

# University and Police Partnership in Cybersecurity

---

**Dr Biju Issac**

Associate Professor

Programme Leader (Networks, Cyber and Forensics)

Computer and Information Sciences

Northumbria University, UK



**Northumbria  
University**  
NEWCASTLE



# Introduction

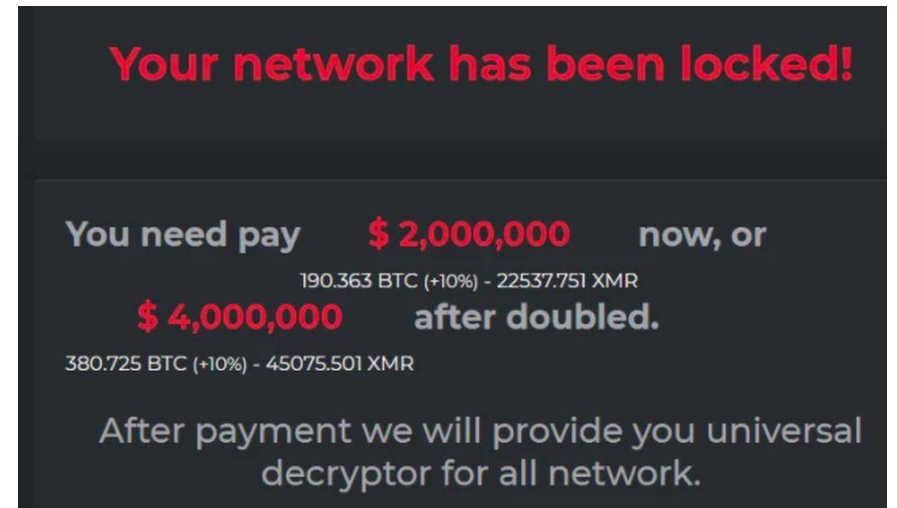
---

- I will talk about –
  - ‘How partnership in ethical hacking and cybersecurity research are helping small and medium businesses?’

# Introduction

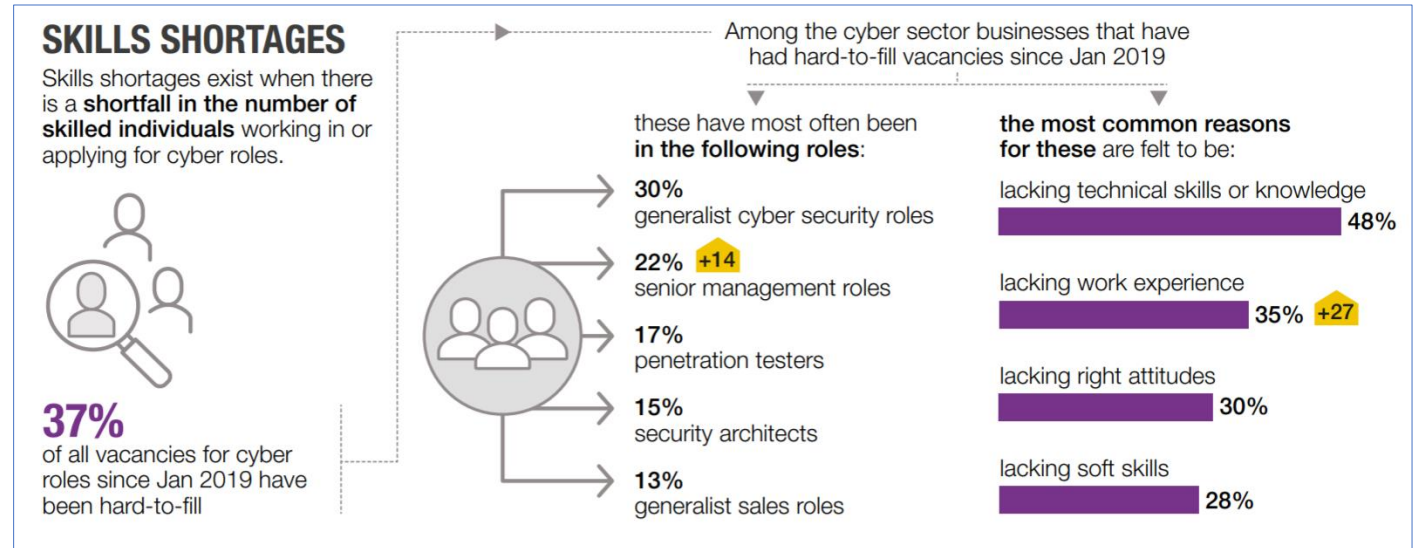
---

- Recent news of cyberattacks in May 2021:
  - BBC News (10 May) – Colonial Pipeline hack
    - A cyber-criminal gang took a major US fuel pipeline offline through a ransomware cyber-attack.
  - BBC News (20 May) - Cyber-attack on Irish health service
    - Health Service Executive (HSE) chief Paul Reid called the ransomware attack as a "callous act".
  - BBC News (22 May) - Air India cyber-attack
    - Attack on its data servers affected about 4.5 million customers
    - Passport, ticket information and credit-card data were compromised



# Introduction

- With increasing cybersecurity attacks and cyber skills shortage, there is clearly a need for cybersecurity experts 😊!
- **Cyber Security Breaches Survey 2021**  
(Published: 24 March 2021)
  - Four in ten businesses (39%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months.
  - Like previous years, this is higher among medium businesses (65%), large businesses (64%) and high-income charities (51%)



Source (1): <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021>

Source (2): [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/975773/20-012025-01\\_cyber\\_skills\\_2021\\_UK\\_cyber\\_sector\\_infographic\\_310321.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975773/20-012025-01_cyber_skills_2021_UK_cyber_sector_infographic_310321.pdf)

# Cybersecurity at Northumbria University

---

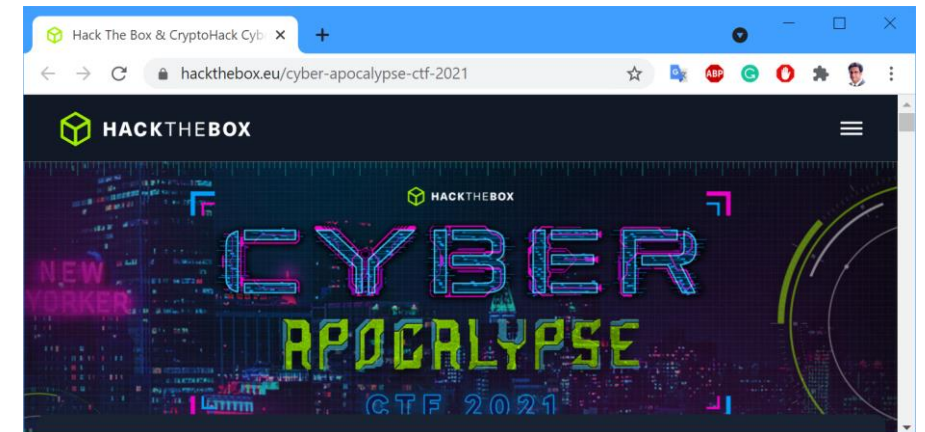
- Two great programmes/courses – ‘Computer Networks and Cyber Security’ & ‘Computer and Digital Forensics’
- Around 275 to 300 students in all the years
- Great opportunity, with a pool of talented students 😊!





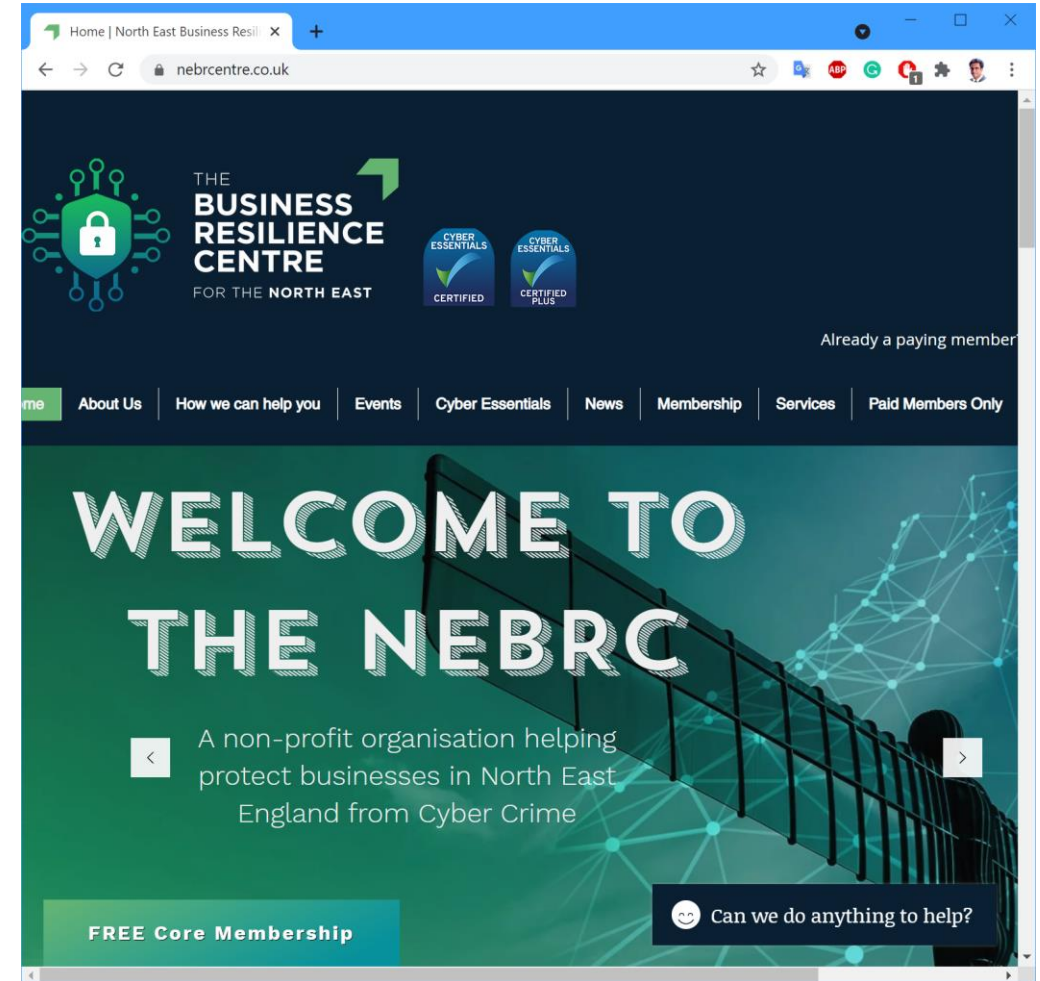
# Cyber Clinic

- Launched in 2018, when I joined Northumbria – seeing the great opportunity
- An informal forum to teach students ethical hacking skills every week (using Kali Linux, CTF etc)
- Student led and run (under my oversight), with guest speakers once in a while – IoC and CIS dept funds the running
- Achievements:
  - Finalists (in top 10 teams) in Cyber Crime Cup 2019 by BCS out of 35 university teams
  - 90<sup>th</sup> out of 4.7k in Cyber Apocalypse 2021 competition (3 student team competing with 10 member teams)



# Partnership with NEBRC

- Hearing about Cyber Clinic, we were contacted by the police (from Durham Constabulary) in 2019 for collaboration
- NEBRC is unique in that it uses students to work as ethical hackers, which is a win-win situation
- Currently nine students are employed by NEBRC as part-time paid cybersecurity consultants and further five students have been newly appointed.



# Experience of Students

---

- Three questions were asked to nine NEBRC students
  - What you have done for NEBRC?
  - What you have learned?
  - How has it benefited you?



# Experience of Students – (1)

---

- What you have done for NEBRC?
  - For the most part a lot of work has involved providing essential information to SMEs through the form of infographics.
  - Webinar on ransomware behaviours, risk factors and meaningful mitigation
  - PDF condensed version of the NCSC security advisory guide for board members
  - Two web app vulnerability tests for the NEBRC, as well as created an infographic on general web app testing.

# Experience of Students – (2)

---

- What you have learned?
  - It's quite difficult to summarise what I have learnt because it has been a constant learning journey.
  - My collaboration with various members and associates of NEBRC has provided me with a lot of insight into how important digital safeguarding and cyber hygiene is for a lot of businesses out there and how fundamental we are to helping bridge the gap between cyber essential strategies and SMEs.
  - Best practise for security
  - Presentation skills
  - Key OSINT (Open Source Intelligence) areas
  - Translating technical details to the layperson
  - Commodity threat landscape awareness
  - Introduction to industry behaviour (meetings and the like were quite alien before this point, still getting used to it)
  - The vulnerability tests were my first introduction to writing reports for vulnerability assessments and have taught me a great deal on what goes into these, including how to phrase findings for different audiences (no technical knowledge vs moderate technical knowledge.)

# Experience of Students – (3)

---

- How has it benefited you?
  - I've learnt a lot about the ways different tools and techniques can be used against SMEs and various mitigation factors from more knowledgeable senior members of NEBRC as well as the other students
  - Free training on top of Uni is helpful
  - Eventual exposure to industry will be nice, and controlled to our comfort level
  - A nice first job that is supporting of cyber preference and skillset
  - I have had many workplaces point it out as a notable part of my CV
  - The vulnerability tests themselves have also allowed me to gain experience in this area which will be very useful for my future.
  - I also recently took on a more supervisory role in a web app test, which involved me meeting with the client, scoping the test, and helping, working with, and supervising other students on the test. This again will provide me with a great deal of valuable experience when I eventually graduate from university.

# Infographics by NEBRC students

**NEBRC**  
NORTH EAST BUSINESS RESILIENCE CENTRE

**STUDENT SERVICES**

Our team of ethical hacking students working together to provide businesses with cyber resilience services.

**CYBER BUSINESS CONTINUITY EXERCISE**

You know what to do in the event of a fire.

But do you know what to do in the event of a cyber attack?

Tailored exercises for your business.

Learn effective communication resilience.

Adapt to the digital era.

Develop a robust continuity plan.

**CONTACT US FOR MORE INFORMATION**

enquiries@nebrcentre.co.uk

www.nebrcentre.co.uk

**FOLLOW US ON**

BE SMART. BE AWARE. BE PROTECTED.

**NEBRC**  
NORTH EAST BUSINESS RESILIENCE CENTRE

**STUDENT SERVICES**

Our team of ethical hacking students working together to provide businesses with cyber resilience services.

**INTERNET INVESTIGATION**

You've researched your stakeholders.

But have you researched you?

**CORPORATE**

Discover how much information can be gathered about your business online.

Includes checks for confidential data.

**INDIVIDUAL**

Discover how much information can be gathered about someone in your business online.

Best suited for VOs such as CEOs.

**EASY TO DIGEST FINDINGS INCLUDED IN OUR FINAL REPORT**

**CONTACT US FOR MORE INFORMATION**

enquiries@nebrcentre.co.uk

www.nebrcentre.co.uk

**FOLLOW US ON**

BE SMART. BE AWARE. BE PROTECTED.

**NEBRC**  
NORTH EAST BUSINESS RESILIENCE CENTRE

**STUDENT SERVICES**

Our team of ethical hacking students working together to provide businesses with cyber resilience services.

**SECURITY**

You may know what it takes to run your business.

But do you know what it takes to protect your business online?

**AWARENESS TRAINING**

Tailored informative sessions on cyber risks facing your business.

Covers a variety of cyber security subjects.

**POLICY REVIEW**

A check of the physical and technical security policies in your business.

Report of Recommendations Provided.

**CONTACT US FOR MORE INFORMATION**

enquiries@nebrcentre.co.uk

www.nebrcentre.co.uk

**FOLLOW US ON**

BE SMART. BE AWARE. BE PROTECTED.

**NEBRC**  
NORTH EAST BUSINESS RESILIENCE CENTRE

**STUDENT SERVICES**

Our team of ethical hacking students working together to provide businesses with cyber resilience services.

**VULNERABILITY ASSESSMENTS**

YOU TEST YOUR FIRE ALARM TO SEE IF IT WORKS.

BUT DO YOU TEST YOUR TECHNOLOGY?

**INTERNAL**

Testing your IT systems inside your business premises and network.

**REMOTE**

Testing your IT systems outside your business premises and network.

**WEB**

Testing your business web applications.

**EASY TO DIGEST FINDINGS INCLUDED IN OUR FINAL REPORT**

**CONTACT US FOR MORE INFORMATION**

enquiries@nebrcentre.co.uk

www.nebrcentre.co.uk

**FOLLOW US ON**

BE SMART. BE AWARE. BE PROTECTED.

**NEBRC**  
NORTH EAST BUSINESS RESILIENCE CENTRE

**BACKUPS ROADMAP**

Check the T&Cs of your cloud backups to understand if that backup is restorable and recoverable.

Perform steps 1-3 periodically in your business schedule.

Identify the data to be backed up.

Test and verify your backup by restoring some data to an alternate location.

Update your disaster recover plan with this new schedule.

**CONTACT US FOR MORE INFORMATION**

enquiries@nebrcentre.co.uk

www.nebrcentre.co.uk

**FOLLOW US ON**

BE SMART. BE AWARE. BE PROTECTED.

# Infographics by NEBRC students



**NEBRC**  
NORTH EAST BUSINESS RESILIENCE CENTRE

## 10 Cyber Tips For Board Members

*The NCSC's Board toolkit at a glance.*

### 1 Use your cyber security experts

You find that those in security do it because they love it. Use their passion for protection, and channel it towards beneficial projects. Mutual communication is really important for success.

The Security Culture Formula:

Board

 + 

Security/IT

 + 

Employees

 = 

A secure environment

### 2 Company wide cyber training



#### Invest in yourselves

- Anti-phishing training
- Prioritised funding for secure systems
- Influx of new talent for areas that are lacking
- Good employee benefits and care - consider morale

*Nobody is born secure, nobody is perfect.*

### 3 Establish the risk

"Did you hear about that company that lost all it's data?"

"Why is the site down? I needed to buy something!"

"They got hacked and now my details are on the web!"

The Cyber Attack Process:

1. Survey - Investigation into available information about the victim
2. Delivery - Finding an entryway into the system
3. Breach - Gaining unauthorised access using exploits
4. Affect - Using the access to carry out malicious actions

#### Common mistakes:

- "I clicked on the link without realising"
- "I was curious what was on the USB stick"
- "We are not a target, we are too small for that"
- "We won't update, it's too important to replace"

### 4 Awareness of defence



- Antivirus solution
- Monitor and block known threats
- Strong, unique passwords
- Install and use only what you need
- Regular and reliable backups
- Security culture and support
- Anti-Phishing policy
- Recovery strategy

*Cyber-Security is really "Managed-Insecurity".  
It will never be perfect, mistakes will happen, but how do you recover from them?*

### 5 Know the facts

*Ensure you keep up to date with the cyber world*

*Know your risk, know your solution*

*Do not reinvent the wheel of research*

Why SMEs are the most at risk:

- Lack of prioritisation for cyber
- Not enough funding
- Illusion of stealth
- An often lacking defence
- Minimal outcome planning for cyber threat

74%

Only 74% of board members consider cyber security a high priority

43%

43% of businesses reported breaches or attacks in 2018

### 6 Understand the Threat

*Make well informed decisions*

*Have insight into the threats that challenge your sector*

*Have awareness of what motivate attackers*

85%

85% of organisations fear malware infiltration via a phishing email

600%

600% rise in Cyber Crime due to the COVID-19 pandemic

Why:

- Majority of organisations are not targeted by nation states.
- Random "Scatter Gun" attacks are just as effective as targeted ones.
- Knowledge is power. Share it with others to improve everyone's Cyber Security.

### 7 Plan for Success, Prepare for Failure

*Create an Incident response plan.*

*Take pre-emptive methods.*

*Use Information you already have.*

Testing

Solution

Solution

Testing can reveal multiple solutions to the same problem so don't be afraid to do it!

### 8 Effective Solutions

*Implement Good Security Measures*

*Get Technical*

*Layer Your Defences*

Why:

- This requires Meeting Regulatory Requirements but reduces the risk of incident
- Getting technical allows you to ask the right questions
- Each measure reduces the likelihood of an incident.

52%

52% of attacks involved hacking.  
Good endpoint protection can prevent breaches

### 9 Assessment

*Have your company tested for flaws*

*Invest in a Cyber Security Baseline*

*Give technical staff time*

Why:

- Testing networks reveals the major flaws in them
- Different types of attackers will be able to exploit different things. Make it harder for them all.
- Allow IT Techs time to implement changes. It could prevent something in the future.

90%

90% of data breaches are caused by human error. Source: ICO 2018

### 10 Professional Standards

*Standards are there to help not hinder*

*There are many standards in every field*

*Get Accredited and stand out*

Why:

- ISO27001 - provides a way to manage information security.
- Cyber Essentials - Reassure customers that you take cyber security seriously
- Cyber Essentials + - Provides higher level of reassurance for customers

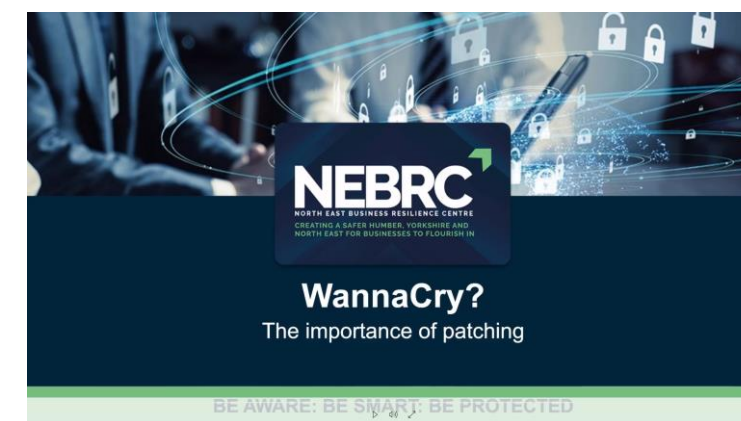
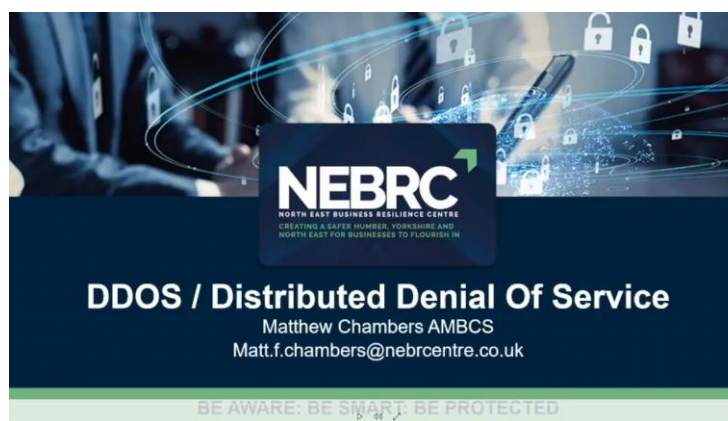
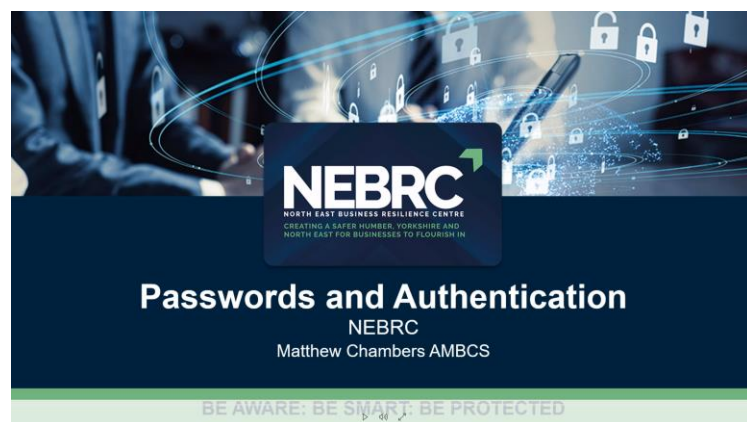
34%

34% of companies in the UK have ISO27001 accreditation.  
Source: Cambridge Network 2018

Sources:  
(Cyber Security Breaches Survey 2018 Main Report, 2018)  
(NCSC Cyber Security Toolkit for Boards, 2019)  
(ICO Data Breach Report for 2019, 2019)

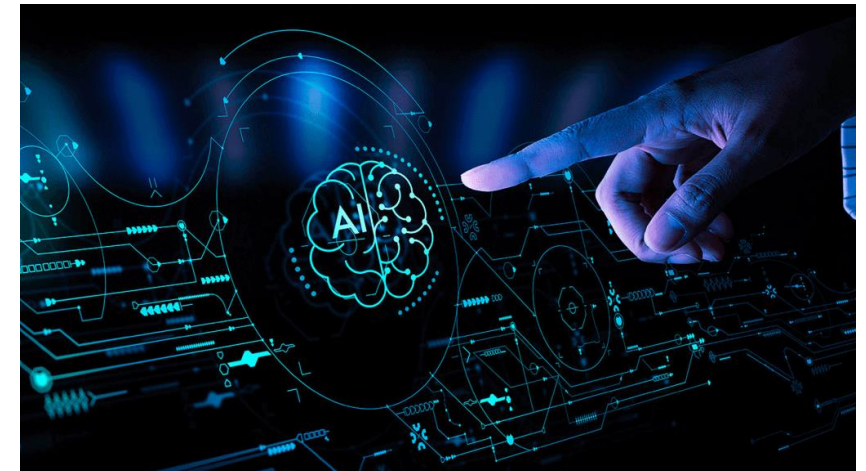
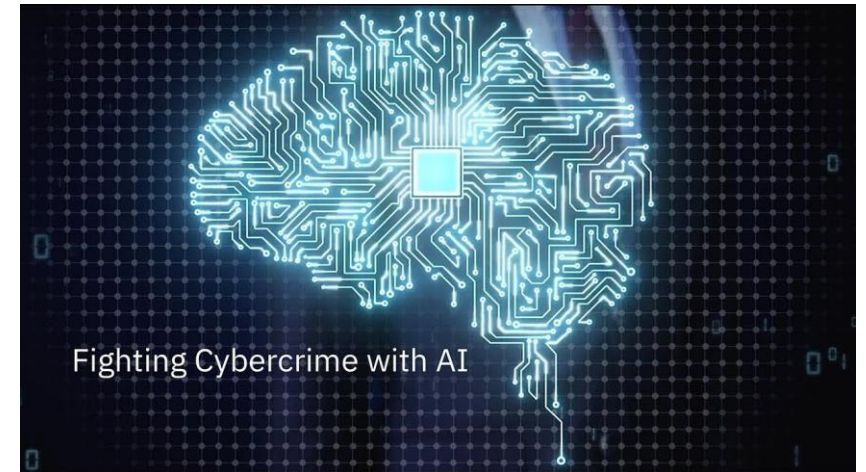


# Videos by NEBRC students



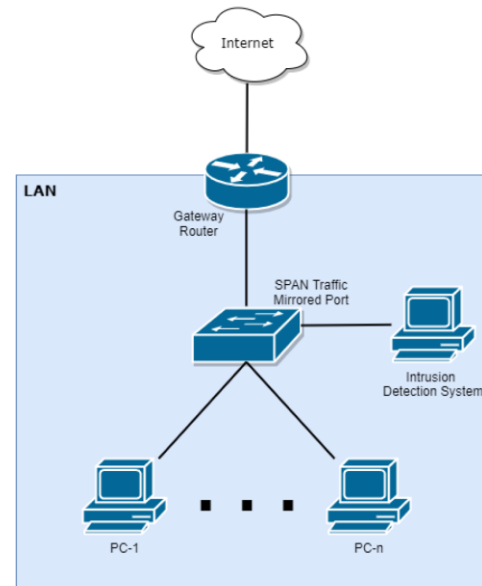
# Cybersecurity Research (UG and PG students)

- Some of the current cybersecurity projects which uses AI are as follows:
  - Online **Hate Speech Detection** through Optimized ML/DL
  - Application and Optimization of Deep Learning in the Anomaly-based **Detection of Botnets**
  - Implementation of Optimized Machine Learning algorithms to **Detect Data Exfiltration** via Covert Channels
  - **Phishing Detection** Using Deep learning and Bio-inspired Algorithms
  - **Spam Email Detection** using Machine Learning Optimized with Bio-Inspired Meta-Heuristic Algorithms
  - **Android Malware Detection** using Optimized Machine Learning



# Cybersecurity Research (UG and PG students)

- We are working with a police force to create an **intelligent intrusion detection system** using AI/machine learning to create alerts
- A software product is being developed through students which can be installed in business/SME premises.



# Conclusion

---

- Cyber attacks are too complex to deal with and no one party can solve them – it needs partnership.
  - Ideally between Government, Police and Universities (which is what CRCs/BRCs are)
- The partnership between Northumbria University and NEBRC (police) is a good example and win-win partnership, where everyone wins 😊!
  - It gives great work experience opportunity for students to get real-world experience
  - It gives NEBRC the ability to work with businesses to secure them against cyber attack
  - Ultimately the businesses are benefited with a great service