modern networks

network security audit

SDI Service Desk Institute GOLD MEMBER

CYBER ESSENTIALS

BIFM CORPORATE MEMBER

modern networks

network security audit

Commercial properties change hands frequently. As a result, a traditional office building's IT infrastructure might be a discordant patchwork of legacy systems that undermine efficiency, security and compliance.

Expanded Attack Surface

Lack of user awareness, weak passwords, excessive network privileges, little or no patch management and inadequate backup already make many commercial properties vulnerable to cybercrime. Now, in the rush to exploit greater automation and smart technologies, property firms might actually be making themselves more vulnerable to cyberattacks. Imagine an office building or shopping centre with literally hundreds of IoT (Internet of Things) connected devices running everything from the lighting and heating to the CCTV systems. The majority of IoT devices are not security hardened, making them extremely vulnerable to cyberattack.

The last thing a building manager or FM wants to do is start adding a load of unsecured IoT sensors to an already creaky IT network. Instead, you need to take a long, hard look at your property's IT infrastructure, network security policies and procedures. Is your IT network fit for purpose?

We Don't Know, What We Don't Know

Many building managers and FMs simply won't know what IT assets are currently deployed across a site. You might have old routers, switches and wireless access points that are no longer supported by the manufacturer and have long since stopped receiving critical security patches and upgrades. You might be running untrustworthy applications capable of spreading malware or monitoring your systems. The situation might be much worse than you currently think, but until you know what is deployed you cannot do anything about it.

modern networks

network security audit

Network Security Audit

Our Network Security Audit generates a ton of useful information about everything connected to your IT network, and the overall condition of your environment.

Our data scans are non-invasive. There's absolutely no disruption to your business, and no-one need know an assessment has taken place until you're ready to share the results. The data we collect is fully encrypted and can only be unlocked by us to ensure your security and privacy.

Straightforward Reports

Once our team of experienced network engineers and consultants have reviewed the data, we will prepare a detailed report of our findings and make recommendations based on industry norms and best practice. We also archive your scans for future reference and comparison. As well as our in-depth technical reports, we prepare a straightforward summary that highlights the greatest risks to your organisation, and a prioritised plan of action to tackle them.

Measured Improvement

A computer network is a dynamic environment and as such is constantly changing. Our Network Security Audit is a snapshot of your network status at the time of our scan. By running subsequent scans we can produce comparison reports that highlight anything that has changed, good or bad, over a given time period.

Any technical issues discovered by our audits can be instantly translated into service desk tickets for existing customers or we can plan remedial work for new clients. We can also offer ongoing reporting and regular business reviews to ensure your network is operating optimally and securely.

modern networks

network security audit

Threat Landscape

Cybersecurity & Data Protection

Our Network Security Audit determines how vulnerable your IT network is to internal and external threats. We examine permissions, user behaviours, password security, anti-virus, patch management, and take a deep dive into internal vulnerabilities.

Adversaries

Malware, phishing, SQL injection, brute force and distributed denial-of-service (DDoS) attacks are just some of the many cyber threats every business faces daily. Cybercrime cost UK businesses £35bn last year. Every day we read of another high profile cyberattack or major data breach. It's estimated that every 40 seconds another organisation becomes the victim of ransomware. However, amidst all the hype and scaremongering lurks an uncomfortable truth. Many organisations simply fail to take the most basic cybersecurity precautions.

Internal Issues

Weak password policies, not removing ex-employees from your Active Directory, failing to patch or replace for known vulnerabilities, using shadow IT applications for business purposes, and opening suspicious emails are some of the most common reasons businesses fall victim to cybercrime. These are crimes of opportunity, like leaving the backdoor of your office building open.

There are too many ways that your network can be compromised to simply leave things to chance.

modern networks

network security audit

Our Network Security Audit will provide you with an in-depth report on your network security risks, policies and permissions. Our audit includes:

HARDWARE	Servers, workstations, printers, and non-AD devices (like switches/routers/printers). Old computers that are still connected to the domain and should be removed.
SOFTWARE	Systems with missing patches/service packs/security updates. Local accounts (per-system) with weak/insecure passwords. Systems with missing anti-virus, anti-spyware, or firewall misconfiguration.
CONFIGURATION	Security policy inconsistencies across network servers/computers. Outbound system access that should be blocked. Lack of content filtering (social media, entertainment, pornography, illegal downloads).
ACCESSIBILITY	Misconfiguration of user access to network shares. Detailed breakdown of AD security group membership.
SECURITY RISKS	Old user accounts that still have access and should be disabled/removed. Internal systems with open ports that pose a potential security risk. External issues that put your network at risk of business disruption or data loss.

Compliance

We can scan your network to identify where sensitive data, such as social security numbers and banking information, is being held for compliance purposes.

Cybersecurity is Good for Business

Any interruptions to a property's IT network can have severe repercussions, from disgruntled tenants and visitors to lost business, compensation claims and bad publicity. Conversely, good cybersecurity does more than protect your IT systems. It demonstrates a commitment to your tenants and partners, which in turn builds loyalty, trust and can generate new business.

According to KPMG, data shows that good cybersecurity has a positive influence on brand loyalty. Customers prefer companies that are open, honest and responsible about cybersecurity and their ongoing investment in it. A recent study by Iron Mountain, a storage and information management company, and PwC found that more than half (58%) of European mid-sized firms would refuse to do business with a company that had suffered a data breach.

modern networks

network security audit

About Us

Modern Networks provides IT and telecoms as a managed service to over 1600 commercial properties across the UK. We provide everything from the desktop to the data centre. All our services are fully managed, continually monitored and expertly supported by our UK Service Desk.

Contact Us

To learn more about our Network Security Audit and how to improve your network security contact us now.

SDI Service Desk Institute GOLD MEMBER

CYBER ESSENTIALS

BIFM CORPORATE MEMBER

Modern Networks 01462 426 500
www.modern-networks.co.uk

modern networks

network security audit

Modern Networks
18 Knowl Piece
Wilbury Way
Hitchin, Herts
SG4 0TY
01462 426 500
www.modern-networks.co.uk
info@modern-networks.co.uk
Company No. 3881576
VAT Reg. GB 750991117

SDI Service Desk Institute GOLD MEMBER

CYBER ESSENTIALS

BIFM CORPORATE MEMBER