Waste Management & Recycling Sector
Briefing
Cyber Security Defence in Depth

The Challenge

Multiple oil transport and storage companies across Europe are dealing with cyber attacks. IT systems have been disrupted at Oiltanking in Germany, SEA-Invest in Belgium and Evos in the Netherlands affecting oil terminals, storage depots and logistics around the globe.[1] In May 2021 a ransomware attack on the US oil supplier Colonial Pipeline saw supplies tighten across the US and multiple states declaring an emergency.

Major utilities and service sectors including Waste Management & Recycling are now prime targets for cyber attacks including but not limited to ransomware.

The Solution – Cyber Security, Defence in Depth

Defence in depth is the use of different successive layers of defence to slow, stop and eradicate an attack. It is not a new concept, its use was reported in the defence of the Hierakonpolis region of Egypt in 2900BCE.[2]

To bring it up to date the UK National Cyber Security Centre (NCSC) employs the concept in its advice on how to reduce exposure to a cyber attack.[3] The basic controls for cyber security are:

- Firewall Management
- Access Rights
- Daily off-site back-up
- Multi-layered Anti Virus
- Software Patch Management

These should be employed across different successive layers of defence. If your accounts department is off line whilst it restores data to deal with a ransomware attack, you do not want your methane sensors and controls at your landfill sites down at the same time. In such an event you could be breaching data privacy (GDPR) and environmental controls whilst trying to get services back online.

IT services for the Waste Management and Recycling sector lend themselves to three layers of defence, each of which employs the basic controls for cyber security:

- Corporate network
- SCADA network
- Cloud computing

Corporate networks need to pay particular attention to bring your own devices (BYOD), endpoint security for remote working and social engineering. The latter requires staff education so that they are aware of common email phishing scams and insecure web site threats. The NCSC has produced an informative video for people working in schools which is equally applicable to staff in the public and private sectors.[4]

[1] https://www.bbc.co.uk/news/technology-60250956
[2] https://www.scirp.org/journal/paperinformation.aspx?paperid=70457
[3] https://www.ncsc.gov.uk/information/reducing-your-exposure-to-cyber-attack
[4] https://www.ncsc.gov.uk/information/cyber-security-training-schools

Supervisory control and data acquisition (SCADA) networks as used on site and with third parties e.g. remote equipment management, sensor logs/controls, CCTV, weighbridges etc. provide a level of separation between corporate services and third party users. Particular attention to, no shared point of failure with nor similar equipment as the corporate network, multi telco provision based on dispassionate performance requirements, rapid third party encrypted link builds and decommissions, network traffic monitoring and IT tech support for sites is required.[5]

Cloud computing is providing evermore IT services including software as a service (SaaS) e.g accounts, email, sales, and infrastructure as a service (IaaS) e.g. file shares and virtual computing (VMs). Particular attention should be given to which country your data is stored in and automatic backup of cloud data to a separate cloud service.

UK Government Support

The UK Government is acutely aware of the risk of cyber attacks which is why the NCSC has been established and the UK Government backs and promotes the Cyber Essentials scheme.[6] Cyber Essentials provides a framework and check list to help organisations implement cyber security.

Cyber Essentials accreditation is also included in the UK Governments Social Value requirements which now constitute at least 10% of Government bid selection criteria.

Benefits & Costs

Third party SCADA network provision by Keyfort reduces CapEx as the equipment is included in the service and the OpEx as it is a single point of contact for service supply, system integration, operational support and decommission. Cloud computing services can also, if suitably specified, provide additional resilience and cost savings.

Implementation of Cyber Essentials embodies good IT practice, improves resilience and reduces exposure to cyber attack.

What if we do nothing

'Doing nothing is no longer an option. You can protect your organisation, and your reputation, by establishing basic cyber defences to ensure that your name is not added to the growing list of cyber victims.' UK NCSC

The time has come for methodical implementation of cyber security using defence in depth, which has been with us for near 5000 years.

Author: Roy Clayton MSc MA FRSA MAPM
Keyfort Ltd
bizdev@keyfort.co.uk
Published: 8th February 2022

[5] Keyfort Ltd provides secure SCADA networks and cyber security services for the Waste Management & Recycling sector. www.keyfort.co.uk
[6] https://www.ncsc.gov.uk/cyberessentials/overview