Special Directors Report

The CEO/CFO Guide To Co-Managed IT

A NEW Approach To Securing The IT Support You Need WITHOUT The Cost And Difficulty Of Hiring A Large In-House IT Department

Provided By: H2o Networks
Author: Adam James Abrahami

T: 020 3475 6551
www.itforcarehomes.co.uk

H2O networks

The Dilemma

Every day, CEOs/CFOs and their executive teams are faced with tough investment decisions about where to allocate their financial resources.

Some of those decisions are easier to make than others because they can be based on logical financial analysis with safe ROI expectations. Investing in marketing, a new product line, an acquisition and strategic hires all build equity and future profits. These investments are relatively safe and dependable.

However, CEOs must also deal with a new category of investments that refuse to behave typically and often don't easily secure a direct ROI. These investments involve IT, and they are growing in number, breadth and scope.

I.T. investments are more difficult to estimate, and the ROI or benefit might not be obvious or easily measured. In fact, you hope some NEVER produce a tangible ROI, like investing in cyber security and disaster recovery protections. However, no company can afford to lag behind in I.T. There's not a single department or function of your organisation that isn't significantly controlled by, enhanced by, facilitated by and outright dependent on I.T. And if your organisation is NOT properly invested in cyber-protection and backup technologies, one cyber-attack or data-breach event could have serious, long-lasting, costly ramifications – or even put you out of business.

But no one has unlimited funds. **So, what do you do about all of this?**

One option is to ignore it. Keep the status quo, make do with the I.T. staff and technology investments you have today (regardless of how old and antiquated they are) and "hope" everything is going to be okay. Trust that your current I.T. department has it "covered." But you have to know this is a perilous tightrope. People in New Orleans trusted the dams and defences to hold – and they did – *until* they were hit with a Category 5 hurricane, not to mention the breach the NHS went through back in 2017.

Your Category 5 might be a ransomware attack or a rogue employee. It might be a failed server that went down, taking all its data with it, never to be revived again. It might be a corrupt SQL database that is beyond their expertise to fix. It could simply be a care worker that clicks on a link unknowingly that creates a data breach and ransomware for your entire system.

Maybe your I.T. department truly does have it "all covered." *Maybe*.

But if you are like most of the CEOs we work with to deliver co-managed IT, your I.T. person or department is significantly understaffed, overwhelmed and simply not able to keep up with the growing demands your company is putting on them. They also may be lacking in specialised knowledge about any number of things – data backup and disaster recovery, cyber security protections, automating your system through cloud, Implementing NHS Security Toolkit and more.

No one I.T. person can do it all or know it all.

The fact is, your IT department might NOT be as prepared and capable as you may think to handle the rising complexity of IT systems for your growing company AND the overwhelming sophistication of cyber threats with the current resources, time and skill sets they have.

If true, **your organisation IS AT RISK for a significant IT failure**.

To be crystal clear, I'm NOT suggesting your IT lead and staff aren't smart, dedicated, capable, hardworking people.

The fact is, NOBODY likes to go to the CEO with "bad news" or to constantly ask for more money or help, particularly if they've already been told "there's no budget." It may be uncomfortable or even embarrassing for them to admit they don't have it all covered or that they're lagging behind, not getting things done as well as they could *because* they're just busy with fighting fire after fire.

Further, it takes a small army to run an IT department for a company of your size and growth – and you may be unfairly expecting too much of them, setting them up for failure.

Signs That You May Be Pushing Your I.T. Lead And/Or Department To The Limit

For the reasons stated above, conscientious IT leaders and staff often WON'T tell you they need more money, more staff, more help. They are trying to be good stewards of your company and budget – so it's up to YOU as the leader of your organisation to ensure you are not setting them up for failure or burnout.

Here are 4 early warning signs you may be pushing your I.T. department too hard:

1. **They're routinely working nights and weekends.** Everyone pulls an extended shift once in a while when a deadline is looming or due to a seasonal surge. But if your I.T. leader and department are ROUTINELY working nights and weekends to catch up, that's a sign they are understaffed, which can lead to an unhealthy workplace environment, exhaustion and burnout. It can also lead to important details being skipped and mistakes being made.

   You might not even realise this is happening, so ask them. How often are you working overtime to get things done? How caught up are you on major projects? It's not uncommon for I.T. staff to be stressed to the max without the CEO/CFO even knowing about it. *This will end up hurting your organisation*.

2. **Projects aren't getting done on time or correctly.** Most CEOs aren't technically savvy, so it's difficult to know for certain if a project is taking longer than it should, costing more than it should. All too often, a manager will jump to the conclusion that the employee is incompetent or lazy – but that may not be the case at all. It could be they're so overwhelmed with tasks and putting out fires that they can't GET the time to do the project

properly.

3. **Heightened emotional display, aggression or resentment.** Some employees will "suck it up" and push through, not wanting to talk to you about desperately needing more help. Or maybe they HAVE brought it up, only to be shut down and told "there's no money." When this happens, it's easy for an employee to become resentful. You might think that emotion and work don't mix, but your employees are only human, and will only tolerate so much.

4. **They aren't rolling out preventative security measures.** Has your I.T. leader rolled out any type of end-user security awareness training? Do they enforce the use of strong passwords and compel employees to change their passwords routinely? Have they put together an Acceptable Use document or training to make sure employees know what is and isn't allowed with company e-mail, Internet, confidential data, etc.? Have they given you updated documentation on the network and an up-to-date disaster recovery plan? Have they updated the documents on how your organisation complies with the NHS Toolkit now and the new requirements coming in 2021? Have they come to you requesting certain changes so that your organisation is fully compliant?

   All of these are essential preventative maintenance that often gets neglected or ignored when an I.T. person or department is overwhelmed – but these are critical for insurance purposes and reducing the chances of a cyber-attack or other disaster that would carry significant financial losses through a fine by the ICO (Information Commission Office) and/or hurt your company's reputation.

This May Be One Of The Biggest Dangers You Face

Without a doubt, the one area that you are most at risk with an overwhelmed and understaffed IT department is cyber security. One incident can lead to data loss, extended downtime and (potential) liability with a cyber security or data breach.

As I stated above, the FIRST thing that gets put on hold is preventative maintenance. If your employees are running into your I.T. team's office every 5 minutes needing a password reset or needing help getting e-mail, it's hard to tell that employee "no" because they're working on server maintenance or updating critical documentation.

It's the classic "important not urgent" work that gets neglected.

To make matters worse, the complexity of knowing how to protect your organisation against cybercrime and how to be compliant with new NHS standards and security toolkit as well as GDPR laws is growing exponentially. These matters require SPECIALISED knowledge and expertise. They require constant monitoring and attention. CORRECT solutions. Regardless of your organisation's size or industry, these are areas you cannot ignore or be cheap about.

In situations where companies were fined or brought to task for a data breach, it was their WILLFUL NEGLIGENCE that landed them in hot water. They knowingly refused or failed to invest in the proper I.T. protections, support, protocols and expertise necessary to prevent the attack.

You'd be foolish to underestimate the cost and crippling devastation of a complete, all-encompassing systems failure or ransomware attack. You don't want to dismiss this as "It won't happen to us." And you certainly don't want to underestimate the level of expertise you need.

One innocent mistake made by an employee. One overlooked patch or update. One missed backup can produce EXTENDED downtime, data loss, business interruptions.

Yes, your I.T. department is probably doing everything they can to protect you – **but it's up to YOU to be certain**. Everyone in your company – including your clients – is depending on you.

Exactly How Can Your Company Be Damaged By Failing To Invest Properly In Cybercrime Prevention And Expertise?

Let Us Count The Ways:

1. **Reputational Damages:**
   When a breach happens, do you think your clients and residents will rally around you if their data is lost or with criminals? Have sympathy? This kind of news travels fast on social media. They will demand answers: HAVE YOU BEEN RESPONSIBLE in putting in place the protections outlined in this report or will you have to tell your clients, "Sorry, we got hacked because we didn't think it would happen to us," or "We didn't want to spend the money." Is *that* going to be enough to appease those damaged by the breach?

2. **Reporting To The Information Commissioners Office with up to £17.5M in fines:**
   Breach notification to the ICO are one of the most active areas right now. The ICO are part of the wider GDPR compliance laws that enable the ICO to give fines. It is well known that companies such as Bupa, Car Phone Warehouse, British Airways Talk Talk as well as Brighton and Sussex NHS have all been fined by the ICO.

   Don't think for a minute this only applies to big organisations: ANY small business that collects customer information also has important obligations to its customers to tell them if they experience a breach. In fact, the care industry has to be compliant with not only GDPR but the NHS Security Toolkit to be able to communicate with NHS Hospitals, Doctors, Consultants and other stakeholders in a secure way. The vast majority of care organisations have under-estimated what it takes to be compliant and protected.

3. **Cost, After Cost, After Cost:** ONE breach, one ransomware attack, one rogue employee can create HOURS of extra work for staff who are already maxed out when things are going well. Then there's business interruption and downtime, backlogged work for your current clients. Loss of new enquiries. Forensics costs to determine what kind of hack attack occurred, what part of the network is/was affected and what data was compromised. Emergency IT restoration costs for getting you back up, *if* that's even possible. In some cases, you'll be forced to pay the ransom and maybe – *just maybe* – they'll give you your data back. Then there are legal fees and the cost of legal counsel to help you respond to your clients and the media. Cash flow will be significantly disrupted, budgets blown up and the fines that would kick in for the breach on top of everything.

4. **Bank Fraud:** If your bank account is accessed and funds are stolen, the bank is NOT responsible for replacing those funds. Take the true story of Verne Harnish, CEO of Gazelles, Inc., a very successful and well-known consulting firm, and author of the best-selling book *The Rockefeller Habits*.

   Harnish had $400,000 taken from his bank account when hackers were able to access his PC and intercept e-mails between him and his assistant. The hackers, who are believed to be based in China, sent an e-mail to his assistant asking her to wire funds to 3 different locations. It didn't seem strange to the assistant because Harnish was then involved with funding several real estate and investment ventures. The assistant responded in the affirmative, and the hackers, posing as Harnish, assured her that it was to be done. The hackers also deleted his daily bank alerts, which he didn't notice because he was busy running the company, traveling and meeting with clients. That money was never recovered, and the bank is not responsible.

   Everyone wants to believe, "Not MY assistant, not MY employees, not MY company" – but do you honestly believe that your staff is incapable of making a single mistake? A poor judgment? **Nobody believes they will be in a car crash when they leave the house every day, but you still put the seat belt on.** You don't expect a life-threatening crash, but that's not a reason to not put your seat belt on. *What if?*

5. **Using YOU As The Means To Infect Your Clients:**
   Some hackers don't lock your data for ransom or steal money. Often they use your server, website or profile to spread viruses and/or compromise other PCs. If they hack your website, they can use it to relay spam, run malware, build SEO pages or promote their religious or political ideals. Are you okay with that happening?

   Do you think your I.T. team would never let that happen? If hackers can break into companies like Bupa, Uber, Facebook and Capital One, they can certainly get into YOURS. The question is: Will your I.T. team be brilliantly prepared to minimize the damages or completely taken off guard?

Co-Managed IT: How Growth Companies Are Solving Their I.T. Resource Dilemma

Because GROWTH companies face the dilemma of needing professional grade I.T. support but can't reasonably afford to invest in all of the tools, software and staff that requires is exactly why we created a NEW solution we call co-managed IT.

In short, co-managed IT is a way for CEOs of growing companies to get the helping hands, specialised expertise and IT management and automation tools they need WITHOUT the cost and difficulty of finding, managing and retaining a large IT staff OR investing in expensive software tools.

This is NOT about taking over your IT leader's job or replacing your IT department.

It's also **NOT** a one-off project-based relationship where an IT company would limit their support to an "event" and then leave your team behind to try and support it (or give you the option to pay them big bucks afterwards to keep it working).

It's also **NOT** just monitoring your network for alarms and problems, which still leaves your I.T. department to scramble and fix them.

It IS a flexible partnership where we customise a set of on-going services and software tools specific to the needs of your I.T. person or department that fills in the gaps, supports their specific needs and gives you far superior IT support and services at a much lower cost.

Here are just a few of the reasons why CEOs of similar size care groups are moving to a co-managed approach:

- **We don't replace your IT staff; we make them BETTER.** By filling in the gaps and assisting them, giving them best-in-class tools and training and freeing them to be more proactive and strategic, we make them FAR more productive for you. As an added bonus, THEY won't get burned out, frustrated and leave.

- **You don't have to add to your head count.** Let's face it: overhead walks on two legs. Plus, finding, hiring and retaining TOP talent is brutally difficult. With co-managed IT, you don't have the cost, overhead or risk of a big IT team and department. We don't take vacations or sick leave. You won't lose us to maternity leave or an illness, or because we have to relocate with our spouse or we've found a better job.

- **Your IT team gets instant access to the *same* powerful IT automation and management tools we use to make them more efficient.** These tools will enable them to prioritize and resolve your employees' problems faster, improve communication and make your IT department FAR more effective and efficient. These are software tools your company could not reasonably afford on its own, but they are *included* with our co-managed IT program.

- **"9-9-9" on-site.** In the unexpected event your head of IT or IT team had been unable to perform their job OR if a disaster were to strike, we could instantly provide support to prevent the wheels from falling off.

- **You get a TEAM of smart, experienced IT pros.** No one IT person can know it all. Because you're a co-managed IT client, your head of IT will have access to a deep bench of expertise to figure out the best solution to a problem, to get advice on a situation or error they've never encountered before and to help decide what technologies are most appropriate for you (without your having to do the work of investigating them ALL).

- **You'll stop worrying (or worry less!) about falling victim to a major cyber-attack, outage or data-breach event.** We can assist your head of IT implement next-gen cyber security regulations from the NHS Security Toolkit to prevent or significantly mitigate the damages of a ransomware attack or security breach. We can also assist in providing end-user awareness training and help you initiate controls to prevent staff from doing things that would compromise the security that lead to a GDPR breach which compromises to your data and a large fine from the Information Commission.

- **We provide your head of IT and team free workshops and training.** We offer quarterly workshops and webinars for our co-managed IT clients so they're more informed on critical topics such as cyber security, disaster recovery, compliance regulations, best practices and more.

- **NO LONG-TERM CONTRACTS.** We're a flexible workforce you can expand and contract as needed.

Scenarios Where Co-Managed IT Just Makes Sense

Scenario 1: Your in-house I.T. staff is more better utilised working on high-level strategic projects and initiatives but needs support in getting day-to-day tasks completed, such as troubleshooting various problems that arise, providing help-desk resources to your employees, software upgrades, data backup and maintenance, etc.

Scenario 2: Your in-house I.T. person is excellent at help-desk and end-user support, but doesn't have the expertise in advanced cyber security protection, server maintenance, cloud technologies, compliance regulations, etc. As in scenario 1, they can do what they do best and fill in the areas where they need assistance.

Scenario 3: A company is in rapid expansion and needs to scale up I.T. staff and resources quickly. This is another situation where our flexible support services can be brought in to get you through this phase as you work to build your internal I.T. department.

Scenario 4: You have an excellent I.T. team, but they could be far more efficient if they had the professional-grade software tools we use to be more organised and efficient, along with our help

desk. We can give them the tools, configure them for your organisation and train them on how to use them. These tools will show you, the CEO, the workload they are processing and how efficient they are (we call it utilisation).

Scenario 5: You have a robust in-house I.T. department but need on-site support and help for a remote location or branch office.

Who This Is NOT For:

Although there are a LOT of benefits to co-managed IT, this is certainly not a good fit for everyone. Here's a short list of people this won't work for.

- **Companies where the IT lead insists on viewing us as an adversary instead of an ally.** As I stated previously, our goal is not to have you replace your I.T. lead or your entire I.T. staff, but some I.T. managers just cannot get beyond this fear.

  As I've said, we NEED an IT-savvy leader in the company to collaborate with who knows how the company operates (workflow), understands critical applications and how they are used, company goals and priorities, etc. We cannot do that job. Co-managed IT only works when there is mutual trust and respect on both sides.

- **IT leaders who don't have an open mind to a new way of doing things.**
  Our first and foremost goal is to support YOU and your I.T. leader's preferences, and we certainly will be flexible – we HAVE to in order to make this work.

  However, a big value we bring to the table is our 18 years of expertise in supporting and securing computer networks. Therefore, the clients we get the best results for are ones that keep an open mind to looking at implementing our tools, methodologies and systems, and adopting some of our best practices. As I said before, this only works if it's a collaborative relationship. But we cannot – will not – take on a client that is doing things we feel compromise the integrity and security of a network, even if that's "how we've always done things" or because "that's what we like."

- **Organisations where the leadership is unwilling to invest in IT.**
  As a Director myself, I completely understand the need to watch costs. However, starving an IT department of much-needed resources and support is foolish and risky. Further, some CEOs look at what they are paying us and think, "We could hire a full-time person for that money!" But they forget they are getting more than a single person – they are getting an entire team, a backup plan, tools and software, monitoring and specialised skills.

  We can only help those companies that are willing to invest sufficiently in IT – not elaborately or indulgently. In fact, we can demonstrate how a co-managed IT option is a far cheaper solution than building the same team on your own.

A Cost Analysis: How Co-Managed IT Saves Your Organisation Money

Below is a summary of what you get as a co-managed IT client, and what it would cost you to build it on your own.

Co-managed Description	Service Response / Description	Cost without Co Managed Per annum
Full Ticket Helpdesk	-within 5 - 15 minutes	Included
Remote Support	-within immediate to 30 minutes	Included
On Site Emergency Support	-within 60 minutes same day	Included
Virtual CIO	- ongoing	Included (£10k pa)
Team Experienced Engineers	- ongoing 24/7	Included (£30 – 50k each)
Care Group IT Solutions	-proven solutions that work	Included (£10k pa)
Cyber Security Specialist	-security operation centre 24/7	Included (£80k pa)
Next Gen End Point Security	-included anti-virus	Included (£12 per pc pa)
Office 365 Secure Backup	-ongoing subscription included	Included (£15 per email pa)
Security Windows Patching	-patching agent and reporting	Included (£2k pa)
NHS Compliance Dashboard	-setup and support	Included (£30k pa)
GDPR Compliance Dashboard	-setup support and subscription	Included (£8k pa)
Documentation	-access when out the office	Included (£2k pa)
Workshops – Internal IT	-every quarter	Included (£3k pa)
24/7 IT Support	-within 15 minutes day or night	Included (£8k per annum)
Average Total	30 to 100 Care Homes	**£213K per annum**

What To Look For In A Co-Managed IT Partner

As I mentioned before, other IT firms in this area will offer project-based support or monitoring only, or they want to take over IT for your entire company, by replacing your IT lead and/or team.

Here's why all of these options are not smart and won't deliver the value for your money.

For starters, if you have a productive, reliable I.T. leader or department, you want to keep those people on staff, but make them more productive. No I.T. provider can fully replicate the value that a full-time IT lead on directly employed by your company can deliver. They will try to sell you on that idea, but candidly, they won't be able to allocate the time and attention that a full-time employee can.

Second, monitoring-only agreements are like smoke detectors. They tell you when a fire is about to happen (or is happening) but they don't do anything to put out the flames, get you out safe or PREVENT the fire from happening in the first place. They are a waste of money UNLESS you have a big IT team that just needs that tool – and if that's the case, you'd be better off buying that software direct, not through a reseller who will mark it up.

We had been called in to help with a Ransomware attack to a well-known care group. The IT company had informed the Internal I.T. team about some suspicious activities, but the I.T. team did not investigate. It was left and by the next morning the entire system was infected with Ransomware and the files could not be opened. In fact most of the system was down including care records and financial information at head office.

Finally, project-based work is often necessary, but you are going to get better results if those projects are not a "one-and-done" where they drop the solution in and take off, leaving your I.T. team to figure it out.

A better approach is a co-managed IT environment when a solution is implemented by the same team that is supporting it.

Why We're Uniquely Positioned To Deliver Co-Managed IT

There are several reasons our company is uniquely positioned to be your co-managed IT partner, starting with the simple fact we're the ONLY IT company that specialises in working with care groups.

We are a partner you can TRUST. We're the team that will stay up into the wee hours of the night fixing a problem. We're the team you can call when an unexpected problem or crisis arises. And because we already know your environment, we can step in at any time FAST.

We are also the only company that run IT training for the National Care Association, work with Digital Social Care and protect care groups by implementing the NHS Security Toolkit. Our specialty is reducing costs, ensuring care groups are security compliant and improve care homes CQC rating through technology. We have spent 18 Years advising care groups and our clients include The Bondcare Group, Care World Wide and Draycott Nursing and Care.

I have invested thousands of pounds and over 18 years into developing the most efficient, robust and responsive IT support system so you don't have to. The co-managed IT support we provide will dramatically improve your effectiveness of your IT team while saving you money.

What Do Other CEOs of Care Groups Say?

"...Thanks to their co-managed IT approach, we were able to reduce our IT overhead by 38% while keeping the same level of very high service and support services – a process that took only a week...Our systems are compliant, much improved and just work faster. Adam and his team are always available to get things done and genuinely interested in how they can support us further". ***Jacob Sorotzkin, Director, The Bondcare Group***

H2o Went Above And Beyond While Saving Us £18,000 A Year

H2o was far the provider of choice. Since hiring them, we've been very happy with the high quality of service we receive on a daily basis. They have been professional, friendly and quick to respond to any queries or issues. They always try to explain things in layman terms and support the IT team and non IT queries. I would not hesitate in recommending H2o to anyone considering using your services. - ***Rene Ritter, Head of Operations, Draycott Nursing and Care***

They've Gone Above And Beyond Whilst Reducing Costs By £21,000

We decided on a co-managed IT arrangement from H2o Networks, which saved us an incredible 33% annually on IT costs. Best of all the process has made our Internal IT team faster and far superior than before. I am confident with our IT as we recently had one of the security team respond to an IT failure 15 minutes after it happened...in the middle of the night!... - ***Mark Mozes, Financial Controller, The Care World Wide Group***

Think Co-Managed IT Is Right For You?
Our Free Diagnostic Consultation Will Give You The Answer

If this letter struck a chord and you want to explore how (if?) a co-managed IT relationship would benefit your organisation, we've reserved initial telephone appointment times with our most senior leadership team to evaluate your specific situation and recommend the co-managed IT approach that would work best based on your specific needs, budget and goals.

We work with your I.T. lead to determine areas that are lacking to unearth potential problems such as 1) inadequate or outdated cyber security protocols and protections, 2) insufficient backups, 3) unknown compliance gaps, 4) workloads that can be automated and streamlined for cost savings and more efficiency, and 5) insufficient (or no) documentation of I.T. systems and assets.

These are just a few of the most frequently discovered problems we find that virtually everyone denies could exist in their organisation.

We can also answer questions you might have such as:

- **Is my I.T. person or team 100% utilised, efficient and as productive as they should be?** We have professional tools that will give you visibility into their activities and allow you to track time against work, as well as how efficiently they are performing their job, what activities they are spending the most time on and whether or not they are maxed out, based on tangible data.

- Do you have sufficient redundancy and documented systems and processes in your I.T. department to avoid a single point of failure?

- Are you overspending and not getting your money's worth in any aspect of I.T.?

- Are you TRULY prepared and protected against a ransomware attack or other cyber security breach? Could you recover quickly? Are you meeting compliance regulations?

The above is NOT designed to make your I.T. team look bad; as we all know, fresh eyes see new things. They also are very unlikely to have the software tools we can provide that would give them insights and help them be FAR more effective for you. All of this will be discussed during this consultation.

To request this consultation:

1. Go online to: www.itforcarehomes.co.uk/consultation.

2. Call us direct on 020 3475 6551

3. E-mail your appointment request to linda@h2o-networks.co.uk

One Important Request

We STRONGLY encourage you bring your I.T. lead into this Diagnostic Consultation so they can discuss where they feel they need the most help, and where your I.T. department is underutilised.

Even if you prefer we work with your I.T. leader directly, I also urge you to be involved. I realise that I.T. is not something you might fully understand, and that you are up to your neck in critical projects and deadlines – but decisions about allocating resources and budget DO require your approval and attention.

Therefore, please note that we are happy to conduct a diagnostic evaluation working mostly with your I.T. lead but would request you be involved, at some level, in looking at what we discover and propose.

We look forward to working with you and your team.

Sincerely,

Adam James Abrahami
Director
H2o Networks

PS – If you would like to speak with any of our CEO care group clients who have our co-managed I.T. services, please e-mail me adam@h2o-networks.co.uk or call 020 3475 6551 and I will arrange for you to speak to them directly.