PT SOLUTIONS PERFORMS A CYBER SECURITY ASSESSMENT FOR CRONDALL ENERGY

"The Cyber Security Assessment done by PT Solutions has provided a valuable, independent overview of our current vulnerabilities, and helped us to prioritise actions needed to mitigate these risks. We are now confident that our data, and that of our clients, is protected to a very high level"

The Background

Crondall Energy is a leading independent consultancy providing strategic, commercial, and technical services for offshore energy projects. Working with a range of project stakeholders, including energy companies, investors, and law firms, Crondall Energy helps clients to manage risks, and achieve positive project outcomes.

Crondall Energy is passionate about the role of the offshore industry in providing society's sustainable energy and is actively engaged in helping clients confront the challenges of generating low carbon energy and renewable energy in the offshore environment.

PT Solutions has provided Internet connectivity to Crondall Energy since it relocated from Winchester to the University of Southampton Science Park in late 2020. In May 2022, PT Solutions met with Crondall Energy's IT Manager, to discuss broader IT security challenges and to identify any potential vulnerabilities.

The Challenge

As an organisation that helps its clients to manage technical, commercial and strategic risks, Crondall Energy clearly has a requirement to ensure that its own IT systems operate as efficiently and securely as possible. Crondall has been keen to ensure that it can demonstrate to clients and partners that it is taking the risks associated with cyber security seriously and doing everything it can to protect IP and clients' data.

The challenge for IT Managers of SMEs, is providing Enterprise level IT Services at a fraction of the cost and without the internal IT resources enterprise businesses have at their disposal. Initial discussions revealed some potential issues so a full Cyber Security Assessment was undertaken to quickly provide Crondall Energy with an overview of the potential vulnerabilities and an action plan that the IT Manager could present to the Board.

The Solution

PT Solutions worked with the IT Manager at Crondall's Southampton office to run through their IT estate and provide setup explanations along with

evidence to show the current status of each system or service. Cyber Security Assessments undertaken by PT Solutions are tailored to the specific needs of clients based upon analysis of the existing IT and security infrastructure. The clear objective was to provide an overview of current vulnerabilities, together with a plan for addressing these and mitigating risks moving forwards.

IT Security Assessments undertaken by PT Solutions typically cover the following areas:

IT Policy and Company Handbook review – an assessment of whether this document adequately covers IT Security Policy and whether these can be enforced given the existing IT technical controls.

IT Security Policy review – an assessment of the policy to determine whether it reflects the needs of the business and enables effective data security.

Training on phishing, handling suspicious emails, social engineering hackers –does the current security landscape deal with the most commonly encountered threats?

Emergency and cyber security plan – review of current plans and assessment of suitability.

Determine all possible sources of business disruption due to cybersecurity risk – assessment of existing documentation and review schedules to ensure they are comprehensive and actively updated.

System hardening plans – review of status and procedures for new systems.

Regular security audits and penetration testing – review of current arrangements and schedules.

Secure Data Policy – assessment of policy and procedures to ensure they are fit for purpose and that users fully understand the policy through training.

Encryption – review of current encryption policy and implementation across the IT estate.

Regular scheduled security testing – assessment of current procedures measured against best practise.

Vulnerability Scanning – review a subset of end-user machines to assess and score vulnerabilities (needed for Cyber Essentials Plus certification)

Port scan against externally facing infrastructure – an overview of the current position and assessment of risk.

Microsoft Secure Score – a benchmarking test against similar organisations. Covering a review of outstanding security improvements, device exposure, sign-in risk policy, and user risk policy.

Endpoint Security Assessment – review of current protection and procedures, and attack surface reduction rules.

Virtual Desktops – review of vulnerabilities and protections in place.

Local admin rights review – assessment of current policy.

USB Restrictions – assessment of current policy.

UAC (User Account Control) – assessment of current policy.

Event Logs Retention – assessment of current policy.

"Crondall Energy is a great example of how a responsible company faces cyber security challenges. They already had very good policies and protocols in place to secure their data and IT systems but engaged us to review and assess their approach, and to bring our experience to bear to address areas where improvements could be made"

Anti-Virus Endpoint Portal Review – assessment of current vulnerabilities and of anti-virus policy.

Multi Factor Authentication – assessment of current policy.

Patch Management – review of policy relating to both servers and workstations.

Privilege Escalation / Accountability – assessment of audit trails of accountability.

Email Security – review of policies relating to anti-phishing, anti-SPAM, safe attachments, DMARK, SPF, and DKIM.

Data Retention Policies – assessment of current policy.

Data Sharing Policies – assessment of current policy.

Data Loss Prevention – assessment of current policy.

Mobile Device Management – assessment of current policy.

Mobile Application Management – assessment of current policy.

Web Content Filtering – assessment of current policy.

The Result

Once the Cyber Security Assessment had been completed and presented, Crondall Energy had a comprehensive assessment of their IT infrastructure, and of the vulnerabilities that had been identified. Crucially, the IT Manager also had a report of specific, actionable recommendations and improvements that would deal with the vulnerabilities that had been identified. This was then presented to the Crondall Energy Board of Directors.

Crondall Energy has taken a highly responsible approach to its cyber security and taken actions that will give its clients even more confidence.

Simon Moon, lead consultant from PT Solutions commented, "Crondall Energy is a great example of how a responsible company faces cyber security challenges. They already had very good policies and protocols in place to secure their data and IT systems but engaged us to review and assess their approach, and to bring our experience to bear to address areas where improvements could be made".

Crondall Energy's IT Manager commented, "Cyber security is a constantly moving target, so any professional IT manager knows that there will always be new vulnerabilities appearing that need to be addressed. The Cyber Security Assessment provided by PT Solutions has provided a valuable, independent overview of our current vulnerabilities, and helped us to prioritise actions needed to mitigate these risks. We are now confident that our data, and that of our clients, is protected to a very high level".