November 1, 2022

TLP White

This week, Hacking Healthcare dives into a recent regulatory fine against a large UK organization for General Data Protection Regulation ("GDPR") violations. We provide a breakdown of the regulator's report and the enormous fine it levied, and we extract some useful takeaways for healthcare organizations, many of which can be applied beyond the UK's jurisdiction.

Welcome back to *Hacking Healthcare*.

1. **UK Regulator Issues £4.4 Million Fine to Hacked Company**

   On October 24th, the UK-based Interserve Limited ("Interserve"), a construction and support services business, was sent a monetary penalty notice of £4.4 million from the UK's Information Commissioner's Office ("ICO") for GDPR violations.[1] The fine — reportedly the fourth largest ever levied by the UK's independent authority set up to uphold information rights — raises questions about how divergent the UK's regulatory regimes may become as Britain charts its post-EU path. Let's examine the ICO report to see why the UK regulator came down so harshly and what healthcare organizations in the UK may wish to be aware of.

   Please note that parts of the publicly available report remain redacted.

   How Did the Incident Occur?

   In late March 2020, a phishing email under the guise of a document requiring urgent review was received by an Interserve employee. The employee forwarded it to a colleague "who downloaded and extracted the [malicious] ZIP file linked in the email."[2] This action gave malicious actors a foothold on the employee's workstation. The ICO noted that the employee who opened the malicious attachment was working remotely and "had access to Interserve's systems via a split tunnelling method," which bypassed controls in place to restrict access to malicious sites.[3]

Within days, this initial access was then used to compromise an Interserve server, which facilitated lateral movement within Interserve's network. At some unspecified point, Interserve's endpoint protection tools detected the activity, "[removed] some of the files resulting from the extraction of the ZIP file, [and] reported that the automatic removal of malware files had been successful."[4] The ICO noted that "no further action was taken by Interserve at this time to verify that all malware had been removed," and in fact, the "attacker retained access to the employee's workstation."[5]

The failure to fully remove access reportedly led to the "compromise of 283 systems and 16 accounts (including 12 privileged accounts) across four domains" within the next few weeks.[6] This access was used to uninstall Interserve's anti-virus solution, and the attacker then compromised servers and databases that "together contained personal data relating to up to 113,000 individuals."[7]

The personal data included fields such as email address, national insurance number, bank account details, birth date, and education. Additionally, it included "special category data" such as ethnic origin, religion, details of disabilities, sexual orientation, and "health information relevant to ill-health retirement applications."[8] The attacker promptly encrypted the personal data on those compromised systems.

Incident Response

Based on the ICO report, it appears Interserve reported the incident promptly, within a day or so of the personal data being encrypted, to the National Cyber Security Centre (NCSC), and several days later to the National Crime Agency ("NCA") and ICO. The ICO noted that Interserve was cooperative with the ICO throughout the investigation.

GDPR Violations

The ICO determined that Interserve had violated two sections of GDPR.

First, it "failed to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures as required by Article 5(l)(f)."[9]

In relation to this article, the ICO specifically called out several issues:

- Interserve processed personal data on unsupported operating systems.

  The ICO noted that the failure to implement supported operating systems was contrary to Interserve's *Systems Management Policy*; Interserve's *Systems Management Standards*; industry best practices standard *NIST 800-53*; Guidance on *Security Outcomes* (2018) issued by the NCSC; and Guidance on *Mitigating Malware and Ransomware attacks* (2020) issued by the NCSC.[10]

Furthermore, the ICO determined that "Interserve ought reasonably to have been aware of the risks posed by running outdated support systems," and Interserve "failed to undertake any formal risk assessments in relation to using unsupported operating systems on its data processing servers."[11]

- Interserve failed to implement appropriate end-point protection at the time of the attack.

  The ICO noted that Interserve's solution was not running its "latest Anti-Virus protection," that it did not have host-based firewalls enabled, did not implement application allow/deny lists, and did not prevent macros from executing on the initial compromised host. The ICO noted that these actions ran contrary to Interserve's own documentation, industry-recognized best practices, vendor communications for the use of their product, and government guidance. The ICO determined that Interserve "ought reasonably to have been aware of the risks posed by failing to implement appropriate endpoint protection."[12]

- Interserve failed to perform adequate vulnerability scanning and penetration testing.

  The ICO noted a failure to undertake adequate vulnerability scanning and penetration testing. This failure was again noted to be contrary to Interserve's own policies, industry best practices, and government guidance. Once again, the ICO found "Interserve ought reasonably to have been aware of the risks posed by failing to undertake regular vulnerability scanning and penetration testing."[13]

- Interserve failed to follow established incident response procedures in the wake of the anti-virus notification.

  The ICO noted, "Following the initial attack, the matter was not investigated by Interserve's Information Security Team." This also ran contrary to Interserve's own policies and industry best practices.

- Furthermore, the ICO found that Interserve had failed to ensure that employees had undertaken all relevant information security training, failed to correctly enforce privileged account management, and continued to use outdated SMB protocols. All of these were found to also be at odds with established Interserve policies, industry best practices, and government guidance.

In addition to that GDPR violation, the ICO also found Interserve to have "failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk as required by Article 32(1)."[14] Much of this violation ties back to issues we just listed, but it also involved the failure to restore availability and access to personal data in a timely manner.

Penalty

In this case, the ICO took "the view that this was a significant contravention of the GDPR."[15] The gravity of the infringement took into account the volume of personal data processed by Interserve, the nature of the personal data involved, the number of individuals impacted, and the length of time data subjects did not have access to or full control of their personal data. The ICO rejected the argument that Interserve's "financial constraints" were a reasonable excuse for the security failures it noted.

The ICO did note that Interserve had "been the subject of two previous personal data breach incidents in 2019 which resulted in reports to the Commissioner. On both occasions the Commissioner directed Interserve to review the Commissioner's GDPR security guidance and on one occasion to advise of the importance of employee training in respect of managing phishing attacks."

The ICO report helpfully walks through the processes of assigning the final penalty amount, including what mitigating or aggravating actions did to decrease or increase the final penalty of £4,400,000.

Action and Analysis
Membership required

Congress

Tuesday, November 1st:
- No relevant hearings

Wednesday, November 2nd:
- No relevant hearings

Thursday, November 3rd:
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

Conferences, Webinars, and Summits

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

About the Author

Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

---

[1] https://ico.org.uk/action-weve-taken/enforcement/interserve-group-limited/
[2] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[3] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[4] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[5] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[6] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[7] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[8] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[9] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[10] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[11] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[12] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[13] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[14] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf
[15] https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf