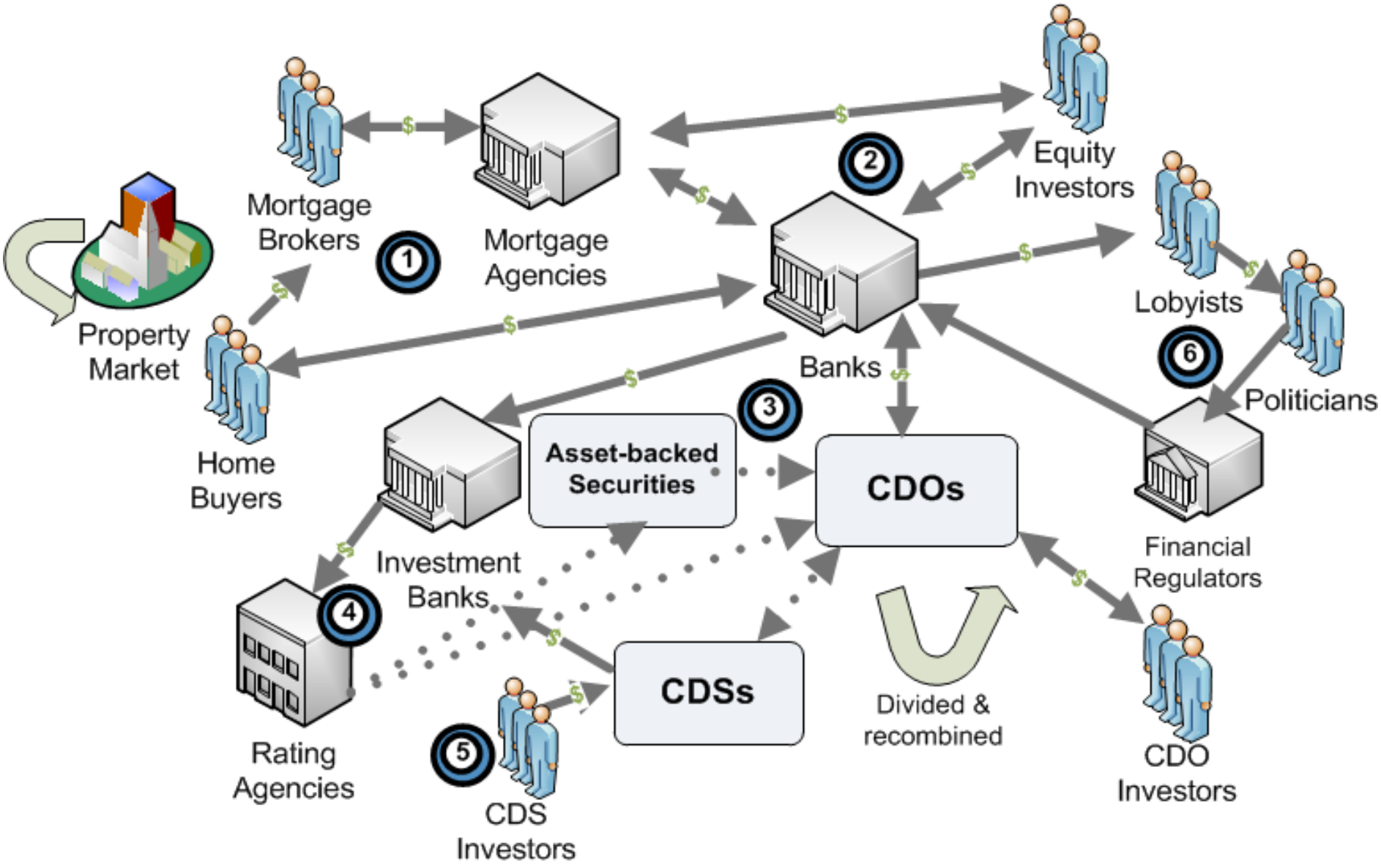
131 APR 21, 2015 6:37 PM EDT

By Matt Levine a | A

Hey look, they caught the guy who caused the flash crash of 2010! His name is Navinder Singh Sarao, and he lives in London and in 2009 he asked someone to help him build a spoofing robot:

http://www.bloombergview.com/articles/2015-04-21/guy-trading-at-home-caused-the-flash-crash

Markets: structural flaws (and regulation)…



N.Y. to Propose Cybersecurity Regulations

Third-Party Risks Require More Due Diligence

By Tracy Kitten, May 18, 2015.

Benjamin M. Lawsky

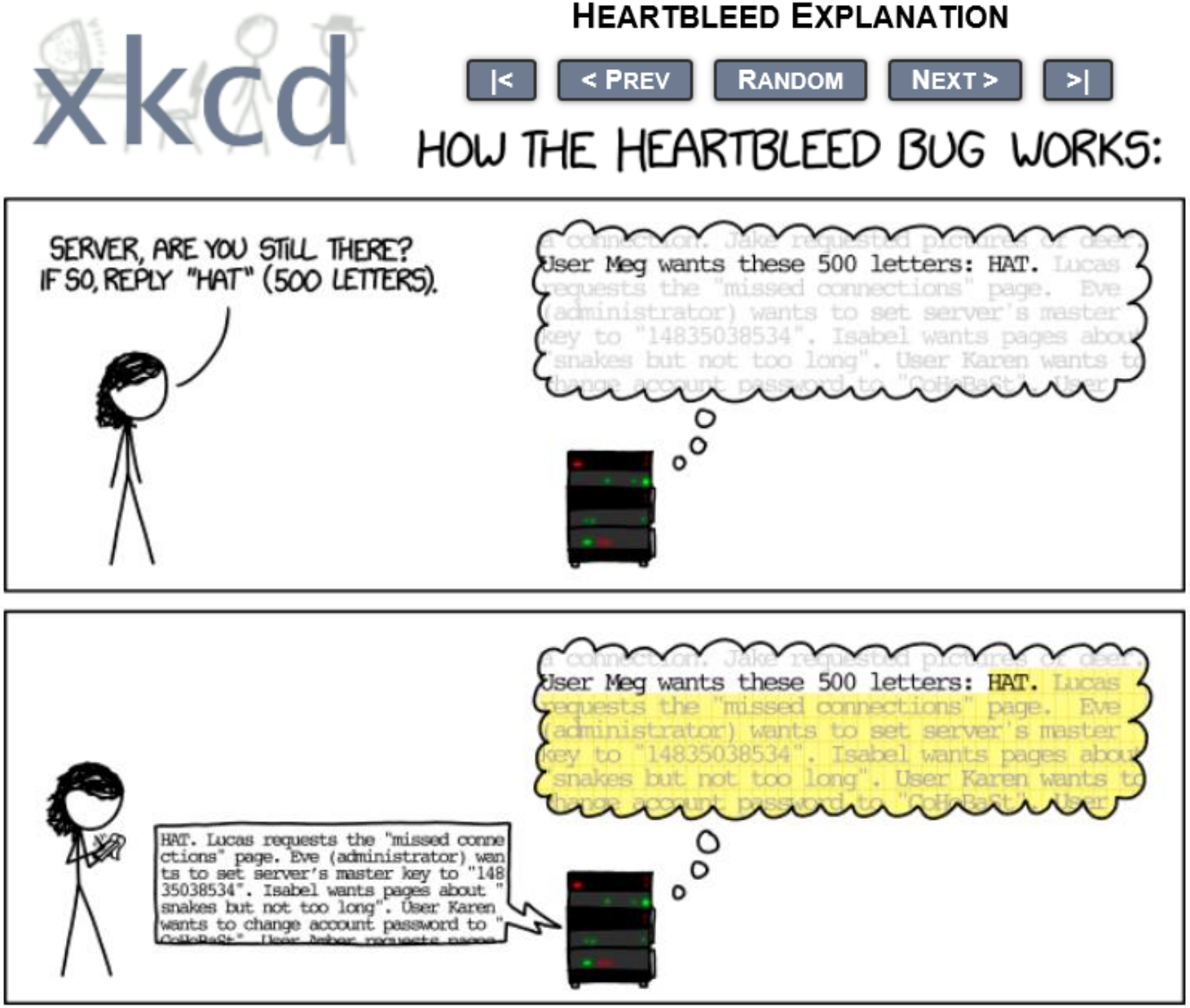
In April, the New York State Department of Financial Services issued a report about significant third-party and **vendor management** risks that numerous banks throughout the state were failing to address (see ***Banks' Vendor Monitoring Comes Up Short***).

See Also: CISO Agenda 2015: Adding Value to a Security Program with Application Security

Recent Content

1. Router Hacks: Who's Responsible?

Brittle and vulnerable systems…



https://xkcd.com/1354/

Brittle and vulnerable systems…

BRICKED

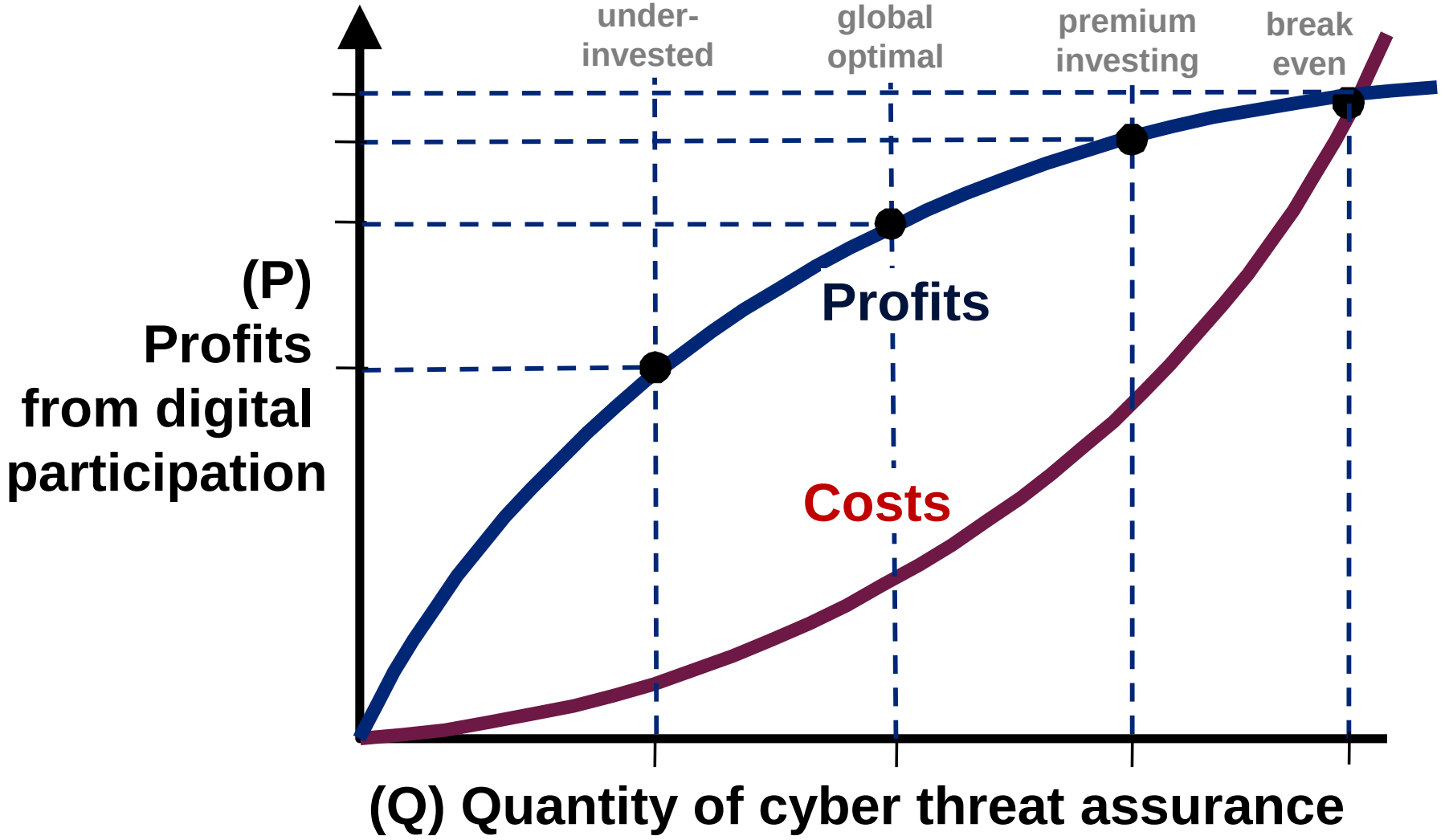
Wi-Fi Hack Creates 'No iOS Zone' That Cripples iPhones And iPads

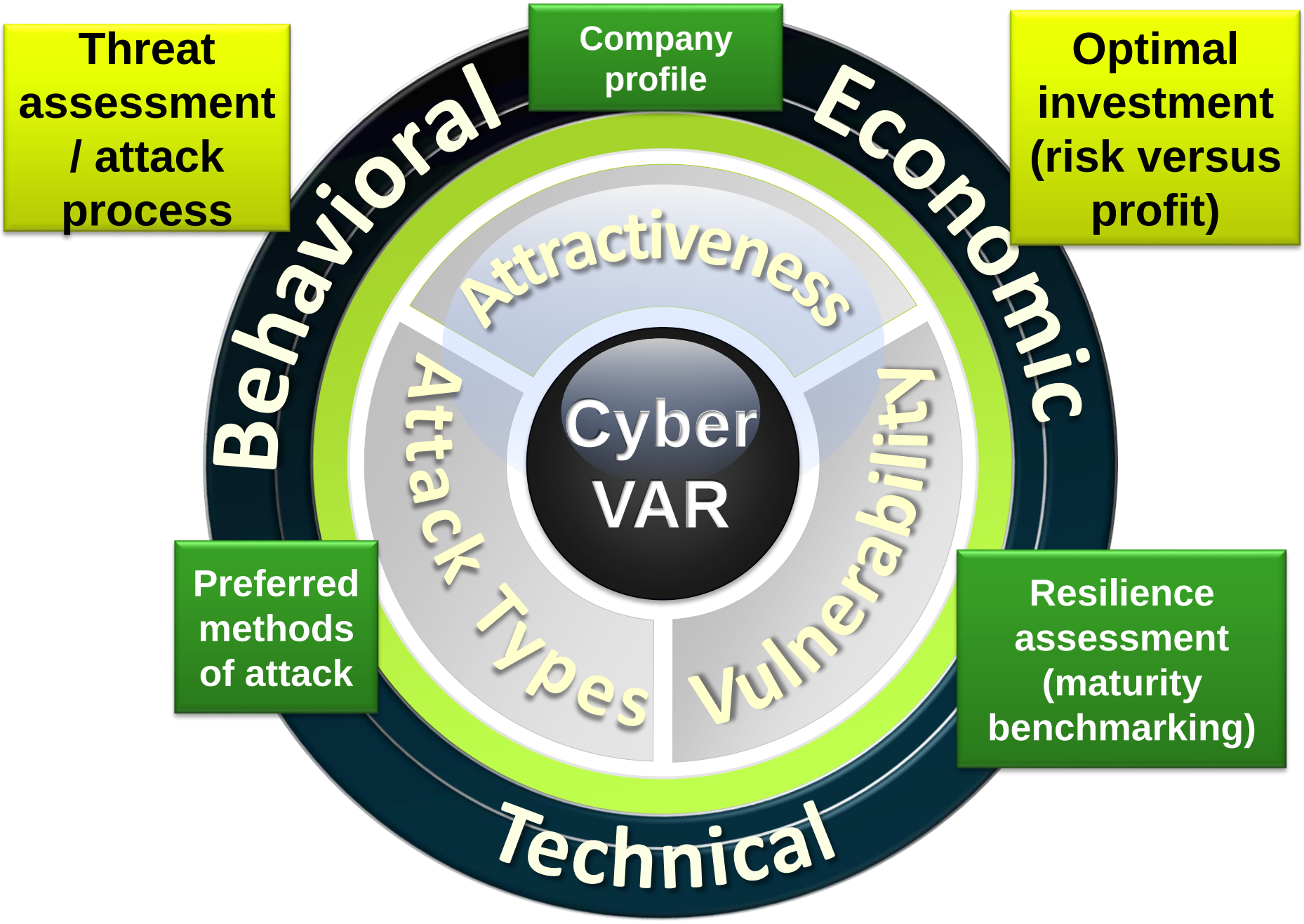
1,972 theguardian.com · Technology

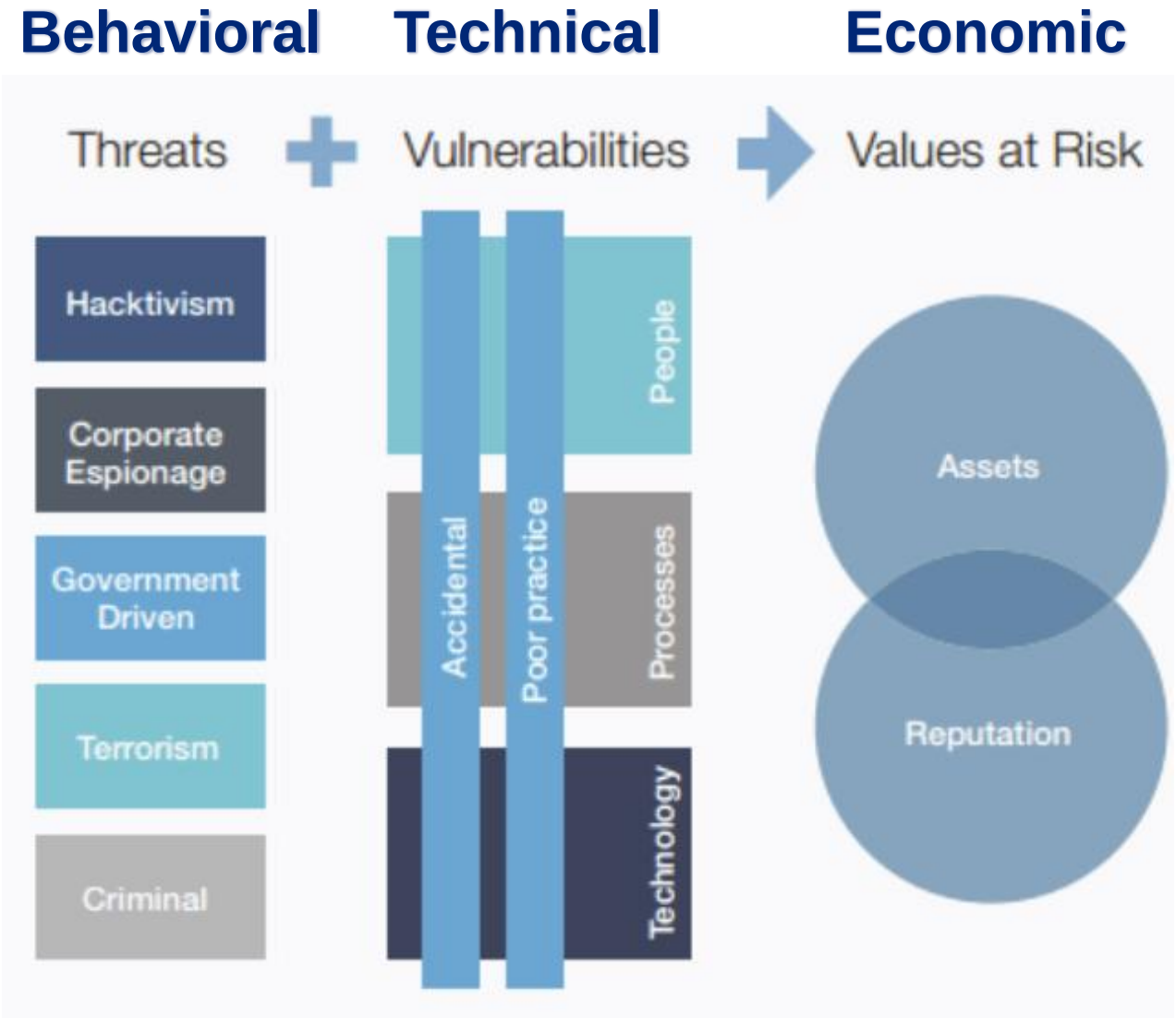
A newly revealed bug in iOS lets attackers force iPhones and iPads into restart loops, repeatedly crashing and rebooting, using nothing but a Wi-Fi network.

Theoretical optimal in cyber resilience investment

Invest to point of optimality




Threat assessment / attack process
Company profile
Optimal investment (risk versus profit)
Behavioral
Economic
Attractiveness
Attack Types
Vulnerability
Cyber VAR
Technical
Preferred methods of attack
Resilience assessment (maturity benchmarking)


Behavioral
Technical
Economic
Threats
Vulnerabilities
Values at Risk
Hacktivism
Corporate Espionage
Government Driven
Terrorism
Criminal
People
Processes
Technology
Accidental
Poor practice
Assets
Reputation

III. TECHNICAL

Medical paradigm

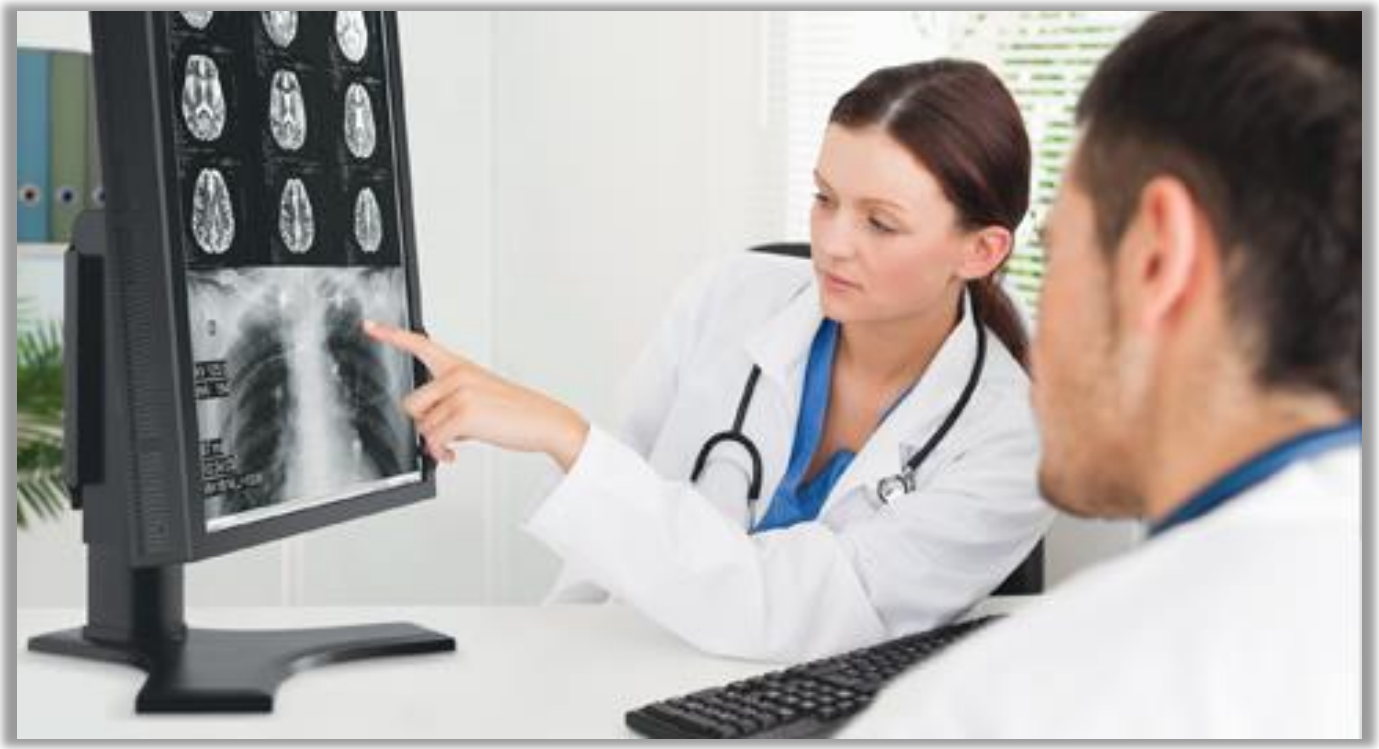
Public health

Emergency care ⟺ Disaster management

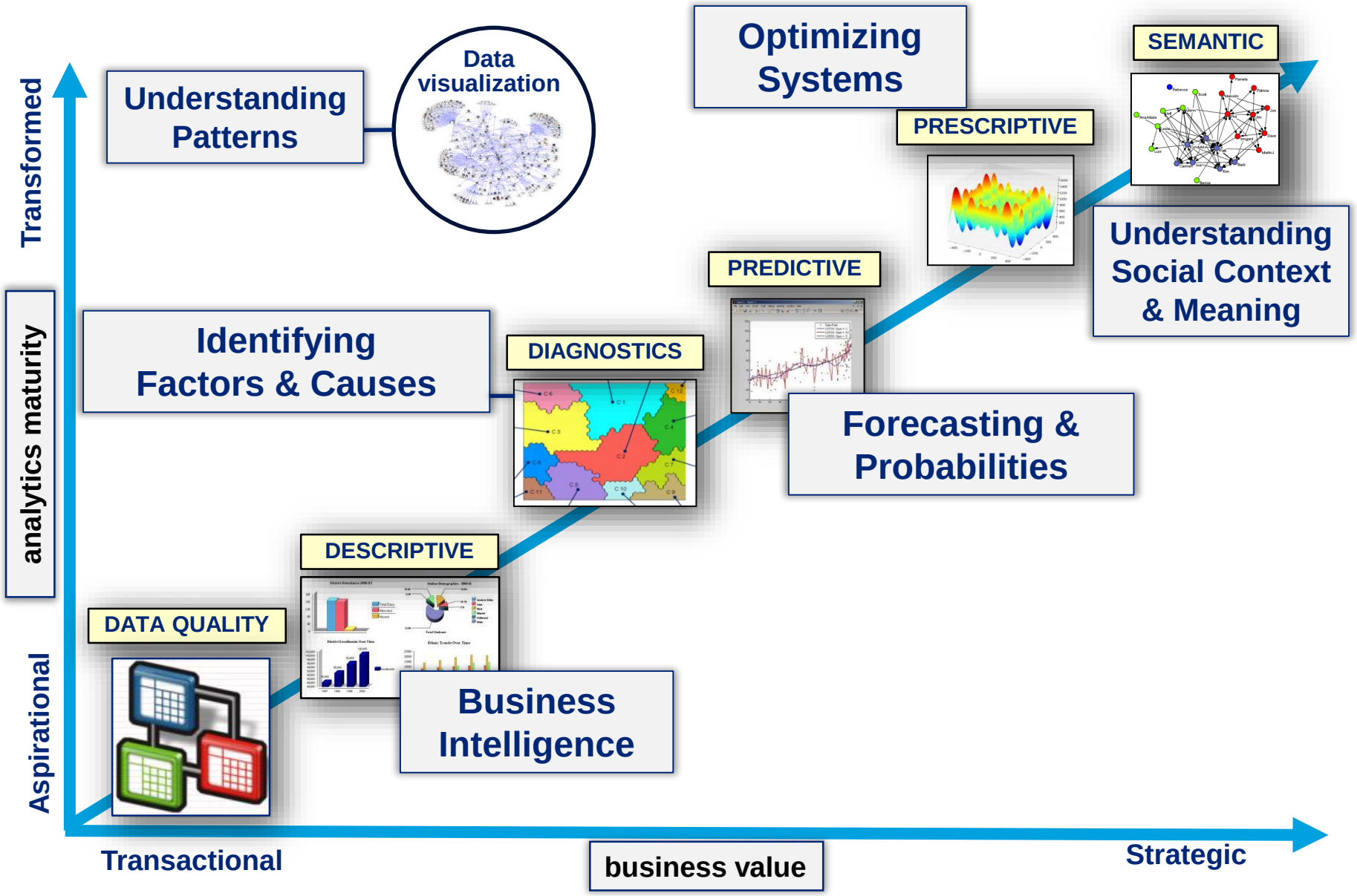
Preventative care ⟺ Risk management

DIAGNOSTICS

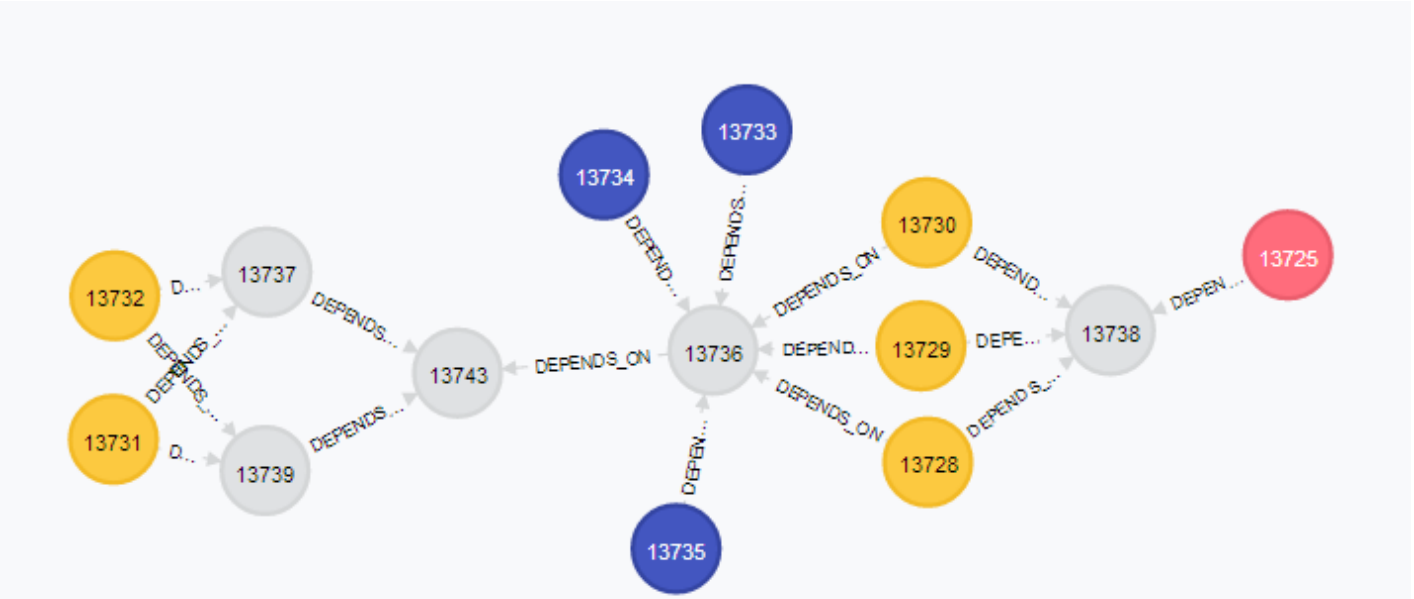
- Evidence-based management
- Clinical prediction
- Biostatistics



Data analytics



Machine-readable, dynamic documentation



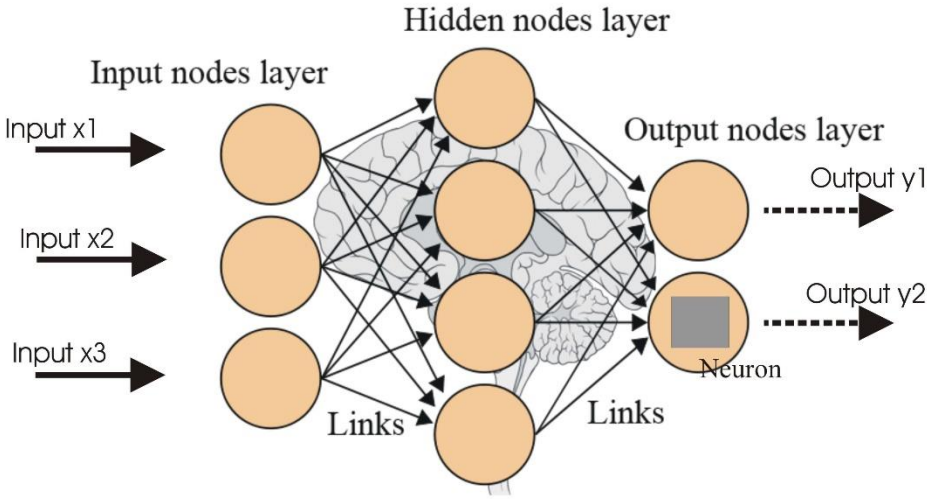
Host	Dependencies
global.acme.com	CUSTOMER-DB-1, WEBSERVER-1
partners.acme.com	WEBSERVER-2, CUSTOMER-DB-2
shop.acme.com	CUSTOMER-DB-1, WEBSERVER-1
support.acme.com	CUSTOMER-DB-1, WEBSERVER-1
training.acme.com	WEBSERVER-2, CUSTOMER-DB-2

EXAMPLE: Neo4j NOSQL graph database

Cyber risk analytics value propositions

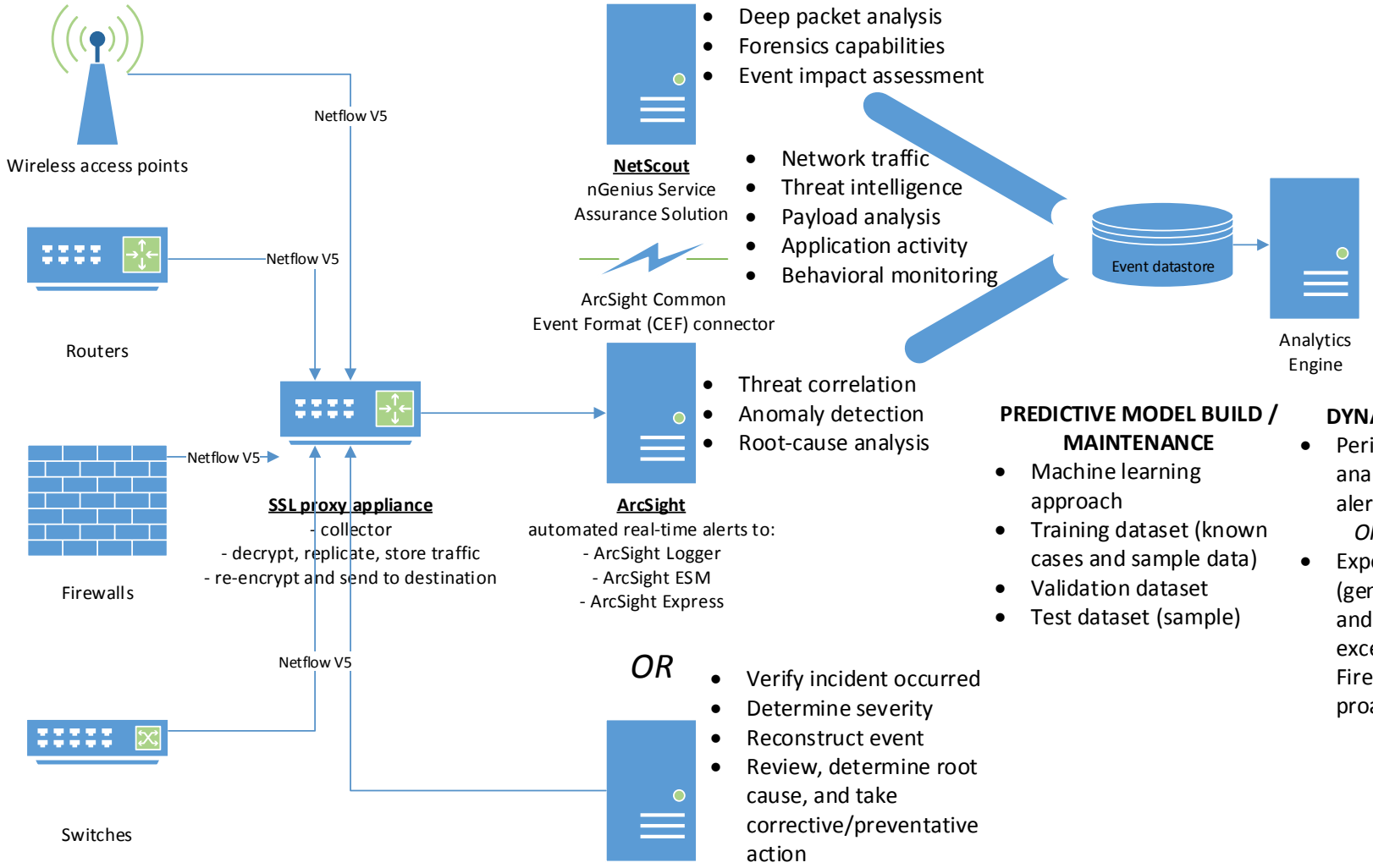
Predictive analytics

- Pattern identification (i.e. cluster analysis)
- Trend analysis (i.e. regression)
- Machine learning (i.e. Decision Tree, SVM, Neural Networks)



Example cyber risk analytics solution architecture:

SIEM + Net Flow analysis + predictive analytics



- Deep packet analysis
- Forensics capabilities
- Event impact assessment

- Network traffic
- Threat intelligence
- Payload analysis
- Application activity
- Behavioral monitoring

- Threat correlation
- Anomaly detection
- Root-cause analysis

- Verify incident occurred
- Determine severity
- Reconstruct event
- Review, determine root cause, and take corrective/preventative action

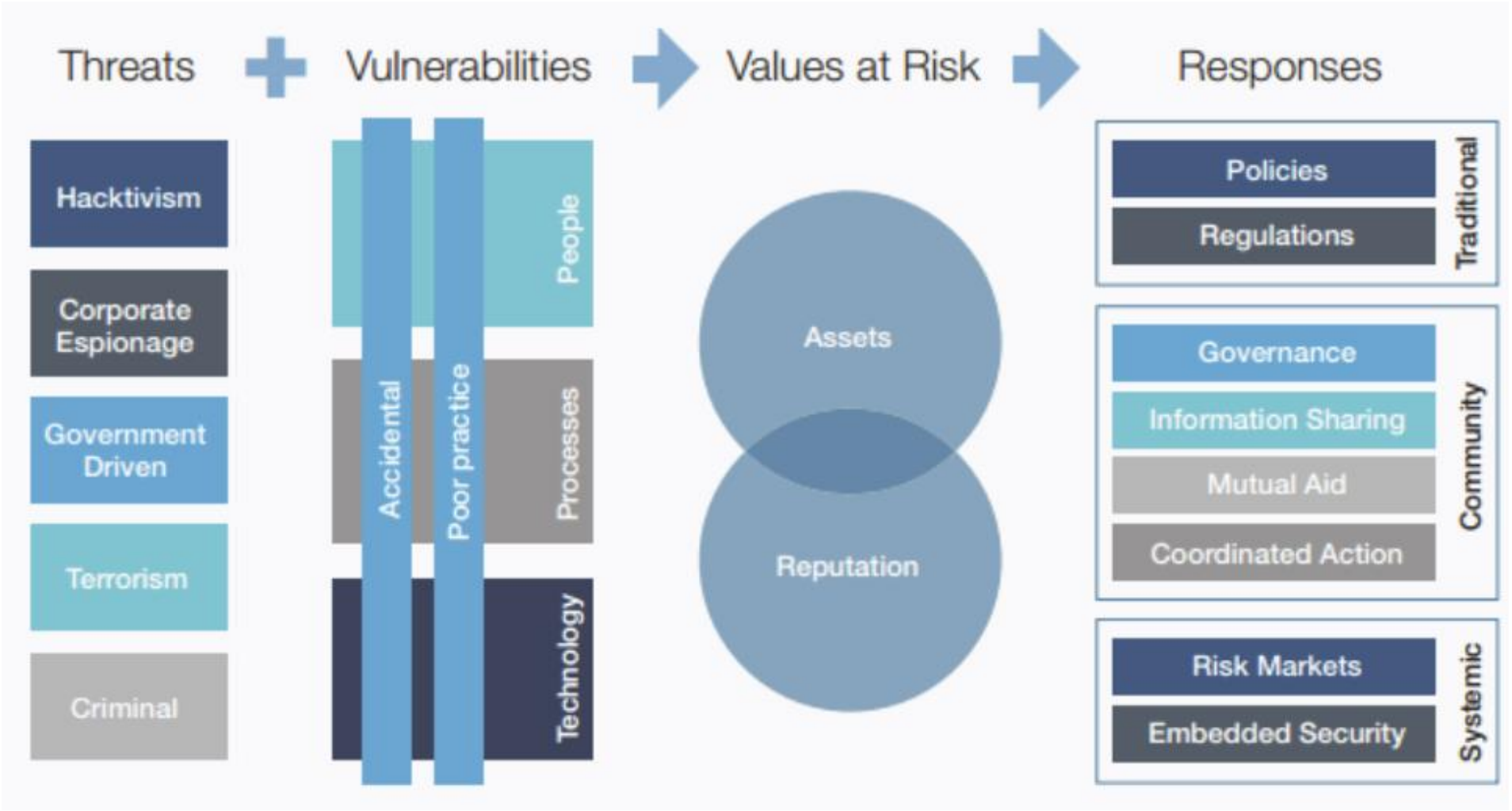
PREDICTIVE MODEL BUILD / MAINTENANCE

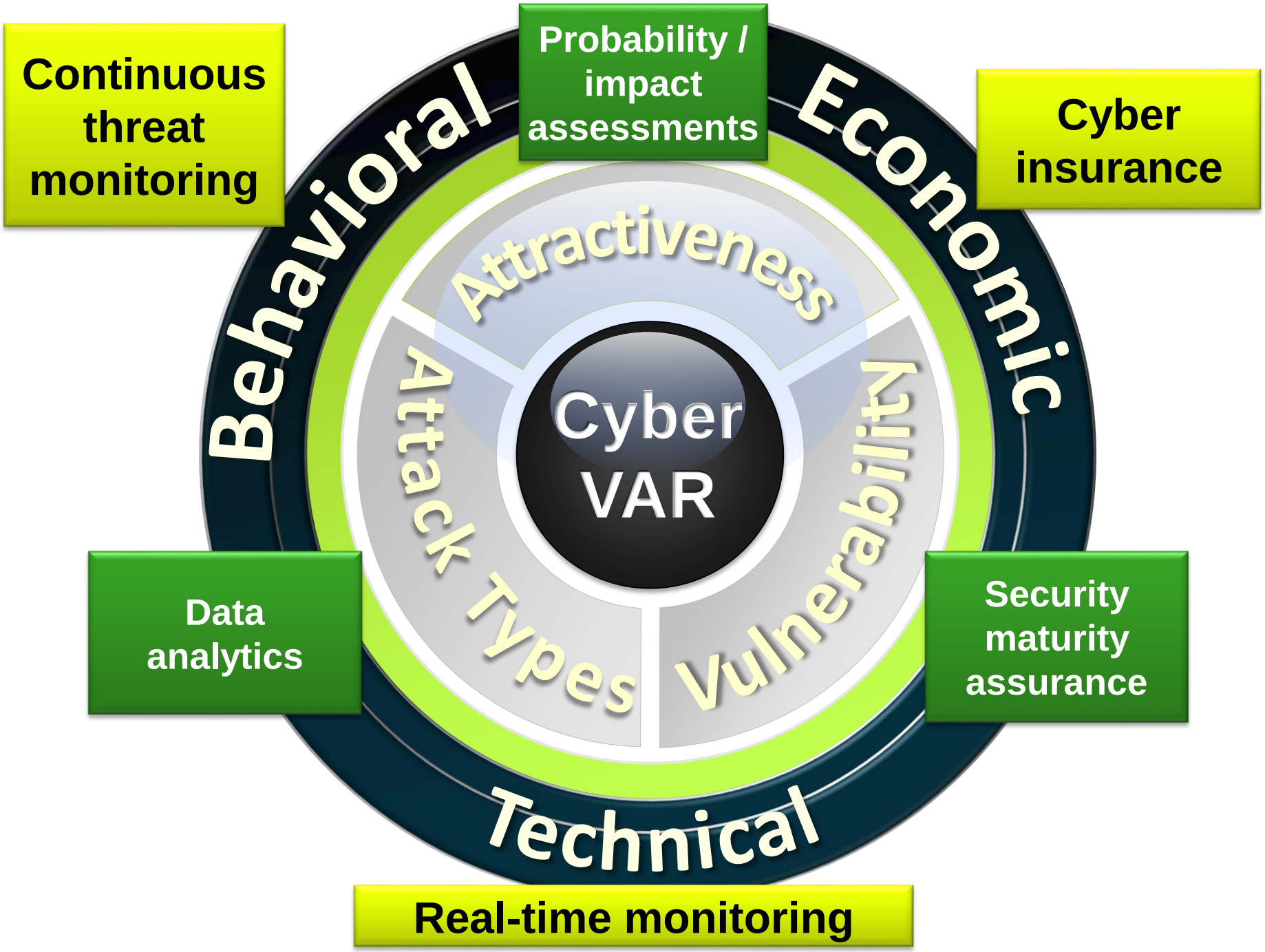
- Machine learning approach
- Training dataset (known cases and sample data)
- Validation dataset
- Test dataset (sample)

DYNAMIC ASSESSMENT

- Periodic on-server analysis which generates alerts
  OR
- Export key risk factors (generated from model) and load as alerts / exception conditions in Firewall (or other proactive network utility)

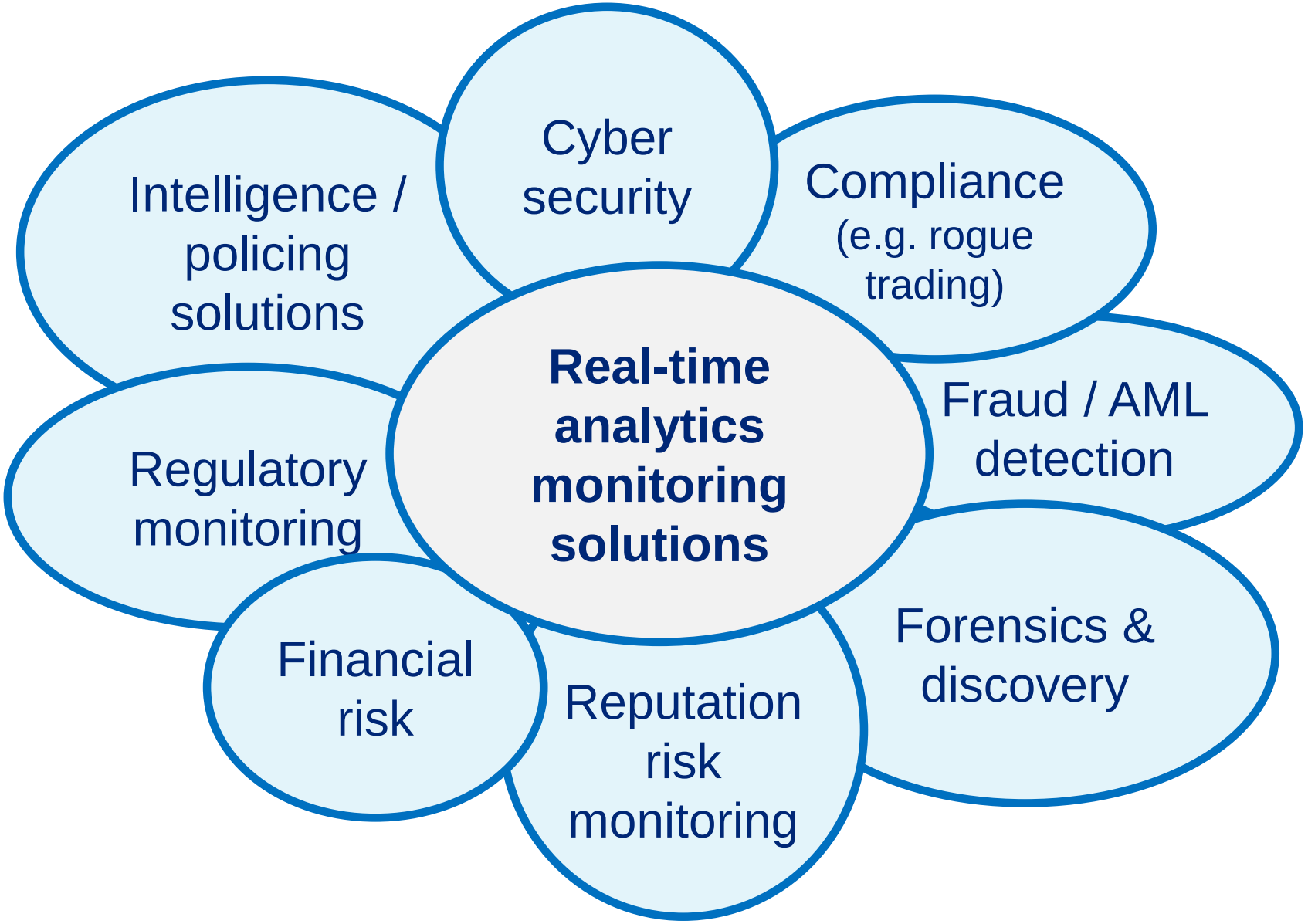
Behavioral Technical Economic




Continuous threat monitoring
Probability / impact assessments
Cyber insurance
Behavioral
Economic
Attractiveness
Attack Types
Vulnerability
Cyber VAR
Data analytics
Security maturity assurance
Technical
Real-time monitoring

Converging and emerging solutions marketplace

Hybrid technology solutions market



End-to-end compliance platform providers

End-to-end solutions that require substantial implementation overhead

SAP

NICE · ACTIMIZE

IBM

sas

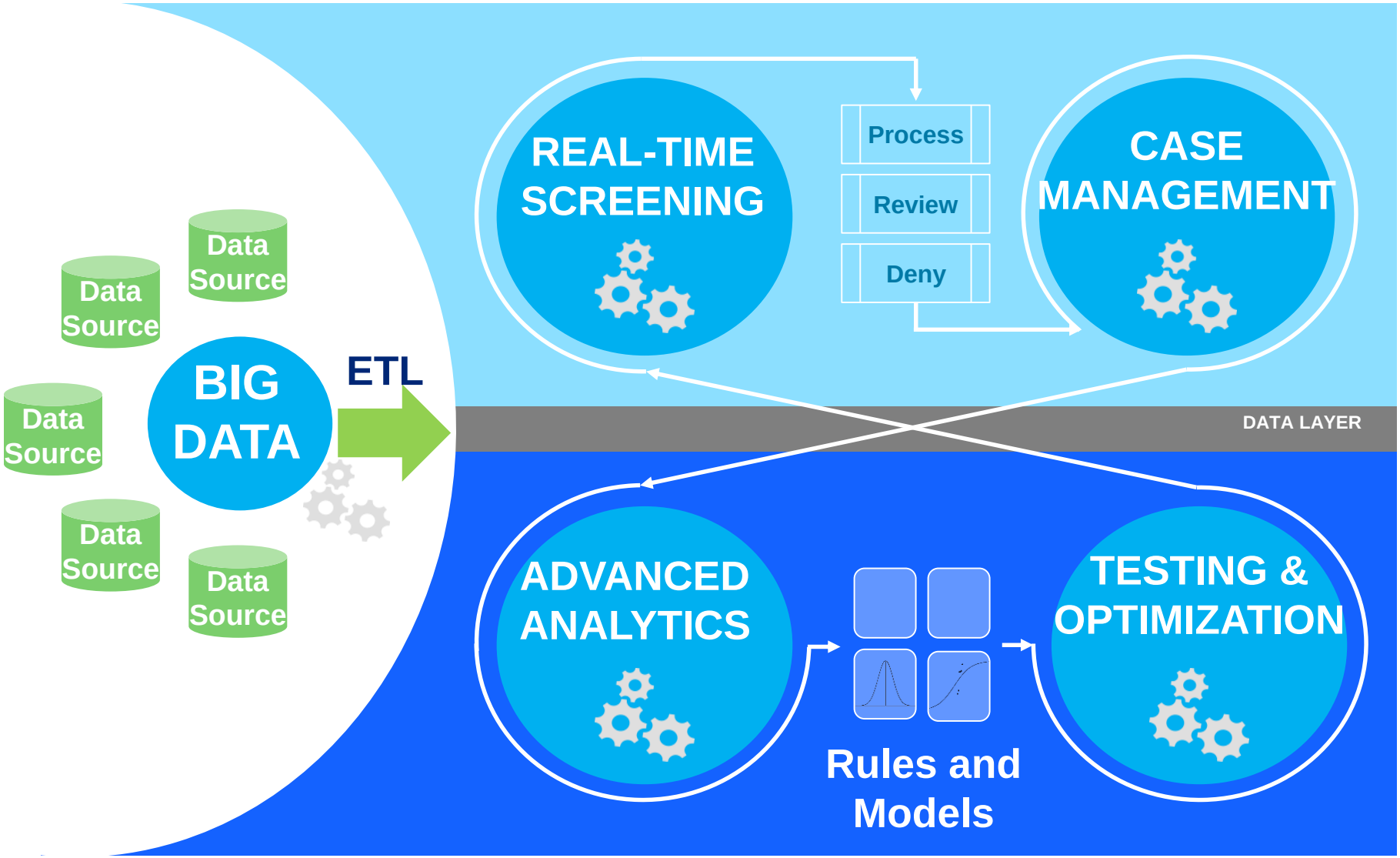
TONBELLER®
Software ■ Consulting

Palantir

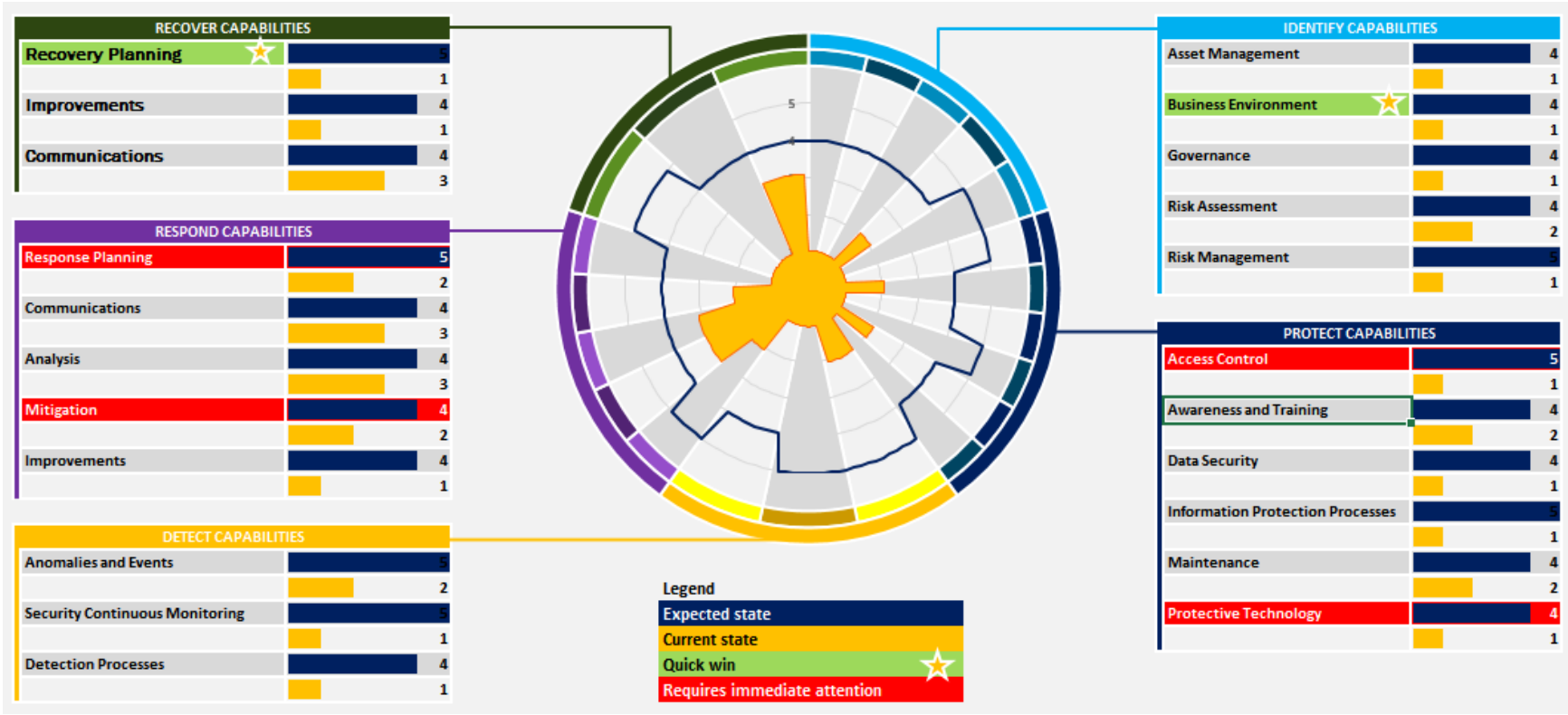
BAE SYSTEMS

Continuous threat mitigation framework

Real-time screening with analytics, alerts, and case-based workflow



DETECTION | ANALYTICS | THREATS | CONTROLS | ASSETS

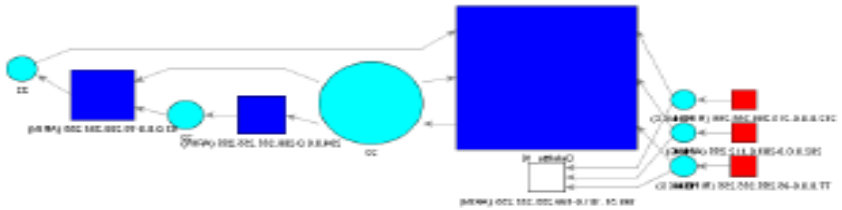


DETECTION | ANALYTICS | THREATS | CONTROLS | ASSETS

Asset Valuation Tracking

ID	Function	FNC	Type	Key indicator	Unit	Benchmark	Norm	Current against norm
ID.KPI.01	Identify	ID	KPI	Recent risk assessment on critical systems	%		95%	95%
ID.KPI.02	Identify	ID	KPI	Asset consistency	%		95%	100%
ID.KRI.01	Identify	ID	KRI	Findings from audits	#		50	0,5
ID.KRI.02	Identify	ID	KRI	Risk findings accepted	%		10%	90%
ID.KRI.03	Identify	ID	KRI	Staff retention Philips / vendors	%		5%	100%
ID.KRI.04	Identify	ID	KRI	Staff retention IT security	%		5%	160%
PR.KPI.01	Protect	PR	KPI	Staff enrolled in awareness training	%		100%	90%
PR.KPI.02	Protect	PR	KPI	Penetration tests executed	#		50%	90%
PR.KPI.03	Protect	PR	KPI	Critical defects from penetration test	#		5	0,6

Key Data Repositories



Key Operating Hardware

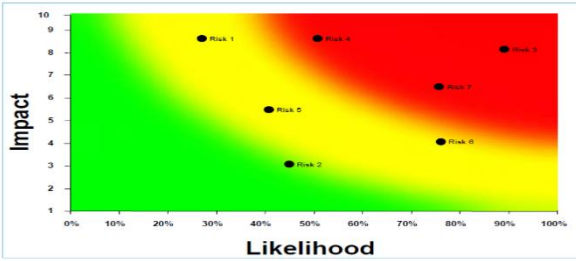
PROTECT				
Access Control	5	1		4
Awareness and Training	4	2		2
Data Security	4	1		3
Information Protection Processes and	5	1		4
Maintenance	4	2		2
Protective Technology	4	1		3

Ownership and Governance

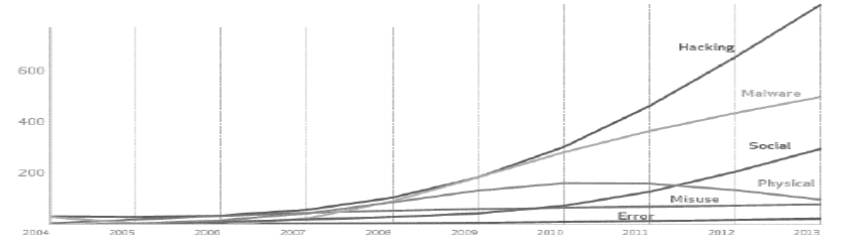
RESPOND				
Response Planning	5	2		3
Communications	4	3		1
Analysis	4	3		1
Mitigation	4	2		2
Improvements	4	1		3

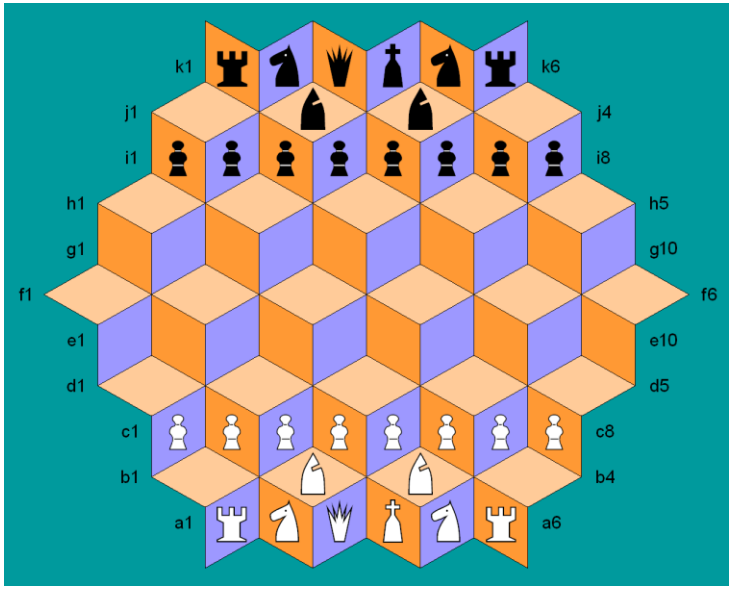
Asset Risk Tracking

Risk	Likelihood	Impact
Risk 1	30%	8,5
Risk 2	45%	3
Risk 3	90%	8,2
Risk 4	53%	8,7
Risk 5	40%	5,5
Risk 6	78%	4,1
Risk 7	75%	6,5



Emerging Threats and Dynamic Cyber Value At Risk



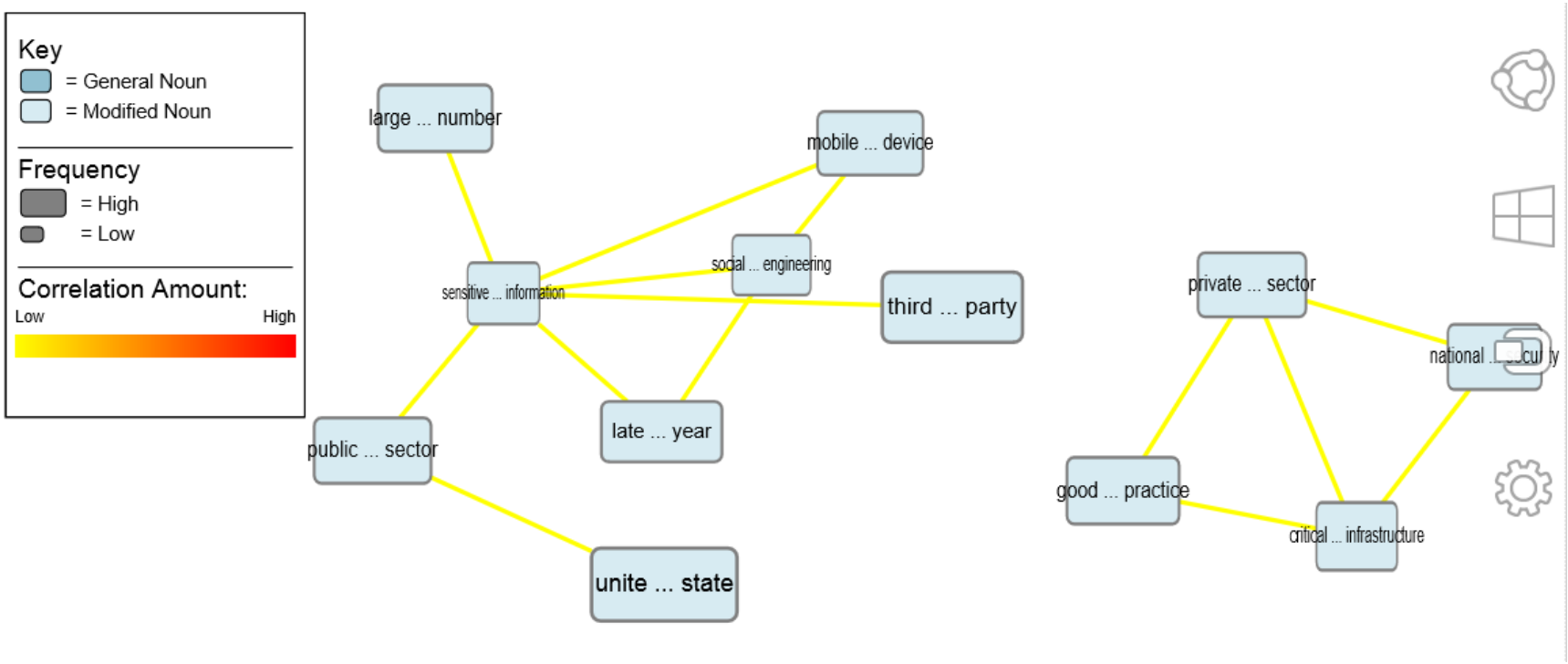

k1
k6
j1
j4
i1
i8
h1
h5
g1
g10
f1
f6
e1
e10
d1
d5
c1
c8
b1
b4
a1
a6


PIENSE
THINK
DENKE
PENSER
$24,000
Who is Stoker?
$ 1,000
$77,147
Who is Bram Stoker?
$ 17,973
$21,600
$5600


Messages
Mail
Phone
What can I help you with?

What does IBM's Watson 'think'?

IBM Watson Explorer Content Analytics



What does IBM's Watson 'think'?

IBM Watson Explorer Content Analytics

Threat monitoring example: IBM X-Force

IBM Watson Bluemix cognitive analytics

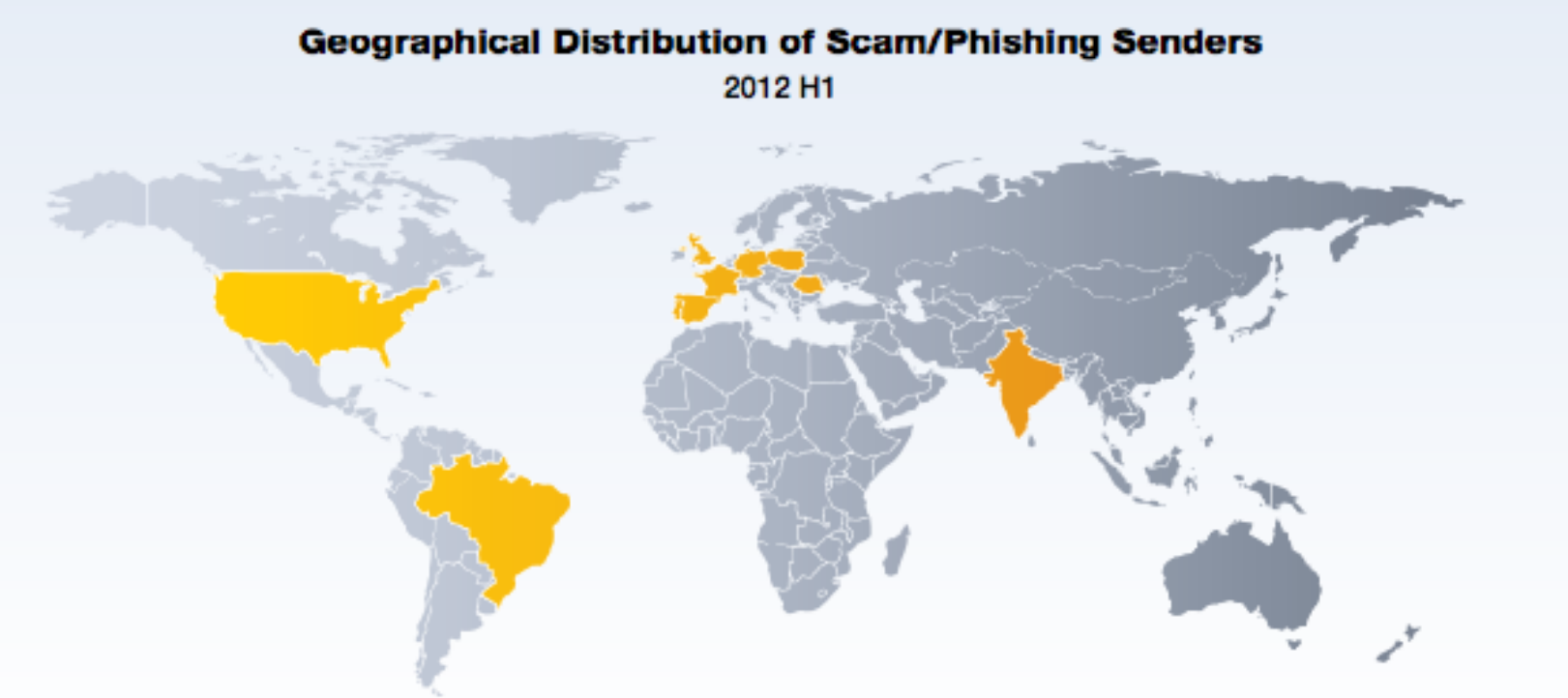


Figure 32: Geographical Distribution of Scam/Phishing Senders - 2012 H1

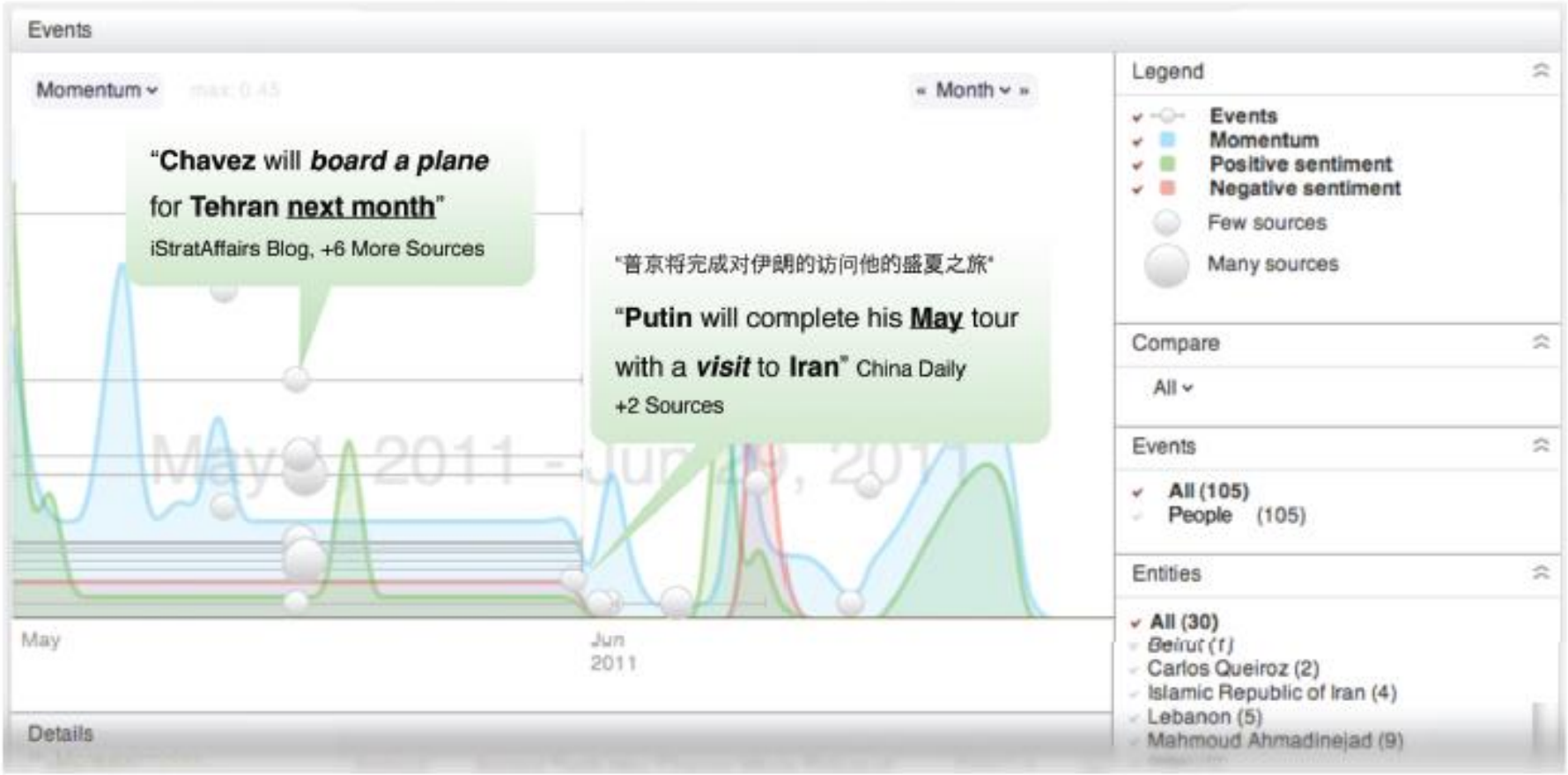
Country	% of phishing
Spain	7.6%
Romania	7.4%
United Kingdom	6.4%
Germany	5.5%
Brazil	5.0%

Country	% of phishing
India	4.9%
Poland	4.8%
France	4.4%
USA	3.8%
Portugal	2.5%

Table 4: Top 10 Countries of Scam/Phishing Origins - 2012 H1

Threat monitoring example: Recorded Future

Pervasive web text analytics monitoring



Locally installed platform for closed networks.

CONTACT DETAILS

drs Scott Mongeau

Analytics Manager
Risk Services
smongeau@deloitte.nl

+31 (0)65 359 8660