CYBERSECURITY JOBS / ROLES

Lecturer: Mark Gillan

INVESTIGATE JOB ROLES

Have a look into the different jobs in Cybersecurity, investigate the role they play and identify any laws / regulations that each one might have responsibility:

- Security Intelligence Analyst (SIA)
- Penetration Tester
- Cybersecurity Engineer
- Chief Information Security Officer (CISO)
- Incident Response Specialist
- Threat Intelligence Analyst
- Security Architect
- Cybersecurity Consultant
- Digital Forensics Analyst
- Security Awareness Trainer

SECURITY INTELLIGENCE ANALYST (SIA)

ROLE

- Monitors and analyses security incidents, responds to threats, and performs vulnerability assessments. Often works in a Security Operations Centre (SOC).

Legislation

- UK-wide GDPR and Data Protection Act 2018: Emphasises breach notification requirements and the safeguarding of sensitive data.
- Investigatory Powers (Scotland) Act 2016: Governs surveillance within Scotland, requiring strict adherence when monitoring systems.

PENETRATION TESTER

ROLE

- Simulates cyberattacks to identify vulnerabilities in systems, networks, and applications, providing actionable recommendations to improve security.

Legislation

- Computer Misuse Act 1990: Requires specific authorisation to ensure compliance during ethical hacking activities.
- Criminal Justice and Licensing (Scotland) Act 2010: Contains provisions regarding the misuse of data or unauthorised system access relevant to this role.

CYBERSECURITY ENGINEER

ROLE

- Designs, implements, and maintains security systems, such as firewalls, intrusion detection systems, and endpoint protections.

Legislation

- Telecommunications (Security) Act 2021: Applies UK-wide but has specific implications for infrastructure projects in Scotland.
- NIS Regulations 2018 (UK and Scotland): Cybersecurity engineers in essential service sectors must meet these standards.

CHIEF INFORMATION SECURITY OFFICER (CISO)

ROLE

- Oversees the organisation's overall cybersecurity strategy, ensuring alignment with business objectives. Manages security teams, risk assessments, and compliance.

Legislation

- UK-wide GDPR (Data Protection Act 2018): Applies equally in Scotland, with additional implications for organisations in devolved sectors (e.g., education, healthcare).
- Computer Misuse Act 1990: Includes implications for any incidents within Scotland or involving cross-border cooperation.
- Public Records (Scotland) Act 2011: For public sector organisations, mandates proper management of records, including electronic data.

INCIDENT RESPONSE SPECIALIST

ROLE

- Investigates security incidents, mitigates damage, and develops strategies to prevent future breaches.

Legislation

- UK-wide GDPR and NIS Regulations 2018: Applies during breach reporting and response.
- Police and Fire Reform (Scotland) Act 2012: If coordinating with Police Scotland during an incident, adherence to this legislation may be required.

THREAT INTELLIGENCE ANALYST

ROLE

- Collects and analyses data on emerging threats, providing actionable insights to protect organisational assets.

Legislation

- Data Protection Act 2018 and GDPR (UK-wide): Governs the handling of personal and sensitive data in intelligence activities.
- Investigatory Powers (Scotland) Act 2016: Ensures compliance with lawful information gathering within Scotland.

SECURITY ARCHITECT

ROLE

- Designs secure IT infrastructures, ensuring alignment with organisational goals and resilience against threats.

Legislation

- UK-wide GDPR: Incorporates privacy by design principles within systems in Scotland.
- Scotland Act 1998: Considerations for infrastructure that intersects with devolved sectors, such as education or local government.

CYBERSECURITY CONSULTANT

ROLE

- Advises organisations on best practices, risk management, and policy implementation.

Legislation

- UK-wide GDPR and Computer Misuse Act 1990: Ensures all advice aligns with cross-border requirements.
- Freedom of Information (Scotland) Act 2002: Applies specifically to public sector organisations in Scotland.

DIGITAL FORENSICS ANALYST

ROLE

- Investigates cyber incidents, collects digital evidence, and supports legal proceedings.

Legislation

- Investigatory Powers (Scotland) Act 2016: Governs lawful interception of communications within Scotland.
- Criminal Procedure (Scotland) Act 1995: Ensures evidence collection aligns with rules of admissibility in Scottish courts.

SECURITY AWARENESS TRAINER

ROLE

- Educates employees on security best practices, phishing awareness, and compliance requirements.

Legislation

- Equality Act 2010 (UK-wide): Ensures accessible training materials for all employees.
- Public Records (Scotland) Act 2011: Emphasises secure record-keeping practices in public sector training.

MANY MORE LEGISLATION

The above expresses some of the more crucial pieces of legislation for each job role in Cybersecurity.

We will look at much more, including:

- Standards ISO/IEC 27001, 2 and ISO/IEC 27035
- Privacy laws and Surveillance Laws (Investigatory Powers)
- Freedom of Information (Scotland) Act 2002
- Protection of IoT devices
- Intellectual Property Rights
- Copyright Design and Patents Act
- Software licensing
- End-user license agreements
- Computer Misuse Act
- ECPA – Electronic communication privacy act USA