Ref no:	452121016
From:	Commercial
Date:	12/10/16
Subject:	Cyber Security Services

REQUEST

I am currently embarking on a research project around Cyber Security and was hoping you could provide me with some contract information relating to following information:

1. Standard Firewall (Network) - Firewall service protects your corporate Network from unauthorised access and other Internet security threats

2. Intrusion Detection - network intrusion detections systems (IDS) and network intrusion prevention systems (IPS) services that detect Web application attacks and include anomaly-awareness in addition to handling older threats that haven't disappeared.

3. Web Applications Firewall - A Web application firewall (WAF) is a firewall that monitors, filters or blocks the HTTP traffic to and from a Web application.

4. Threat Monitoring - organizations and security analysts to identify and protect against security threats.

5. Anti-virus Software Application - Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

6. Encryption Facilities - s a host based software solution designed to encrypt sensitive data before transferring it to tape for archival purposes or business partner exchange.

For each of the different types of cyber security services can you please provide me with:

1. Who is the existing supplier for this contract?

2. What does the organisation spend for each of contract?

3. What is the description of the services provided for each contract?

4. What is the expiry date of each contract?

5. What is the start date of each contract?

6. What is the contract duration of contract?

7. What is the hardware brand? If available.

8. What is the software brand? If available?

9. The responsible contract officer? Full name, job title, contact number and direct email address.

RESPONSE

The Trust must do its utmost to protect patient and staff information.

Patient information and staff information are the foundations upon which healthcare is built, and the Trust have a clear responsibility to safeguard this information to ensure we are able to provide the necessary care to our service users.

To provide the requested information would highlight any vulnerability, should any such vulnerability exist, within our IT infrastructure which could be exploited for the purposes of ransomware, other malware, or to withhold/disrupt IT functionality within the Trust. Therefore, to confirm or deny such vulnerabilities in our IT network is likely to assist criminal offenders thereby seriously threatening the effective delivery of healthcare by the Trust. The act of gathering information as requested, in the hacking arena is known as foot-printing and our network architecture is closely protected to at least NHS protect if not NHS Confidential. Therefore:

To confirm or deny what Standard Firewall (Network) - Firewall service protects our corporate Network from unauthorised access and other Internet security threats would motivate attacks against our network which

would massively hinder our abilities to safeguard the service user healthcare information and staff information that we require to coordinate our services.

To confirm the infrastructure IDS, Firewalls, anti-virus etc. hardware & software could expose vulnerabilities within one or more of our IT infra-structures which could subsequently lead to attacks, data loss, and loss of public confidence. Our patients must have confidence that their very sensitive personal data will be held securely.

Again, providing information about what contracts/suppliers could also expose what applications we use (hardware brand & software) and aid to the foot printing phenomena.

They (patients) must have confidence that we'll be able to provide the services they need.

Providing the requested information would put their confidence at risk.
Furthermore, loss of patient and staff data by such an attack would massively impact upon our ability to provide effective healthcare to our service users.

This would be extremely harmful to the public.