

Intelliflo Cyber Security Webinar

4 October 2017
4.00pm – 5.00pm



Agenda

- Introduction
- 10 top tips
- Questions?

Hosted by: Rob Walton, Chief Operating Officer, Intelliflo
Stephen Bailey, Head of Privacy, NCC Group



Both Intelliflo and NCC Group are active members of UK Gov National Cyber Security Centre (NCSC) Cyber Security Information Sharing Partnership (CiSP)

<https://www.ncsc.gov.uk/cisp>

Background

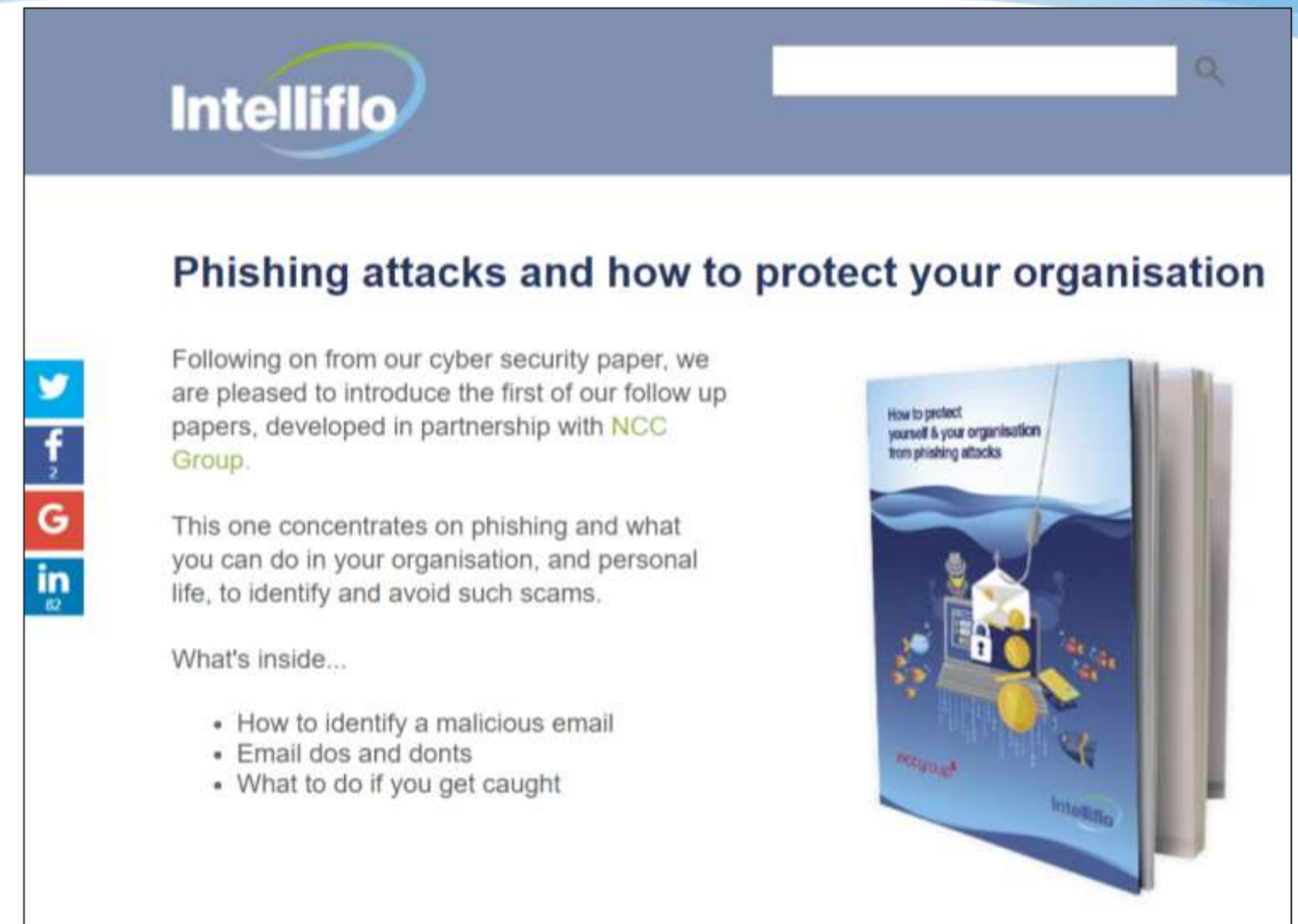
- 44% of advisers have direct experience of cyber attack
- 82% of consumers would look to change their adviser if they were hacked
- 72% of breaches in the UK are the result of fraudulent emails
- 61% of data breaches in Verizon's annual security report were business with less than 1,000 employees
- Attacks are on the rise – 20,000 in 2015 v 700,000 in 2017
- WannaCry2 ransomware struck in 150 countries globally across many sectors
- Every week there is new name on the big hack list.
- FCA report year on year increase in cyber attacks
- The GDPR regulation takes effect May 2018
 - Up to 20m euro or 4% turnover for breach
 - Up to 10m euro or 2% turnover for not reporting
 - Consumers can sue for distress upwards

Purpose

- Top 10 approaches that any firm can simply adopt to reduce the risk of a security breach and mitigate the impact should the worst occur.
- Easy to understand strategies backed up by a wide range of experience and industry analysis
- No high tech solutions, just basic 'base camp' security best practise.
- We want to emphasise that good security is built on:
 1. People
 2. Process
 3.and then technology

Types of Security Incidents - Phishing

- The most common attack type currently. Attempt to access sensitive information or systems by pretending to be a trusted source
- Often the entry point for a lot of security incidents. 95% of successful phishing attacks result in malicious software being installed
- Uk Gov cyber security survey found that 72% of all security incidents started via a person engaging with an email
- Phishing – widescale automated attacks
- Spear Phishing – targeted and orchestrated attacks
- The latter was typically used by criminals to generate \$\$\$, however WannaCry is the start of a major shift
- Used for:
 - Fraud
 - Harvesting Credentials
 - Delivering Malware
 - Extortion



The screenshot shows a webpage from Intelliflo. At the top left is the Intelliflo logo. To its right is a search bar. Below the logo is a vertical stack of social media icons for Twitter, Facebook, Google+, and LinkedIn. The main heading is 'Phishing attacks and how to protect your organisation'. The text below reads: 'Following on from our cyber security paper, we are pleased to introduce the first of our follow up papers, developed in partnership with NCC Group.' This is followed by a paragraph: 'This one concentrates on phishing and what you can do in your organisation, and personal life, to identify and avoid such scams.' Below this is a section 'What's inside...' with a bulleted list: 'How to identify a malicious email', 'Email dos and donts', and 'What to do if you get caught'. On the right side of the page is a 3D rendering of a white paper titled 'How to protect yourself & your organisation from phishing attacks' with the Intelliflo logo at the bottom.

Click [here](#) to download the Phishing attacks white paper

Types of Security Incidents - Ransomware

- Software is downloaded on to your systems that encrypts your data so that it cannot be accessed – you pay to get it back
- Typically delivered via a successful phishing attack
- Increasing significantly year on year
 - US Dept Justice – 300% yoy(2015 v 2016)
 - Increase, 4,000 reported attacks per day
- Big target for criminals as a source of \$\$
- Previously typically associated with targeted spear phishing attacks, WannaCry has changed this
- Can be extremely disruptive to a business. You NEED plans for this to mitigate AND handle.



The screenshot shows a webpage from Intelliflo. At the top left is the Intelliflo logo. A search bar is located at the top right. The main heading is "Don't be held to ransom....". Below this, there is a paragraph: "Ransomware attacks are often indiscriminate and can be extremely damaging to businesses of all shapes and sizes." This is followed by another paragraph: "The disruption caused by an attack can leave a lasting impact on a business, with the effects being felt for weeks or even months afterwards." Underneath is a section titled "What's inside..." with two bullet points: "What is ransomware?" and "How can you prevent an attack?". A final paragraph states: "The guide has been produced in conjunction with global cyber security experts NCC Group so download it now." On the right side of the page, there is a 3D rendering of a white paper titled "Surviving ransomware" with the Intelliflo and NCC Group logos on the cover.

Click [here](#) to download the Phishing attacks white paper

1. Security awareness training for staff



Security incidents almost never start like this



Security incidents very often start like this

1. Security awareness training for staff

- Training employees is a critical element of security as they are your first line of defence. They need:
 - to understand the value of protecting customer and colleague data and their role in keeping it safe.
 - a basic grounding in risks and how to make good judgments
 - understand the core principles of security good practise
- Confidentiality – Information should only be seen by those persons authorised to see it. Information could be confidential because it is proprietary information that is created and owned by the organisation or it may be customers' personal information that must be kept confidential due to legal responsibilities.
- Integrity – Information must not be corrupted, degraded, or modified. Measures must be taken to insulate information from accidental and deliberate change.
- Availability – Information must be kept available to authorized persons when they need it.
- Delivered in the form of:
 - In person training
 - Online training

1. Security awareness training for staff

- Security Awareness Training will:
 - Inform and/or reinforce good secure practise and behaviours; more importantly help them identify poor ones (very important for GDPR).
 - Identify potential phishing attacks.
 - Build understanding of Data protection
 - Assist compliance with FCA SYSC 5.1
 - Show you have applied the minimum level of effort – given the data you handle you would struggle to explain to any regulator (FCA or ICO) why all of your staff have not had security training
- Intelliflo customers have NO excuses
 - Free Security Awareness training course on the Intelliflo Academy eLearning platform

Free Security Awareness Training

There is a free Security Awareness Training Course on the Intelliflo eLearning Academy for customers to use with their staff. Email academy@Intelliflo.com if you have any questions.

The screenshot displays the Intelliflo Academy eLearning interface. On the left is a dark blue navigation sidebar with icons and labels for Home, Course Library, Achievements, Live Sessions, Messages, Collapse Menu, and Help. The main content area has a light grey header with the Intelliflo Academy logo and a user profile icon. Below the header, the breadcrumb 'Course Library / Security Awareness' is visible. The central focus is the 'Security Awareness' course card, which features a blue padlock icon, the title 'Security Awareness', a description: 'This course is designed to assist our clients with raising awareness of cyber and information security.', and a green 'Continue this course' button. To the right of the course card is a circular progress indicator showing '0%'. Below the course card are tabs for 'Modules' and 'Discussion'. At the bottom of the main content area, there is a search bar with a green magnifying glass icon and the text 'Security Awareness'.

1. Security awareness training for staff

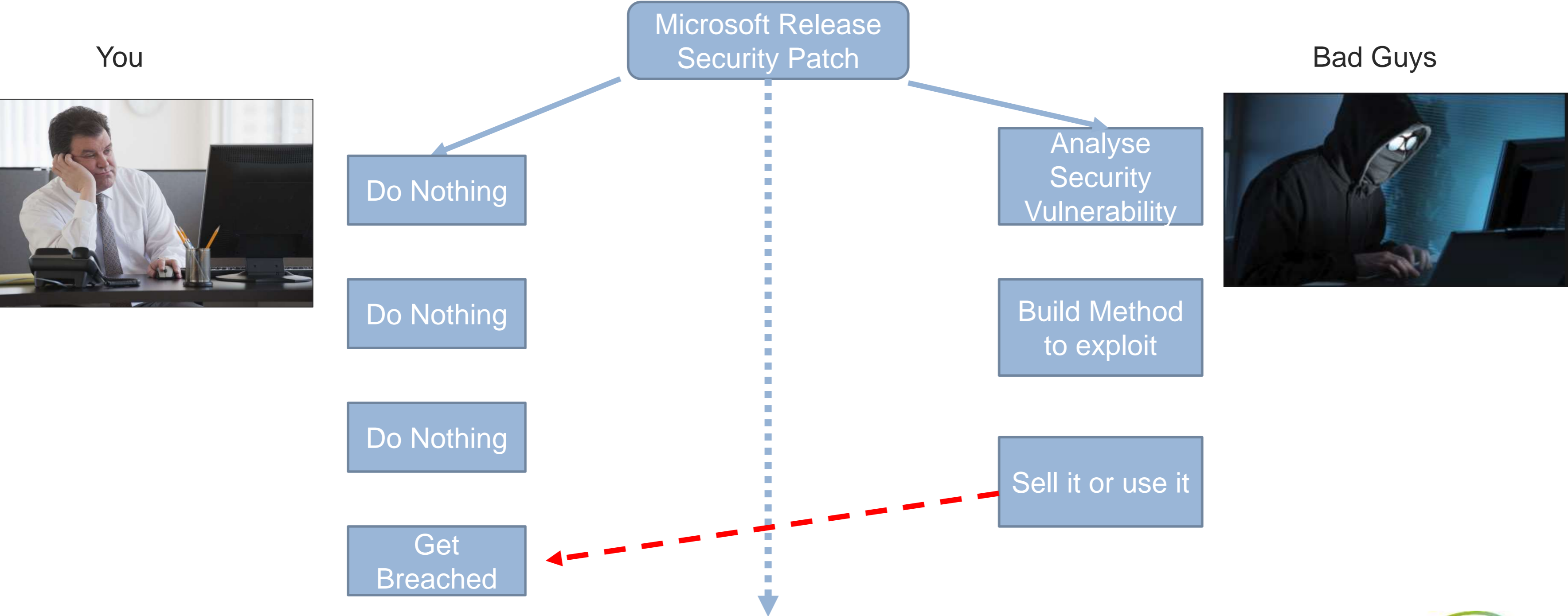


How to increase the likelihood of a security incident going unreported

2. Apply patches and updates

- What is a Patch?
 - A **patch** is a piece of **software** designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such **patches** usually called bugfixes or bug fixes, and improving the usability or performance
 - All major technology vendors release patches, either adhoc to respond to specific vulnerabilities or on a set schedule
 - Microsoft has patch Tuesday
 - Arguably the biggest challenge to Cyber Security – the patching paradox
- According to the Verizon Data Breach Analysis – 24% of all Cyber Security incidents would have been prevented by applying patches in a timely manner

2. Apply patches and updates – the race



2. Apply patches and updates

- Equifax data breach – 143million+ personal data records including UK residents
 - **Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.**
 - Patch released 10th March 2017, they were breached mid-May, knew in July, started telling people in September.
 - Under GDPR they could be looking at £88m fine for the breach, possibly additional £44m for delay in notifying AND they could be sued by individuals.
- WannaCry - 150 countries, 200k impacted systems 12th May 2017.
 - A patch was available in all supported operating systems ~2 months earlier, 14th March 2017.
 - A lot of impacted systems were running Windows XP, which hasn't had security updates on public release since

2. Apply patches and updates

Step 1 use software and applications that can actually receive security updates:

- Amazingly we still have 17 firms who use Windows Vista and 12 firms who use Windows XP
- Windows XP has not received security updates (excluding WannaCry) for 3.5 years!

Step 2 Apply patches:

- Ensure security patches are applied to all systems as quickly as possible, managing the risk
- **Desktops and laptops – within 24hrs of release. This can be a technically enforced policy**
- Other systems – within 1 month is good, 2 months is ok, no more than 3 months after release
 - Need to have process in place for deploying critical security patches asap
 - The speed of patching is becoming increasingly critical
- Don't forget mobile devices!

3. Use strong password protection on everything

Passwords are the keys to your important digital assets - almost every device, application or service you use will either mandate, or support some, form of authentication.

- Verizon's Security Report states 80% of hacking related breaches leverage stolen or weak passwords.
- They should be enabled on everything i.e. mobile devices too
- Enable two factor authentication if available

All Passwords can *eventually* be cracked but we shouldn't make it easy. The big password problem is that obvious passwords keep making the charts year after year.

Intelliflo analysis of passwords used in Intelligent Office shows incredibly common use of weak passwords in the form of a capitalised dictionary word followed by the number 1 e.g. Football1.

Top 25 most common passwords

- 1 123456
- 2 123456789
- 3 qwerty
- 4 12345678
- 5 11111
- 6 1234567890
- 7 1234567
- 8 password
- 9 123123
- 10 987654321

3. Use strong password protection on everything

Password Best Practise:

- Password best practise is no longer change your password every 90 days and to muddle up words by adding capital letters, numbers and symbols - so, for example, "protected" might become "pr0t3cT3d4!"
 - <http://www.bbc.co.uk/news/technology-40875534>
- Making people change their passwords frequently makes them choose weak passwords they can then do small variations on, that they then reuse across systems/devices
- Use passphrases or a random string of words:
 - Line from a song – Agirlwithkaleidoscopeeyes
 - Random words - Carmoneywindow

How Long to Hack my Password

Ever wondered just how secure your password really is? How long it would take someone to break into your email, facebook, or other sensitive materials that are online?

Find out right here. Simply start typing in your password and the form will tell you about how long it would take a brute force attack to get into your personal business.

Your password can be hacked in at the most
8.997439862812012e+25 years

How Long to Hack my Password

Ever wondered just how secure your password really is? How long it would take someone to break into your email, facebook, or other sensitive materials that are online?

Find out right here. Simply start typing in your password and the form will tell you about how long it would take a brute force attack to get into your personal business.

Your password can be hacked in at the most
11969669 years, 10 months

3. Use strong password protection on everything

Other things to consider to make it harder for those with malicious intent by:

- Adopting a risk-based approach to your passwords, for example, the most important ones should not be used for multiple systems or applications
- Not sharing passwords or using generic ones. When people leave, it makes it harder to remove people's access
- Ensure password lock out or retry delays are enabled where possible
- Not letting standard user accounts have administrative access on your network
- Using different passwords for home and work
- Checking if your log in details may have been compromised when breaches are publicised. The first thing hackers do with a new set of log in credentials is throw them around the internet to see if they work in other places. The Experian breach just gave them another 143,000,000 to try
- Never writing them down!

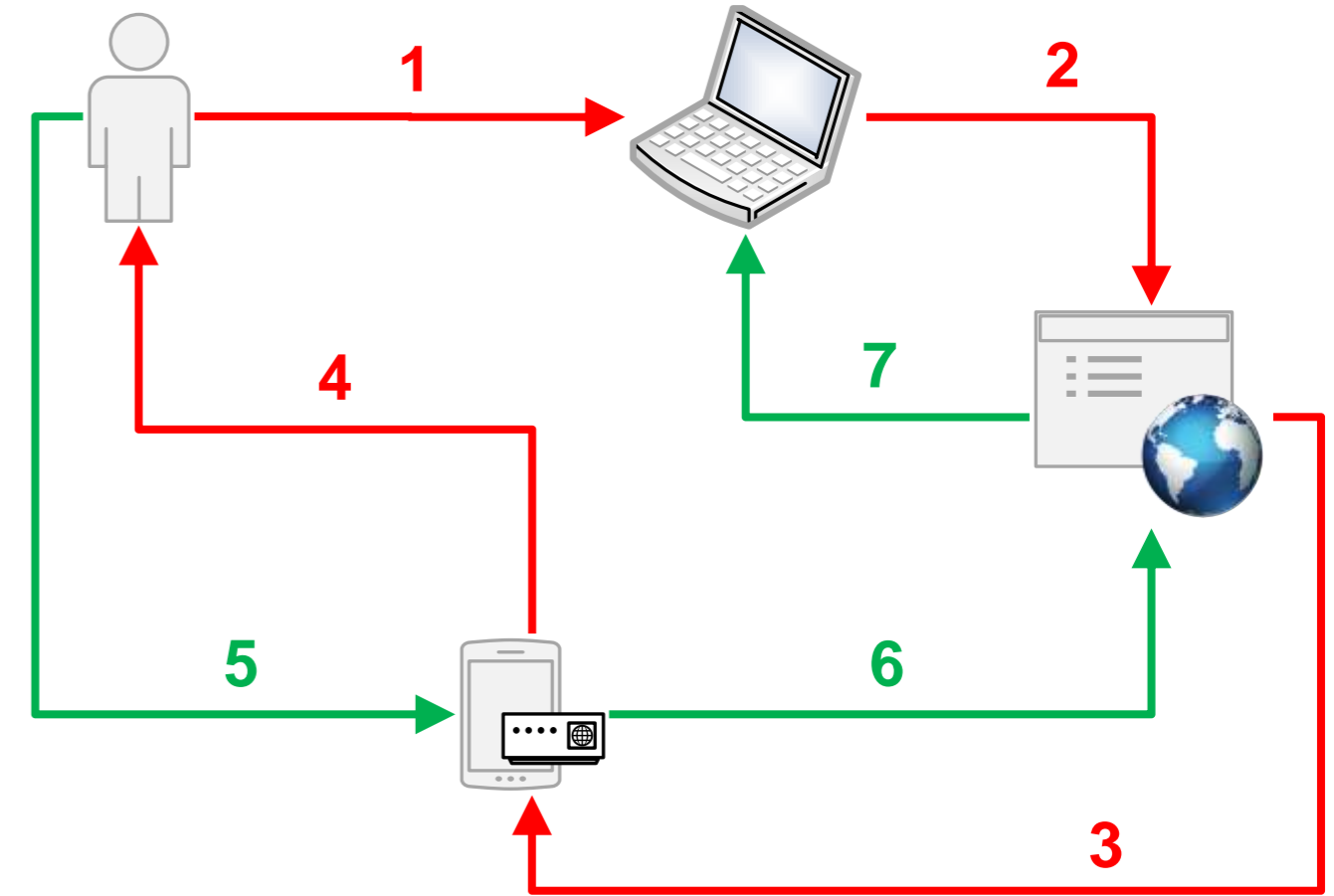
4. Two factor authentication

- Two factor authentication, 2FA, provides an additional layer of security for your important accounts by including something you have in the process
- It makes it harder for someone who has your 1FA (log in and password) to actually access your account(s)
- More and more providers are offering 2FA through your phone, removing the need for users to have a physical token
- Verizon breach analysis report states that 24% of all security breaches would have been stopped by 2FA
- Banks are now using phone apps to confirm that new payment recipients that are being set up are genuine
- Most recent big name example is Deloitte.



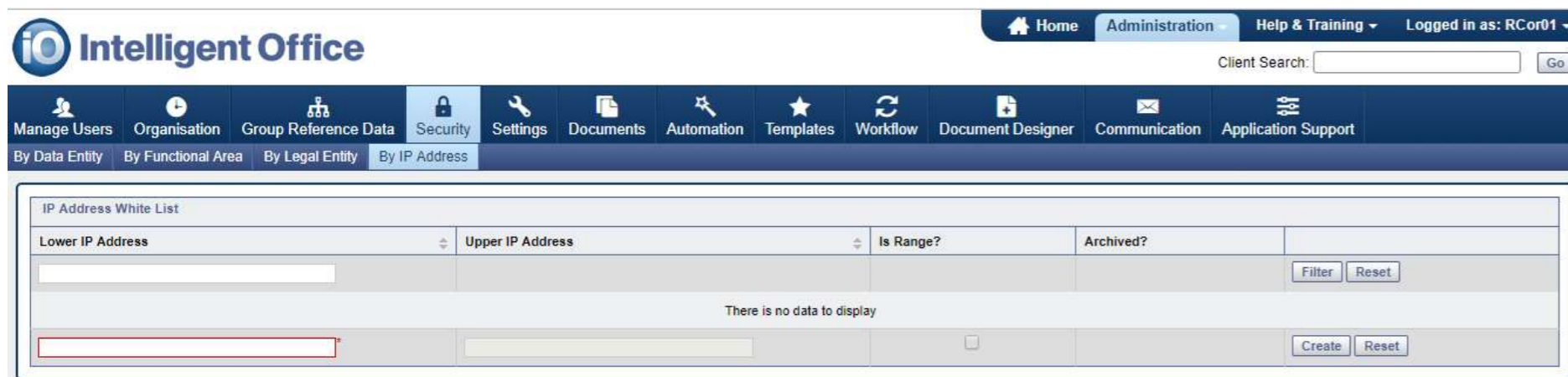
4. Two factor authentication

- 2FA works by require you to know something and to have something
- We use Duo - <https://duo.com/>
- Intelligent Office doesn't currently support 2FA directly but other customers have gated Intelligent Office behind 2FA by leveraging the IP restriction. Remote workers have to connect to Intelligent Office via their office VPN
- 2FA is currently on the Intelligent Office backlog



- 1 – User logs in
- 2 – Request sent to application
- 3 – Code sent to phone/token
- 4 – Code presented to user

- 5 – User responds
- 6 – Applications checks response
- 7 – Access given if response is correct



5. Back up your data

Resilience is an important part of any business, backing up your data is a key element of that resilience but taking back ups is not the end point ...

You must test that you are able to restore from back up effectively, which means:

- Within a timeframe you are happy with (availability)
- The quality of the data is good (integrity)
- You go back to a point in time that you are happy with

5. Back up your data

Having a good back up policy will help to mitigate the impact of and recovery from attacks such as ransomware:

- You need to consider where your back-ups are held, they are no good if the hacker can encrypt them too
- Intelliflo off sites last night's encrypted back-ups in Amazon S3 for absolute worst case
- GDPR is not just about confidentiality of data, it says you must have a set of risk-based, technical and organisational measures in place to ensure you can “***ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services***”.

6 and 7 – Leverage the cloud

Cloud used to be a dirty word but now it is how you get more secure.

- Cloud services are generally going to benefit from a well-resourced and focused security engineering team.
- Consider whether your IT security engineering team is going to be better or worse at security management for a major commodity product, offered - as a service - by the major vendor who developed it.
- Who is going to be able to roll out patches and hotfixes for security problems faster, and be more able to monitor for problems as a result? Even if your team is really good at this (well done!) is this always going to be true? Are you reliant on one or two key individuals?
- You get the *benefit of security at scale*. If the SaaS offering is well run, then the provider should be looking across all of their customers and connections to observe security patterns, to do transactional monitoring, and to learn what unusual activity on their platform looks like, meaning you should be protected before the problems reach yours. We often speak about the benefits of sharing threat information to protect each other. In a well-run SaaS provider with many customers, this should essentially be happening for you, behind the scenes.
- Cloud services provide an air gap from your corporate environment to your customer data
- Microsoft, as an example, spends \$1bn a year on cyber security for Azure
- The CIA have signed a \$600m contract with Amazon

6 and 7 – Leverage the cloud

Of course, you would say that you're a cloud provider...

<https://www.ncsc.gov.uk/blog-post/debunking-cloud-security-myths>

<https://www.ncsc.gov.uk/blog-post/brightening-outlook-security-cloud>

6 and 7 – Leverage the cloud

Intelliflo walks it's talk.... Our primary preference is for cloud delivered solutions, as such the following systems we use are all cloud delivered:

- Office365
- Telephony and communications system
- Finance System
- CRM
- Support Ticketing System
- Marketing platform
- Development toolset
- Knowledge and collaboration platform
- Project management toolset
- Product management toolset

8. Conduct due diligence

You can't outsource responsibility – a breach can still be down to you according to the FCA. The ICO, under GDPR, might also blame you, in full or in part, if something goes wrong.

When you are looking to use a third party to deliver products/services with/for you it is important that you carry out risk-based due diligence.

Some of the key areas to focus on are:

- What data do they actually need to collect/process on your behalf?
- Where will they be storing the data?
- How good is their security?
- Do they have good, tested back up and incident management plans in place?
- Do they understand their role as a data processor under GDPR?

9. Assume the worst, make a plan

Plan for the worst so that the process is smoother when something goes horribly wrong. Things get a bit confused and manic in the midst of an incident.

You need to know:

- Who the key people are that need to be involved, not just your own people but also outside advisors/specialists
- That the people involved know what they are supposed to do during an incident
- Your regulatory reporting requirements. For personal data, there are tougher requirements coming for breach reporting
- Where your data and systems are. Seems obvious, but when you are trying to assess the impact of an assessment you need to know in detail what you have and where it goes.
- You can contact the Intelliflo Security Helpline - security.help@intelliflo.com

10 Test rigorously

You talk the talk, but do you walk the walk?

- Only one way to find out if all of your efforts have put you in a position of good security; either simulate or actually attempt a break in and see what happens.
- Covers three key areas
 - The security awareness training given to your staff
 - Your security architecture and processes
 - Your response plan

10 Test rigorously

Testing your plan:

- Just having a well written plan that everyone has read and confirmed they understand doesn't mean it is going to work in reality
- Test it. Lots.
- Don't just test it quickly on a Tuesday lunchtime and skip over any bits that don't quite work as well. Do a thorough test at least once a year. Do it at (or simulate) a time and day that you know could be tricky for your company
- Actively identify areas for improvement, agree them and communicate them
- If everyone leaves at lunchtime on a Friday, use a Friday early afternoon scenario. It is pretty much a fact that serious incidents are magically timed to happen at the worst possible time and usually on a Friday!
- Do it in-house or employ the services of an external body, like NCC Group.

10 Test rigorously

Testing your security:

- Phishing exercises
 - Send phishing emails to your staff and see if they fall foul
 - Share the details with staff and use to target training
- Penetration testing
 - If you host your own systems then get security specialists to try and break in
 - Ask your service providers for dates and management summary of their last test
- Red Team testing
 - The ultimate test of your people, your security architecture and your response plans.
 - Typically, only some of your very senior staff know that you are paying security specialists to use all means to break in.

Useful links

- ‘Mitigating cyber risk in the financial services sector’ - white paper [here](#)
- ‘Phishing attacks and how to protect your organisation’ - white paper [here](#)
- ‘Don't be held to ransom....’ – white paper [here](#)
- Password Best Practise [here](#)
- Two factor authentication – [Duo](#)
- Debunking cloud security myths – National Cyber Security Centre – [here](#)
- Brightening the outlook for security in the cloud – National Cyber Security Centre - [here](#)
- Is your business ready for GDPR? Intelliflo page [here](#)
- Intelliflo GDPR consultation paper [here](#)
- Verizon’s 2017 Data Breach Investigations Report [here](#)
- Verizon’s website [here](#)