Cambridge Judge Business School

Cambridge Centre for Risk Studies 2018 Risk Summit

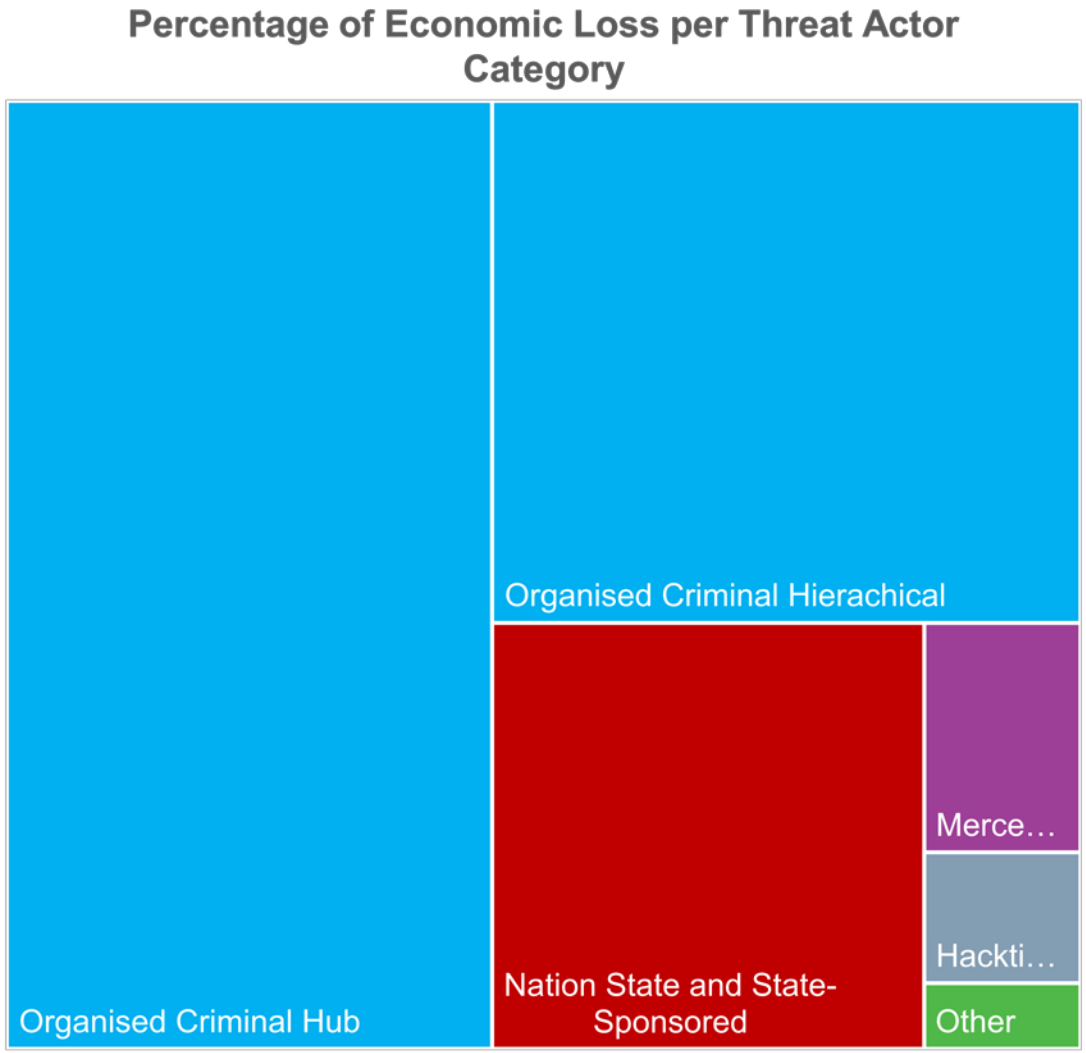
THREAT ACTORS IN THE CYBER BLACK ECONOMY

Andrew Smith, Research Assistant
Centre for Risk Studies

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Economic Loss Caused by Threat Actor Categories



Estimated **$1.5 Trillion** of economic loss caused by threat actors

- Nation State and State-Sponsored
- **Organised Cyber Criminal: Hub and Hierarchical**
- Mercenary Hackers
- Hacktivist
- Other: Script Kiddies, Cyber Terrorist

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for **Risk Studies**

Sample of Known Threat Actor Groups

- Nation State
  - NSA
  - GCHQ
  - Comment Panda
- State-Sponsored
  - Sofacy (Fancy Bear)
  - Lazarus Group
  - Equation Group
- Mercenary
  - Hidden Lynx

- Organised Crime
  - Carbanak
  - Wolf Spider
  - Butterfly
  - Carberp
  - Cobalt
  - DarkHotel
- Vigilante Hackers
  - Lulsec
  - Lizard Squad

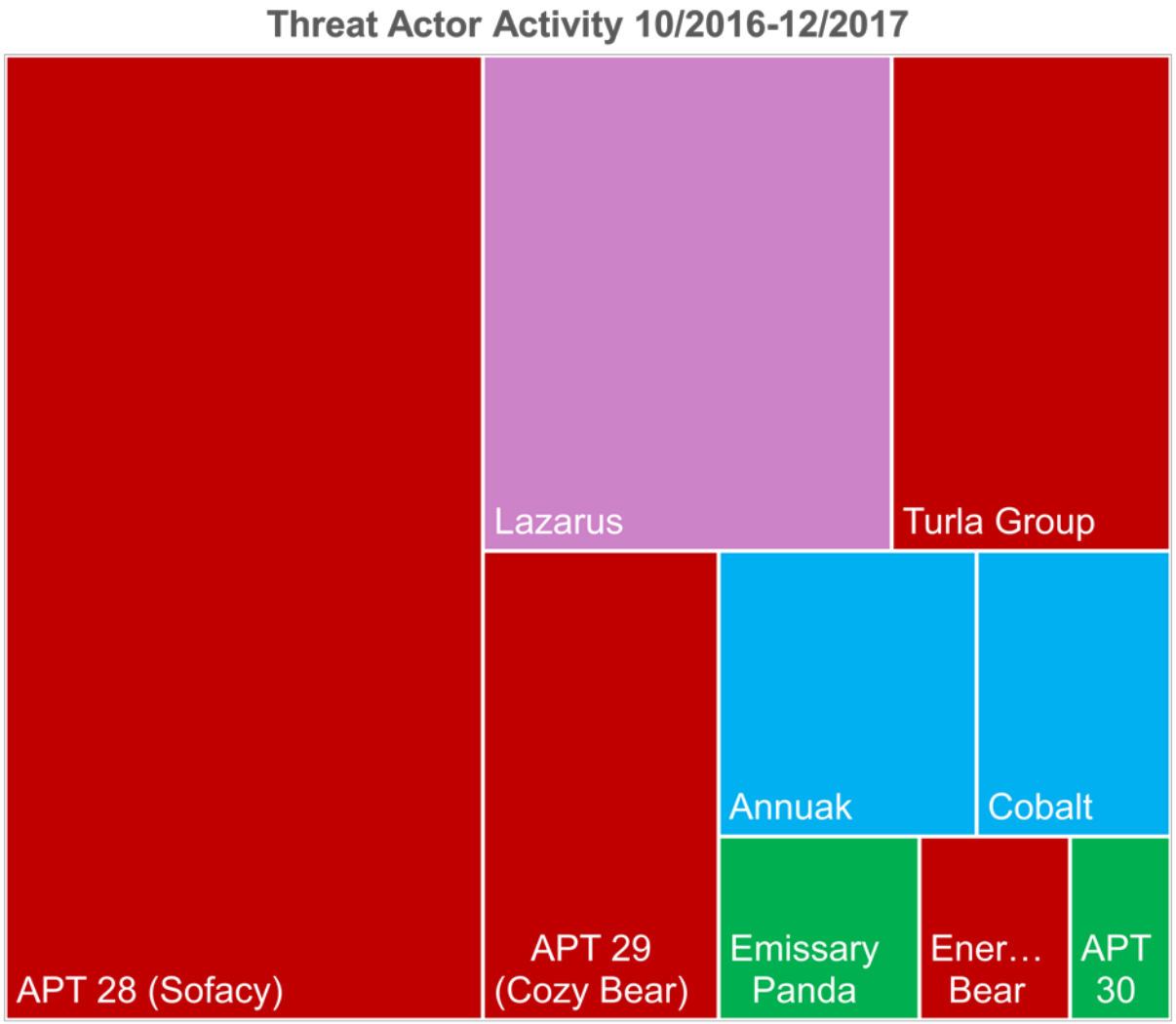
- Hacktivists
  - Anonymous
  - Syrian Electronic Army
  - TeaMp0ison
- Cyber Terrorism
  - Hezbollah Cyber Group
  - Tunisian Fallaga Team
  - United Cyber Caliphate

Energetic Bear

Lulsec

Syrian Electronic Army

Threat Actor Annual Activity



11 Events
To Scale

- Russian State-Sponsored
- Organised Cyber Criminal
- North Korean State-Sponsored
- Chinese State-Sponsored

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for **Risk Studies**

Organised Cyber Criminals Groups: Hub and Hierarchical

- Organised cyber criminal groups are motivated by financial gain
  - Maximise profits
- Two distinct business models of cyber criminal organisations
- Hierarchical groups are similar to traditional organised crime groups
  - Clear management structure
  - Division of labour
  - Often operate in physical premises
- Hub groups operate solely as a ‘black e-commerce’ organisation or as a ‘hybrid’
  - Core group of threat actors
  - Solicitate the help of associates in their network

Threat Actor	Skill Level	Labour	Resources	Visibility	Targeting	Motivations	Geo Target	Threat Rank	Count
Hub	Medium	8*	$0.1m	Covert	Opportunistic	Monetary	No	4	6400
Hierarchical	Medium	27	$1-3m	Covert	Opportunistic	Monetary	No	3	4500

Hackonomics: Behaviour of Cyber Criminals

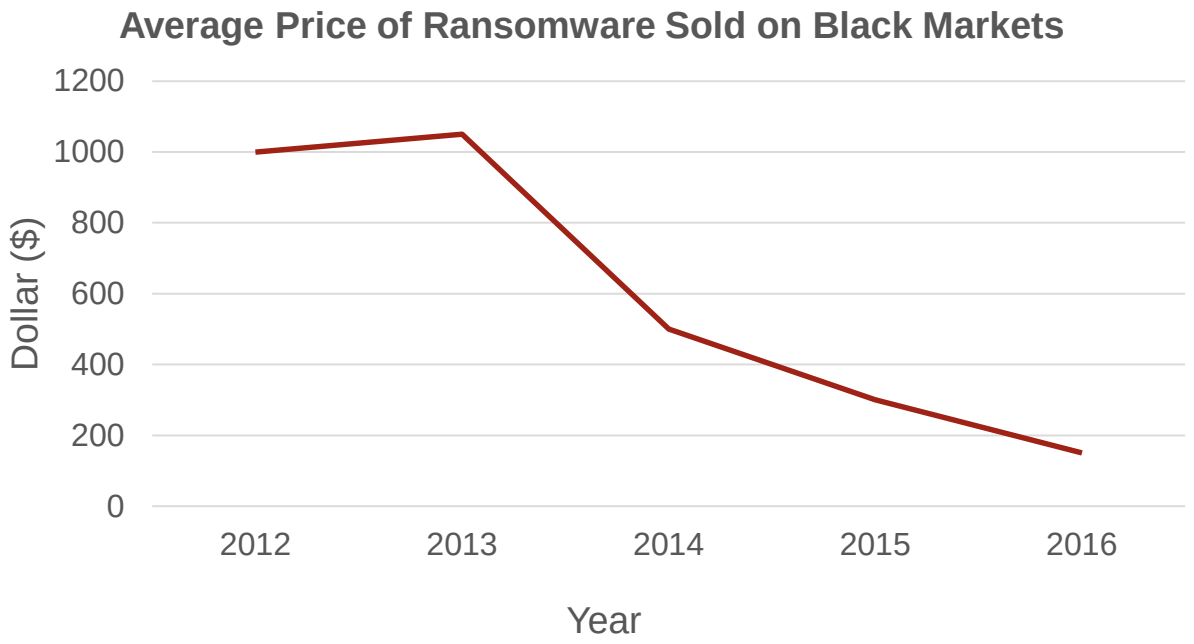
- Hacknomics perspective: business model of threat actors
- Cyber threat actors have scarce resources
  - Opportunity cost
- Targeting decisions based on a cost-benefit framework
  - Logistical burden vs expected benefits
- Regime changes in the cyber risk landscape alter the equilibrium of the cyber black economy

Regime Shift: Cyber Black Markets

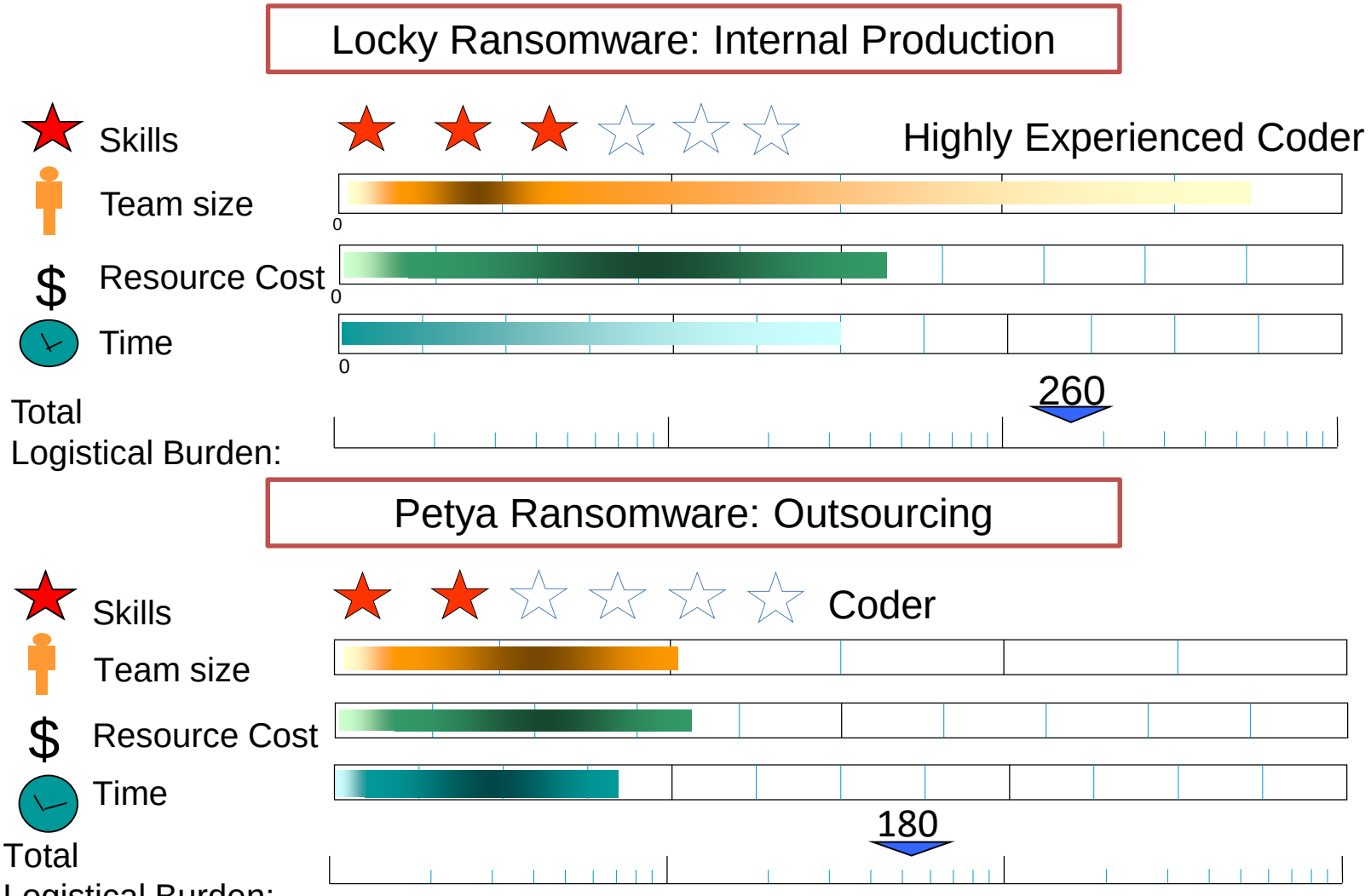
- The development of black markets has changed the business model of cyber criminals
- Estimated 18 active markets in the cyber black economy
- Emergence of new business model: Crime-as-a-service
- Marketplace products
  - Stolen records
  - Zero-day exploits/exploit kits
  - Malware
  - Mercenary hackers

Decreasing Price of Commodity Malware

- Cyber criminal business models are not following internal economies of scale
  - Outsourcing
- Commodity malware decreases the skill level and resource cost per attack
  - Lowers logistical burden
  - Reduces barriers to entry
- More cyber criminals in the black economy
- Likely increase in the frequency of attacks

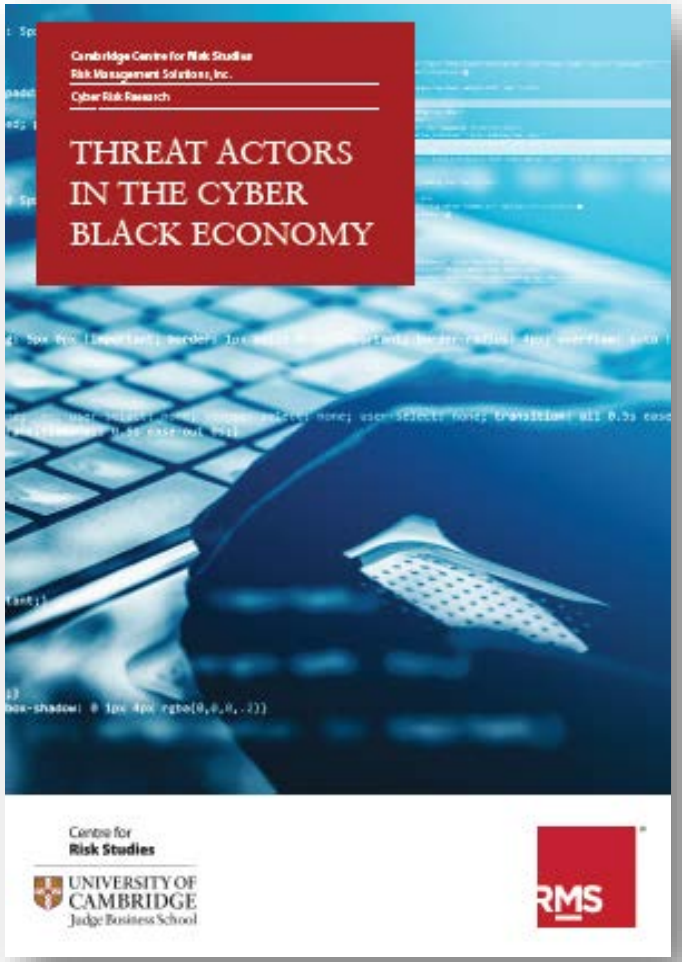


Internal Production vs Outsourcing Example



Mitigating Threat Actor Activity

- **What does hackonomics teach us about reducing cyber risk?**
- Targeting behaviour
  - Map companies characteristics to motivations and capabilities of threat actors
  - Target substitution: path of least resistance for threat actors
- Combat crime as-a-service model
  - Patch maintenance
  - Incentivise ‘white/grey’ hat actors
  - Increases logistical burden
- Understand how future trends alter the fragile equilibrium between cyber attackers and defenders



Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School