CAPITA

Security as a Service

Access to specialist expertise for application support.

Corporate systems are increasingly exposed to internet based threats whether via email or rogue websites. Customers of all sizes face the challenge of protecting against constantly evolving threats to internal systems and colleagues both inside and outside the security perimeter.

Remote workers, such as teleworkers and employees at remote offices, are susceptible to security risks since they frequently access the Internet outside the protections available through the corporate network or VPN. When outside the corporate network, IT users may inadvertently expose themselves to threats simply by visiting a website.

Email threats have evolved, going beyond viruses and spam alone. Virus, spam and spyware writers are now taking advantage of each other's methods. Some attacks are so targeted that they never appear on the anti-virus industry radar and are not properly identified or stopped by standard signature-based anti-virus scanners.

Impact of failure to Act

- Infected and compromised systems will harm your organisation's reputation as malware attempts to replicate to your customers and partners.
- You may expose your business to legal action by failing to comply with the wide range of legislation governing areas such as human rights and data protection.
- Compromised systems may underperform or may even rendered inoperable impacting business operations leading to resources being diverted to remediate and work around problems.
- When email systems are not managed carefully, costs soon spiral. Accumulating spam can push data storage costs up exponentially, while your resources are also being diverted to manage ever increasing demands.
- The web now offers more potential distractions for staff where access controls are not in place. The key activities which can lead to a drain on employee productivity include chat rooms, auction sites, streaming media, online games and file downloads.

Business Requirement

For any organisation, any size, your key objectives are to:

- Ensure the integrity and availability of all systems and networks, regardless of location, by protecting against mail and web based malware with an integrated solution that provides web vulnerability scanning, spyware protection, spam filtering and virus protection.
- Maintain employee productivity by restricting access to non-work related internet content and services.

Published: 27/03/13

- To protect your reputation, it's crucial to ensure information contained within email and web communications is properly controlled, archived and managed.
- Ensuring the organisation is compliant with Data Protection, Freedom of Information, Human Resources Policies and other directives to avoid legal actions with a comprehensive Acceptable use Policy (AUP) that is enforced effectively by the latest technologies.
- Ensure the potential impact of monitoring employee web use is properly assessed and proportionate to the perceived risk by engaging specialist legal advice.

Capita Security as a Service

The service inspects all web and email traffic for viruses, spyware and inappropriate content ensuring that internal and remote staff are protected from risk and comply with usage policies. As the service is operated on your behalf, you are relieved of the burden of managing infrastructure and attempting to keep pace with the latest threats.

Key features include:

- Stops viruses, spam, spyware and other web-based threats before they reach your network.
- Tighten holes in your business web security with an integrated Web vulnerability scanner and endpoint spyware detection.
- Real time, high-performance scanning of all web requests.
- Blocking of websites by pre-defined categories, specific URL and by file types.
- Create rules based on time of day and Internet consumption.
- Roaming and remote user support extends policy enforcement to distributed workers.
- Multi-layered, multi-vendor spam and anti-virus engines to provide maximum possible protection.
- On-demand reporting.
- Enforce acceptable use policies with powerful web filtering capabilities.
- Reduce total cost of ownership (TCO) with our business web security service; no hardware or software to purchase or manage.

Benefits of Capita Security as a Service

With Capita Managed IT Solutions managing internet content and access, you're assured that the most advanced technology and up-to-date threat intelligence is constantly protecting your business and enforcing policies.

Benefits include:

- The costs are affordable, always predictable, and do not require any investment in security infrastructure.
- Controlled access to adult content, gambling, content sharing and social media sites mitigates the legal risks while maintaining access to business related resources.
- Saves time and resources wasted dealing with outbreaks and clean-up.
- Reduces bandwidth usage by blocking content before it enters your network.
- Ensures effective protection against new and unidentified virus and malware threats.
- Allows administrators to set and enforce or devolve flexible, customised policies suited to your organisation's specific needs.
- Gives you reassurance and allows you to focus on business growth.
- Provides visibility, accountability and confidence in the service's effectiveness with detailed reports.
- Capita has even thought about keeping you connected in the event of disaster. Our Disaster Recovery archives incoming and outgoing emails.