Information Commissioner's Office Our Focus

Heather Toomey

Principal Cyber Specialist

Empower Through Information

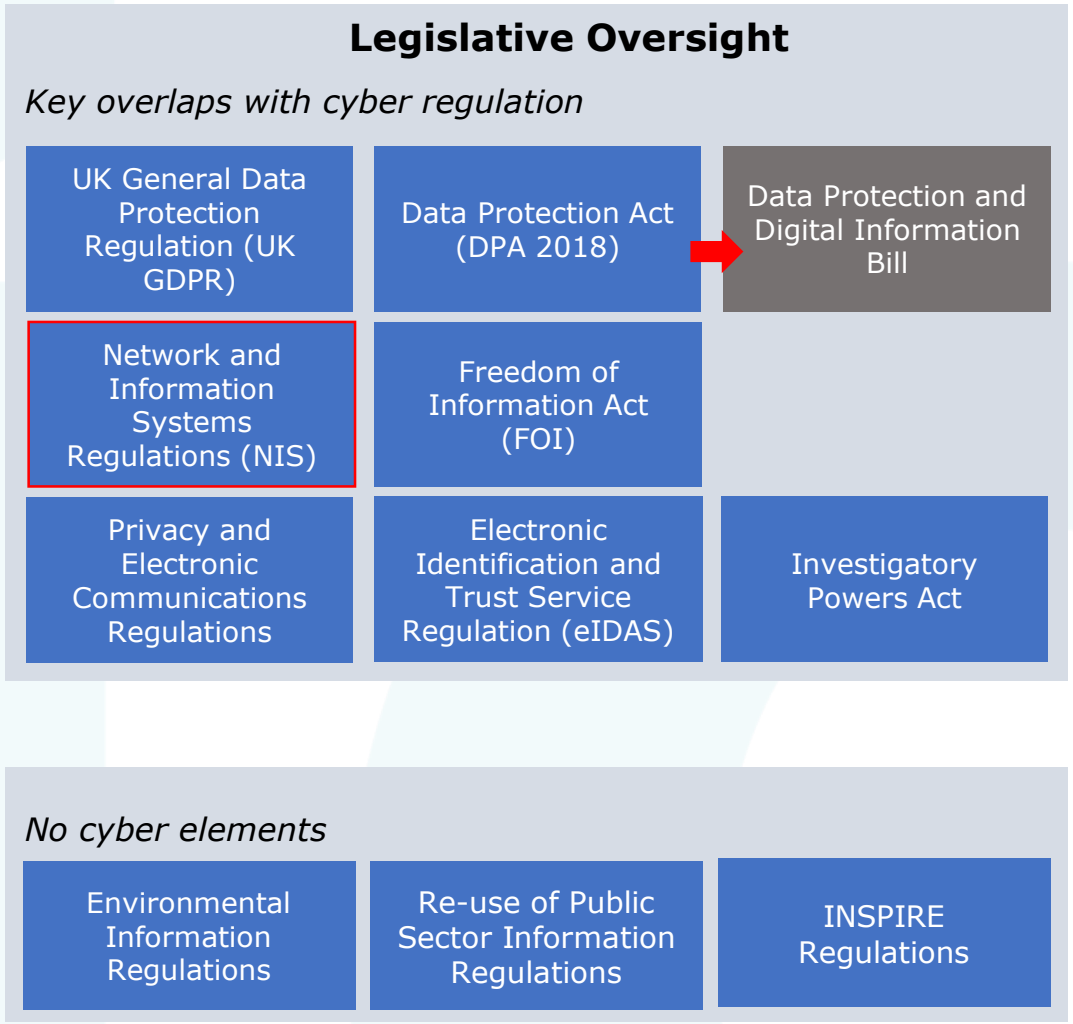
Safeguard and empower people

Empower responsible innovation and sustainable economic growth

Promote openness transparency and accountability

Continually develop the ICO's culture, capability and capacity

The Legal Context



The ICO regulates data protection laws in the UK, as the identified competent authority.

The ICO also has a regulatory function with regard to 'Network and Information Systems Regulations 2018' (NIS)

The Security Principle

A key principle of the UK GDPR is that you must process personal information securely, by means of 'appropriate technical and organisational measures'

Network and Information Systems Regulations (NIS)

NIS applies to operators of essential services (OES) and relevant digital service providers (RDSPs)

- RDSPs are organisations that provide specific types of digital services:
  - online search engines
  - online marketplaces
  - cloud service providers (IAAS, SAAS, PAAS)
  - exemptions for small and micro businesses

Managed Service Providers (MSP) who provide IT services such as security monitoring and digital billing will soon be brought under the scope of NIS to keep digital supply chains secure

Cyber Assessment Framework (CAF) is used to assess cyber security capability in RDSPs

Register as an RDSP

NIS regulations intend to address the threats posed to network and information systems, thereby improving the functioning of the digital economy.

If you are an RDSP, Regulation 14 of NIS requires you to register with the ICO.

Unlike registration under data protection law, **there is no fee required for NIS.**

Email – NISRegistration@ico.org.uk

Helpline – 0303 123 1113

Regulatory Interventions

- The provision of advice
- Offering guidance and tools
- Publishing formal opinions
- Undertaking audits and inspections
- Issuing recommendations from complaints and breach reports
- Mandating changes to practice or processes
- Where necessary, issuing reprimands and monetary penalties

Our aim is to provide regulatory certainty to help organisations comply with legal obligations

Current Trends / Issues

ICO Website Dashboard

https://ico.org.uk/action-weve-taken/data-security-incident-trends

Current Issues

Ransomware continues to be a significant issue.

Current global conflicts have been mirrored with a corresponding uptick in hacktivism.

AI and related security is a global concern, but there are no regulatory gaps in this space.

Human-centric security design is increasing, with more organisations focussing on employee experience, rather than relying on technical controls alone.

Incident Handling and Approach

Risk assessment

The first priority with any incident is to ensure that data subjects are protected.

Ensure any risks posed to data subjects are mitigated as soon as possible.

Our teams look at the impacted categories of personal data and number of data subjects from an initial triage, before looking in more detail at the organisation's post-incident steps.

Recital 87

"It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish **immediately** whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject."

Key Enquiries

1. Nature of data processing activities affected
2. Impact on data subjects and other organisations
3. Data exfiltration / encryption / integrity issues
4. Risk assessment for data subject notification
5. Recovery activities
6. Evidence available to the organisation
7. Relevant organisational policies and procedures
8. Outputs of organisation’s investigation (e.g. forensic report)
9. Incident containment and whether the attacker still has access to network
10. Evidence of data publication

Risk assessment

Once we are satisfied that data subjects have been protected from risks arising from the incident, we investigate how the incident occurred.

1. How the attacker initially accessed the network (attack vector)
2. Vulnerability references
3. Authentication types
4. Evidence available to determine cause
5. Any known information relating to reconnaissance or resource development pre-incident.

Incident to investigation

Where the evidence shows that:

- The incident posed a high risk to data subjects
- Contraventions of the UKGDPR are present

or

- Additional information suggests the incident requires further investigation

We to conduct an in-depth review of the organisation’s security compliance.

Example considerations:

1. External / internal tools
2. Compromised third party software
3. Privilege escalation
4. Credential compromise
5. Any lateral movement and how it occurred.
6. If and how data was exfiltrated.

What is appropriate?

- Your organisation may need to implement different measures to those of other organisations, depending on the **level of risk.**
- Avoid benchmarking against other organisations, even if they appear to have a similar structure / operating model / provide similar services. Your organisation will have its own mission and objectives and only you can assess your current state against your target state.
- The best baseline for measuring your performance, is your own.

Security Measures

We look to understand how the attack occurred, both in terms of initial access and actions taken once access was gained.

We then evaluate the security measures the organisation had in place.

Example considerations

1. Measures in place to protect compromised systems.
2. Use of recommended security measures (e.g. multi-factor authentication)
3. Access controls
4. How the attacker evaded or bypassed security measures.
5. Logging and monitoring.
6. Encryption / pseudonymisation of personal data
7. Heightened security of special category data
8. Following the principle of least privilege.

Organisational Measures

Example policies and procedures

1. Incident response policy
2. Backup policy
3. Access control policies
4. Logging / Monitoring procedures
5. Least privilege policies
6. Third party / processor due diligence and contracts
7. Staff training

Data Processor Incidents

Where a data processor incident has impacted multiple data controllers, we will often focus on the **security measures** of the **data processor** and the **organisational measures** of the **controller.**

As a regulator we do not only focus on what went wrong when an attack occurs.
We also consider what an organisation did correctly – both technically and organisationally.

Enforcement Considerations

1. The nature, gravity and duration of the failure;
2. The intentional or negligent character of the failure;
3. Categories of personal data affected by the failure;
4. Action taken by the controller or processor to mitigate the damage or distress;
5. Degree of responsibility of the organisation, taking into account technical and organisational measures in place;
6. How the infringement became known to the ICO, including notification
7. Co-operation with the Commissioner
8. Relevant previous failures and compliance with previous enforcement / penalty notices
9. Aggravating or mitigating factors applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure
10. Whether a penalty would be effective, and what would be proportionate and dissuasive.