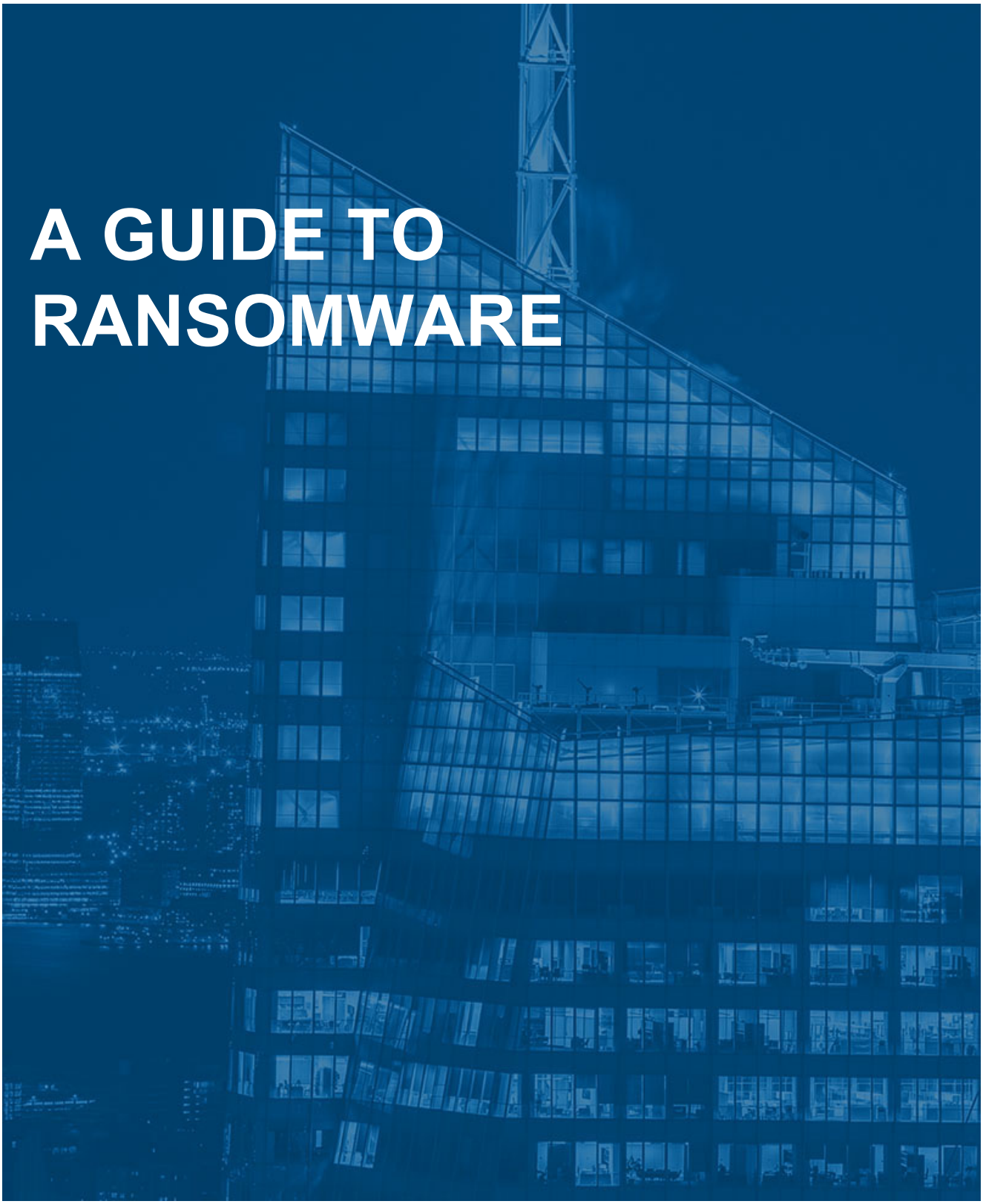
astro

# A GUIDE TO RANSOMWARE



www.astro.co.uk

# Table of Contents

# Introduction

Many of us have felt that horrible sinking feeling after clicking on a link in an email only to realise it isn't what it claims to be. You want to kick yourself because even though it was from someone you know and trust, maybe even someone in authority, there was something about the email that didn't feel right. Then comes the awful wait in anticipation. Those seconds that feel like hours while you continue to punish yourself as you now know you wouldn't have clicked on the link had you given it a second thought.

Then the moment arrives when your world comes crashing down around you as the stark message appears on your screen informing you your data has been locked and you are required to pay a sum of money in Bitcoins to unlock it. You may also see a clock counting down second by second. The countdown timer informs you your fine will double in 36 hours and after 72 hours the key to your data will be destroyed, and your data lost forever.


You have just fallen foul of Ransomware - malicious software (malware) that infects your device and encrypts or locks your data. Your data has been taken hostage. If you have any USB drives connected or you are logged in to a network with access to shared drives, they will almost certainly be infected too. Your colleagues will also lose access to locked data on shared drives. Your infected device may now infect other devices on the network exacerbating the problem.

What should you do next? Should you pay the ransom? What can you do to protect ourselves from an attack like this future? Who is ultimately responsible for your online safety? This document provides answers to these questions and is aimed at anyone who uses a PC, tablet or smartphone to access online services or email.

## Who should read this document and why?

IT users and the IT teams supporting them. You should read and digest this information as soon as possible to reduce the risk of becoming the next ransomware victim. In fact, this document applies to anyone who uses a PC, laptop, tablet or smartphone at work or home is at risk of being infected by ransomware. Much of the content in this document applies to protecting personal photos on our smartphones as much as it applies to protecting corporate data on our work PCs and laptops. There is not too much mention of technical aspects of cyber security and there is a good reason for this. This document intentionally focusses on the human element because the majority of incidents are the result of someone clicking on a link leading to a malware download. As soon as we succumb and click on the link, all but the most sophisticated security systems will be largely ineffective.

## What this document is not

This is not intended as a detailed technical document for prevention and recovery from ransomware attacks. However, some basic but important technical aspects have been included to support the overall purpose of the document.

# What is ransomware?

There are two types of ransomware: encrypting ransomware and locking ransomware. Locking ransomware has been around since the mid 2000s. CryptoLocker was the first encrypting ransomware, this appeared in 2013. A brief description of each type of ransomware follows.

## Locking Ransomware

When locking ransomware runs on a device it locks the user out of the computer. It may just provide the ability to type into a specific area in order to communicate with the cyber criminals to pay the ransom. A locking ransomware attack typically leaves the files intact, we just cannot get to them. Locking ransomware often presents itself as a notice from a law enforcement agency such as the FBI stating you have been viewing inappropriate content. This is a scare tactic to encourage the user to take action and pay the ransom.

## Encrypting Ransomware

When encrypting ransomware runs on a device it typically (but not always) generates a key and uses this to encrypt the files on any visible drives. The malware overwrites the original files with the locked version, so the original files are irrecoverable even using the most advanced forensic techniques. Cyber criminals hold the key to unlock the data which they hold until a ransom is paid. There is no guarantee the key will be released if the ransom is paid.

There are many different types of encrypting ransomware including: CryptoLocker, GoldenEye, Locky, GrandCrab, WannaCry and many more. Security experts have cracked some variants of encrypting ransomware and made the encryption keys available free of charge. However, later variants are impenetrable and cannot be unlocked without the key.

## How does ransomware infect my device?

Ransomware is mostly spread by social engineering. Cyber criminals play on our weaknesses, enticing us to click a link in an email, click on a web site ad, or visit an infected web site. It may be a reputable web site hacked by cyber criminals and infected with malware that pushes ransomware out to unsuspecting visitors, or it may be a malicious clone of a reputable web site created with meticulous detail. The cyber criminals trick you into infecting your own device.

Malware and can be hidden in documents, propagated through social media and via messenger services, hidden on web sites, hidden in vendor software updates, pictures, videos and any other file you access in your day to day life. Once your machine is infected malware is very good at self-preservation and it may spread to other devices in the network.

Cyber criminals are constantly developing their software and new versions of ransomware are using SSL (Secure Sockets Layer). Secure Sockets Layer is used extensively by legitimate web sites to reassure users that their web site is safe. We are told to look out for the little padlock in the address bar which is cited as being a sign of safety. The cyber criminals know this, so they have increased their focus on creating attacks via what appear to be secure connections. Can you be sure the site below is secure?

## What devices can ransomware infect?

No device is safe from ransomware. The most popular targets for cyber criminals are Windows PCs, laptops and servers. However, ransomware can infect Macs, tablets, smartphones, wearables and home automation systems. Who knows what next. Drones? Autonomous vehicles?

# What should I do if I suffer an attack?

It doesn't matter how prepared you are for events such as this, the impact of those first few moments will be the same. The fear of not knowing what damage is going to ensue. Loss of hours' - maybe even days' work, loss of business, business disruption and not to mention the embarrassment. But, it is important to note, as well as being very well organised, these cyber criminals are also very clever, in fact they are expert at enticing us to click on their links. They have succeeded so many times before and have taken down household names including cyber security consultancy firms, public network operators and government departments. We know the cyber criminals only care about themselves as they do not hesitate when attacking NHS systems which is potentially putting lives at risk.

If you suspect you have just clicked on a link that has infected your device, it is important to put your emotions to one side and stay calm while acting swiftly. Time is of the essence. I must emphasise that you should take this action even if you only have a slight suspicion you have just clicked on something sinister. You should not wait for any symptoms for confirmation. Always err on the side of caution, if you wait for something on your screen to confirm the infection it is likely to be too late. The sooner you take action the better.


## Disconnect your network connection immediately

Always be aware of your network connection and how to disconnect it quickly if the need arises. Disconnecting your device from the network may reduce the risk of shared network drives and other network attached devices being infected. It will also stop the ransomware affected device from communicating with the cyber criminals Command & Control (C&C) server. I cannot emphasise this enough, you need to disconnect your device from the network as quickly as possible and if you are quick enough you may contain the infection on your device.

To break a physical connection, simply disconnect the network cable. If your device has a fixed and wireless interface and the wireless interface has been set up to work on your local Wi-Fi network, you will need to disconnect both. If you do not disconnect the wireless network, the wireless connection may establish when you disconnect the network cable, allowing the infection to spread. If you have a wireless network connection, you will need to access your system settings and disable Wi-Fi as quickly as possible.

## Record events

Make sure you record as much information regarding the attack as possible. Write down a timeline of events leading up to the attack and your subsequent actions. If there is anything on your screen either take a photo of it or make a note of the message and any other relevant details. This information gathering exercise is essential for recovery and reporting.

## Report it

As soon as you have disconnected your device, notify your IT team. Again, timing is of the essence as your IT team will want to contain the infection as quickly as possible to reduce disruption. They will also need to identify the source and type of infection as quickly as possible to enable them to take remedial action.

Make sure you have a note of what you were doing just before the malware struck. Whether that was visiting a web site, clicking on a link in an email, opening a document, etc. The IT team need this information.

When the situation is under control any ransomware infection or attempted ransomware attack should be reported to ActionFraud, the UK's national fraud and cyber crime reporting centre.

https://www.actionfraud.police.uk

## Recovery

The recovery process is a specialist task and depending on the extent of the infection can require significant resource and time to restore. Your IT team must first isolate the infection and identify all of the infected devices. They must then use tools to remove the malware. When they are sure the malware has been removed from every infected device and only then, they can determine the best option to recover or reinstate the data - assuming you have backup data to reinstate.
Before taking the decision to delete locked data or reformat disk drives to restoring your latest clean backup onto, check the 'No More Ransom!' site as they may be able to help you to locate a key to unlock your data. Their 'Crypto Sheriff' service will locate a decryption tool if there is one available. All you have to do is upload two files encrypted by the ransomware, along with the ransom note details.

https://www.nomoreransom.org/

If you are unsuccessful in finding a decrypting tool, proceed with the recovery process and reinstate the files. If you use a Cloud service such as Azure, Dropbox or Google Drive, and your folders were linked to your device when the attack occurred, some or all of your Cloud stored files may also be encrypted as a result of your device synchronising with the Cloud. If this is your only backup you may be able to revert back to a previous date before the infection occurred. If the Cloud copy is the only backup, bear in mind it could take some time to synchronise with your local device or devices, depending on the speed and performance of your internet access circuit.

# What can we do to prevent getting infected?

## We are all responsible for our cyber safety

With our systems under constant threat of attack from Ransomware, we all have a responsibility to defend our organisation's data and our personal data from cyber criminals. That data could be business critical documents, plans and spreadsheets or it could be an irreplaceable personal photo collection or music library. It all has significant value to someone.

If we are to keep ourselves as safe as possible from these cyber criminals, we need to adopt a health and safety type approach. Everyone has a responsibility to work safely to ensure we do not put ourselves or our colleagues at risk. If we are as vigilant about cyber safety as we are about health and safety, we will significantly reduce the risk to our business and personal data.


## Organisation culture

Some years ago, I watched a TV documentary on airline safety. The researchers analysed many air crashes and they discovered a common thread, the crew were unable to challenge the decision of the pilot. They then analysed the airline with the best safety record. They discovered the safest airline gave authority to the entire crew to question the pilot's decisions when facing a challenging situation. From the co-pilot to the in-flight attendants, they all knew they could question any decision without fear of retribution.

The culture of the organisation is vitally important in the fight against cyber crime. Employees must feel they can challenge instructions from people in authority. A personal email from the CEO urging the recipient to click on a link or open a document may not be what it seems. If we are going to encourage everyone in the organisation to be vigilant we must also make sure we empower them to question any email without fear of reprimand.

Organisations can be proactive by setting some ground rules for email use and ensuring directors, managers and team members are regularly informed of these rules. The organisation can make it very clear to all that directors and managers will never ask you to click on a link without prior warning or without a plausible explanation. While on this subject it is also wise to state that directors and managers will never ask team members to transfer funds.

## IT Team Responsibilities

I appreciate this may seem like I am trying to teach my grandmother to suck eggs and it is not an exhaustive list of preventative measures but in my experience, some or all of these are often missed. IT teams working in a retail environment taking credit card payments are well versed in the technical aspects of securing their network, but there are many business IT teams constantly in a firefighting situation with little or no time for planned maintenance updates or security reviews. It is important to make sure you review all of these topics regularly.

### Accurate Documentation

Accurate documentation has to be the top of the list. If you do not have an accurate record of your entire network infrastructure and how it operates you cannot secure it. Without records you will be relying on an element of guesswork to establish the extent of an infection and it will significantly increase the amount of time required to establish whether the infection has been removed - a fundamental requirement before you start to reinstate files. This may seem obvious, but I have seen many installations with poor to zero documentation.

### Security suite

All devices should be protected by security software. IT teams should ensure their users devices are adequately protected, especially if users are allowed to use their own devices to access corporate data.

### Patching policy

Ransomware often takes advantage of historical vulnerabilities. Many of the most recent headline ransomware attacks targeted old operating systems or unpatched devices. It is vitally important for all devices to maintain the latest security update patches.

## Backup policy

Your backups are the best recovery option you have for a ransomware attack. Even if you pay the ransom there is a very strong possibility that you will still not receive a decryption key. Make sure your backup policy and procedures meet your business requirements should you lose access to your live data.

## Restore policy

Having a well-rehearsed plan to restore your data is essential. But, make sure the network is safe and all infected devices have been cleaned before commencing the restoration. Always make sure you have an offline backup before exposing your data to the network. If you intend to restore from the Cloud, remember to factor in the synchronisation time as any encrypted files will have to be synchronised over your internet connection so this may have a significant impact on the time it takes to restore your files. Make sure you know in advance what the Cloud provider restore policy is. Now is not the time to learn that certain caveats have not been met to achieve a full recovery of all files.

## File Extensions

Ransomware is often delivered in a file with an executable extension on the original extension, however, the default setting on Windows is to hide the extension. For example, a legitimate invoice sent from one of your trusted suppliers may have a filename of invoice3098.pdf. A cyber criminal may send their ransomware as invoice3098.pdf.exe. With Windows in its default setting you will not see the .exe extension. Changing Windows settings to display the full filename will make it easier to identify potentially malicious files (i.e. files with what appear to be double extensions). If you receive any files ending in .exe, .scr or .vbs, never click on them.

## Educate users regularly

Provide a clear one-page plan of what you expect of your users to keep your systems safe and the actions required of them should they suspect or know their device has been infected.
Consider running test phishing emails to familiarise your users with the type of emails you expect them to spot. Monitor and record 'click-through' activity and use the results to fine tune user education.

Make sure your users know how to disconnect their device if they suspect it has been infected. Check they know how to disconnect from the physical or wireless network. Provide clear instructions as to how to do this without hesitation.

## If you are experiencing a live cyber attack

ActionFraud have a 24/7 help line with specialist advisors. Make sure you have a timeline of events, gather as much information as possible in relation to the attack.

ActionFraud 24/7 help line 0300 123 2040.
(for cyber attacks in progress only)

## Every IT user has a responsibility to for cyber safety

I cannot emphasis enough, we all have a responsibility for our cyber safety and that of our organisations'. I would go further to say that we all have a responsibility for the cyber safety of everyone we come into contact with, and it is reasonable for us to expect the same in return. The list below is not meant to be exhaustive, that isn't possible because who knows what cyber criminals will come up with next. Cyber criminals are expert at enticing unsuspecting people to do follow their instructions such as click on a link to download their ransomware. So, stop being 'unsuspecting' and always be on your guard. Trust no one, because you never know when, where or how cyber criminals will strike or who's disguise they will be wearing.

Here are some pointers for starters:

- Be very careful when opening emails from people you don't know, especially if they have attachments.
- It is easy to fake an email address, the email you are reading may not be from who you think it is from.
- If the email subject is out of character for the person sending the email, think twice before opening it.
- If something doesn't look or feel right in the grammar or style of the email trust your instinct and always question it.
- If you are managing your emails on your mobile be extra careful as it may not be as easy to check email addresses or assess the validity of the email. If you are not sure, wait until you can get to a PC and reassess the situation.
- If necessary, call the person concerned and confirm they really did want you to carry out a particular action.
- If you have online access to your data on a Cloud service so will the malware.
- Always, always, always stop and think before you click on any link.
- If you do receive a suspicious looking email notify your IT team immediately. Do not forward the email unless you are specifically asked to.

## Should I pay the ransom?

Never pay the ransom. If you do there is a high probability the cyber criminals will not honour their part of the deal and you will still not gain access to your data. Paying the ransom makes you a natural target for future attacks. Even if your files are restored the cyber criminals could leave a back door to attack you again. Your ransom payment could be funding the cyber criminals' business growth enabling them to attack more targets in the future. Worst still, you could be financing more serious crime such as terrorism.

## Are we going to win the war?

Ransomware is a very lucrative business stream netting in the region of $1 billion in 2016. Although some cyber criminals work alone or in small groups, others are pooling resources and knowledge growing into organised crime syndicates on a global scale. These organised groups are operating traditional business models with contact centres staffed with agents handling ransom payments and issuing the unlocking keys. Some syndicates have research and development teams driving innovation and creating more advanced ransomware products which they sell to budding cyber criminals, either as a boxed software package or a joint venture Ransomware as a Service partnership.

We are operating our businesses and the cyber criminals are operating theirs, so ransomware is going to be around for the foreseeable future. Cyber criminals are constantly upping their game looking for new vulnerabilities to ply their trade so we must be forever vigilant as prevention is better than a cure. We must always be prepared to lose the occasional battle as it is not a matter of if we are going to become a victim of ransomware, it is a matter of when. We cannot win the war, but we can maintain and improve our defences.

## Sharing is caring

There is a famous quotation by the then Cisco CEO John Chambers. "There are two types of companies: those that have been hacked, and those who don't know they have been hacked." When we hear of organisations being hit by a ransomware attack it is human nature for us to breathe a sigh of relief when we learn our organisation is not among the victims. Some organisations see this as a business opportunity. If one of their competitors gets hit, they immediately go public in blogs and in the press extolling the virtues of their organisation over their unfortunate competitor.

I attended a recent security event where the security expert presenter used the analogy of two hikers being chased by a bear. One hiker stops to put on his running shoes. The other hiker says there's no point doing that because you cannot possibly outrun the bear. The first hiker replies “I don't have to. I only have to outrun you”. The analogy is that you only have to be more secure than other organisations and in particular your competitors as the cyber criminals will target the lowest hanging fruit. This approach is flawed as it creates a false sense of security as well as an 'I'm alright Jack' attitude.

Cyber criminals share information, they are resilient, they have better Disaster Recovery and Business Continuity plans than most legitimate businesses. If they are taken down by enforcement agencies, they are back up and running in days. The ransomware 'industry' is so lucrative that cyber criminals will continue to launch attacks on as many organisations as they can. The attacks will become more prolific as the number of cyber criminals enter the industry. We cannot assume that if we are more secure than our neighbour we are safe. Cyber criminals only need an email address and it doesn't matter how secure our networks are, it only takes one email to arrive in our inbox when we are stressed, tired or have a momentary lapse of concentration and they have snared their prey.

Taking the above into consideration the only way we are going to maintain an effective defence against cyber criminals is to collaborate. We must refrain from attacking the victims of cyber crime, even if they are our arch rivals. And do not even think of trying to outrun the bear. Cyber criminals collaborate on a very organised scale to attack us, so we must collaborate too; with the police, our suppliers, customers, other organisations in our industry and with anyone who can add value to our collaborative defence, even if they are our competitors. In recent years rival banks combined forces to form the Cyber Defence Alliance to share information about cyber crime attacks and to collaborate in building effective defences. We must follow their lead, it is a matter of survival.

## Summary

As law abiding citizens we all have a role to play in protecting our organisations' data as well as ensuring our own devices are secure and protecting our own data. We have a duty to maintain our own cyber safety and the cyber safety of those around us. If you follow the advice in this guide it will help you to be a safe cyber citizen.

## About the author

Steve Smith started out in the industry in 1973 as a Post Office Telecommunications Apprentice. After six years he joined Cable & Wireless UK Services and embarked on a retraining exercise at the C&W training school in Porthcurno. In January 1985 Steve co-founded Astro Communications with Rob, who was a colleague at C&W at the time. Steve has been responsible for the design and delivery of some very innovative technology solutions including a satellite overlay system for Wide Area Networks, safety systems for the North Sea Oil industry and many others. As CTO at Astro Steve still loves the industry and the daily challenges it provides. Steve is a Freeman of the City of London, a Liveryman in the Information Technologists Livery Company and is a member of The ITP, The IET and The IEEE.