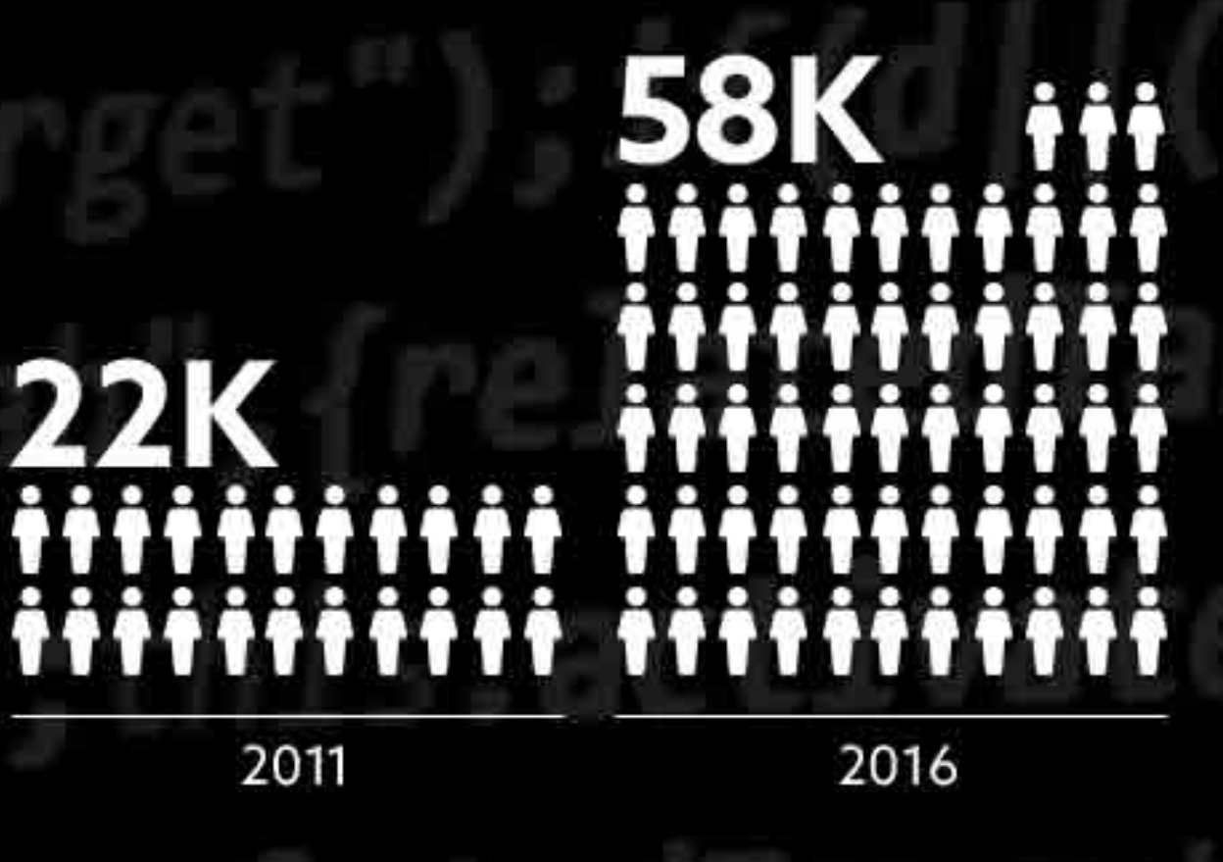
Northumbria University
NEWCASTLE

Newcastle • London • Amsterdam

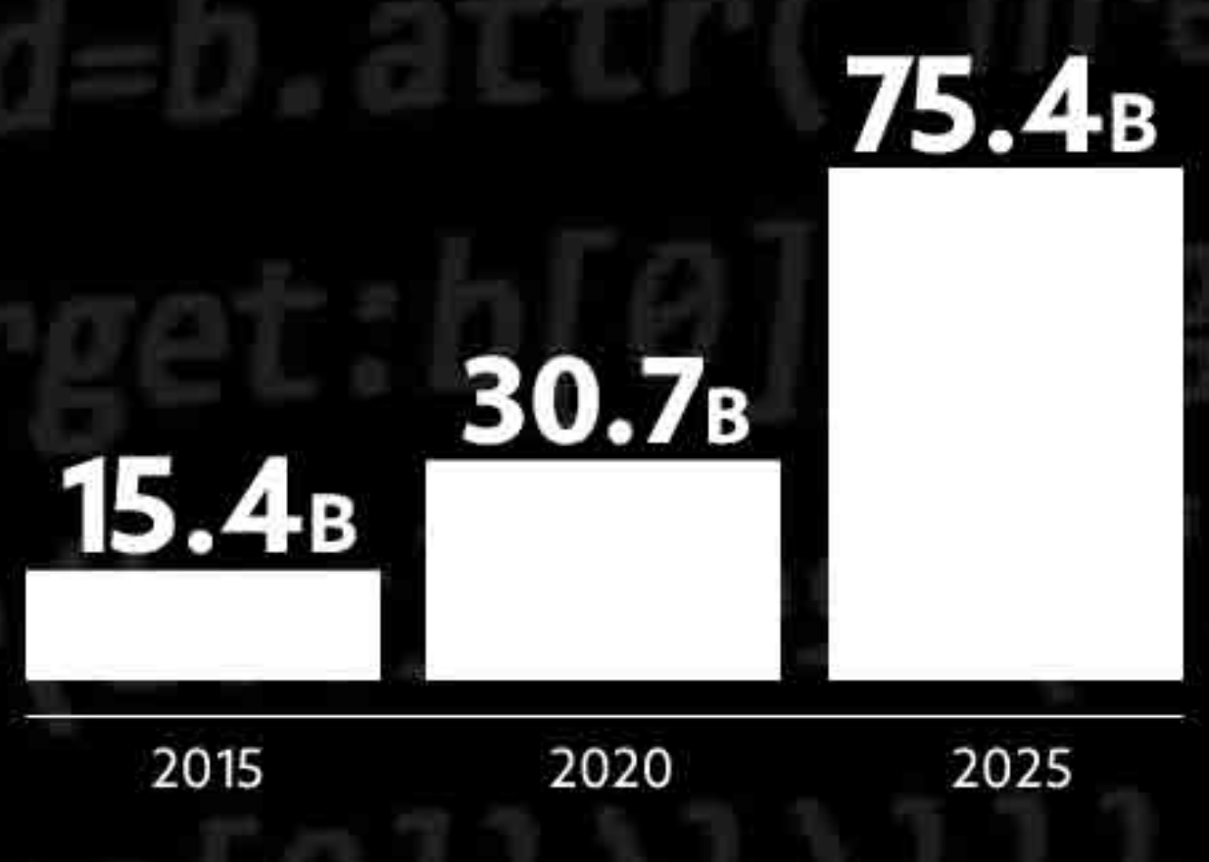
THE STATE OF CYBER SECURITY

The demand in London and beyond for cyber security experts is increasing daily, with a report from Frost & Sullivan[1] forecasting a shortfall of 1.5 million skilled professionals by 2020. Here, we explore some of the most significant contributing factors to the constantly evolving cyber security landscape and the most relevant courses to help you to become a part of the solution.

A CYBER SECURITY SNAPSHOT



A total of **58,000 people** are currently working in this expanding sector, up from 22,000 in 2011, according to Digital By Default News.[2]



IoT is **expanding rapidly**, creating **significant data security vulnerabilities** for companies and individuals, driving the demand for IoT specialists.[3]

£100K

The current skills shortage is **supporting salary growth** with some top jobs securing salaries of **£100,000** according to Forbes.[4]

£600K £1.15M

"The average cost of a data breach is £600-£1.15 million according to the National Cyber Security Centre."[5]

General Data Protection Regulation (GDPR). GDPR will apply in the UK from 2018 and has a primary objective to **give citizens control over their personal data** and aims to **simplify regulations across international business.**[6]

$1 Trillion

According to Cyber Security Ventures, 'alongside the increasing cost of a data breach, **organisations are increasing their spend on cyber security products and services** with Cybersecurity Ventures predicting the figure will exceed $1 trillion over the next 5 years.'

THE BIG ISSUES

The cyber security landscape is constantly evolving with companies, governments and individuals falling victim to increasingly inventive attacks. Here are some of the most prevalent topics in cyber security today:

BREXIT

Despite the UK's impending exit from the European Union, Britain's Information Commissioner's Office (ICO) has confirmed that the General Data Protection Regulation (GDPR) will apply in the UK from the 25 May 2018. Failure to adhere to the new sanctions can incur severe fines up to 4% of the company's global annual profits.[7]

SNOOPER'S CHARTER

The Investigatory Powers Act 2016 – also known as the Snoopers' Charter – provides 'unprecedented transparency and substantial privacy protection' according to the Home Secretary Amber Rudd. Critics of the new legislation believe the new law is 'more suited to a dictatorship than a democracy' (Jim Killock, Open Rights Group). Tech giants including Apple, Google, Microsoft and Facebook have also raised concerns over possible forced implementation of backdoor or forced decryption which could weaken product security. [8]

INCREASE IN HACKING CAPABILITIES

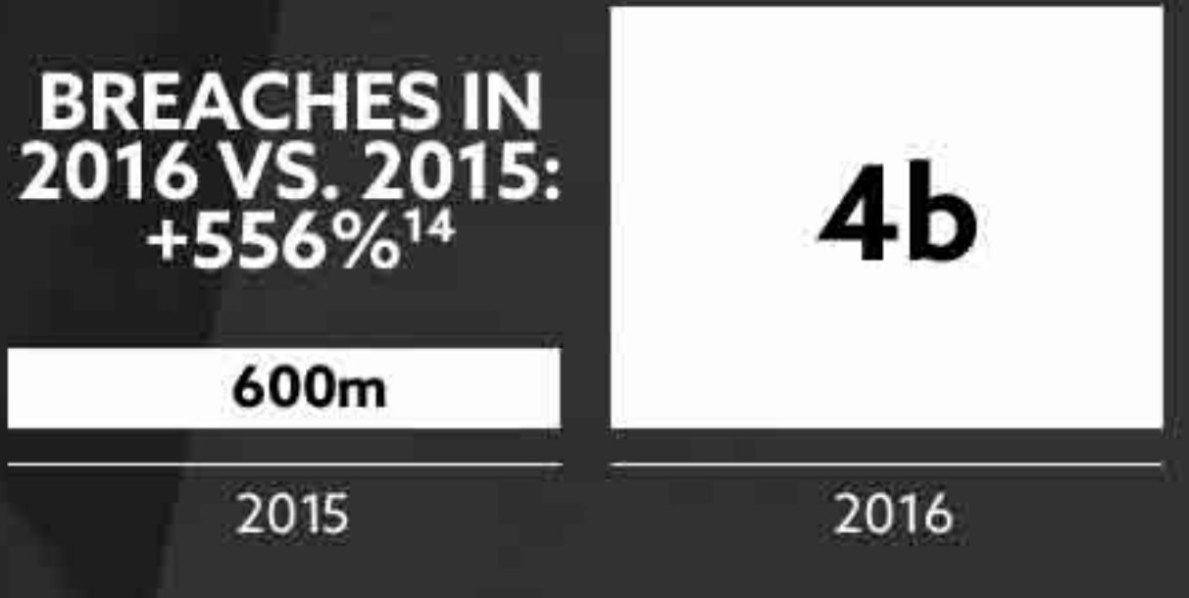
Almost every month a large-scale hack or data breach is unearthed, and software vulnerabilities are discovered and (hopefully) patched.
Three of the biggest hacks of 2016 include:

1. Presidential election hacks: Hackers attempted to influence the US Presidential Elections through the release of private emails, compromising the systems of various officials and committees with wide-reaching global consequences. [9]
2. Yahoo data breach: A data breach in 2013 – only discovered in 2016 – affected nearly a billion user accounts containing personal information, affecting customer data security in what is considered the biggest data breach in history. [10]
3. The Dyn DNS hack: Weaponising the Internet of Things. Major web services including Twitter, Reddit, Amazon, Netflix and Paypal were affected by a 'denial of service' botnet designed to flood their hosting provider with traffic, restricting access for consumers. [11]

OTHER MAJOR FACTORS

A LACK OF EDUCATION IN SMES

According to Small Business, 1 in 3 UK companies are failing to educate their employees about cyber security or how to protect their mobile devices from harmful malware.[12] According to the UK's Information Commissioner's Office[13] , human error accounted for 62% of incidents reported, highlighting the need for proper information security training for all staff.



A BANNER YEAR FOR CYBER CRIME

IBM Security's 2017 X-Force Threat Intelligence Index reported that **4 billion records** were leaked in 2016, defining it the year of the 'mega breach' with a total increase of **556%** on 2015 data. [15]

84% OF CHIEF EXECUTIVES EXPECT DIGITAL CHANGE TO INCREASE PROFIT MARGINS [16]

THE CHANGING ROLE OF A CIO

The Chief Information Officer (CIO) role has increased in importance within organisations with 44% of CIOs reporting directly to the Chief Executive Officer (CEO) according to the CIO Magazine's 'State of the CIO survey'. Responsible for leading business transformations, they are responsible for reducing IT costs whilst also innovating digital strategy. [17]

OUR CYBER SECURITY

Northumbria University London's **part-time MSc Cyber Security** is designed to prepare working cyber security professionals for the day-to-day challenges of the industry through a series of classroom based weekend **lectures** spread over 2 years.

Taught by **industry experts**, this Masters programme provides in-depth coverage of the **fundamental concepts, principles and technologies for network and information security.**

MSC CYBER SECURITY (PART-TIME)

Level of study: Postgraduate
Fee: £9,950 (UK/EU)
Entry requirements: 2:2 or above undergraduate degree from a recognised university in a computing-related discipline, or professional qualifications that are equivalent to an honours degree
Mode of study: Part-time classroom
Duration: 2 years
Assessment methods: Coursework and exams
Student finance: Available

View Latest Dates and Enquire Now

LINKS

[1] http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html
[2] http://www.digitalbydefaultnews.co.uk/2017/02/09/uk-cyber-workforce-grows-160-in-five-years-tech-partnership-figures-show/
[3] http://electronics360.globalspec.com/article/6551/75-4-billion-devices-connected-to-the-internet-of-things-by-2025
[4] https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#1a2ddc8427ea
[5] www.ncsc.gov.uk
[6] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/introduction/
[7] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/introduction/
[8] https://www.ft.com/content/40d2ede4-adac-11e6-9cb3-bb8207902122
[9] http://www.reuters.com/article/us-usa-trump-russia-cyber-idUSKBN15X0OE
[10] https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached
[11] http://www.ioti.com/security/weaponizing-iot-it-nuke-or-pop-gun
[12] http://www.itsecurityguru.org/2017/03/21/ultima-13-uk-companies-failing-educate-staff-cyber-security/
[13] http://www.computerweekly.com/news/450297535/Human-error-causes-more-data-loss-than-malicious-attacks
[14] http://news.fraud.net/ibm-security-x-force-uncovers-556-increase-in-breaches-in-2016/
[15] https://assets.documentcloud.org/documents/3527813/IBM-XForce-Index-2017-FINAL.pdf
[16] http://www.cio.com/article/3064592/cio-role/why-ceos-must-go-big-in-digital-or-go-home.html
[17] http://resources.idgenterprise.com/original/AST-0124066_CIO_SOTCIO14_WhitePaper.pdf

Northumbria University
NEWCASTLE

Newcastle • London • Amsterdam

Visit london.northumbria.ac.uk for more information,
or contact us at pt.admissions@northumbria.ac.uk
or call us on 0207 444 0980