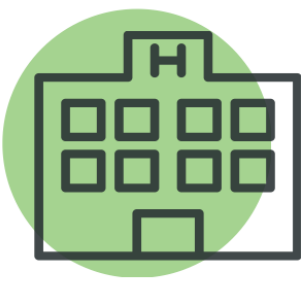
4 Bad Cyber Security Habits

CORE SECURITY

That Your Healthcare Organization Should Avoid

1



Increased "Awareness" Doesn't Mean Increased "Enforcement"

Deployment of malware detection, pen-testing for security vulnerabilities, endpoint security, security analytics network-threat detection and any other solution should be installed and enforced - not just suggested.

If anyone can get access to your data, their access, movements and activities on your network should be monitored and security regulations enforced

2

Fear vs. Over-Confidence

There is quite a difference between living in fear of the next cyber-attack and being overconfident that your policies and processes will save you; however, both are dangerous

While there is no such thing as being "too prepared" for an attack, make sure that you're putting in place processes that will help prevent attacks as well as alert and prepare you to deal with them once they happen

3

No Strategy for the Future

Cyber-attacks continue to evolve and impact the, healthcare industry where personal data can be exploited.

Professionals both in and out of cyber-security should be worried about expanded attacks along with more sophisticated spear-phishing, privileged account exploitation, social engineering, ransomware and whatever else may come as this industry grows.

4

Lack of Corporate Accountability

Bridge the gap between awareness and enforcement with corporate accountability.

With more attacks and the increasing loss of patient data, you can expect regulations to increase for cyber-security in the healthcare industry.