orbis

orbis

the compelling alternative

Brighton & Hove City Council

East Sussex County Council

SURREY

orbis

Brighton & Hove City Council

East Sussex County Council

SURREY

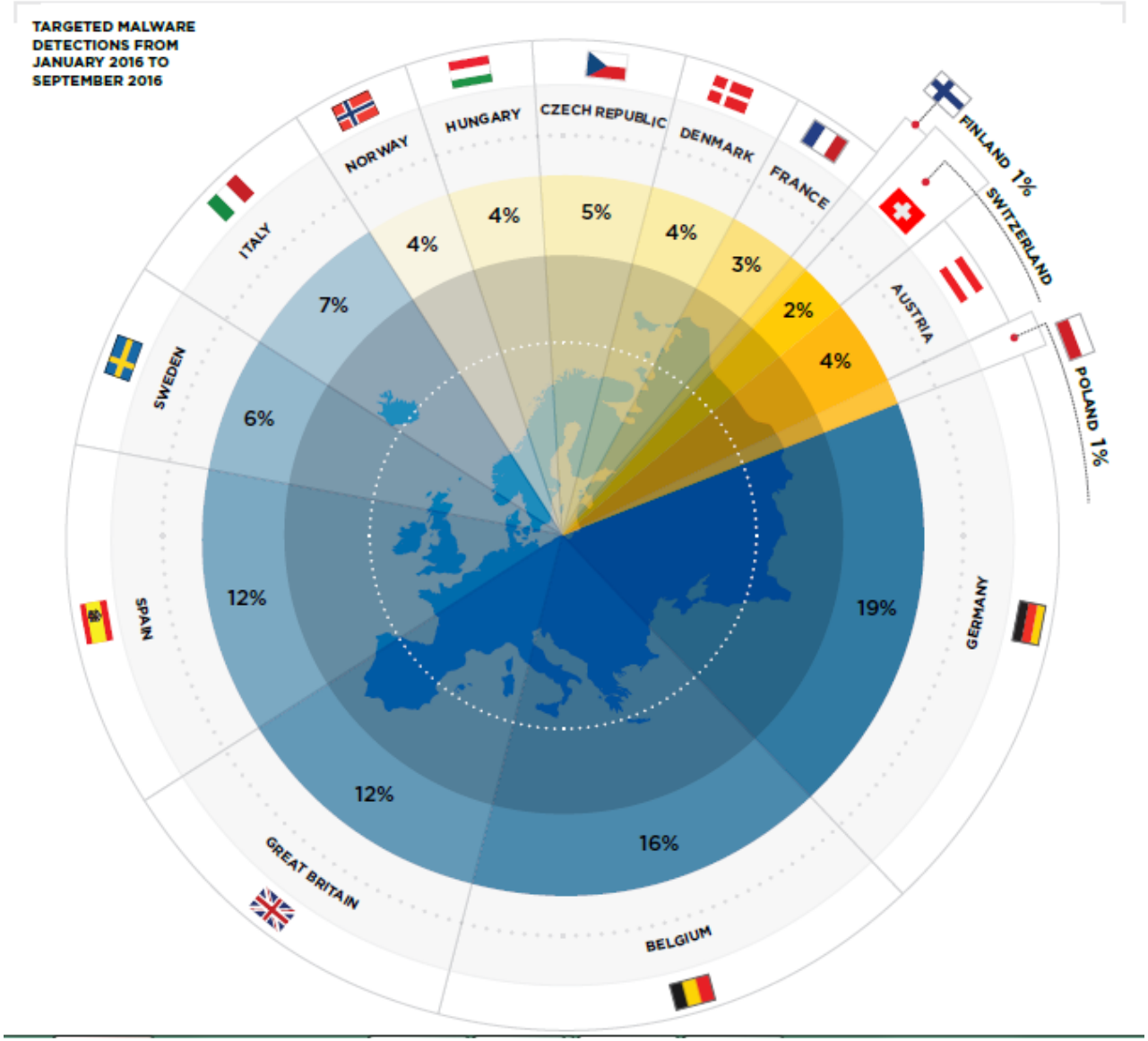
What is Cyber Security?

Definition used:

Protection of information systems (hardware, software and associated infrastructure), the data on them and the services they provide, from **unauthorised access, harm or misuse**.

This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

Scale of threat



Targeted Malware infections across Europe

Brighton & Hove City Council

East Sussex County Council

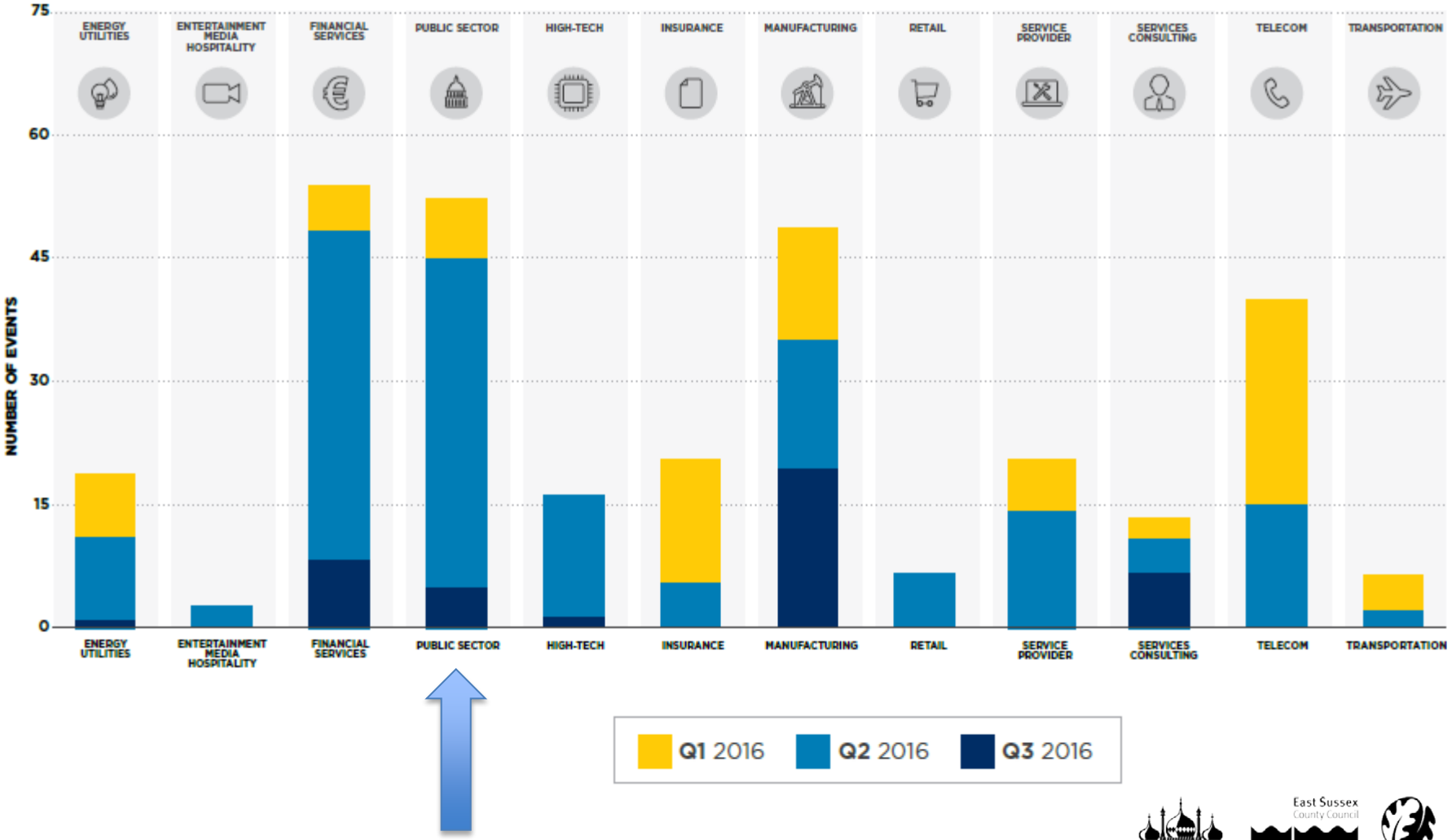
SURREY

Scale of threat

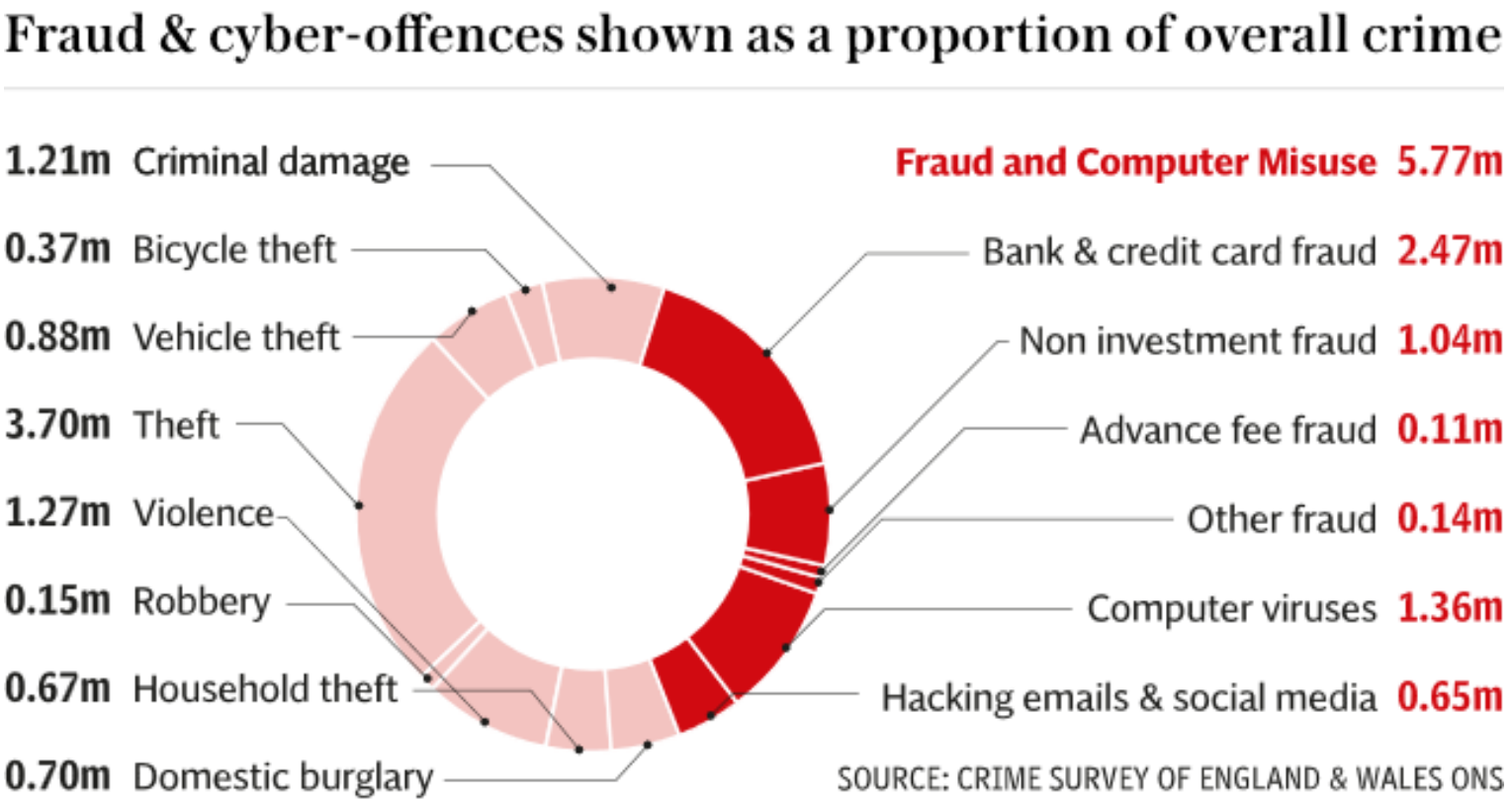
RANSOMWARE EVOLUTION

THREE MOST TARGETED INDUSTRIES IN EUROPE

Scale of Threat



Rise of Cyber Crime in the UK



Why attack Local Government ?

- Financial Gain

  Medical and personal Information for resale
  Fraudulent activity (fake invoices, bank details)
  Intelligence gathering for future attacks
  Ransom of information

- Politically Motivated Attackers

  Anger at closing services, digging roads on green belt, perceived injustice, personal political attacks, political activists, face of authority and bureaucracy, disgruntled employees

- Script Kiddies

  Easily available toolsets used by low skill attackers looking for easy targets

Brighton & Hove City Council
East Sussex County Council
SURREY

Global Cybercrime Stats

Cyber crime damage costs to hit $6 trillion annually by 2021.

It all begins and ends with cyber crime. Without it, there's nothing to cyber-defend. The cybersecurity community and major media have largely concurred on the prediction that cyber crime damages will cost the world $6 trillion annually by 2021, up from $3 trillion just a year ago.

Cybersecurity spending to exceed $1 trillion from 2017 to 2021.

The rising tide of cyber crime has pushed cybersecurity spending on products and services to more than $80 billion in 2016, according to Gartner. It's not clear if that includes an accounting of IoT device protection and total consumer spending on security. Global spending on cybersecurity products and services are predicted to exceed $1 trillion over the next five years, from 2017 to 2021.

Global Cybercrime Stats cont.

Cyber Attacks on people to increase to 4 billion people by 2020.

As the world goes digital, humans have moved ahead of machines as the top target for cyber criminals. Microsoft estimates that by 2020 4 billion people will be online—twice the number that are online now. **The hackers smell blood now, not silicon**.

Global ransomware damage costs are predicted to exceed $5 billion in 2017. That's up from $325 million in 2015—a 15X increase in two years, and expected to worsen. Ransomware attacks on healthcare organisations—the No. 1 cyber-attacked industry—will quadruple by 2020.

What does it all mean? Last year, Ginni Rometty, IBM's chairman, president and CEO, said, "Cyber crime is the greatest threat to every company in the world."

Statistics

Email Security on Global level

205 Billion email sent every day
39% attachments contain malicious files
34% of links embedded in email are malicious
77% of all malware is installed via email.

Statistics

Email Security at East Sussex (1 Month)

Received 5.5 million messages
Rejected 4.8 million messages (poor reputation)
Rejected 20k as SPAM
Rejected 55 with direct Virus attached
11.5k needed additional checks
Clean Messages received 670,000

Statistics
(Example of incident)

In 2015 a single virus evaded 3 different anti virus checks, a global reputation filter and a single user opened the malware attachment that arrived via email.

In 10 minutes 20,000 files where encrypted.

IT and Digital fully restored all the lost files within the hour and contained the outbreak

The Operations and Information Security team lost a day's work with ongoing checks and due diligence. The user's team lost ½ days work.

In Information Security the good guys have to be right every time.

The bad guys just need to be right just once!

What are we doing to stop attacks?

What does good security look like?

- Risk Management of systems and services
- Information Governance
- Technical Security

What are we doing to stop attacks?

Risk Management

Has been subject to internal and external auditing, awarded Substantial Assurance

Risk management is embedded in every stage of information handling development and procurement.

i.e. New and existing software and hardware, cloud services and web technologies are risk assessed as part of the procurement

Managed by staff that hold international accredited security credentials.

What are we doing to stop attacks?

Information Governance

Essential role to ensure that only needed information is retained, processed legally and is shared only with authorised individuals.

Independently accredited by NHS N3

Lead by GDPR Certified Practitioner

Accredited by Orbis Internal Audit and Mazars

What are we doing to stop attacks?

Technical Security

Government accredited security standard on our infrastructure (PSN)

NHS certified network connections (HSCN)

ISO 27001 certified (and award winning) Orbis Primary Data Centre at Redhill

Meet PCI standards on Card payments

Security is embedded in every level of provision.

Our technical defences are attacked several times a year by friendly (white hat) hackers looking for flaws and vulnerabilities. (Penetration Testing)

This helps keep our infrastructure resilient and safe.

What are we doing to stop attacks?

Threat Sharing

Founder members of the South East Cyber Cluster
Members of the Sussex and Surrey NHS Cyber Security Group
Work with Cabinet Office, Ministry of Justice, NHS, Department of Work and Pensions, National Cyber Security Centre.

Employ 2 CISSP (Certified Information Systems Security Professionals)

Only 5,000 in the UK

Challenges

There is a world wide shortage of cyber security trained staff, Central Government advises “growing your own”.

World wide security budgets are going up to meet the escalating threat to all Organisations. Local Government funding cuts threaten to undermine security standards , weaken public trust in local government and open up substantial losses through fines and civil action.

Cuts on Operational IT staff reduce the capacity for incident handling and could threaten the detection, response and resolution time of cyber incidents.

What's coming?

Enhanced user awareness training – users to be Phished and given learning experiences at point of use in a safe and secure environment

SIEM – A new Security Information and Event Management system is due come online Q4 (Enhanced logging and analysis of potential issues or threats within the network)

Policy Notification Software – Mandatory training and notifications of critical statutory changes pushed to users desktops.

What's coming?

GDPR training and workshops to cascade vital skills and information to those affected by new Data Protection laws.

Move of ESCC servers to the Orbis Primary Data Centre (ISO27001 certified Tier 3 environment)

Development of "Security Advocates". Trained staff that can cascade and share cyber security insights and highlight potential issues.

What happens when it goes wrong?

Nottinghamshire County Council

31 August 2017, Monetary penalties, Local government

A council has been fined £70,000 by the Information Commissioner's Office for lea...

London Borough of Islington

17 August 2017, Monetary penalties, Local government

Islington Council failed to keep up to 89,000 people's information secure on its par...

Cheshire West and Chester Council

10 August 2017, Undertakings, Local government

An Undertaking to comply with the seventh data protection principle has been sign...

Medway Council

13 June 2017, Enforcement notices, Local government

Medway Council has been issued with an enforcement notice by the Information C...

Gloucester City Council

12 June 2017, Monetary penalties, Local government

The Information Commissioner's Office has fined Gloucester City Council £100,000 ...

What happens when it goes wrong?

What happens when it goes wrong?

WannaCry

Map of the countries initially affected[55]

Surrey – Major Hacker apprehended

A British man accused of being behind a cyberattack on two of the UK's biggest banks has been extradited from Germany to face charges.
Daniel Kaye, 29, of Egham, **Surrey**, is facing nine charges under the Computer Misuse Act, two charges of blackmail and one of possession of criminal property. He's accused of using the Mirai botnet to launch DDoS attacks on Lloyds, Halifax and Bank of Scotland over two days in January this year.
He's alleged to have asked Lloyds for a ransom of £75,000-worth of Bitcoin, which was not paid. Kaye is also charged with endangering human welfare with an alleged attack against Liberia's biggest ISP, Lonestar MTN.

The UK's National Crime Agency said: "The investigation leading to these charges was complex and crossed borders. Our cybercrime officers have analysed reams of data on the way. Cybercrime is not victimless and we are determined to bring suspects before the courts."