REMORA

CORPORATE CYBER DEFENCE

CEO impersonation email at a Manufacturing Firm

Background

Remora were invited by a Manufacturing Firm to investigate an email breach that resulted in a fraudulent email impersonating the CEO being sent to the Finance Team and improper payments being made totalling over £150,000.

Services performed

- A Forensic Assessment of the Breach;
- Risk Assessment with strategies to prevent similar incidents from happening again.

Time Taken: 5 days

Observations and Approach

Our investigation revealed that the firm had been riddled with malware for over a year. The typical warning signs such as slow network performance, had been ignored by their IT provider. Security software solutions had been purchased and installed prior, but those have not been configured and activated correctly.

The combination of different factors which were observed, but never prevented, allowed hackers to compromise all Finance Department machines, understand both the payment process and communication between team members, and granted the ability to create an internal "look-alike" phishing email account from which, on the day the CEO went on holiday, payment requests were sent to the Finance Team seemingly from the CEO.

2 payments were made before the Financial Controller spotted the issue and halted the process.

Deliverables and Conclusions

Our work ultimately led to:

- Immediate reconfiguration of the IT security software, tightening of the IT security policy;
- The firm's Payment Processes being strengthened and consistently enforced;
- A significant restructuring of the firm's senior management roles to incorporate data and Information Security functions performed.
- A reinforcement of software patch management procedures.

Find out more :

hello@remora.co.uk

0203 617 6990

www.remora.co.uk