

Cambridge Judge Business School

Cambridge Centre for Risk Studies 2017 Risk Summit

CYBER THREAT ACTORS: HACKONOMICS

Andrew Smith, Research Assistant
Centre for Risk Studies







Centre for
Risk Studies








UNIVERSITY OF
CAMBRIDGE
Judge Business School

Cyber Risk Scenario and Data Schema Research

Information Technology Loss Processes

-  **Data Exfiltration**
(‘Leakomania’)
-  **Denial of Service Attack**
(‘Mass DDoS’)
-  **Cloud Service Provider Failure**
(‘Cloud Compromise’)
-  **Financial Theft**
(‘Cyber Heist’)
-  **Ransomware**
(‘Extortion Spree’)
-  **Malware**
(‘Sybil Logic Bomb’)

Operations Technology Scenarios of Asset Damage

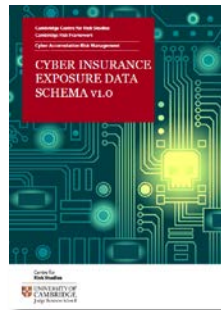
-  **Cyber Attack on US Power Generation**
(‘Business Blackout’) * v1.1
-  **Cyber Attack on UK Power Distribution**
(‘Integrated Infrastructure’)
-  **Cyber attack on Commercial Office Buildings**
(Laptop batteries fire induction’)
-  **Cyber attack on Marine Cargo Port**
(‘Port Management System’)
-  **Cyber Attack on Industrial Chemical Plant**
(‘ICS Attack’)
-  **Cyber Attack on Oil Rigs**
(‘Phishing-Triggered Explosions’)



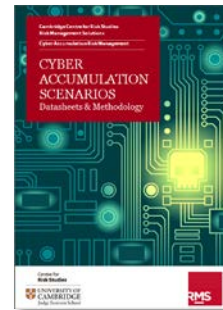
Sybil
Logic Bomb



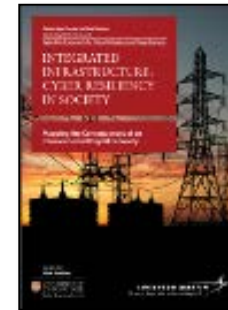
US Cyber
Blackout



Exposure Data
Schema



Accumulation
Scenarios



UK Cyber
Blackout



Cyber
Terrorism

'Hackonomics'

- Economic perspective of hacking
- Profile cyber threat actors behaviour:
 - Case study approach to profiling
- Create threat actor matrix
- Understanding the 'business models' of hacking groups
 - Cyber-criminals are 'profit maximisers'
- Model threat actor targeting using economic framework



Sample of Known State Sponsored/ Nation State Groups



Chinese Actors

- APT 1(Comment Panda)
- APT 3 (Gothic Panda)
- APT12 (Numbered Panda)
- APT 16
- APT 17(Deputy Dog)
- APT 18(Dynamite Panda)
- Putter Panda
- APT30 (Naikon)



North Korean Actors

- Bureau 121
- DarkSeoul Gang
- Lazarus Group



Russian Actors

- APT 28 (Fancy Bear)
- APT 29 (Cozy Bear)
- Energetic Bear (Crouching Yeti)
- Turla (Venomous Bear/Snake)



US Actors

- Equation Group
- NSA
- Tailored Access Operations
- Animal Farm



Iranian Actors

- Tarh Andishan
- Ajax Security Team/ 'Flying Kitten'
- ITSecTeam



Israel

- Unit 8200
- Duqu Group



Palestine

- AridViper



Lebanon

- Volatile Cedar



Syria

- Syrian Electronic Army



Vietnam

- APT32

Estimated total state-sponsored/nation state groups: **91**

Sample of Non-State Threat Groups

- Organised Crime APT/Hierarchical (**Estimated total: 35**)
 - Singing Spider
 - Union Spider
 - Andromeda Spider
 - Dexterous Spider
- Organised Crime (Swarm)
 - Carberp users groups
 - Rove Digital
 - Shadow Brokers (could be Russian state backed)
- Hackers (Vigilante)
 - The 414's
 - FinnSec Security
 - Derp
 - Hackweiser
 - Lulsec
 - Lizard Squad
- Elite Mercenary hackers
 - Hidden Lynx
- Hacktivists
 - Anonymous
 - Decodidio
 - DeadEye Jackal
 - Ghost Jackal
 - Corsair Jackal
 - Extreme Jackal
- Cyber Terrorist Groups
 - Islamic State Hacking Division
 - Hezbollah Cyber Group
 - Al Qaeda Electronic Army
 - Al Qaeda Electronic in Egypt
 - Tunisian Cyber Army
 - Cyber Caliphate Army (CCA) (Islamic State Hacking Division)
 - Afaaq Electronic Foundation
 - RedHack
 - Fallaga Team (Tunisian)

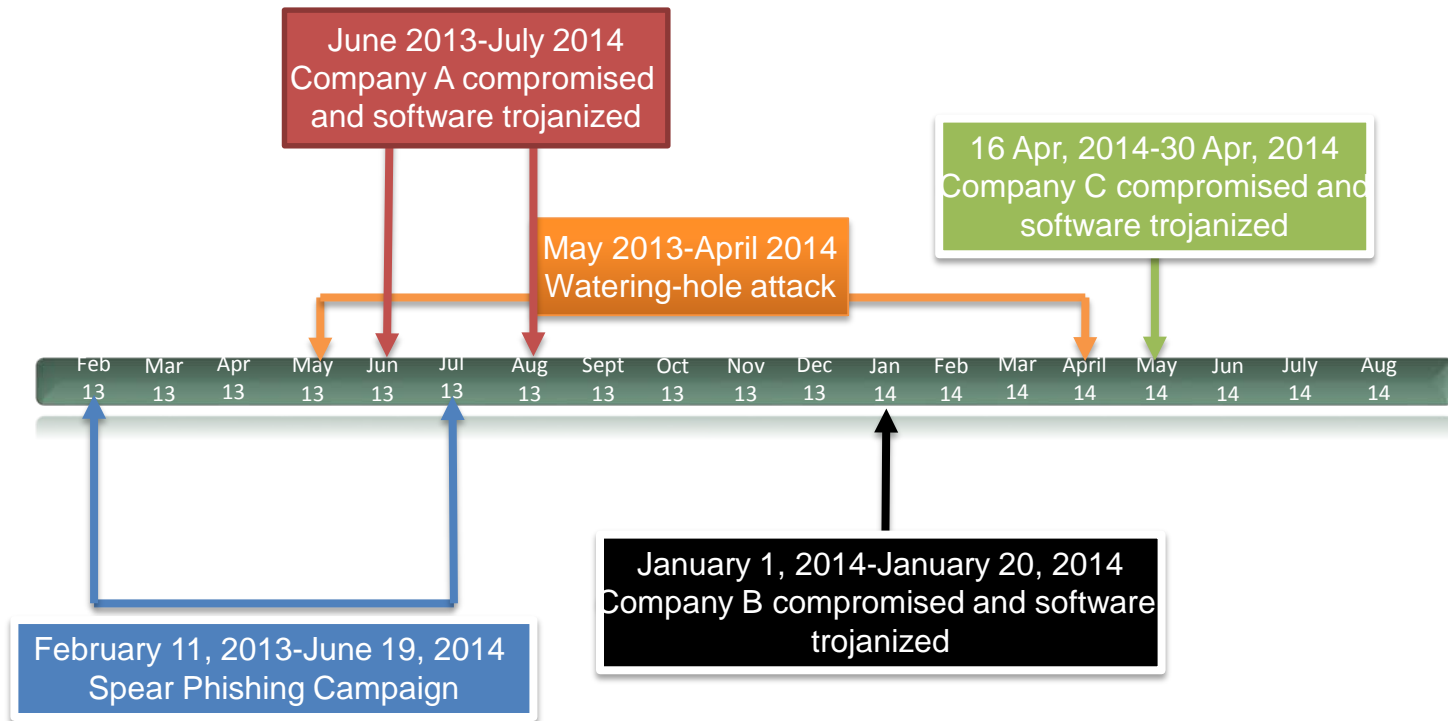
Creating Threat Actor Profiles

- Threat actor profiles are created using case studies
- Case studies outline the following attributes:
 - Motivations
 - Category of threat actor
- Tactics Technique and Procedure (TTP)
 - Skill level
 - Covertness
 - Targeting function (opportunistic vs targeted; geographic targeting)
- Attribution and objectives
 - Resource levels (first order approximation)

Case Study: State Sponsored APT-Energetic Bear



Energetic Bear Operations: Timeline 2013-2014



Source: Symantec (2014): 'Dragonfly: Attacks Against Energy Suppliers'

Energetic Bear Threat Profile

- Motivations: Stealing IP and sabotaging the industrial sector
 - Objective: Intelligence gathering and destruction.
- Skill: High
- TTP: APT, water holing, trojanised software, malware developers.
- Attribution study:
 - Direct targeting: Industry specific targets.
 - Geographic targeting: Focused on the West (Europe/ N.America).
 - Visibility: Covert
- People: 100+
- Resources: \$1-\$3 million



Threat Actor Matrix

		Elite mercenary	State-Sponsored	Hacktivist
	Attributes	Hidden Lynx	Energetic Bear	Anonymous
Skill	Low			X
	Medium			
	High	X	X	
People	0-10			
	10-20.			
	20-50			
	50-100	X		
	100+		X	X
Resources (\$)	0-100,000			X
	100,000-1,000,000	X		
	1,000,000-3,000,000		X	
	3,000,000+			
TTP	Website Defacement			X
	Phishing/Spear Phishing			
	DDoS			X
	Ransomware	X		
	Malware Developers	X	X	
	Water holing	X	X	
	Social Engineering	X	X	
	Single Purpose Malware	X	X	
Advanced Persistent Threats	X	X		
Visibility	Covert	X	X	
	Intentionally Overt			X
	Overt			
Targeting	Opportunistic			X
	Direct	X		
Objective (ideology)	Defacement			X
	Destruction			X
	Business Interruption		X	X
	Intelligence gathering	X	X	
Objective (monetary)	Obtaining IP	X	X	
	Data Exfiltration (for resale)	X		
	Business Interruption (RW)	X		
Geographic Targeting	Yes		X	
	No	X		X

Economics Of Threat Actor Targeting

- Targeting fundamentally a matter of economics.
- Cost-benefit decision making.
- Cost benefit ratio:

Pay-out/Benefit

$$\frac{M_b + P_b}{LB_c} \geq 1$$

Logistical Burden

- Benefit per attack:
 - M_b = Expected monetary benefit
 - P_b = Expected psychological benefit
- Rank companies by target attractiveness

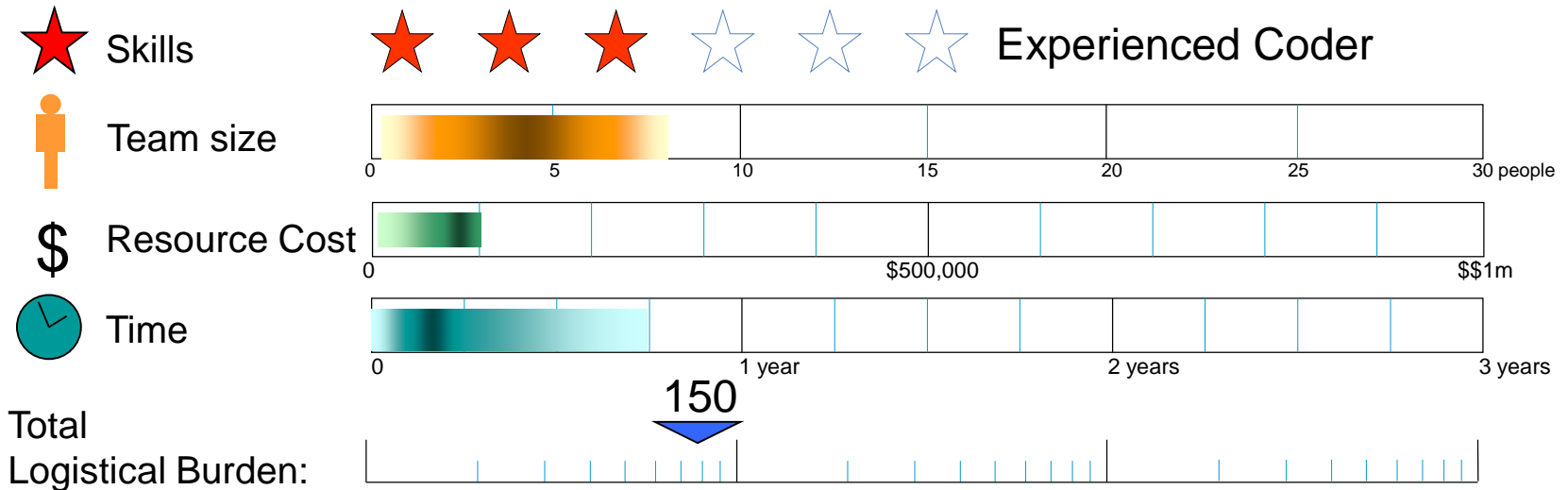


Logistical Burden for Cyber Attacks

- Derived from game theoretic principles.
- Estimate relative difficulty of cyber attacks.
- Logistical burden uses four parameters:
 - ★ Skill level: Requirement of the project architect or lead coder.
 - 👤 Team size: Number of people (of different skills) required to complete the project.
 - 💰 Resource cost: Monetary value of the equipment, purchasing, outsourcing, travel, and other financial outlay to implement the project.
 - 🕒 Time for planning and preparation, development, testing, executing.
- Use subject matter specialists to estimate numbers.

Logistical Burden for a Cyber Campaign

WannaCry Ransomware Attack



Relative Logistical Burden of Different Cyber Attacks

Cyber Attacks	Skill Level	Team Size	Labour Cost	Months	Resource Cost per Month	Team Cost	Total Cost LB Index
Financial Transaction Theft - Upper Stress Test	STOL	60	1,000,000	24	200,000	4,800,000	5,800,000
Financial Transaction Theft - Reference	STOL	48	750,000	18	150,000	2,700,000	3,450,000
Leakomania - Upper Stress Test	STOL	30	500,000	12	146,000	1,752,000	2,252,000
Financial Transaction Theft - Lower Stress Test	Systems Architect	36	500,000	12	100,000	1,200,000	1,700,000
Mass DDoS - Upper Stress Test	Systems Architect	12	500,000	12	90,000	1,080,000	1,580,000
Mass DDoS - Reference View	Systems Architect	8	300,000	9	90,000	810,000	1,110,000
Leakomania - Reference View	Systems Architect	25	250,000	9	90,000	810,000	1,060,000
Extortion Spree - Upper Stress Test	Systems Architect	20	250,000	12	50,000	600,000	850,000
Mass DDoS - Lower Stress Test	Systems Architect	6	200,000	6	90,000	540,000	740,000
Leakomania - Lower Stress Test	Highly Experienced Coder	16	200,000	8	32,000	256,000	456,000
Extortion Spree - Reference View	Highly Experienced Coder	16	150,000	8	32,000	256,000	406,000
Extortion Spree - Lower Stress Test	Experienced Coder	12	90,000	6	24,000	144,000	234,000
WannaCry Ransomware Attack	Experienced Coder	8	50,000	10	10,000	100,000	150,000

Concluding Remarks

- Extensive literature exists on cyber threat actors.
- Applying economic analysis to threat actor modelling.
 - Cost-benefit framework: mapping threat actors to potential targets
- Rapid evolution of attack vectors and introduction of black markets increasing capabilities.
 - Commodity malware
 - The rise of ransomware

Centre for **Risk Studies**



UNIVERSITY OF
CAMBRIDGE
Judge Business School

Andrew Smith
a.smith@jbs.cam.ac.uk