wavex

I.T. Managed Services

What does good look like?

Microsoft Gold Partner

Microsoft 1-Tier Cloud Solutions Provider

ISO 27001 CERTIFICATION EUROPE

CYBER ESSENTIALS PLUS

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★

IT EUROPA EXCELLENCE AWARDS FINALIST

European IT & Software Excellence Awards FINALIST MANAGED SERVICE SOLUTION OF THE YEAR

Living Wage Employer

computing Technology Product Awards

SHORTLISTED BEST SMALL ENTERPRISE MSP SDI

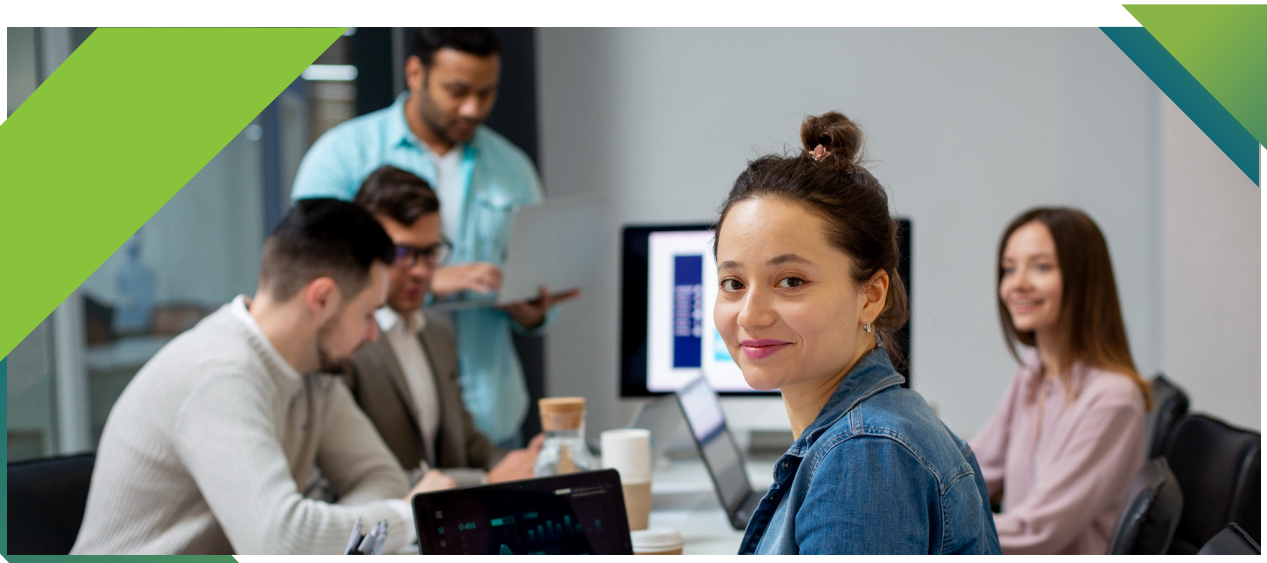
Contents

I.T. Managed Services –
What does good look like?

With many organisations relying on outsourcing their IT needs, and therefore without in-house IT skills, they end up assessing the quality of the IT service based on the volume of complaints they receive or cyber-attacks they experience.

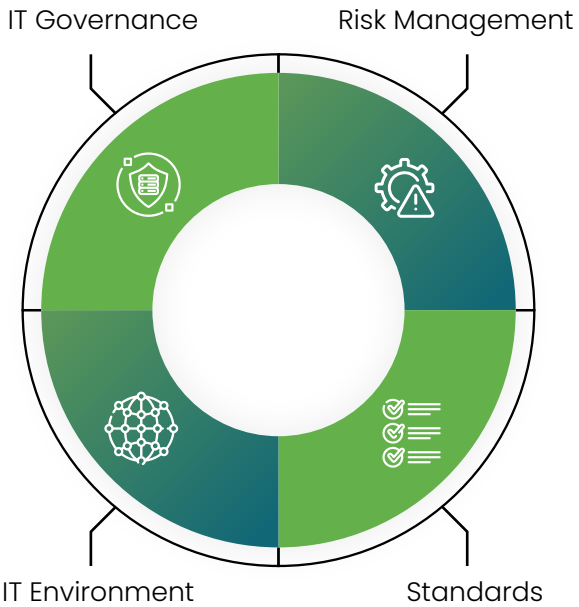
The consequence of this approach is many organisations are operating with significant IT risks, which will eventually impact their operations.

Consider your IT environment like your home: if you leave your windows unlocked, you might not get robbed today or even this year, but the risk is substantial. Evaluating your IT's quality solely based on whether an incident has happened overlooks the ongoing risk and the potential of future problems. Of course, the challenge with IT security, its often not obvious that your organisations “windows are unlocked”.



Therefore, what does good IT look like to a non-technical person?

To answer that question, we need to break IT down into a few critical components. These are, “IT Governance”, “IT Environment”, “Standards” and “Risk Management” and irrespective to the size of your organisation, whether you are a 10 staff business or 1000 staff multi-national, each of these areas still need consideration.



The benefits of good IT are huge and should always exceed the investment necessary to achieve it.

The main advantages are:

Reduced risk of cyber-attack:
Taking a proactive approach substantially reduces an organisations risk profile. And should you have a GDPR breach and are unable to prove you took a proactive approach to IT risk management then you could receive a hefty fine.

Efficient users and improved user experience:
With well setup modern IT systems and the removal of legacy systems, staff will have a positive experience, and their technology will help them to perform their role efficiently with minimal risks.

Improved collaboration:
Improved ability for staff to work together, and with your external 3rd parties.

Reduced risk of operational interruptions:
Modern and well managed systems operate more reliably.

Reduced costs:
Through the increase in staff efficiency and reduction in risks, in the long term, a modern and well managed system will save you money.

Due-diligence:
Many organisations now assess their supply-chains (e.g. Cyber Supply Chain Risk Management), the better your IT, the more likely you will pass through a due-diligence process.

Return-on-investment:
Obtain a greater return on your investment into technology. Without appropriate IT lifecycle management, investment in new systems will be far more costly.

Scalability and flexibility:
Modern systems provide you the ability to adapt quickly to changing demands.

Innovation:
The ability to leverage new technologies like AI and avoid being left behind your competitors.

So, let's look at the main constituent parts of good IT:

IT Governance

IT Governance refers to a structure for organisations to ensure that IT investments support their business objectives. It involves aligning IT strategy with business strategy, managing IT-related risks, and ensuring compliance with regulations (GDPR, Cyber-Essentials, SRA, FCA, ISO27001, ISO9001, company policies etc).

What does good look like?

Accurate IT documentation
Everything is well documented and kept up to date.

RACI matrix clearly defining responsibilities
It is clear the responsibilities of the IT stakeholder, in-house IT resources, and outsourced partner(s).

Standard-operating-procedures (SOPs)
Appropriate procedures have been created to ensure the structured response to requests or security incidents.

Controls and audits
Established controls and regular audits are performed to validate, amongst other things, processes, procedures, and access-rights.

Reports and dashboards
You have comprehensive visibility across your IT estate. This should cover the support, user satisfaction, 3rd parties, asset, licenses, security and risks.

Change control
When the IT environment is changed it goes through a change-control process to ensure the risks are understood, the change is recorded, systems are updated, associated documentation and procedures are reviewed, and a potential roll-back plan is considered should the change fail.

Passwords / Domain administration
Are controlled, and not assigned to any normal users, and access is audited.

License management
Licenses are controlled and managed to ensure compliance.

Defined IT budget aligns to financial objectives
IT budgets are defined, and capital invested to achieve the organisational goals.

What does bad look like?

Documentation
Non-existent or out-of-date procedures, knowledge articles, or network.

Licenses
No clarity around license exposure of Microsoft or 3rd party applications (e.g. Adobe).

Change control
Changes are immediately performed without much consideration causing documentation, processes and management systems to become quickly outdated.

Audits
Rarely performed (for instance, when did your IT provider last review user-accounts to ensure no old accounts remain active?).

Administration
Users have local administrative accounts and can make changes to their machines (which places the organisation at a high risk of serious damage should a cyber-attack occur).

Having domain administration rights assigned to a user can invalidate any cyber-security insurance claims.

Three simple questions to test your IT governance.

Ask for your security incident response process?

Should a cyber-attack occur, a clearly defined process must exist to ensure a coordinated response to limit the damage.

Ask for a few of your standard operating procedures?

If they don't exist or are out-of-date (or you wait days/weeks for a response) then these are not deemed important. Without processes different engineers will approach requests differently (some good, some bad), this approach will significantly increase your risks, likelihood of a security-breach, and create a poor end-user experience.

Ask what audits and controls are in place?

If you haven't seen any audit results, these are unlikely to be occurring. For instance, do you have any staff who have left the firm but their account is still active? Its possible people forgot to inform their IT provider, however without regular audits these mistakes will never be detected and so the risk posture of the organisation slowly diminishes.

IT Environment

The “IT environment” refers to all your technology, both physical and virtual. Within your overall IT environment, you’ll most likely have a mix of different types of technology; IT processes, instances, systems, components, and software. It is crucial to maintain full visibility and control over your IT environments to ensure operational efficiency, and to minimise complexity and risks.

Security is only as strong as your weakest link; it only takes one end-of-life of vulnerable software to give a hacker access to your data.

What does good look like?

Vendor recommendations
Your organisation aligns to vendor recommendations (e.g. Microsoft). Going against vendor recommendations complicates the IT environment and increases your costs substantially.

IT Strategy responsibilities
The IT strategy includes a plan to continuously improve and evolve your IT environment.

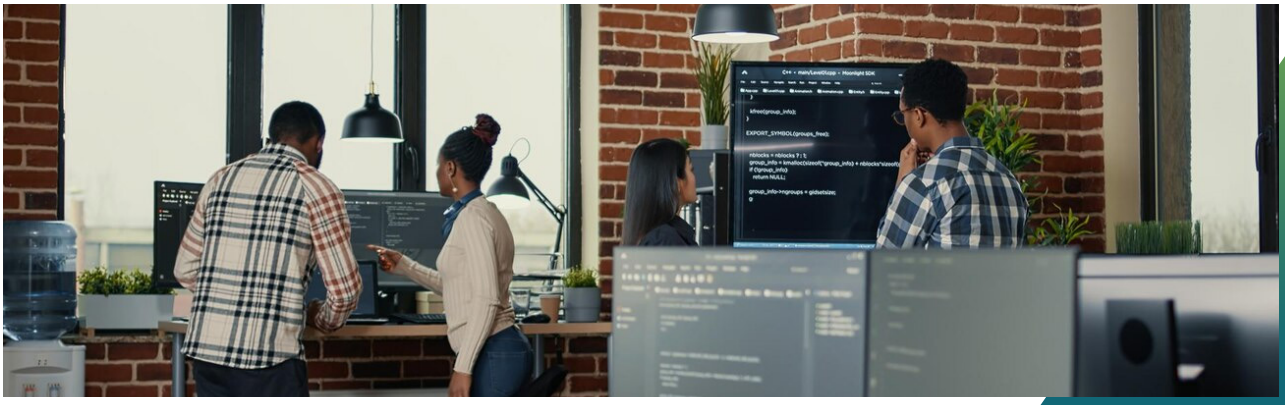
Legacy infrastructure
You do not have any legacy infrastructure (for instance, on premise servers unless there is a strong business justification for instance, you handle very large files).

Warranties
All equipment is within warranty, especially critical infrastructure so it can be rapidly replaced should it fail (Note: many organisations are unaware that should a firewall fail, there can be long lead-times to receive a new replacement)

What does bad look like?

Out of warranty devices and critical infrastructure
Where a failure could create a significant and long-running outage, or users' machines are old and slow (often experiencing a range of IT issues stemming from resource constraints).

End-of-life (EOL) software
Old versions of software running which likely have multiple serious vulnerabilities (e.g. old versions of Adobe Acrobat allow hackers to remotely access a device). When software goes end-of-life (EOL) the vendor stops releasing security patches which provide hackers unlimited time to find ways of exploiting the software. This is far more common that many organisations think.



Three questions to test your IT environment maturity.

Do you have a list of warranties?

Without a central repository you won't know what is now out of warranty.

Do you know what end-of-life software is installed on your devices?

Without visibility of this, you do not know your risks, which normally means they will be significant.

Do you have a 12-24 month costed IT strategy?

This should cover the necessary activities to continually modernise your environment. Without a plan, you can not control your IT budget, this will increase your IT spending, and likely direct investment in the wrong areas.

IT Standards

IT Standards are rules or guidelines that ensure the compatibility, security, and efficiency of IT systems and processes. They provide a framework for managing IT services and infrastructure, ensuring that the IT meets industry best practices and complies with regulatory requirements.

What does good look like?

Device standards
A group of devices are chosen for different types of staff. This may be a high-powered model for a designer, or a medium-spec device for an office user.

Operating system standards
All employees are running the same vendor recommended operating system (e.g. all running Windows 11. Keeping aligned with vendors is critical as the vendor will reject any support escalation until the machine in question meets their minimum recommended standard).

Software standards
An agreed group of software is associated with different types of staff.

Minimal builds
Unnecessary software is removed from devices (remember, you don't need to run the software to be at risk if it is end-of-life).

Microsoft management system recommendations
Microsoft recommended tools like InTune or Autopilot that are used to manage IT risk, and the management of software to help to keep the IT aligned to the organisations standards.

What does bad look like?

Purchase any device
Choosing different models, often with different operating systems (some Windows 10, some 11, some pro, some home edition), with each of these devices coming with completely different pre-installed software means some perform well, others poorly. And as subsequent updates or new software is deployed, it is common that a subset of these devices often experience unexpected issues.

Software
Everyone runs different applications with only a subset managed by the IT provider (often only the Microsoft applications). Because much of the software is "unmanaged" some has gone end-of-life, significantly raising the risk of a cyber-attack.

Risk Management

A critical area often ignored by organisations is IT Risk Management. This is the process of identifying, assessing, and mitigating IT risks. It involves proactively evaluating potential threats and implementing controls to minimise these risks. Effective IT risk management practices significantly improve an organisation's risk posture, and limit exposure to costly IT security incidents.

Every type of cyber-attack or IT issue originates from a risk. For instance, using a simple password is a risk, and the consequence of this is your account is far more likely to get compromised. There are thousands of potential IT risks which left unmanaged collectively determine an organisations risk-profile or in other words, how likely they will experience a serious attack. Those organisations without standards or poor IT governance will have a poor risk posture and consequently, it's only a matter of time before they experience a serious cyber-attack.

It's far better (and cheaper) to take a proactive approach to cyber-security. If your risks are managed, you significantly reduce the types of attack you are vulnerable to. So much so, that many insurers now stipulate IT risk-management must be used.

SharePoint backup has significant limitations, so additional software is required to enable most businesses to remain compliant and restore older file versions.

What does good look like?

Software supported
Everything is well documented and kept up to date. all software is up-to-date and supported by the vendor (who actively releases security updates)

Adhere to a recognised risk framework
IT is assessed against a recognised IT risk framework which provides visibility into areas of risk across the organisation.

Boards
The Board review their IT risks as part of their fiduciary duty to ensure the organisation's assets and data are protected from potential cyber threats.

Patching schedules
All software, infrastructure, and endpoints, get regularly patched including Microsoft and 3rd party applications (3rd party applications are often missed).

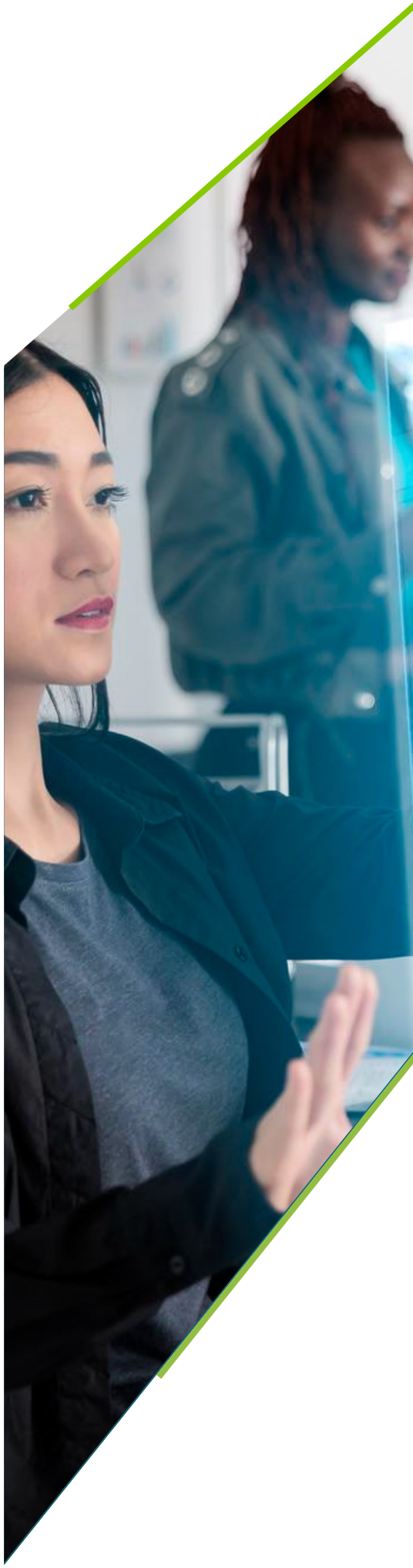
Vulnerability management
IT is constantly assessed for security vulnerabilities.

Security incident
There is a tried and well-tested security incident response process designed to respond quickly to a range of likely threats.

Administrative credentials
Are appropriately stored with named users and access logs.

Penetration test
Often called a "pentest," is a simulated cyberattack conducted by security professionals to identify and exploit vulnerabilities. The goal is to uncover weaknesses that could be exploited by malicious actors, allowing organisations to check and strengthen their defences before an actual attack occurs.

Disaster recovery (DR)
Systems are checked against a range of scenarios to ensure the organisation can continue to operate should these scenarios occur. This may be a "technical" DR, or a "full" DR test that also involves staff.



Backup

All systems including Cloud, are backed-up, to enable the restoration of data should an attack occur (just because it's in the Cloud does not mean the backup will meet your requirements).

User training

Users participate in a range of cyber-awareness training to ensure they remain vigilant

What does bad look like?

Many unmanaged/unpatched devices and software.

IT risks rarely or never discussed at board meetings.

Rarely or never perform a disaster recovery test.

Rarely or never perform a penetration test.

Rarely or never perform a backup recovery test.

No visibility of vulnerabilities.

No controls around administrative access.

Risk management takes time (and money) so if you are not aware whether it is occurring, it most probably isn't.

Three questions to test your IT risk maturity.

What are my vulnerabilities?

What staff are likely to click on a phishing email?

What is the process followed should a security incident occur?

The positive impact of IT modernisation

The main reason organisations underinvest in their IT is, unsurprisingly, because it costs money, or they question the objectivity of their IT providers advice to invest. However, appropriate investment saves an organisation far more money than the investment itself.

Everyone accepts that owning a car, and never performing any maintenance, will likely end with the car failing at the most inconvenient time, and costing a lot of money to repair. And the driver will be unaware of the dangers. IT systems are no different.
Here is an example of a 150-user organisation, who had underinvested over many years, and as a result had experienced a number of cyber-related incidents, and frustrated staff due to continuous IT issues.

Client has 150 users

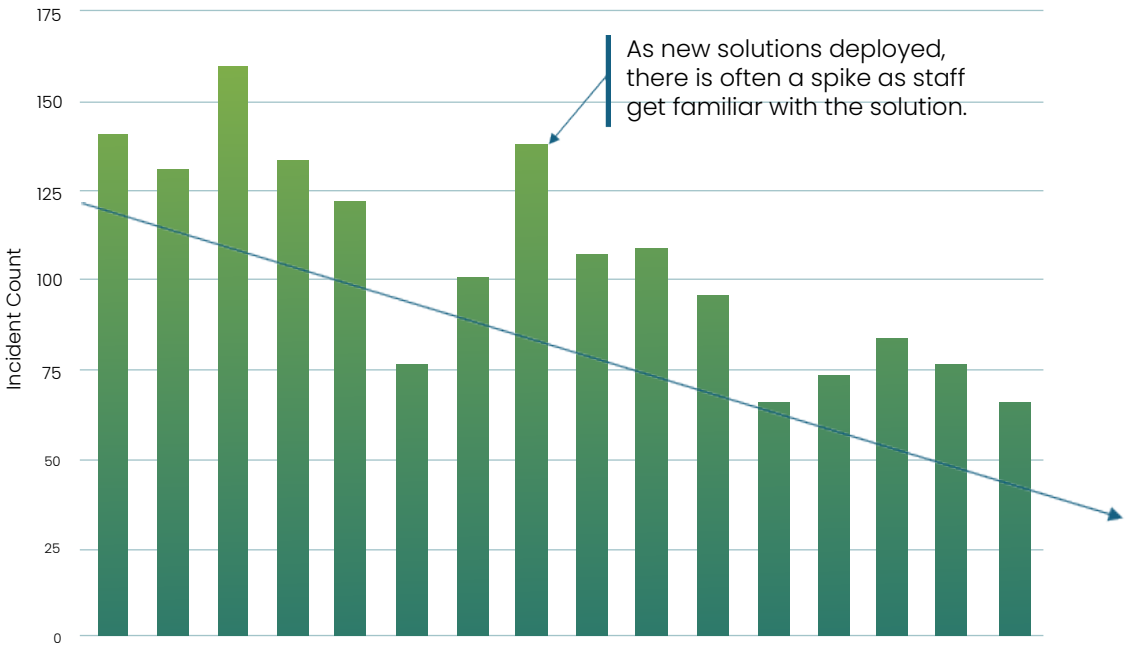
Projects performed (over 15 months):

- Removed legacy infrastructure.
- Deploy Microsoft recommended applications.
- Deploy suitable security and risk management platforms.
- Proactive monitoring, providing early detection and trend analysis.
- Modernise equipment, upgraded devices, ensure warranty cover.
- Fully documented environment to ensure support staff could quickly address staff requests.
- Change control to ensure systems, and documentation remains up to date.

The result was significantly more productive staff (and happier due to less issues), improved risk posture, and a reduce incident volume.

IT modernisation by the numbers:

The chart shows how the issues slowly reduced as the environment and processes were modernised and brought in line with standards and vendor recommendations.



Obviously, depending on the extent and duration of the underinvestment, it can take time to stabilise the environment (things won't get better immediately). In the above example it took 15 months.

Through an unexpected cyber-attack or the need to deploy new software, you will likely be forced to make the investment eventually. However, the sooner your IT is modernised, the sooner you and your colleagues will reap the benefits and reduce the risk of a cyber-attack.

Next steps

It is simple to ensure you are receiving a quality IT service which is proactively addressing your IT risks.

Questions

Ask the questions outlined in this document to better understand the scope and quality of the current IT services. Ask yourself whether the answers give you confidence in the service you have? You don't need to understand all the technical answers, you just need to know that your IT provider has an answer.

Seek competitive proposals

Remember you will likely get what you ask for – use the above areas to ensure you ask for a quality and proactive IT service, stating what you need from "IT Governance", "IT Environment", "Standards" and "Risk Management" will give you an accurate idea of what it will cost for a quality and future-proof IT service.

Good luck!

Are you ready for
Forward Thinking IT

wavex

www.wavex.co.uk

0845 644 8060

tellmemore@wavex.co.uk