Cambridge Centre for Risk Studies

The 10th Anniversary Risk Summit

TECHNOLOGY RISKS – CCRS RESEARCH OUTLOOK

Kelly Quantrill

Cyber Risk Researcher

20 June 2019

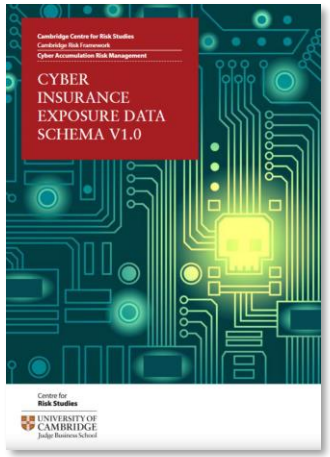
Cambridge Judge Business School

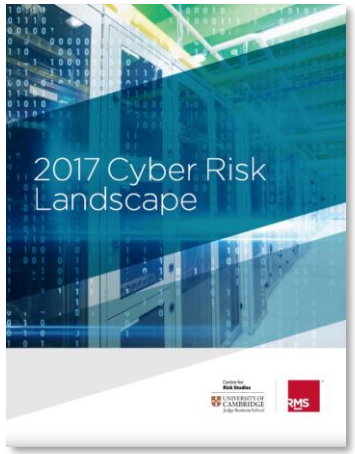
Centre for Risk Studies

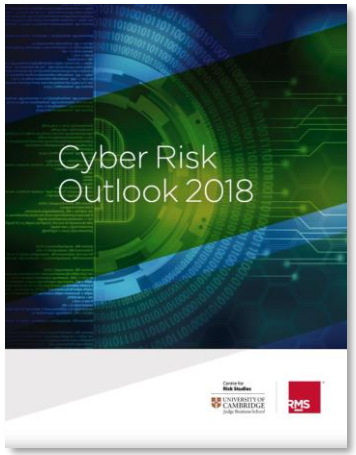
UNIVERSITY OF CAMBRIDGE Judge Business School

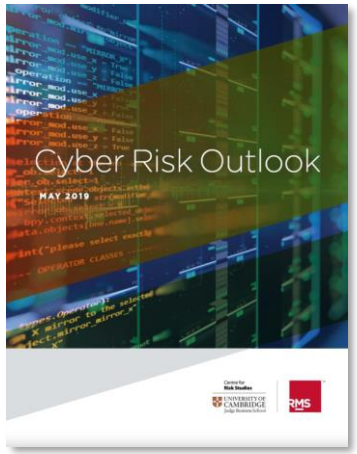
RISK 10

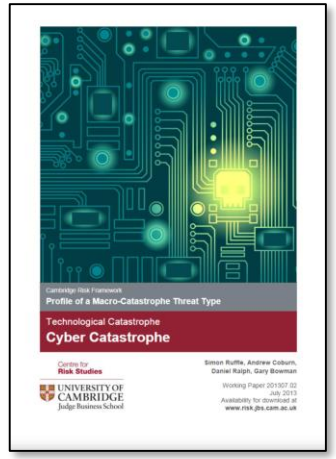
A Decade of CCRS Cyber Research

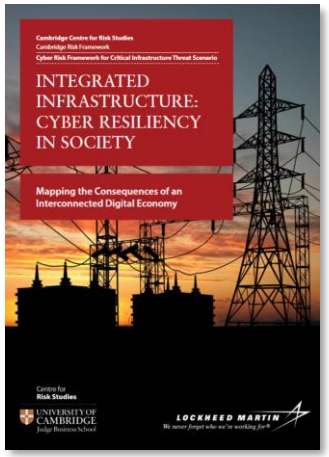


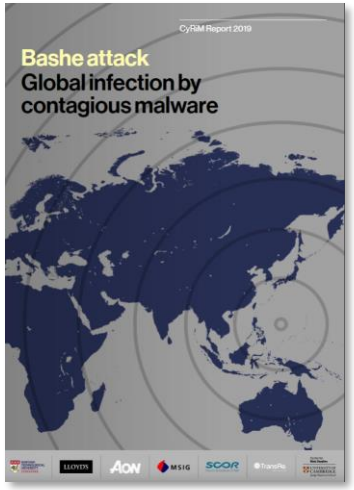


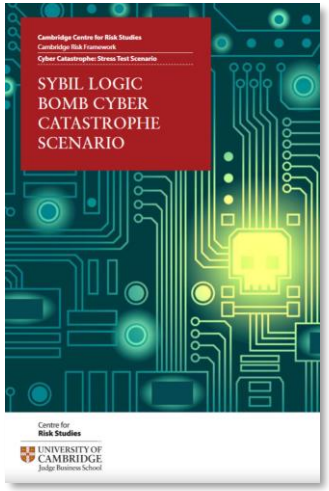


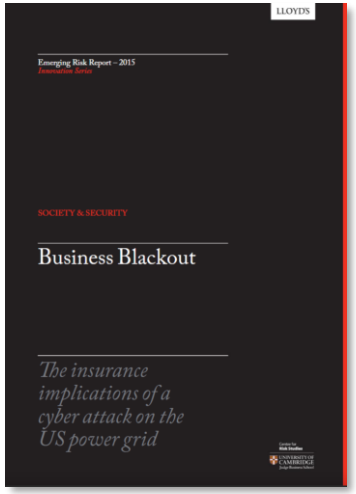


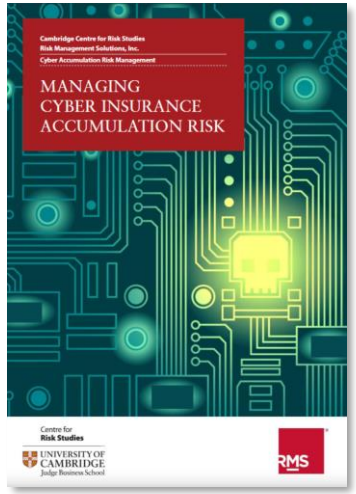


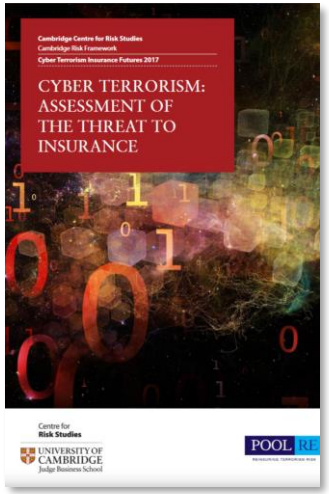


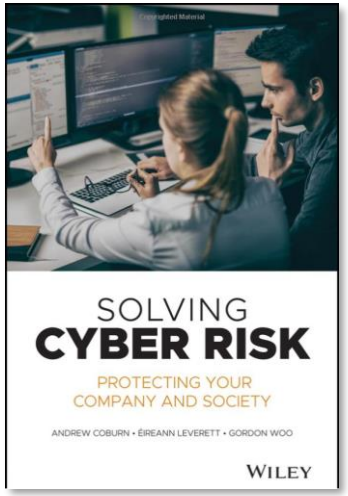












UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

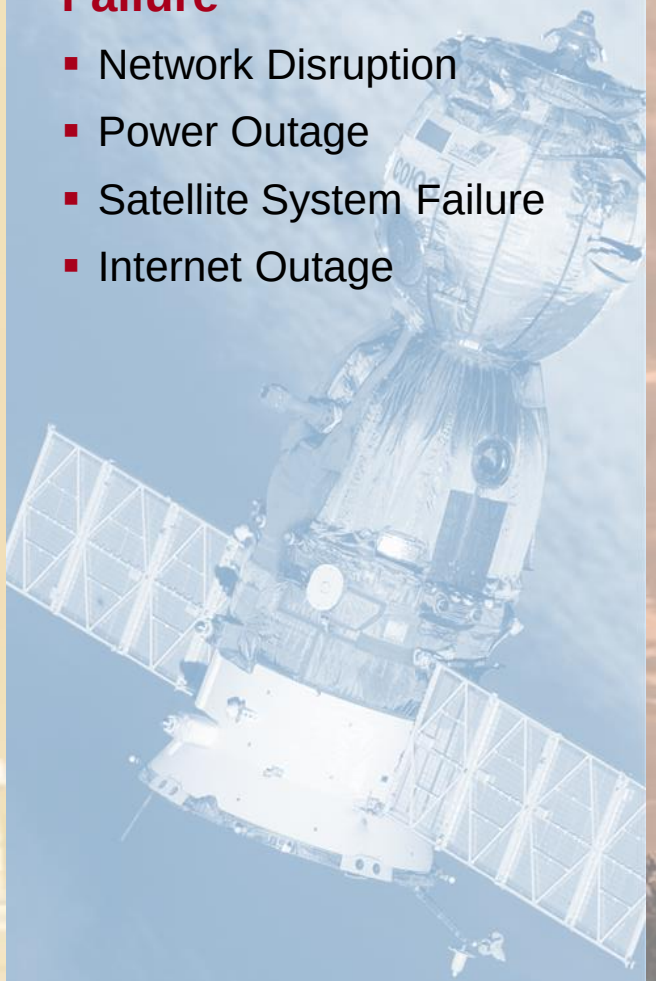
Cambridge Taxonomy of Business Risks: Technology

Disruptive Technology

- E-Commerce
  - Clicks & Mortar
- Gig Economy
- Robotics & Automation
- Artificial Intelligence (AI)
- 5G Technology
- Augmented Reality/Virtual Reality
- Blockchain

Infrastructure/System Failure

- Network Disruption
- Power Outage
- Satellite System Failure
- Internet Outage



Industrial Accident

- Explosion
- Fire
- Nuclear
- Pollution

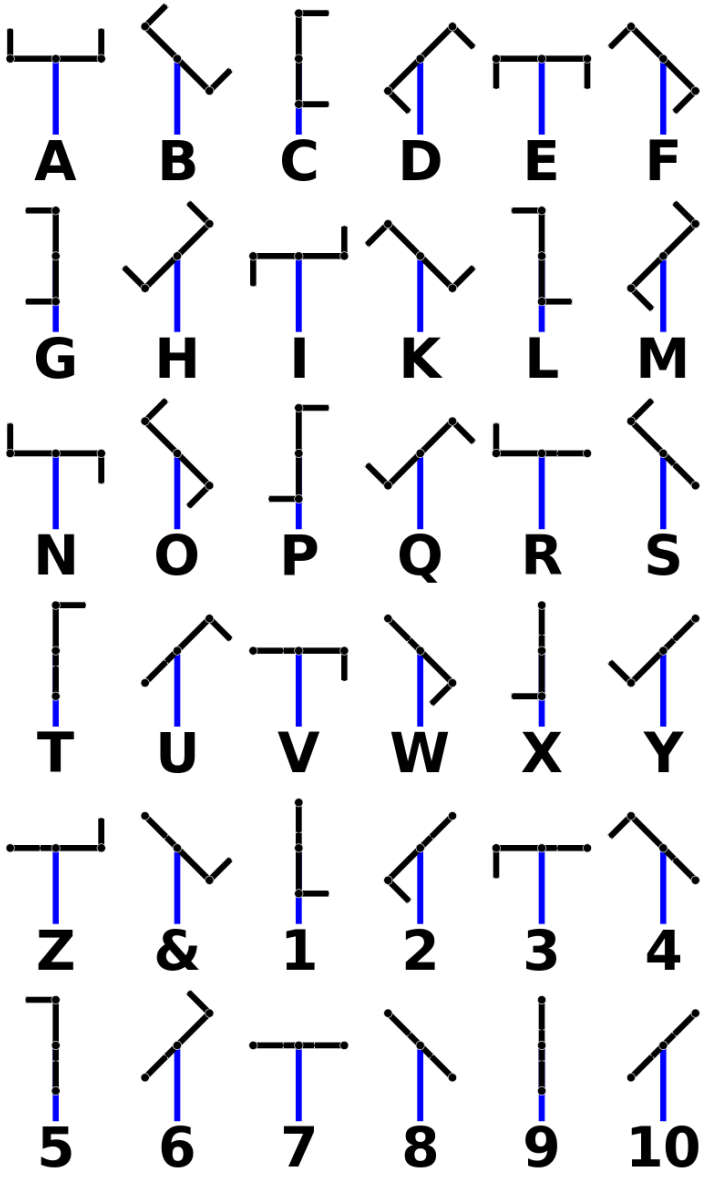
Cyber Attack

- Contagious Malware
- Data Exfiltration
  - Intellectual Property Loss
- Distributed Denial of Service Attack
- Cloud Service Provider Failure
- Internet Service Provider Failure
- Counterparty or Supplier Failure
- Financial Transaction Theft
- Industrial Control System Compromise

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

The First Cyber Attack - 1836

The "Chappe Network" in France. By Jeunamateur – Own work d'après "La télégraphie Chappe", FNHAR, 1993, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=19700042



Semaphore telegraph – Chappe system (Wikipedia)

A Decade of Cyber Attacks

ANDY GREENBERG SECURITY 08.22.18 05:00 AM

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

DDoS attack that disrupted internet was largest of its kind in history, experts say

Tesla Breach: Malicious Insider Revenge or Whistleblowing?

Baltimore government held hostage by hackers' ransomware

WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled

Ohio Provider Pays $75K Ransom After Serious Hack on IT System

Hacker Group, Anonymous, Hits Federal Reserve

Trump Is Losing the Fight to Ban Huawei From Global Networks

Stuxnet Worm Attack on Iranian Nuclear Facilities

Cyber-attack causes aircraft parts maker to close indefinitely

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

Target to Pay $18.5 Million to 47 States in Security Breach Settlement

Equifax Data Breach Impacts 143 Million Americans

WannaCry, 2017

$4 billion economic loss,150 countries

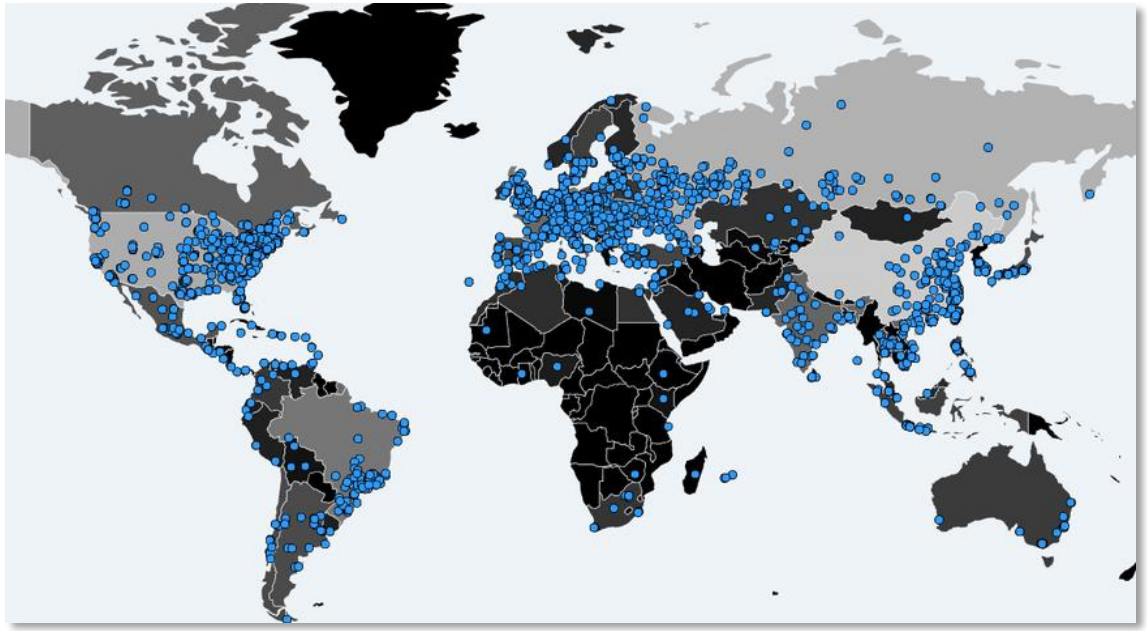
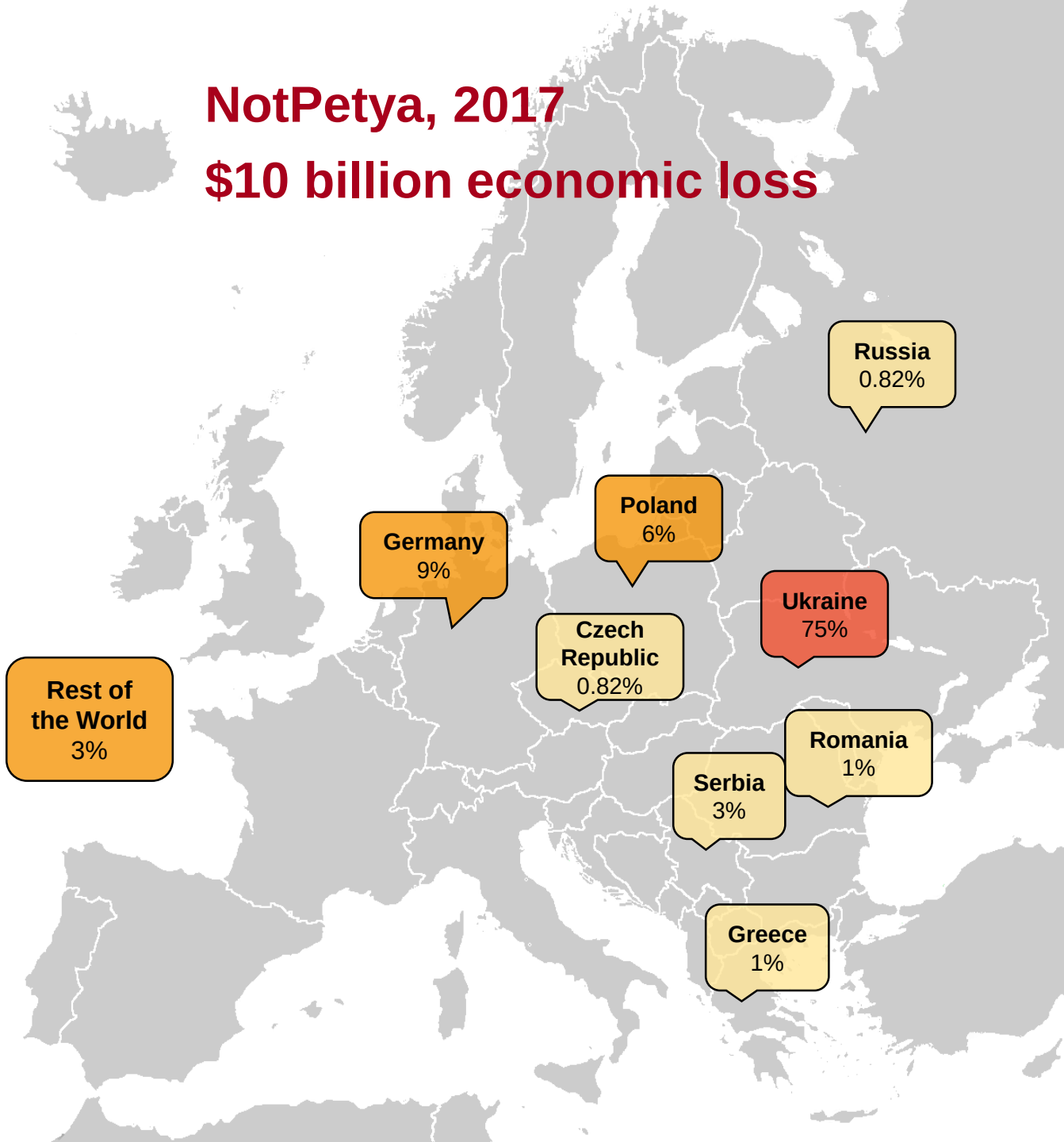


Image Source: MalwareTech's WCrypt botnet tracker

NotPetya, 2017

$10 billion economic loss



UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

2018 Cyber Attack on the City of Atlanta, Georgia

Creative Commons

- $9.5 million spent restoring services
- SamSam Ransomware
- Multiple municipal services down
- Years' worth of data destroyed
- Officials and residents had to resort to pen and paper
- Systems remained offline up to three months later
- Two Iranian hackers indicted later that year

Critical National Infrastructure

- Assets essential for the functioning of a society and economy
- Facilities, systems, sites, information, people, networks, and processes
- The UK Government's 2016 cyber security strategy states that the cyber security of the UK's critical national infrastructure (CNI) from the physical infrastructure to the digital networks and data is critical because *a successful attack "would have the severest impact on the country's national security".*

Security warning: UK critical infrastructure still at risk from devastating cyber attack

Not enough is being done to protect against cyber attacks on energy, water and other vital services.

Critical infrastructure under relentless cyber attack

Critical infrastructure attacks: nations are not ready

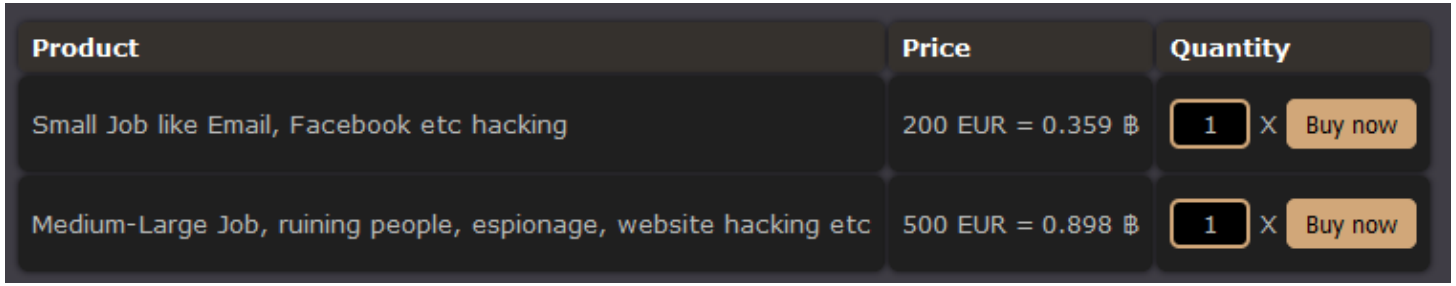
Pixabay

Cybercrime Commoditisation

- DDoS-for-Hire
- Rent a Hacker
- Ransomware-as-a-Service (RaaS)
- Mobile trojan development kits
- Cryptojacking

Category	# Listings
App	144
Botnet	125
Exploit	115
Malware	310
Phone	261
Remote-access Trojan (RAT)	105
Website	664

"Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets". Tajalizadehkhoob, S., Klievink, B., Akyazi, U., Christin, N. August 2018. 27th USENIX Security Symposium, USA.



Anonymous .onion service reachable via the Tor network

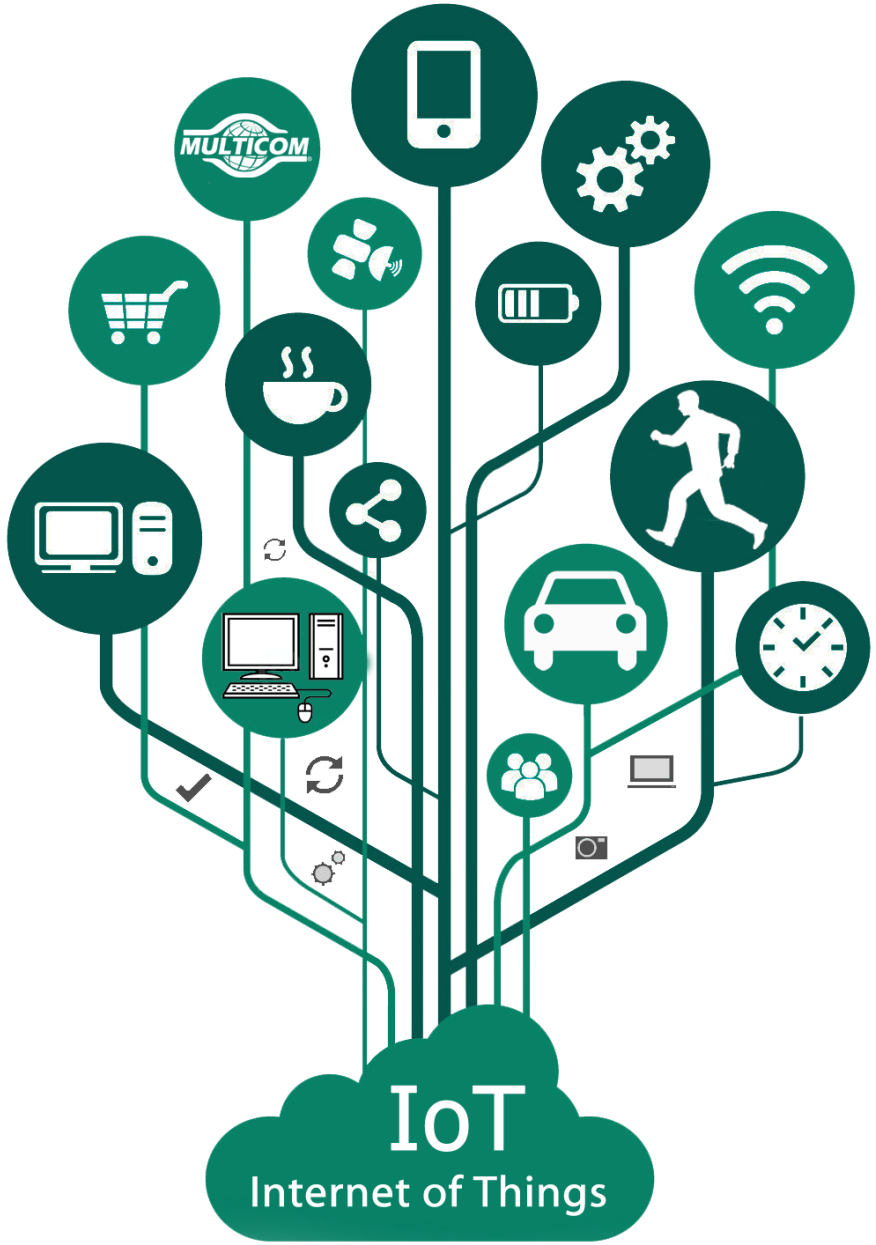
Type of Malware	Kit Name	Price (US$)
Exploit Kits	Whitehole	$600/month
	Sweet Orange	$1,800/month
	Elenore	$1,000
	Gpack	$1,000
	Cool (+ cryptor + payload)	$10,000/month
Zero-day	Windows	$60,000
	Microsoft Office	$50,000
	Mac OSX	$20,000
	iOS	$100,000
	Chrome/Internet Explorer	$80,000
	Adobe Reader	$50,000

Ablon, Lillian, Martin C Libicki, and Andrea A Golay. 2014. *"Markets for Cybercrime: Tools and Stolen Data. Hackers' Bazaar."* RAND Corporation - National Security Research Division

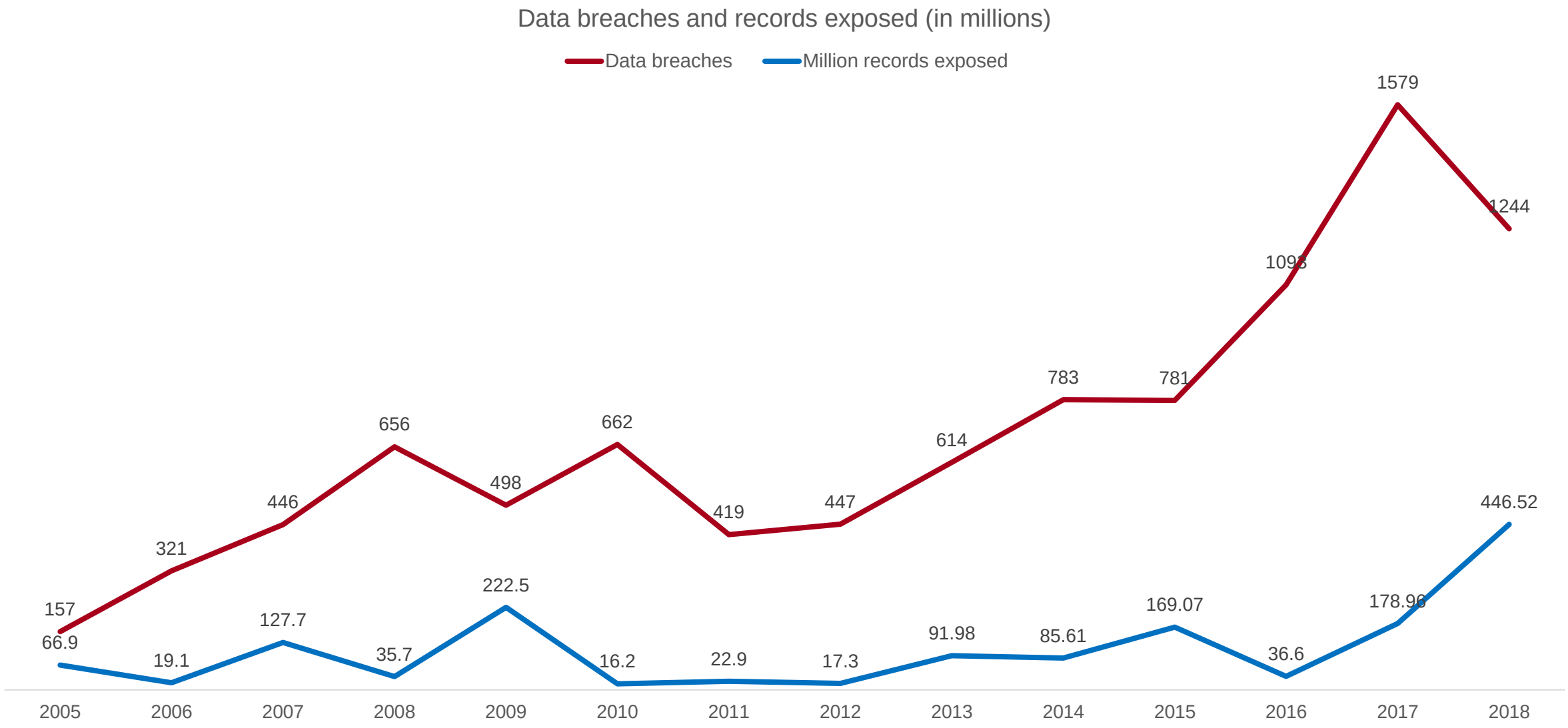
The Internet of Things (IoT)

- 20 billion connected devices by 2020, requiring the support of 400 million servers
- *California became the first state with an IoT cyber security law*
- The rise of botnet armies
- Bridge between digital and physical worlds
- Internet-connected security cameras account for almost half of the IoT devices compromised by hackers

- Google Cloud service failure led to Nest failure
- AWS failure led to “If This Then That” (home automation) failure
- Driver locked out of Tesla Model S in Arizona

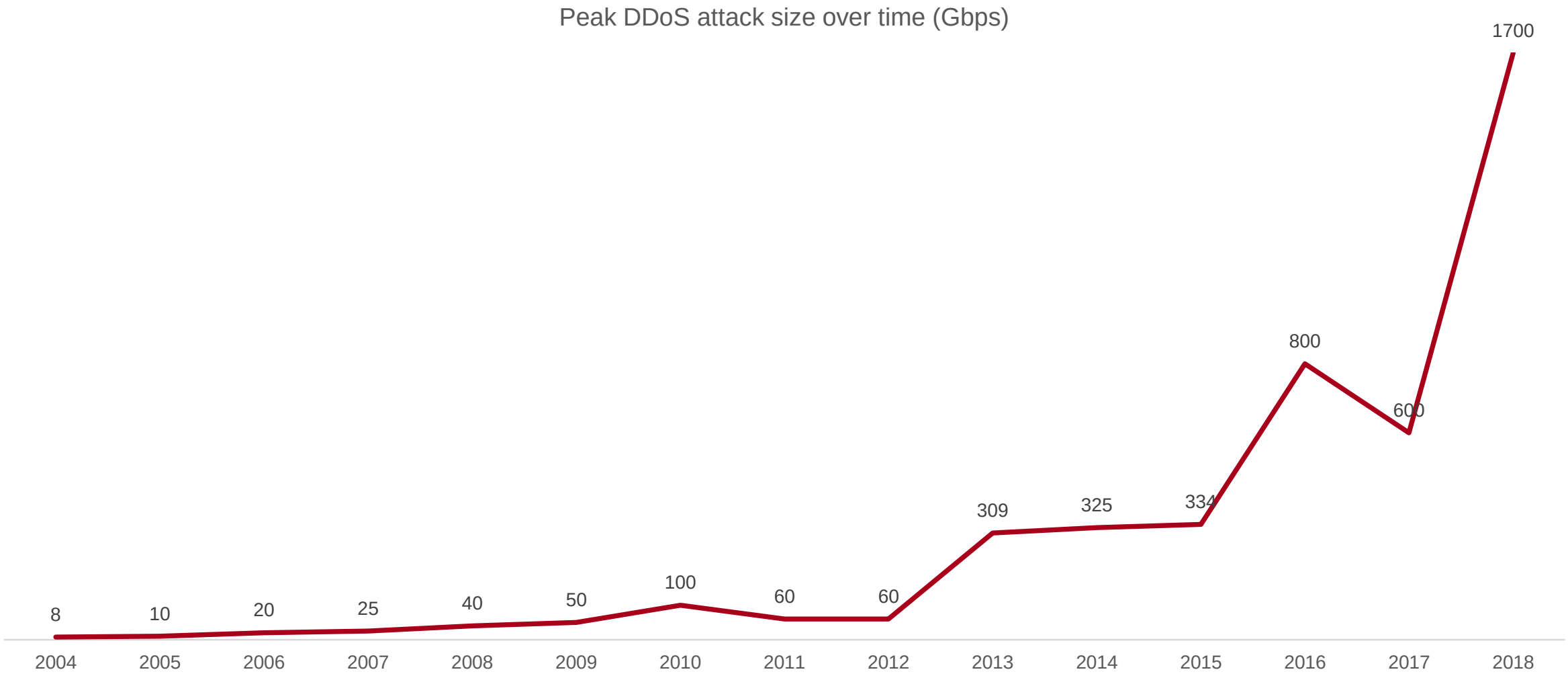


Data Breaches



Identity Theft Resource Center – *ITRC 2018 End-of-Year Data Breach Report*

DDoS Attacks



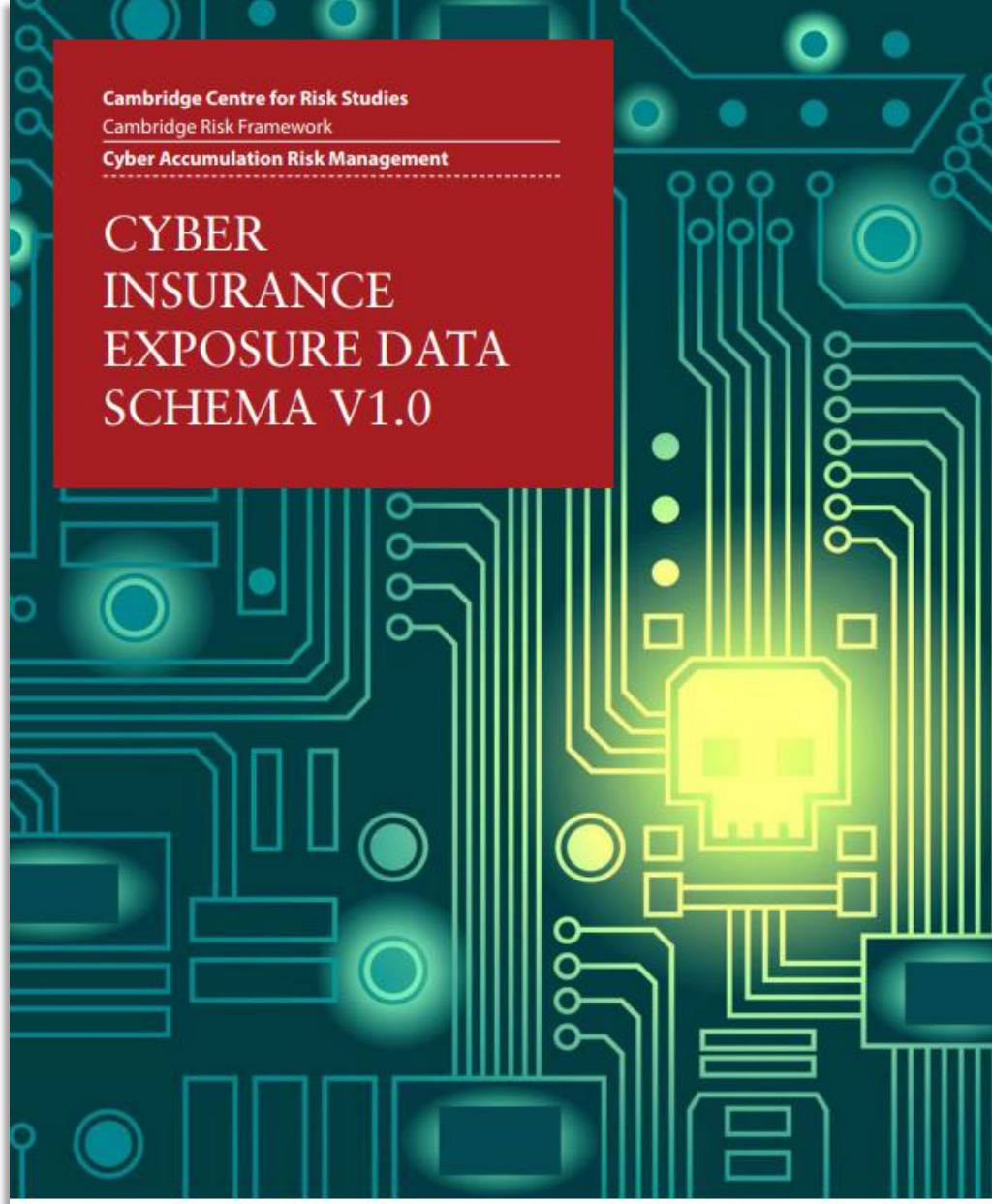
NETSCOUT Arbor – *Annual Worldwide Infrastructure Security reports*

Cryptocurrency

Bitcoin Price – Coinbase. 19 June 2019

Risk Accumulation

- CRS published a cyber risk accumulation data standard in 2015 (schema and data definitions)
- Interconnected software and systems requiring changing business models and adoption of industry standards.
- More consolidation and accumulation of risks.
- Rapidly changing rate of device connectivity and device ownership.
- Increasing complexity causing more technologies to take on a systemic nature.
- Cyber security used to be a technology issue but is now a business issue.
- A single event can be global and impact thousands of businesses at different scales.
- The accumulation of liabilities could expose an insurer to high financial losses

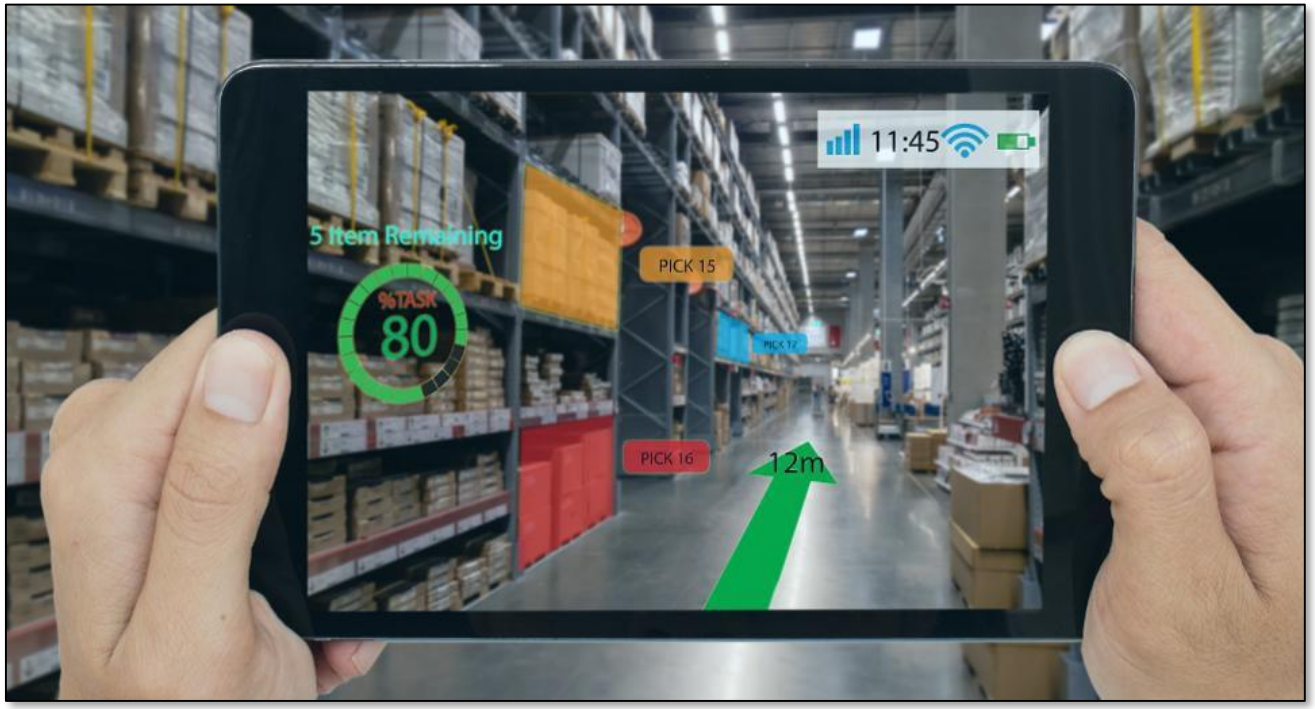


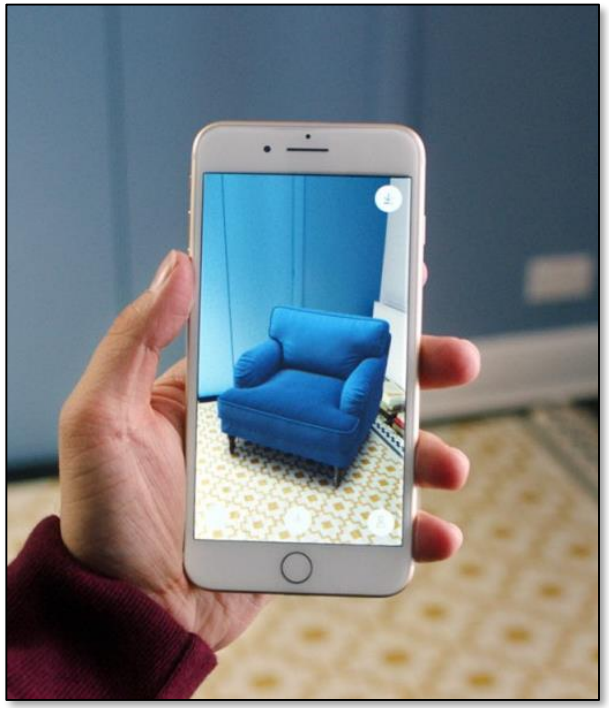
UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

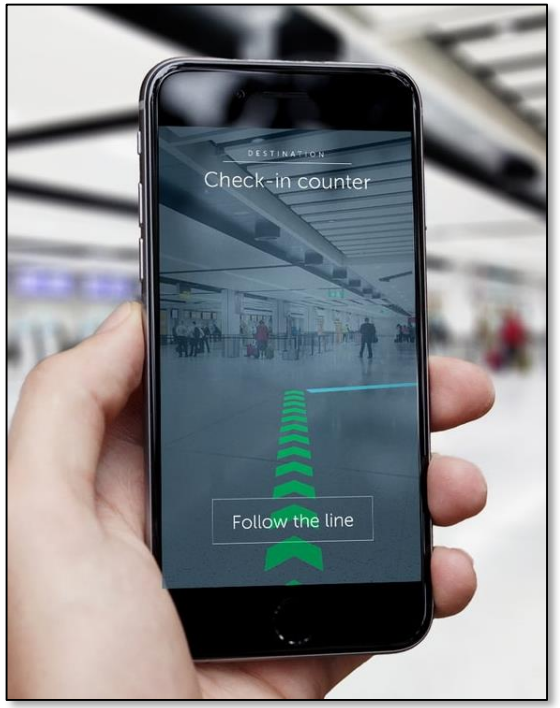
Emerging Risks

- Increasing data privacy encroachment
- Increased robotics and automation
- Augmented Reality / Virtual Reality
- Artificial Intelligence
- Quantum Computing and the end of encryption
- Internet Service Provider failure
- Cloud Service Provider failure
- Industrial Control System compromise
- Financial transaction theft
- Power outages
- Increase in nation-state cyber espionage, technologies, and attacks

Pixabay


11:45
5 Item Remaining
%TASK
80
PICK 15
PICK 16
12m



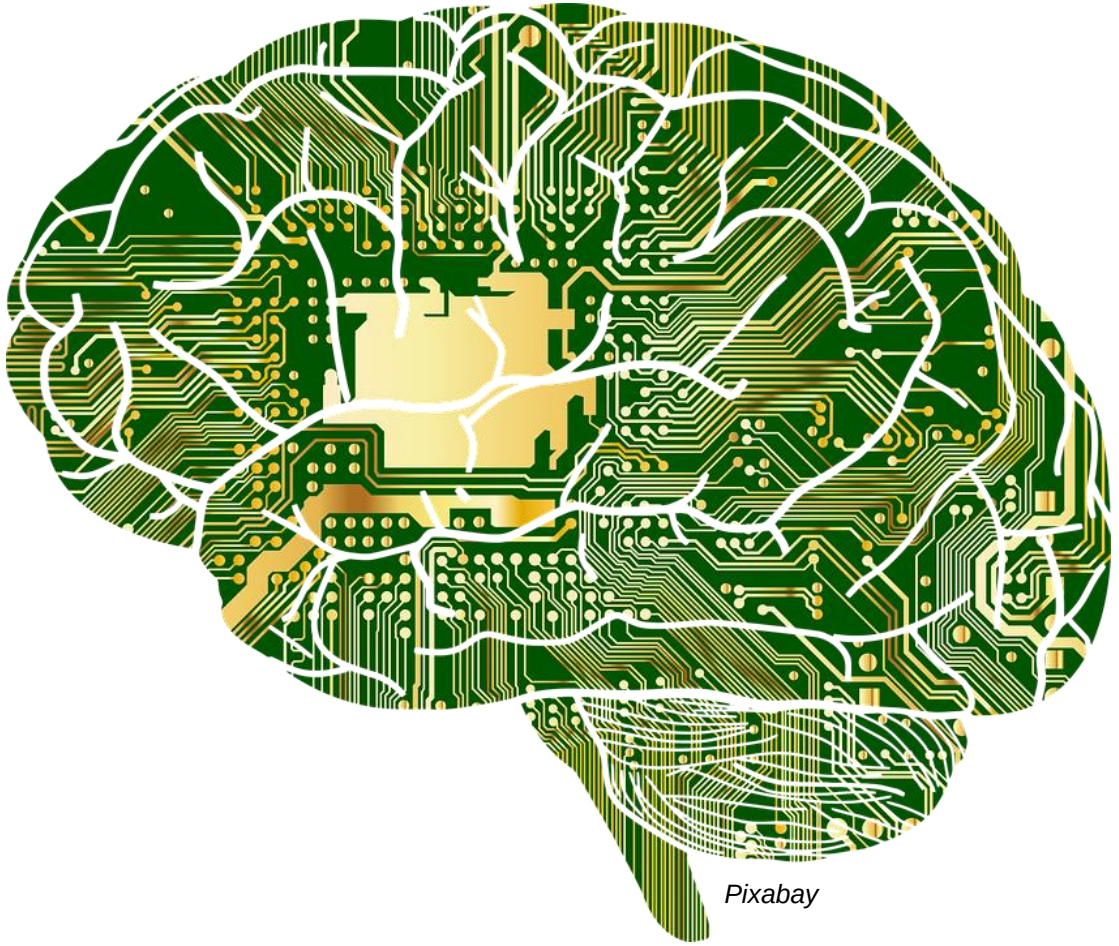

DESTINATION
Check-in counter
Follow the line


SERVICE &MAINTENANCE AUGMENTED REALITY

Weaponised AI

- Existing open source AI technologies can be combined with malware
- AI can make attacks evasive, targeted, scaled, and fast
- Autonomous approaches built to work independently from the attackers
- Malware can use AI to understand the context of their target's environment
- AI can learn and retrain on-the-fly to get past defences

- AI can also be used to prevent cyber attacks
- Multiple benefits
- Requires ethical data usage and responsible regulation



Pixabay

This Week's Headlines

US and Russia clash over power grid 'hack attacks'

Is Facebook's Libra currency a case of corporate megalomania?

National Bank of Ukraine under DDos attack

The GoldBrute botnet is trying to crack open 1.5 million RDP servers

Ubisoft hit with string of DDoS attacks just as R6's Operation Phantom Sight goes live

Machine Learning Is Helping To Stop Security Breaches With Threat Analytics

Baltimore Ransomware Attack: Calls for Assistance From Annapolis to Washington

Exposed Docker APIs Abused by DDoS, Cryptojacking Botnet Malware

Transgender support charity apologises for data breach

Facebook's Libra could threaten the global financial system

Airplane parts maker ASCO under ransomware attack

The Future of Cyber Risk

- The Future of Cyber Risk: Anticipating Strategic Surprise
- One Day Conference, **July 24, 2019**, Cambridge Judge Business School
- CCRS in collaboration with Cambridge Cybercrime Centre and Cambridge Computer Laboratories

- Risk Landscape
- Security Advances
- Technology and AI
- Risk Management
- Threat Actors, motivations and capabilities
- Cyber Insurance

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School