Cambridge Judge Business School

Centre for Risk Studies

TECHNOLOGY AND SPACE

Dr Jennifer Daffron
Research Associate, Cambridge Centre for Risk Studies

4 December 2018

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Technology and Space

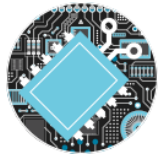
Cyber Attack — *Increased*

Nuclear Accident — *Stable*

Power Outage — *Stable*

Solar Storm — *Slightly increased*

Cyber Attack: A Growing Threat

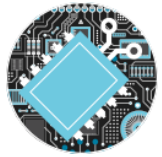


Cyber Attack

The cyber threat continues to develop at a rapid pace. Cyber attack loss severities are increasing with several recent attacks showing the potential for **systemic impacts** with global reach.

- The Internationalisation of Cyber Threat
- Increasing Size and Cost of Data Breaches
- Continued Disruption from DDoS Attacks
- Threat to Critical Infrastructure
- Rising Complexity and Sophistication with Less Effort

The Internationalisation of Cyber Threat

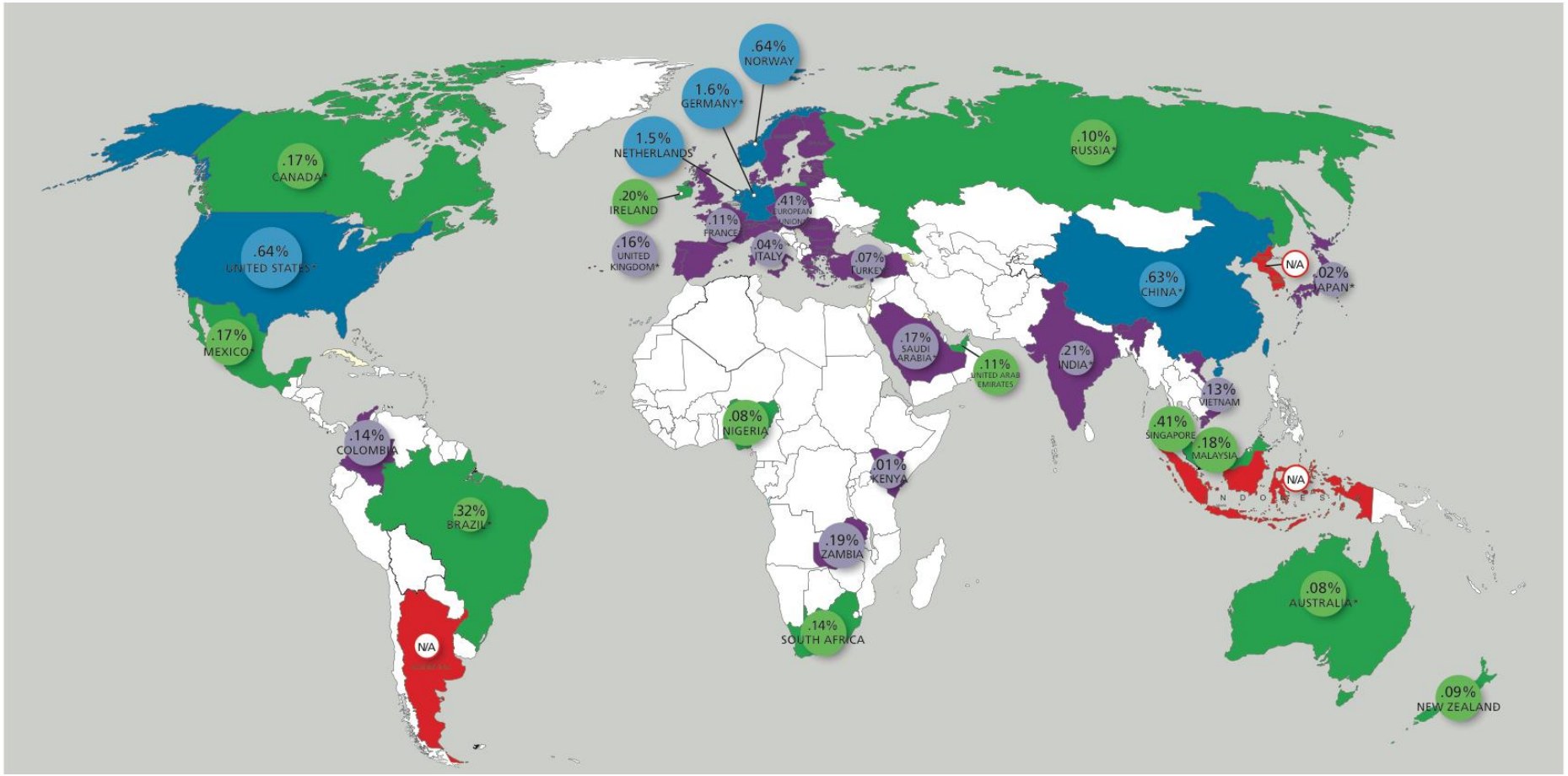


Cyber Attack

Cyber losses are now being reported in almost **every country** of the industrialized world.

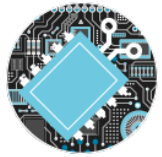
McAfee
An Intel Company

CYBERCRIME LOSS AS A PERCENT OF GDP (GROSS DOMESTIC PRODUCT)



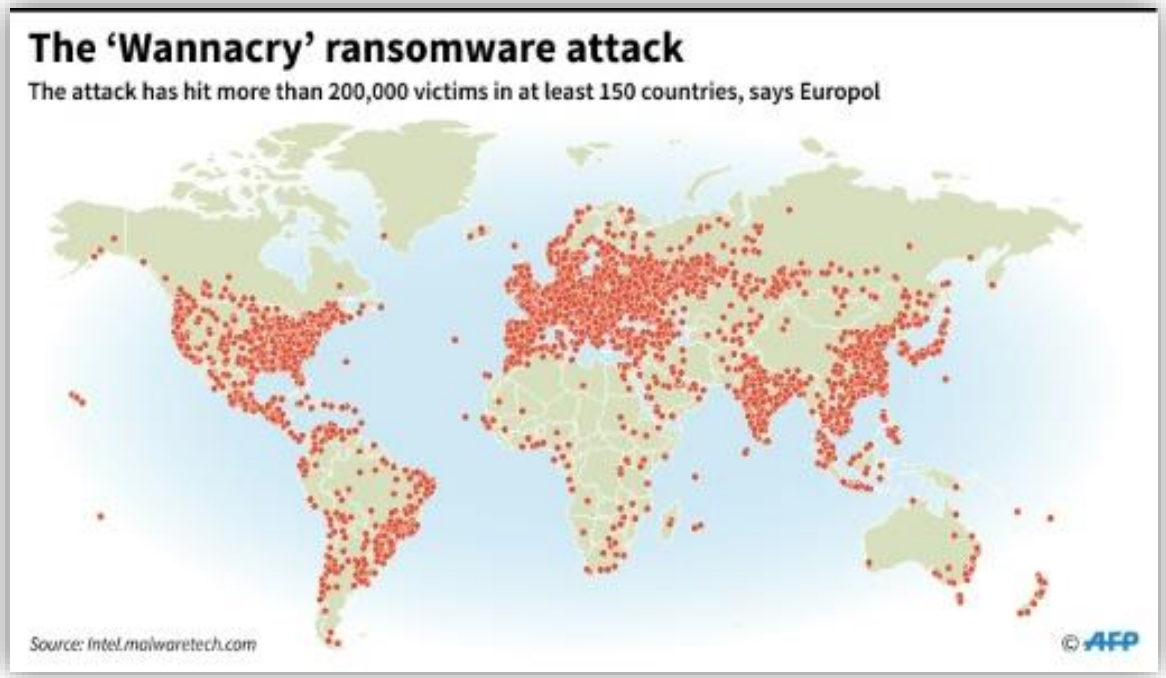
UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

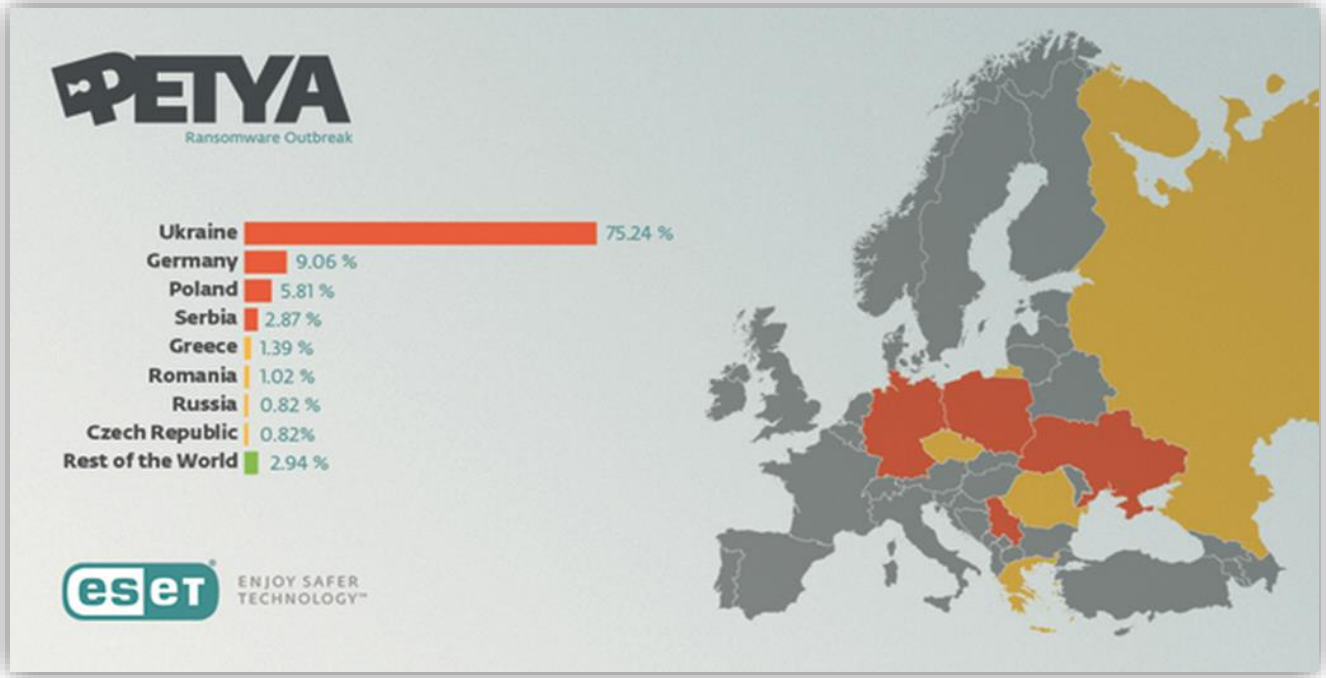
The Internationalization of Cyber Crime



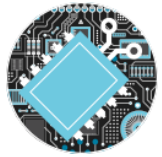
Cyber Attack

Cyber attacks have **no** regard for traditional country **boundaries**.





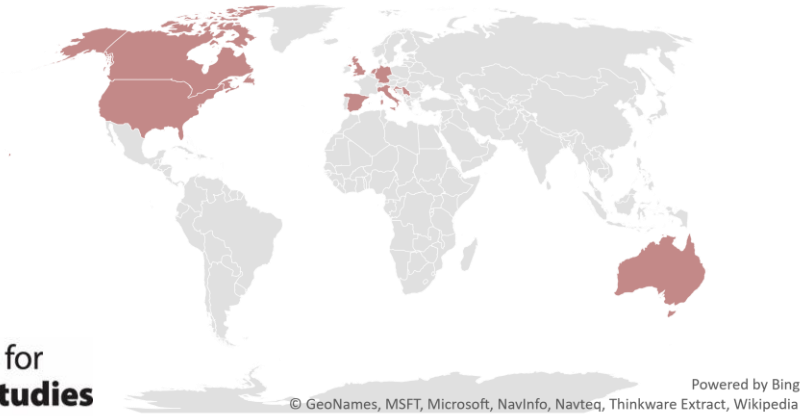
The Internationalization of Cyber Crime



Cyber Attack

- Cyber attack as a means of driving real-word politics
  - The recent **trade dispute** between the United States and China is mainly driven by corporate espionage and intellectual property theft through **cyber means**
  - Nation state cyber **election interference**, such as experienced during the 2016 United States Presidential election

- International Collaborations
  - **Operation Power Off** culminated in the seizure of infrastructure and the arrest of members of the world's largest DDoS-as-a-service website, *Webstressor.org*.

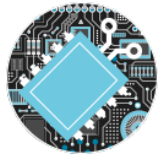


UK (National Crime Agency)
The Netherlands
Germany
Scotland
Australia
Canada
Italy
Spain

Serbia
United States
Croatia
Hong Kong
Europol
Joint Cyber Action Taskforce

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

Data Breaches



Cyber Attack

Data breaches are growing in size and impact.

The largest data breach of 2018 was **1.1 Billion Records**.

Average cost per lost stolen record:

$148

Average total cost of a data breach:

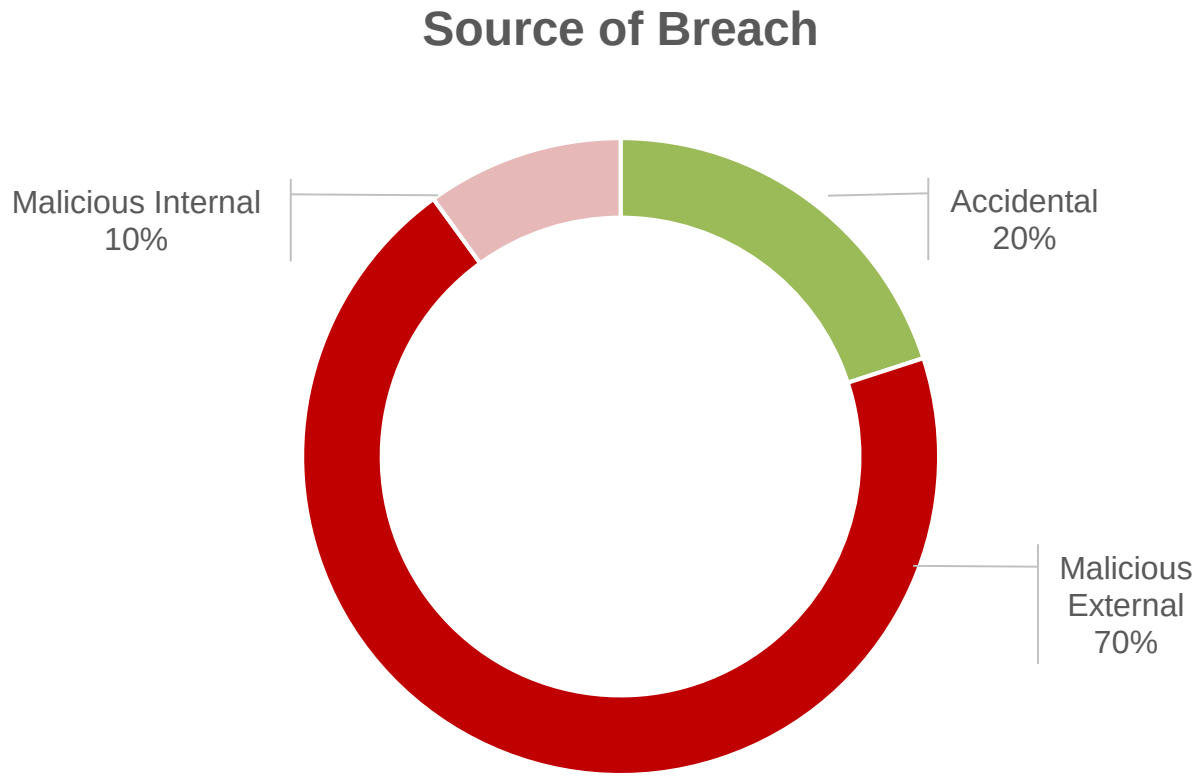
$3.86 million

Average cost per megabreach of **1 million** records:

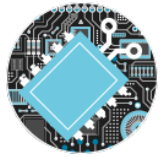
$40 Million

Average cost per megabreach of **50 million** records:

$350 Million



DDoS Attacks



Cyber Attack

The frequency of DDoS attacks continues to increase year-on-year.
In 2018, DDoS attacks increased by **40%** as organisations faced an average of **8** attacks per day.

Organizations with DDoS attack reputation and brand damage

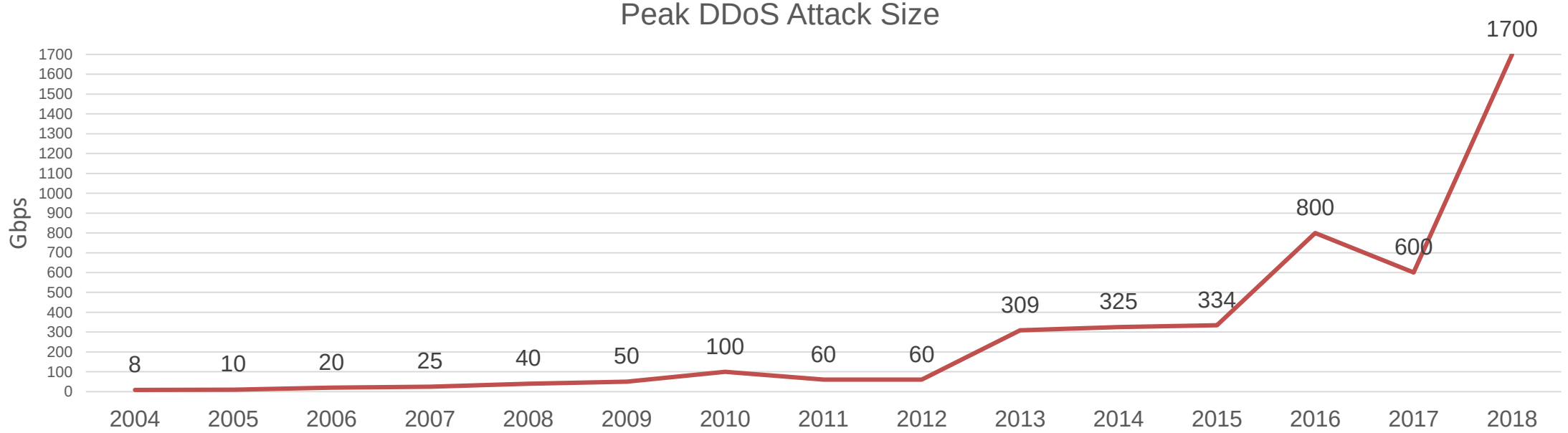
57%

Over half of victims reported a financial impact ranging from

$10,000 - $100,000

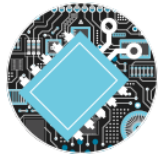
Highest cost of DDoS for a single attack

$2.5 Million



UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

Threat to Critical Infrastructure



Cyber Attack

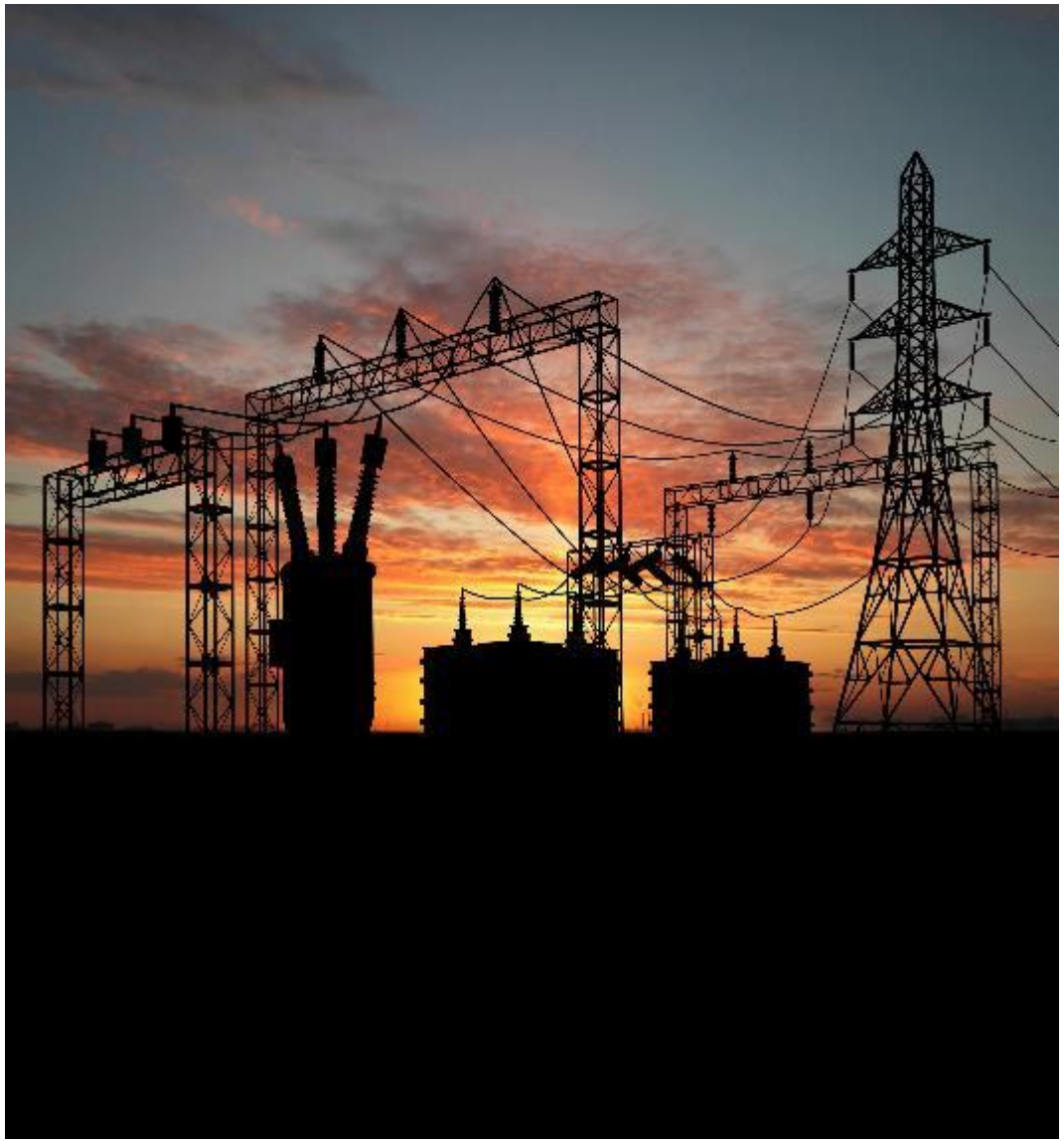
The **greatest potential** for economic loss from cyber attacks is the threat to critical infrastructure.

Atlanta Cyber Attack – *Ransomware*

- More than **one third** Atlanta's **necessary programs** were knocked **offline** or partly disabled
- 30% of those affected apps were ***"mission critical"***
- Courts Lost 10 years' worth of documents
- **$2.6 Million spent** with another **$9.5 Million expected**

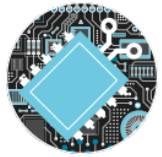
Boeing Cyber Attack - *Ransomware*

- Two plants completely **shut down**
  - Plant 1: 24 hours
  - Plant 2: 96 hours
- Configuration files that controlled machines were **lost**
- Systems had to be **reinstalled** before production could restart



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

Rising Complexity and Sophistication with Less Effort



Cyber Attack

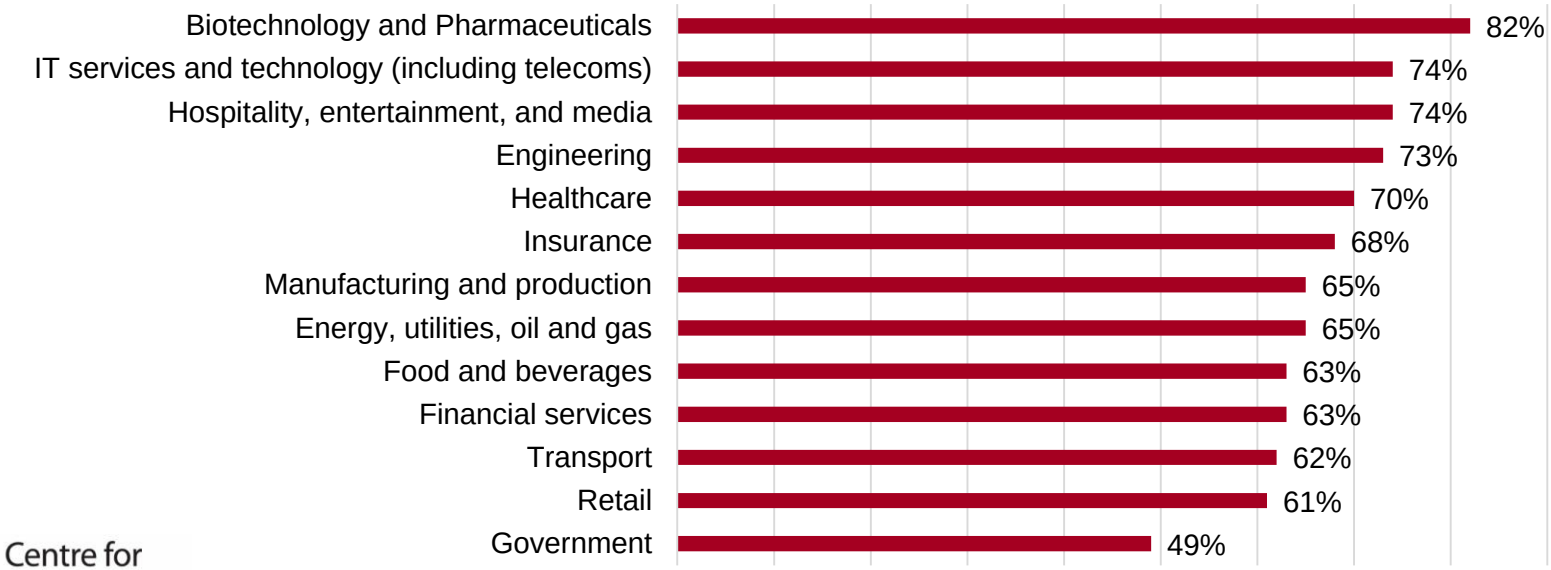
Supply Chain Attacks

A supply chain attacks seeks to damage an organization by targeting or gaining access to less-secure elements in the supply network

Estimated that **66%** of companies have experienced a supply chain attack.

Costing those companies an average of **$1.1 million per attack**

Sectors Experiencing a Software Supply Chain Attack



UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

Rising Complexity and Sophistication with Less Effort

Cyber Attack

State Backed Actors

For private sector companies, state-sponsored groups becoming financially motivated is a worrying trend as these groups are often labelled by the cyber security community as an ‘advanced persistent threat’ (APT) with the highest levels of training and largest budgets.

For Sale Malware

The evolution of for-sale malware sold on online black markets forever changed the threat landscape companies face and has resulted in new trends in attack vectors.

Type	Kit Name	Price
Exploit Kits	Whitehole	$600/ month
	Sweet Orange	$1800/month
	Elenore	$1000
	Gpack	$1000
	Cool (+ crypter + 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

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School