New ICO Guidance on Ransomware and Data Protection Compliance

Published 24 March 2022

Earlier this month, the UK's Data Protection Authority, the Information Commissioner's Office (the "**ICO**") published its Guidance on Ransomware and data protection compliance (the "**Guidance**"). The Guidance, presented through eight scenario-based examples, provides helpful commentary as to the ICO's approach to ransomware incidents and also serves as a useful reminder of steps which can be taken to mitigate the risk of such attacks. .

According to the ICO, ransomware is becoming increasingly damaging - a trend which is expected to continue, driven by the surge in threat actors' use of data exfiltration and subsequent publication as methods of exerting additional pressure on victims to pay. The Guidance, while not legally binding, is likely to be central in advising the ICO's approach to considering enforcement action against controllers who submit data breach notifications arising from ransomware incidents.

We have summarised herein the key takeaways from the Guidance by reference to the eight main topics it addresses.

Scenario 1: Attacker Sophistication

The ICO seeks to challenge the popular belief that ransomware attacks are strictly targeted in nature and aimed solely at large corporations, by noting that "scatter gun" campaigns undertaken via mass phishing are common. Accordingly, the Guidance advises that SMEs should consider obtaining the Cyber Essentials certification by the National Cyber Security Centre (the "**NCSC**") in order to boost their protection capabilities against more commonplace attacks. For larger organisations, the Guidance recommends an assessment against the NCSC's "10 Steps to Cyber Security" guidance and certification under the ISO27001 Standard for Information Security Management.

Scenario 2: Personal Data Breach

In its Guidance, the ICO reminds controllers that when they become the subject of a cyber-attack, such as ransomware, the UK GDPR confers on them a responsibility to determine if the incident has led to a personal data breach. The regulator is clear that even temporary loss of access to personal data amounts to an availability-type data breach, as much as a breach of confidentiality does. Whether the breach is notifiable to the ICO or to data subjects under the UK GDPR is a matter of a risk assessment.

Scenario 3: Breach Notifications

The Guidance confirms that the issue of exfiltration is an important factor when conducting a risk assessment after a ransomware incident. Whether data has been exfiltrated by a threat actor is a factor when considering the risks to individuals following such an incident.

It is notable that where, following a breach notification, a controller claims that there has been no data exfiltration, the ICO will expect appropriate logs evidencing this. If such logs are not present to enable informed decision-making, it may be helpful to determine if the threat actor had the "*means, motivation and opportunity*" to exfiltrate the personal data.

Although the UK has left the European Union, the ICO's website advises that guidelines issued by the European Data Protection Board and its predecessor, the Article 29 Working Party, continue to be "*relevant*". This would include the Guidelines on Data Breach Notification, as well as their case-based supplement, the Guidelines on Examples regarding Data Breach Notification which may provide controllers with additional assistance when conducting a data breach risk assessment. Controllers should also be aware of any recommendations issued under relevant codes of conduct or sector-specific requirements they may be subject to.

Scenario 4: Law Enforcement

The ICO recommends that victims of ransomware should contact law enforcement (such as Action Fraud or local Police) in parallel to any notifications mandated under the UK GDPR or other laws. However, while recognising the importance of law enforcement agencies' role in the "*multi-agency response to ransomware*", the Guidance states that requests to delay data subject notifications by law enforcement bodies do not automatically mean controllers should delay these notifications. Instead, the three parties (controllers, the ICO and law enforcement) should work together to assess the risk to the individuals.

Scenario 5: Attacker Tactics, Techniques and Procedures

The Guidance summarises the most common tactics, techniques and procedures ("**TTPs**") threat actors use to gain access to IT systems and compromise data. It also provides steps organisations should take to mitigate against these.

- **Phishing**. The Guidance recommends that controllers' security strategy ensures that all relevant staff receive basic awareness training in identifying social engineering attacks.
- **Remote access**. According to the ICO's own observations, the most common entry point into a network are exploitable remote access solutions. The regulator recommends that controllers risk assess and document their remote access solution, identify appropriate measures in response to the risks, and document these in an Access Control Policy.
- **Privileged account compromise**. The ICO recommends that the security of privileged accounts is a high-priority issue for all controllers. "*Basic account hygiene*" is recommended, in the form of regular risk assessments and reviews of permissions, as well as observance of the principle of "*least privilege*" (i.e. giving users the minimum level of privileges required for the fulfilment of their role).
- **Known software or application vulnerabilities**. In order to allow controllers the opportunity to manage any existing vulnerabilities on their IT estate which are known to the wider information security community, the Guidance recommends that companies utilise the NCSC vulnerability management guidance.

Scenario 6: Disaster Recovery

The ICO considers the backup of personal data processed by an organisation as one of the most important controls in mitigating the risk to individuals arising from ransomware. Consequently, it notes that attackers often attempt to delete or encrypt backups. The Guidance recommends that controllers undertake a threat analysis of their backup solution to ensure their disaster recovery plan remains effective, considering the following questions:

- Is the backup segregated or offline?
- What would an attacker need to compromise to gain access to the backup?
- Is the controller able to detect changes to the backup?
- What device or IP address or both can access the backup repository?
- How would the controller respond if an attacker deleted or encrypted the backup?

It should be noted that these measures are already part of the NCSC's Small Business Guide and its 10 Steps to Cyber Security, referenced above. Consequently, compliance with the "basic prevention" measures listed at the beginning of the Guidance will put controllers in a good position in relation to their disaster recovery preparedness. However, restoration from backups does not necessarily entitle controllers to consider the severity of the risk to individuals as "low" or "unlikely" to materialise, especially where there is known or suspected data exfiltration.

Scenario 7: Ransomware Payment

The Guidance states that the ICO supports law enforcement's position to not encourage, endorse, nor condone the payment of ransom demands. Even where payment is made and the data restored or not disclosed publicly following exfiltration, the ICO is clear that it will still consider the cyber incident in itself as a breach of individuals' data protection rights, such as transparency of processing and subject access rights.

The Guidance reminds readers of the terminology within the UK GDPR requiring organisations to implement "appropriate measures" to restore the data in the event of a disaster. The Guidance is clear that the ICO does not consider the payment of a ransom as an "appropriate measure" to restore personal data. Even if controllers pay the ransom, they should still presume that the data is compromised and take additional mitigating actions as required under Article 33 UK GDPR.

Scenario 8: Testing and Assessing Security Controls

The Guidance highlights several methods of testing, assessing and evaluating an organisation's appropriate measures, including:

- **Breach notification** – document and regularly test the organisation's incident response plan;
- **Account management** - regularly review user accounts and consider existing privileges;
- **Patch management** - implement a method of checking for vulnerabilities including missing patched;
- **Attacks tactics** - assess security controls to check if they can resist TTPs;
- **Audit** – perform regular audits of the organisation's IT estate against a proven security standard; and
- **Disaster recovery** - perform tests of the organisation's disaster recovery plan to ensure efficacy.

To assist organisations with the above assessment process and enable them to evaluate their general preparedness for a ransomware attack, the ICO has also produced a 10-step checklist for controllers to utilise, encompassing all key issues discussed in the Guidance.

The full text of the Guidance is available here.

Authors

Eleanor Ludlam

London - Walbrook
+44 (0)20 7894 6098
eludlam@dacbeachcroft.com

Alexander Dimitrov

London - Walbrook
+44 (0) 20 7894 6443
adimitrov@dacbeachcroft.com

DAC BEACHCROFT