necs Partners in improving local health

Case Study:
Effective Management of Cyber Security

We pride ourselves on our proactive approach to preventing cyber threats and ensuring our client information is fully secure. The NECS IT Security team regularly make significant investments in current anti-virus solutions. We are committed to protecting our clients' data first and ensuring critical systems are secure at all times. Because of our proactive approach we are always fully aware of emerging threats and we inform our clients first when a risk arises - we go to them, clients don't have to come to us.

Problem

Cyber security is rapidly becoming a major challenge for organisations on a global scale.

Data security in the healthcare sector is of paramount importance;

patient information must be fully secured with safeguarding procedures in place to ensure data is protected.

Organisations around the globe face dangerous online threats on a daily basis from a number of different sources. Consequences can be detrimental in a number of ways: from PC malfunction, forcing normal service to seize; to unwanted data encryption, when hackers render data inaccessible to health organisations meaning zero access to patient information, including names, addresses and bank details.

These infections can come from a number of sources including:

- Staff connecting personal writeable USB sticks to corporate PCs
- Clicking on links in spam and phishing emails
- Clicking on malicious links in web apps
- Browsing the Internet without due care and attention

Our Solution

NECS IT Security team automatically monitor and analyse potential threats on a daily basis, to ensure all NECS clients are fully protected against key online attacks. In many cases we detect and locate threats, block those threats and ensure data is fully secure without our clients being affected in any way. Clients may not be aware of potential threats as they are neutralised and blocked before any damage can be done.

35%

35% of the world's computers are infected with malware

50x

Healthcare data can be up to 50 times more valuable to criminals

The Results

Client 1 Clinical Commissioning Group NECS IT Security team detected a Ransomware* attack.

The team was able to locate this threat clean it up and resolve it rapidly and efficiently. Identifying the threat, file recovery and completion of clean up took around 2 hours and all of our client's data remained fully secure.

Client 2 Clinical Commissioning Group based in the UK NECS technical team detected one of their GP practices' hardware was infected with Ransomware*.

The technical team were able to scan the data and restore all information, ensuring the GP practice was back up and running and all threats were neutralised. This fast action from the NECS team ensured there was no ransom to pay and their client data was secured and out of harm's way.
The GP surgery was able to resume normal operations within a matter of hours.

**Ransomware is a form of malicious software which prevents users accessing key information, unless a ransom is met to re-enable access.*

For further information please contact:
Jacquie Fawcett: Head of Programme Development and Delivery Service **Email:** Jacqueline@nhs.net

Visit our website for more information about our other services www.necsu.nhs.uk, call 0191 301 1300
or email necsu.enquiries@nhs.net

Case Study:
Effective Management of Cyber Security

About NECS Anti-virus Software

- NECS security software protects data and reduces the risks of many cyber threats
- Save money by using NECS Anti-virus Software – reduce the downtime and financial risks of ransomware, ensuring normal practice can resume as quickly as possible
- By using NECS Anti-virus Software we can help ensure the healthcare sector is providing an efficient and effective service by maximising secure system and data availability

About NECS Cyber Security Services

We respond to customers' specific needs.

We worked with a GP practice which specialised in dealing with asylum seekers.

This brought with it some unique challenges regarding data security. It meant the practice dealt with a large number of transient patients who were there for short periods of time. They needed specific health checks and the practice had to meet additional regulations as well as usual national standards on integrity of patient data.

We examined the customer's specific requirements, reviewed the current processes and then mapped them onto a new clinical system that would align with the business and security needs.

We also involved other NECS experts in business change and training to offer an all-round service. Data quality and reporting requirements needed bespoke changes before implementation of the new system.

Our support continued after go live to validate that the business changes worked as desired and cyber-security measures were effective.

10 CCG Customers in 6 Markets, and 4 Regional Offices

Our main customers are the 13 NHS Clinical Commissioning Groups (CCGs) covering the north east and Cumbria. They in turn have responsibility for providing health and social care for a population of over 3.5 million people.

During our first year we have also been delighted to work with other commissioning organisations across North Yorkshire and Humber, Teesside, Durham and Tyne and Wear, Lancashire, Suffolk, Cambridge, Peterborough and Anglia.

For further information please contact:
Jacquie Fawcett: Head of Programme Development and Delivery Service **Email:** Jacqueline@nhs.net

Visit our website for more information about our other services www.necsu.nhs.uk, call 0191 301 1300
or email necsu.enquiries@nhs.net