03 March 2022

Heightened Cyber Security Threat Level

This Bulletin summarises our response to the heightened cyber security threat level resulting from the current situation in Ukraine.

In response to the heightened threat, we have conducted focused threat simulations based upon potentially malicious email traffic, reinforced organisational awareness of the threat landscape and raised vigilance through additional staff training and blocked access/internet traffic from specific countries.

As a matter of course, we continually review all aspects of our physical and logical security and implement improvements on an ongoing basis. Some of the more important elements of our current security posture are outlined below:

- Frequent internal threat simulations, to increase our employee's awareness of (and test their response to) phishing emails and other cyber threats
- Enforce strict infrastructure configuration and hardening policies. All network interlinks are firewalled, with rules to restrict communication based on source destination. Only specifically defined traffic is allowed to the destination. All firewall communication is logged. Traffic from trusted/untrusted networks is encrypted and passes through a web application firewall and Identity Access Management System. All servers are CIS level 2 hardened and are built from the same gold build. Server builds are tested independently as part of our annual cyber security review. All servers are subject to anti-virus scanning and logging
- Review all guidance and advice issued by The National Cyber Security Centre NCSC). We are a member of CiSP, the Cyber Security Information Sharing Partnership, which is a joint industry and government initiative run by the NCSC
- ISO 27001: 2013 certified. Our Information Security Management System is externally audited every six months by the British Assessment Bureau
- Cyber Essentials certified. This is a UK government backed scheme, which demonstrates that we have technical controls in place to defend against the most common cyber-attacks
- Engaged a leading UK security consultancy, Pen Test Partners LLP, to provide us with incident response services
- We conduct a programme of annual cyber security reviews, subjecting our software

©Heywood Limited trading as Heywood Pension Technologies

products and our internal and external IT infrastructure to comprehensive security tests. These are carried out by our independent security consultants, Pen Test Partners LLP. These were last completed in January 2022, and we received very positive feedback in relation to the security controls that we have in place.

- All employees complete mandatory information security assignments each month.

We will continue to closely monitor the cyber threat landscape, particularly threats connected with events in Ukraine. When necessary, we will take immediate action to mitigate against new threats as they emerge.

©Heywood Limited trading as Heywood Pension Technologies