# **SLIDE 1**

Hi I’m Nadia, I’m co-founder and CEO of Naq. A few years ago, my co-founder Chris, who is British, was working as a contractor in The Hague, in the Netherlands. He had an accountant to help him with his tax returns and payroll, as he had no clue about Dutch tax rules. He, however, did have a clue about cybersecurity and was curious as to what his accountant had done to protect his data. The accountant answered: I know I have to do something, but I don’t know what to do or where to start. This is where the idea for Naq was born.

Naq protects small businesses. That includes anything from a one-man band (or freelancer), to a quartet (micro-business) to 200 people organizations (i can’t think of a musical ensemble analogy here). We also make them GDPR compliant. And all through our app.

Integro asked me to co-host a webinar with them today and of course, I couldn’t say no. What we’re gonna talk about today is why you, as a contractor or microbusiness, do need to take cyber security measures and ensure that you’re GDPR compliant. We’re going to go into a bit more detail on why you are liable as a contractor, even if you’re working on site, and what the quick wins are to ensure you’re better protected.

# **SLIDE 2**

Firstly, some stats. 41% of contractors and micro businesses were breached in 2021, translating to 1 hack every 25 seconds. This number is quite high, especially considering that 80% of freelancers don't think they are a target to cybercriminals. Moreover, cyber incidents don’t only occur as a result of cybercrime, but actually 90% of incidents are due to human mistakes.

 Cybersecurity breaches cost small businesses between £8,000 and £308,000. These costs consist of downtime, resolving the incident, costs of losing customers or losing potential new customers, legal fees, and then the costs for services and tools you’re inevitably going to buy after you’ve fallen victim to a cyber incident.

# **SLIDE 3**

Now how does it all start? Attacks, which only make up about 10% of all incidents, mostly start with phishing. Over 40% of small businesses breaches began with a phishing attack. The other 90% as I mentioned are due to simple mistakes. These simple mistakes are then often exploited by cybercriminals to start attacks such as ransomware attacks. This was for instance the case in the Optionis Group incident. Poor cyber hygiene such as obvious passwords, reused in several accounts, visibly stated on a desktop in a file called “try and hack me if you dare” or just “useful links and passwords”, then caused an attacker to get access to the Network and start encrypting all the files, demanding a ransom to be released.

# **SLIDE 4**

If something were to happen, who is liable? A lot of contractors come to me and say that they’re not liable because they are working on site at their client’s office. This is simply not true. Not only from a data perspective, but any type of legal liability lies with the entity which is responsible for carrying out work, processing data, etc. Contractors usually have professional indemnity insurance or business liability insurance because they know that if they give the wrong advice or if they break something that belongs to their client, they can be help liable.

This is not different in the cyber security context. You are the entity responsible for your clients information and if you cause any of their data or systems to be compromised you are the one responsible for it.

## **SLIDE 5**

Now I spoke about compromising systems or data, but what does this mean? It is important to realise that cyber security is all about the people, processes and technology that form part of the business. And these people, processes and technology are called assets. Systems and data are examples of these assets. And it is a company’s responsibility (however small they may be), to protect three aspects of those assets. The Confidentiality, Integrity and availability of the assets need to be protected. This is the same for GDPR, but the GDPR limits itself to the CIA of data.

There are a number of very important basic cyber hygiene measures that can help protect your assets and they are quite straightforward.

# **SLIDE 6**

The first one is use a strong, unique password for each account. Remember what I just told you about Optionis? So delete those files that have a convenient list of all of your passwords and use a password manager instead. Having a secure account password is only half of the work, turning on 2FA is the other half that completes it. It’s a bit of a faff, I know, but it gives you a 100% increase in security as a result.

It is also good to secure your connections with the internet by using a VPN. This ensures that your internet traffic is not visible to outsiders and can protect the information you’re working on.

# **SLIDE 7**

Antivirus

# **SLIDE 8**

Backups. This really determines how much impact an incident or attack will have on you and your clients. If you have a backup that is two months old and you need to restore the last two month’s worth of data and documents, it is likely that this will take you a while. You might feel inclined to decline new work as a result or offer your clients a discount. If you have a day-old backup, you can just take off where you left off. Moreover, regularly backing up your data can make it much easier to re-access your valuable information if your device is infected with ransomware.

Ransomware is a type of malware that can lock you out of your device or files unless you pay a ransom.

In almost all cases, there is no guarantee that paying the ransom will give you access to your data. Regularly backing up your files means you won't lose any critical information or work even if your device is infected.

# **SLIDE 9**

As a freelancer or contractor, it's likely that you have a range of different devices, programmes and services that you rely on to carry out your work.

A new client could mean installing additional software, signing up for a new service, or creating an account with yet another communication tool, all of which can quickly add up to quite a medley!

It's essential to keep track of all the different assets that you rely on for work and any associated passwords, usernames, and contact information for customer support. Creating an Account Map -- a list of all your open accounts and services - will quickly highlight all of the places where you're currently storing data.

# **SLIDE 10**

As well as putting the necessary systems and processes in place to protect your limited company business from a cyber-attack, it's also essential to have an Incident Response Plan in place for when the worst happens.

Your plan should include actions like:

identifying who to contact in the event of an incident;

which devices need to be isolated from your network;

what data needs to be preserved; and

how you will restore any lost or damaged data.

The most essential part of your Incident Response Plan is practice, practice, practice. In other words, an actual security incident should not be the first time your plan is put to use. Set out some time to go through a ‘test incident,’ note precisely what happened, which accounts or documents were compromised, and what steps you took to resolve the situation.

# **SLIDE 11**

No matter how big or small, any organisation needs to abide by the GDPR. You are liable for any damage as a contractor. And having a privacy policy on your website is unfortunately not enough.

Contractors are now faced with GDPR fines for breaches of the GDPR as well as larger corporates. The fines are quite small at the moment but are rapidly increasing as the ICO is trying to ensure that the UK is one of the front-runners when it comes to privacy.

Some contractors need to show their customers (e.g. Government, enterprises) that they’re compliant. It’s best not to start thinking about compliance when you’re asked to prove it, but rather be proactive and ensure you’re compliant from the outset. How do you ensure compliance? → Policies, contracts, organisational measures, technical measures & training