RECRUITMENT AGENCY CASE STUDY

Protecting SMEs from Cyber Security threats since 2016.

Background

An Online Recruitment Agency, aware that it held a considerable amount of Personally Identifiable Information (PII), was struggling with their data protection issues, and ensuring that its staff fully understood their responsibilities with regards to data protection and cyber security.

The key challenges were:

Staff did not fully grasp their responsibilities as regards to GDPR, and did not have a good understanding of the potential dangers of cyber attacks and scams.

They had difficulty in tracking the PII they held, had no audit trail, and were concerned that multiple copies of the data were held insecurely.

Being aware that similar size companies had received fines from the ICO, they were keen to ensure they were not vulnerable to this, and were not confident that they could handle a Data Access Request in a timely manner.

At a Glance

Challenges

- Large amounts of PII
- Multiple copies of the data
- No Cyber Awareness training
- Concern over potential data breaches

Kevin Hawkins

Director, H2

"Since 2016, H2 have worked with National and International SMEs to secure their data and provide ongoing Cyber Security support"

customersupport@hah2.co.uk   www.hah2.co.uk   0800 494 7478

Solution

H2 used a Cyber Maturity Assessment to discover where the client currently stood., which experience suggested would highlight other areas for attention, and this approach quickly led to the introduction of Actifile.

- Automated discovery of personally identfiable information (PII) stored locally, on servers and in cloud apps used for collaboration. This quickly quantifies data risk exposure

- Encrypts senstive files to protect data regarcless of where it resides across the hybrid work environment. Encryption causes minimal disruption to users

- Continuously monitors movement of sensitive data to detect suspicious activity and data exfiltration risks. Detailed audit logs for forensics

- Lightweight agents on endpoints ensures high adoption by employees, and cloud-based management minimises ongoing admin workload.

Results

- Production of a data protection handbook

- Rollout of cyber awareness training

- Actifile deployed in less than 3 days without disrupting employees. Quickly discovered major data risk areas , specifically unprotected cloud storage instances.

- Identifiied and Encrypted over 80% of sensitive files, dramatically improving security posture. Remainder of files were tagged for remediation.

- Implementation of File movement monitoring enabled proactive alerts on suspicious data activities for further investigation. Addressed several risky IT uses.

- Automated subject access requests now possible with detailed data inventories. Access logs in Actifile's system. Report generation was reduced from weeks to minutes.

- With improved data protection controls now in place, the recruitment company reduced their regulatory risk and business exposure substantially. Compliance process improvements also resulted.