THE DPP'S

10 things

YOU NEED TO KNOW ABOUT CYBER SECURITY

dpp™
digital production partnership

Enabled by VERA

INTRODUCTION

Hack to the Future

For over 20 years the media industry has largely avoided the risks around the corruption and leakage of content by working on digital tapes. Security was achieved through obscurity: unless you had an HDCAM tape machine at home, it was pretty unlikely that you were going to be able to digitise that material and post it online.

Two years ago, driven by the Digital Production Partnership, the use of tape was removed from the production process. This was a huge step forward for the evolution of digital production. Content that is recorded as digital files in the camera now remains that way right through the chain to programme playout.

This means that programmes are now digital files by default. This development has huge benefits. But it does also mean that those programme files are easy to copy, to intercept, to manipulate; and they can easily leak to online platforms. This vulnerability comes at a time when media companies are becoming more of a target. From the BBC website to TV5 in France, it appears broadcasters, and often their news agenda, are considered fair game by cyber criminals.

To try and tackle this issue the DPP has worked with its Members to examine the topic of trust and security. Our work looks at all the points in the production chain where we believe that trust and security are an issue.

With so much sensitive digital content now flowing around the industry, the challenge for every production office is how to plan for when someone tries to steal, modify or damage that content.

So what does this mean for productions? It means a fresh approach to risk management. It means taking a look at where in the production chain you need to think about security and then building in appropriate control measures.

It's about getting serious about security. And to help you the DPP has brought together security experts from its Membership to create this simple – but authoritative – introduction to cyber security.

What is Cyber Security?

We often hear of major brands that have suffered from data leaks, and news headlines about attempts to buy stolen logins and passwords. Being online and connected can put a person or a company at risk. A cyber attack is an electronic attack designed to steal information from your computer, online service or to prevent people from using their systems or devices. The global scale of the Internet means that cyber attacks can come from anywhere.

Until recently the media industry has escaped relatively unscathed: hackers have tended to attack financial institutions or governments. But that's starting to change. Some media organisations now experience several cyber attacks daily.

In the past those who wished to cause damage to broadcasters had to infiltrate their buildings and studios to disrupt output. Today it can be as simple as downloading and running some freely available malicious computer scripts.

And it isn't only broadcasters who are at risk. Any media company or organisation that uses connected systems – or buys services from other companies that do – can become victims of an attack.

INTRODUCTION

The consequences for those victims can be huge – from causing financial loss to suffering irreparable reputational damage. Cyber security exists to reduce those risks.

This *10 Things You Need To Know Guide* is aimed at anyone who wants to understand how to reduce the risk of being harmed by a cyber threat, by protecting themselves or their business.

1

Know your enemy

Threats can come from inside or outside your organisation: understanding who might attack you will help you defend yourself.

A threat to your content can come from anywhere. Threats can be external to your company or internal: uncomfortable though it sounds, threats can even come from your own employees.

There are five different categories of attacker. It's important to think about which type might be most attracted to your production. Depending on your programme content, you could be a target.

1 **Casual hacker**

A casual hacker is a threat from a person or a group who are curious about different systems and attempt to cause disruption just because they can. If a computer or an app has a flaw they can exploit, they will do so for the pure thrill of it.

2 **Hacktivist (activist campaigner)**

Recent geo-political turmoil has seen the rapid growth of Hacktivists. These are global groups made up of individuals and casual hackers with a shared cause. The cause can vary; however it tends to be associated with geo-political and social movements in areas of perceived injustice. These groups will target institutions, whether it's a government, civil or corporate company in order to highlight their cause.

There are a number of these groups but perhaps the most famous ones are *Anonymous* and *Lulzsec*.

3 Organised crime

Networks of criminals exist whose sole job is to access your systems, steal sensitive information and sell it to the highest bidder.

They are extremely imaginative in their attacks and spend significant time planning sophisticated ways to access your information. They don't care if the target is a business or an individual.

One of their most common tricks is to use spam emails designed to look as if they have come from a legitimate anti-virus company. If the spam email is opened and attachments are clicked, it will look as if an anti-virus program is scanning through your computer, but instead it's actually infecting your computer with a virus.

Once the scan completes it will alert you that a virus has been identified and will offer you the ability to pay for anti-virus to clean it up. Once you make the payment nothing happens; the attackers have your money and you're left with a virus.

Some criminals go even further, using cyber extortion. They infect a computer with a "Cryptolocker" virus that makes the machine unusable. It encrypts all the information on that machine, including any programme content. The only way to decrypt the computer is to pay the criminals for a decryption key. Quite often payment of the ransom doesn't actually lead to decryption. Imagine if that computer held all your production rushes: how much would it cost to reshoot them?

4 Nation states

These attacks come from governments who want to disrupt or interfere with services or content.

It could be the case that you're shooting a programme about a sensitive topic in another country, or investigating a foreign government. It's important to think very carefully about the groups that you may be antagonising through your programme, as they may choose to retaliate against your company by infiltrating your systems.

A large US movie studio recently made a film that satirised a foreign government. That government allegedly hacked the studio – including their backup systems. It took them almost three months to recover. On a smaller scale, a UK production company shot a factual documentary about events in East Asia. The day after the show went on air their website was down for the whole day.

It's important to remember that certain governments have full control over Internet access in their country: they can easily intercept and access your smartphones or laptops when you are working there. Extra care and consideration therefore needs to be given when thinking about what equipment you're using and what information you may be sharing when working overseas.

5 Internal threats

An internal threat can arise from an employee (past or present), freelancer, contractor or other trusted third party who has some kind of access to the company's information and content.

These internal attacks tend to fall into one of three categories:

Accidental

Where an insider, without realising, causes harm or increases the probability of future harm to a company's content or resources. For example, employees could lose a work smartphone that carries sensitive information, or share pictures of their office environment on social media without realising that important security information is visible.

Opportunistic

Where an insider will seek deliberately to cause harm because they believe there is no way of detecting their actions. Often a visible deterrent, such as CCTV cameras, can be sufficient to prevent this.

Determined

Where an insider has a plan to cause harm and disruption. Such a person could be an employee with a grievance, or an individual with access to the building who is aligned to an external threat.

TOP TIPS

- Preparation and planning is key to ensuring threats from hackers are minimised. If you're going to be working on a production that could potentially attract hackers then you need to be prepared.

KNOW YOUR ENEMY

- Keeping websites, software, apps, and anti-malware programs updated on a regular basis will make it harder for hackers to exploit your systems and software.

- Make your colleagues aware of how to recognise email scams (known as *phishing* attacks). This will help you avoid becoming a victim of scams by organised criminals.

- If you're travelling abroad for a shoot, be aware that your Internet connection may not be as secure as you think it is and that different encryption and privacy laws can apply. Further information is provided later in this guide.

2

Be an informed decision-maker

The first line of defence against cyber attacks is informed decision-making at the top of the organisation.

The very first step in countering any threats is to ensure that someone in your organisation, no matter how large or small it might be, is responsible for ensuring cyber security measures are in place – and keeping them up to date.

That individual needs to be a senior leader, who has the ability to raise the profile of cyber security, and can assign budget to protect the organisation.

Cyber security needs to move from being an afterthought, to being an integral part of pre-production planning – just like health and safety. For example, just as a factual documentary being shot in a hostile environment would bring to mind health and safety risks, so it should also bring to mind cyber security risks.

If you cannot identify a senior leader who has the time to spend on security related matters, then it may be necessary to consult a dedicated security expert who can help your productions to protect themselves.

TOP TIPS

- The nature of information (content plus metadata) being collected will determine what measures need to be put in place to protect information. If you're working with sensitive information – such as for a programme containing children – or if you have content of high commercial value, you will need to factor in additional measures, such as encryption, or dedicated communication links.

- To help your responsible person make informed decisions about how to protect your data, they will need to know how and where that data is stored. You can keep simple logs in a spreadsheet that track where information is being stored and who is responsible for it. For example: is it stored in local hard disks, Internet storage, printed hard copy in a filing cabinet?

- A culture of cyber security awareness needs to be raised within the organisation. Hold regular briefing, training and communications sessions. Think about putting up posters to help your team members and colleagues remember simple tips.

- Treat cyber security risks as you would health and safety risks – the impact of either can be enormous.

3

Use security tools

To protect your content and work securely
you need effective and up to date security tools.

You wouldn't use an old black and white TV to view UHD content. Security is the same. Software and hardware gets old and out of date, and no longer fit for purpose.

It's easy to forget that the output you produce or the rushes you create all have significant value. The sheer cost of creating them makes them worth protecting. So it makes sense to have security tools built into all the key processes when content is created, changed or moved.

That content, whether rushes or a finished programme, will be passed from storage device to server and back again a number of times during a production. These are naturally points at which content can be lost, stolen, or corrupted and points at which extra diligence is required.

It's not only the content that needs protecting, it's also the associated information – such as scripts, call sheets, freelancer contact details, bank accounts and metadata. Remember that data protection legislation requires you to keep all personal data safe and secure.

So what are the tools that will help? To start with **you will need anti-virus and anti-malware software**. What do these terms mean?

Virus

Is a type of highly infectious malicious program that's been designed to cause harm and spread – much like an organic virus.

Malware

Is a collective term that describes different types of malicious computer programs such as Viruses, Trojans, Worms etc. In this guide we will refer to malware/anti-malware as it collectively describes all sorts of different malicious programs.

Anti-malware

Software protects your laptop, computer or smartphone from very harmful and malicious programs that have been designed to cause damage and disruption to your data. Once they cause harm to you, some have a propensity to self-propagate and infect others. Within a short period your whole office could be infected with malware.

The damage caused by malware varies. A very mild case could result in changes to your screen saver or annoying ad popups appearing on your computer; a severe case could result in lost or corrupt data rendering your computer useless. Don't forget your smartphone is also a computer: malware can infect mobile devices just as easily as desktop or laptop computers. Even Macs can be vulnerable.

Anti-malware software is commonly available. Some software is free to download and use. Take care to ensure that this comes from the official company website, since fake anti-malware also exists that you can download by mistake.

Paid-for anti-malware software is strongly recommended. These tools tend to offer additional features such as the ability to scan websites for malware, and to provide regular software updates. Updating protection software is extremely important as new malware threats are created by hackers on a daily basis.

When dealing with files on a portable drive it's always best to ensure the drive is scanned with an anti-malware program. When buying portable drives (such as USB memory sticks, or memory cards) think about where you're buying them from as some cheaper unbranded products may come preloaded with malware.

Most correspondence these days still takes place over email. Care and caution needs to be taken when you receive an unexpected email inviting you to open an attachment or to download something. It's good practice to scan the download for malware. Indeed, it's a good idea to do this even for attachments you were expecting.

Encryption

Encryption is a way in which information can be scrambled either when stored on a drive or in transit over the Internet, and only unscrambled with a unique code. It's important to use encryption on programme files that are sensitive, high value or may be linked to spoilers in plotlines.

When dealing with content pay particular attention to the metadata and ensure that sensitive information is not being transferred unencrypted as part of the metadata. It's important that business details are used where possible. Sensitive information includes personal data, which is anything that can uniquely identify an individual, such as a combination of name, telephone number, email address, date of birth, GPS data, and so on.

USE SECURITY TOOLS

If you work on location or primarily work on the road from a laptop, then it's good practice to encrypt your whole laptop, this way if you lose it or it gets stolen your information would remain scrambled to anyone who tries to extract it. It can take a while for laptops with large hard disks to fully encrypt, so preparing well ahead of a trip is recommended. An encrypted tablet with the right apps could be a suitable alternative if you plan on reviewing proxies.

Call sheets and other confidential non-video information are often stored on computers or laptops used on location. These documents can be individually or collectively encrypted and then shared over email or exchanged by other means, such as a secure file transfer service. There are many free tools available that will let you do this easily. Most will require you to create a password, and if you need to share this password ensure you exchange it separately – for example by phoning or Skyping the recipient, or sending an SMS message.

Encryption exists in other places, which may not be so apparent to everyone. For example when you are browsing the Internet, the majority of official and corporate websites will now only serve you web pages over an encrypted Internet link. You can identify these by looking at the web address. These normally start with HTTPS and an icon of a green locked padlock is often used to indicate that it's a secure encrypted web link.

If you operate a website for your company then you need to make sure your web pages are encrypted. Speak to someone about getting an SSL certificate implemented for your website. If your website contains a login for customers or users then you should make sure that the passwords are encrypted.

Finally, if your production requires a high level of sensitivity and secrecy then you should consider investing in software that will allow you to encrypt emails. This level of protection is a bit more complicated and will require specialist advice.

Logins and Password

Remembering logins and passwords can be frustrating but they are an important safeguard. A weak password is essentially one that is 7 characters or less and consists of any dictionary words. Such passwords are weak because a hacker can run a script that goes through a dictionary trying words as passwords. All in fractions of a second.

Strong passwords are made up of 8 characters or more, containing a mixture of letters and numbers, special characters and upper and lower case. Ideally you'd want to use a memorable phrase as the basis of your password. The longer it is the more difficult it is to hack – for example, *elephant in the room* could become *3l3phant1nther00m!* Avoid using the same password across multiple sites. Otherwise once a hacker has one password they will have access to all of your accounts.

It is common for teams to use generic accounts which have a specific username and password that is shared amongst a team. But generic accounts should be avoided because if you happen to have an insider threat it becomes very difficult to identify who they are. For example, if your archive system login and password is generic, then an individual could delete it all without being identified. For the same reason, individuals should never share their own accounts with other colleagues.

Secure networks

One preferred method of disruption, especially by hacktivists, is to bombard your company website with requests for pages to such an extent that the site becomes overloaded and unable to fulfil genuine requests. This is known as a 'denial of service' attack.

The same kind of attack could be made to your Internet link or communications network. This will make your Internet become unusably slow.

If you have a domestic broadband Internet link your Wi-Fi device will have some basic functionality that can be enabled to reduce risk. However these are basic levels of protection for the home user and are not really suitable for business use. Investing in a firewall will give you enhanced protection from denial of service attacks. It can also scan for malware and offer a whole host of other beneficial features.

Wireless networks are great for mobile working, but they need to be set up securely. Most newer Wi-Fi devices given away by consumer broadband providers tend to be secure out of the box. They make use of a strong form of encryption called WPA2. An older form of encryption called WEP must not be used.

If you're working on a sensitive production think about whether you can use 3G/4G for general web browsing and email and dedicate your wireless/wired network to programme making activities. This would reduce the likelihood of spreading malware, from emails or malicious websites, across your wireless/wired network.

TOP TIPS

- Make use of anti-malware programs and ensure that they are kept up to date.
- Scan all new drives for malware, as well as scanning cards before an important shoot. Follow up by scanning drives and cards when they come back from a shoot.
- When sending sensitive information through email, many compression tools have built in encryption capabilities. Use one of these to create an encrypted Zip file and send that instead of the original file, though before sending anything, first check with the recipient that they are able to receive encrypted Zip files. Otherwise an alternative method will need to be used. Ensure that you exchange the decryption password securely, via a separate method, such as SMS.
- Passwords and passphrases can be difficult to remember, so spend time devising secure but memorable ones. Don't write them down and display them.
- When connecting to wireless (Wi-Fi) networks make sure they are using WPA2 encryption and not WEP. This will keep the information you send between your device and the wireless access points secure and encrypted.
- Think about what software you need on that laptop you are using for assembly edits. Does it need email and a web browser? Take that temptation away and use your mobile for email to avoid infecting the edit machine and risking your rushes.

4

Secure your smartphone

Keep your contacts and personal information safe with a few simple steps to secure your smartphone.

It's no surprise that smartphones have become one of the most important production tools. By enabling us to check emails, view call sheets, look up location maps or use group messaging, the smartphone has made working in the field far more flexible. However, by putting all that production information on a single portable device, they present a whole new area of risk.

Imagine you are working on a factual programme for children, and you are on your way home on the train. Someone emails you a list of all of the contributors, with their contact details and health conditions. You open the email and download the attachment. Suddenly you've arrived at your destination and rush to get off – not realising you've left your phone on the seat. The phone is set to the default four-digit pin entry system – which means it can be unlocked in less than a day using a device that costs less than £200.

Would you be worried at this point? You should be. Not only have you just lost your phone, but also under the Data Protection Act the loss of sensitive personal data is reportable to the Information Commissioner's Office and can lead to prosecution.

SECURE YOUR SMARTPHONE

You're likely to take your smartphone with you when visiting or shooting in an overseas location. Extra care needs to be taken when visiting certain countries (especially those that are under international trade sanctions and embargoes). If possible, avoid taking a personal phone and instead use a fresh phone that doesn't have too much data on it – although it's important to remember that a completely fresh phone can arouse suspicion for some authorities.

When using your smartphone for work, consider the following actions to help reduce the risk of malware attacks or loss of data.

TOP TIPS

- Change the default 4 digit pin code to a longer code with a minimum of 6 digits.
- Install an anti-malware app for your smartphone.
- Enable whole disk encryption on your phone.
- Enable the *Find My Phone* feature or install an app that offers similar functionality.
- If your phone has a fingerprint scanner then you can enable that too for additional security. Fingerprint scanners can provide additional security compared to pin codes, as people tend to use weaker pin codes if they have to enter them regularly.
- Avoid downloading apps that don't come from an official app store (this mostly applies to Android users).

5

Beware free Wi-Fi

A VPN network will help you protect against the dangers of free Wi-Fi and an evil twin!

Our mobile devices are always on the prowl, searching and scanning for Wi-Fi access. If free Wi-Fi is detected, many of us will instinctively make use of it – especially if we are on location with a laptop and need to get important material back to base.

It is very easy for a hacker to create a malicious Wi-Fi network, give it an appealing name such as Free Wi-Fi and then all of a sudden they have access to hundreds of devices.

Once connected, the hacker could be happily intercepting all the information that you're sending from your device – especially if, like many email services, your communications are not encrypted.

When connecting to a wireless network (Wi-Fi) you normally identify the network by its SSID (Service Set Identifier), which is essentially the name of the network. Hackers can easily setup a Wi-Fi network with the same name as other popular Wi-Fi networks. How would you even know the difference? Some hackers will go a step further and will redirect you to a very genuine looking banking or social media login page, all designed to capture your login and password. Say hello to the evil twin!

BEWARE FREE WI-FI

One solution to avoid malicious access points and evil twins is to make use of VPNs (Virtual Private Networks).

A VPN is a type of secure connection that you create using a program between your device (smartphone, tablet, laptop) and your VPN service provider. The connection to the VPN will be encrypted, so even if you're on a malicious Wi-Fi access point, anyone snooping will find the information incomprehensible.

There are free VPNs available that are very good and paid for services that are relatively cheap. One of the additional benefits of using a VPN is that it effectively hides your online identity, so when browsing websites intended for a UK audience from a foreign territory the VPN can make it look as if you're browsing from the UK.

TOP TIPS

- When visiting hotels, or coffee shops ask for details of the Wi-Fi service, so at least you know what the official access point is called. For example if the genuine access point is called *CoffeeShop1*, a fake one could be setup called *_CoffeeShop1*.
- If possible avoid logging into social media or banking sites. Try and restrict your activities to just browsing web pages.
- If you have to use social media or banking sites then keep an eye out for tell tale signs. Fake websites will often have spelling mistakes, and the colours and fonts might not feel right.
- Either invest in a paid-for VPN service or use one of the free ones.

6

Understand the content lifecycle

The risks associated with your content will vary over time and you may need to be prepared to strengthen your protection.

The value of content can vary depending on genre, and where it is in the production lifecycle.

Some content – such as live events – has high intrinsic value when it is first produced, but that value deminishes over time. In this instance the greatest threat is at the moment of creation when there is a risk that someone might hack into or disrupt a live feed.

A high-end primetime drama production on the other hand would have a different risk profile. Initially there may be great secrecy about plot information, and all the edits and the script have great value. Once the film is released its value changes: secrecy regarding the narrative no longer matters; but the film may still have great commercial value, especially if it is popular.

A current affairs documentary meanwhile may generate rushes that contain a significant amount of confidential data.

It is important to make a risk assessment of each stage of the production and archiving journey, giving consideration to who requires access to the

material, and who does not. Think about physical material – such as scripts – as well as online data. You should also consider your locations and working environments. One of the simplest ways of protecting an edit for example is to ensure your edit environment is not connected to the Internet. But remember that every mobile device that gets brought into that edit suite could be a way of breaching that secure environment, as it can easily be plugged into the computers in the edit suite and used to access the Internet.

TOP TIPS

- During pre-production planning think about what content and information will be created and the cyber security risks associated with it. Consider the whole production chain, from commission all the way through to long term archiving. Make a judgement about the value of the content at each stage, as well as the confidentiality and sensitivity of the information it contains.

- For content that is no longer high risk or has gone to air, the tolerance to loss, corruption or theft of content would now have changed. So you may wish to review the security controls in place for it.

- High value content with a risk profile that is maintained or increased with time should be archived in such a way that a copy exists in more than one location. More than likely a readily accessible version would be required for onward sales and distribution, but copies can be kept offsite on tape-based storage such as LTO, on Secure Optical Discs designed for archive, or in secure cloud-based storage.

UNDERSTAND THE CONTENT LIFECYCLE

- Don't forget that associated metadata – especially anything that contains personal data – must be kept safe and secure under the Data Protection Act. Any personal data that is not essential should be deleted.

7

Know the law of the land

Travelling overseas with encrypted devices and sensitive data can land you in trouble.

When travelling overseas you need to be aware that there are different laws and rules which apply to data and storage, depending on the country you are in. One unintended consequence of programme rushes being stored as encrypted digital files is that it will cause some governments to wonder if you have something to hide. In extreme examples they may attempt to confiscate your material.

There is a very common encryption technology, known as AES, that was developed in the US, and which the US government forbids from being exported – or transported in equipment – to certain other countries. Some countries may also have local laws that prevent you from taking any encrypted data, tools or software into that country. It is best to seek guidance on import and export regulations from an expert, since regulations change all the time.

In the UK, general consumer products with encryption-related functionality are not subject to export licences. However if you have professional products with specialist encryption software then an export license may be required. As before, if you are travelling with sensitive material it is best to consult a security expert.

KNOW THE LAW OF THE LAND

Other laws that you need to be aware of are privacy-related laws. In the UK the Data Protection Act regulates what personal data you are allowed to store and transfer. Other territories have laws around the use of personal data. More information about the Data Protection Act can be found at **https://ico.org.uk/for-organisations/guide-to-data-protection**.

TOP TIPS

- If you need to exchange sensitive information with others outside of the UK then ideally it should be encrypted during transit. You can use encrypted Zip files to do this.
- Once sensitive information has reached its final destination, it should reside on a system that has a similar level of protection to your own systems.
- Sometimes you will be required to remove encryption from your devices, so it may be best to carry sensitive information on a device of its own.
- Be careful about what and when you communicate in an overseas environment. In some countries the state will eavesdrop on your electronic communication. Avoid talking about sensitive information, or logging into social media. A VPN service (as mentioned in previous sections) will help.
- Before travelling to a high risk nation state, cleanse your laptop of sensitive information. You can do this by backing up all relevant information and then deleting contacts lists, research information and anything else that could be of potential value to a cyber criminal or a thief.

8

Know your friends

Don't become the victim of a social engineering attack. Only download and open files from trusted sources.

Social engineering is probably the easiest method by which potential hackers get what they need from their victims. Hackers will manipulate their victims into revealing usernames and passwords. The range of techniques deployed to carry out an attack is getting increasingly sophisticated.

One social engineering technique often used by hackers is to phone the victim and pretend to be an official from a large IT company or a bank. They ask for login and password, and even bank details. We have all heard of these tricks – but we have also heard of sensible people who have fallen for them.

Responsible companies do not normally contact you directly out of the blue. Did the caller address you directly by your name? Did you even raise an IT support call and if not then why are they actually calling? A genuine support team would normally only contact you if you had contacted them first. However if in any doubt, get their details, and then call them back using the official contact details from the company website.

KNOW YOUR FRIENDS

Many of us may feel we wouldn't fall for a hoax phone call. But sometimes the simplest tricks of all can catch people out. Ever taken up the offer of a free USB stick?

In one recent piece of research, USB drives were dropped around a university campus. Nearly half of the drives were picked up and plugged into a computer, some within a few minutes of being dropped. So imagine if the USB drives all contained malware – it could have taken out the entire campus network.

A hacker could potentially send malware-laden USB sticks or hard disk drives to a post facility or production company, and if they got picked up and used by someone in the edit suite the consequences could be disastrous.

If anyone sends you an unsolicited USB stick or hard drive, gives you an unsolicited link to download a file, or asks you to provide log-in information over the phone, reject the request. Any legitimate organisation will respect your caution, and work with you to ensure you have the information you require to confirm their legitimacy.

TOP TIPS

- To avoid being victim of a phishing scam or other social engineering attack, don't be hasty in opening email attachments. Pay particular attention to the fine details. Is the tone of the language in the email as expected? Is the name spelt correctly and from the correct email address? Remember that *name@gmail.com* is not the same as *name@gmail.company.com* – they are from different providers.

- Similarly, pay particular attention to any web addresses used in emails. Before clicking on a link, hover over it and then view the actual web address on the bottom right hand side of your browser window. Sometimes scammers will send a link that appears to be genuine, such as *www.google.com*, but the underlying link could direct you somewhere else.

- Memory cards or hard disks can come preloaded with malware, so always make sure you buy them from reputable dealers, and scan them using anti-malware tools before storing data on them.

9

Dispose responsibly

Take care to dispose of old technology securely.

You've had a successful production and the time has now come to return all the equipment you hired. You return everything – only to realise that the laptop you hired still has a copy of your edit. The next hirer is about to either get a sneak preview of your latest production, or have to delete all your files.

Secure disposal of hard drives, memory cards, laptops, smartphones or any device that stores data is extremely important. You need to make sure any sensitive or confidential information is securely removed. And remember that pressing delete does not necessarily delete material for good. You need to know that a hard drive has been securely wiped.

Secure disposal is less of an issue if all the data on the device was encrypted in the first place – although it is still wise to remove it.

There are free tools available to download that will securely erase your data. As always, make sure you are downloading from a reputable source. Some new laptops also have features that will securely wipe your data.

DISPOSE RESPONSIBLY

TOP TIPS

- Make sure that if someone leaves the company or is no longer working on a production, their access to company software or systems is removed. If using file sharing and collaboration services make sure you revoke their permissions to access these tools.

- When erasing data on a drive remember that if it is sensitive, confidential or has business importance then it needs to be erased securely. It isn't sufficient just to press delete or to reformat the drive.

- It is a good idea to keep a checklist of all of the steps needed to dispose of data securely.

- In some cases you will need to physically get rid of equipment. There are companies who can offer secure disposal services. They will remove your data and safely dispose of your drive in accordance with waste disposal regulations.

10

Be prepared by planning

Planning and preparation is key to ensuring that your production and the information that it generates has the lowest risk of being exploited through cyber security vulnerabilities.

This guide contains a lot to remember. To help you, the DPP is releasing a risk assessment checklist that you can either use to self-assess the cyber security of your own company, or ask suppliers to complete when you purchase equipment or services from them.

The checklist will give you some assurance that if you store or transfer your content with a third party, that content will be kept safe and secure – and you will be able to get it back if needed.

Before embarking on a project, prepare for a scenario where you come under some form of cyber attack. Think about what you are prepared to lose and what you must keep, then determine the balance of security measures. Have a plan for how you would manage an attack. If you are hacked what would you do?

If your website was shut down by a hacker, how would you get it back? Do you have a backup site available? If hard drives or servers are hacked or stolen, do

you have backup drives available? What happens if programme information is leaked and made available to the public to download?

Once you have formulated a plan make sure it is communicated to the whole production team.

When recruiting think about whether you need to carry out any background Disclosure and Barring Service (DBS) checks. You may even wish to carry out credit checks against service providers. Certainly for scenarios where you could be working with children or on high-end productions it may be worth carrying out these checks. This could reduce the risk of being targeted by an insider threat.

Cyber security is a growing problem, however there is a whole range of information and resources available on the Internet to help guide you should you wish to increase your understanding of this area. Some of the measures mentioned in the guide will go a long way to prepare and protect you, but consider approaching specialists if you're working on particularly confidential or sensitive information.

Remember, if you're a victim of cyber crime then you should report it to the police. The National Crime Agency (**http://www.nationalcrimeagency.gov.uk**) has been set up to deal with cyber crime and any cyber attacks can be reported to the police via the Action Fraud Service, (**https://www.actionfraud.police.uk**). Keep a record of their contact number (0300 123 20400) as part of your emergency contacts list.

ABOUT THE DPP

The DPP is the media industry's fastest growing business change network. Originally founded by UK Broadcasters the BBC, ITV and Channel 4, it is now a not-for-profit company with an international membership base drawn from the whole media supply chain – broadcasters and distributors to manufacturers and service providers, production to post production, trade bodies to educational institutions. The DPP harnesses the collective intelligence of that membership to generate insight, enable change and create market opportunity. For more information, or to enquire about membership, visit **www.digitalproductionpartnership.co.uk**.

ABOUT VERA

Vera is a next-generation data security company that enables businesses of all sizes to secure, track, and share any kind of data, no matter where it's stored or how it's shared. Vera protects data with strong encryption, enforces access controls, and applies dynamic data protections, letting employees collaborate with any application, on any device, while ensuring the highest levels of security, visibility and control. It's like having a recall button that actually works. For more information, visit **www.vera.com**.

This DPP production was brought to you by Abdul Hakim and Andy Wilson, with the help of the DPP's designer Vlad Cohen. The DPP would very much like to thank the many DPP Members who contributed their expertise to this publication, and especially Rick Bancroft, Brian Brackenborough, Wes Curtis, Steve Daly, Haydn Jones and Ben Roeder.