Client-centred cybercrime training

for Scottish

Small-to-Medium Sized Enterprises (SMEs)

Juraj Sikra

[Delivered as a part of PhD research]

Table of contents

09 May 2023

Introduction

The information contained within this client-centred cybercrime training booklet is basic.

Yet, cybercrime experience teaches us that these things are not obvious for far too many people regardless of their level of education or net worth.

In addition, I have a feeling that a lot of people could provide the correct answers for questions on how to avoid scams. It's not always the lack of knowledge that is the problem, sometimes it is the inability to correctly transfer it into the real-world setting.

If you are encountering the information within for the first time, then I hope it will be helpful in safeguarding you and your SME at least during the year it was published.

This booklet was designed in collaboration with a Scottish SME post-attack to address their learning and developmental needs. I am thankful for their open-mindedness and courage to collaborate with me on this research.

Juraj Sikra

Cybercrime affecting Scottish SMEs

When I refer to cybercrime, I am referring to computer facilitated crimes of dishonesty that have been committed for an economic incentive.

Scottish SMEs and Scots as individuals are often victims of cybercrime although these are rarely reported to the Police, which skews the official statistics and makes it look as if cybercrime was less of a problem than it really is.

Whilst official statistics find that Scottish individuals on average fall victims to lower value cybercrimes (i.e., £18 per person)[1], there have been individuals victimised for thousands and even millions of pounds. People are usually more forthcoming to report cybercrime when the amount of money lost is life-threatening or alternatively when they spotted that something is likely to be a scam before they have fallen

[1] Daily Star (2022). *Are you being scammed? Worst regions for cybercrime and how to avoid being a victim.*

victim[2]. Cybercrimes that fall in between those two categories tend to go underreported.

This booklet does not confer sufficient space to supply a detailed analysis of who the offenders and victims are. Instead, I will focus on Scottish SMEs for the most part whilst touching upon a few common cybercrimes affecting employees' private lives towards the end.

Scottish SMEs are frequent victims of cybercrime for various reasons. Firstly, the nature of their business usually requires that they maintain some form of online presence for informational and advertisement purposes. Hence, apart from having a website, Scottish SMEs will usually maintain multiple social media accounts for disseminating up to date information about the business. Cybercriminals use these sources to carefully profile the SME over a period of time much like a hunter will adapt his approach to the particular animal that s/he is stalking. Hence, Scottish SMEs face a

[2] Sikra, J. (2023). *The role of RNPAs in improving cybercrime reporting in Scotland.* 6th Cambridge Cybercrime Conference, 22 June, Cambridge – UK.

complex task of balancing what information is essential and useful for the provision of services and what information is excessive.

Cybertips for safely promoting your business online include supplying only information that is essential for the smooth running and promotion of your business whilst removing non-essential noise information. If you have a very precise idea of what information you are putting out, then you will have an easier time monitoring what is happening with it. Consider discussing the following questions with your team and trusted associates:

1. How does the information that I'm putting out increase my profit?

2. What evidence will I have that it has increased my profit?

3. If I was a criminal, how could I use the information about my SME to impersonate a credible other?

Answering these questions might help you discern what information should be publicised and what information is excessive.

Scottish SMEs will frequently fall victim to cybercrime and they will often respond in line with the principle "loose lips, sink ships[3]." Indeed, because of shame, stigma but also an ineffective governmental and policing strategy Scottish SMEs will aim to soldier on in silence after an attack. This perpetuates the problem of cybercrime because it means that patterns of offending are not identified. Hence, cybercriminals can use the same modus operandi to victimise other SMEs. In addition, not reporting cybercrime could result in Scottish SMEs unintentionally passing on the information of their clients to their attackers if they failed to contain and resolve the situation themselves.

So, who attacks Scottish SMEs and why? Simply put, it can be anybody. Nevertheless, consensus is that many of the attackers operate from abroad. They attack Scottish and more broadly UK SMEs as a way of practicing their trade much like a hunter might escalate from smaller

[3] Finney, G. (2020). *Well Aware: Master 9 Cybersecurity Habits to Protect Your Future*. Greenleaf Book Press. Adapted from p. 26.

animals to larger game[4]. Hence, cybercriminals will attack Scottish SMEs before escalating to the bigger game which are major corporations and government agencies mainly in the USA[5]. The USA receives the highest amount of cyberattacks from all countries worldwide.

Identifying your assets

If a Scottish SME is to safeguard itself effectively against cybercrime, then it needs to have a very precise idea of what it is safeguarding. Safeguards that do not include priceless and prized assets will not protect your company. Equally, safeguards that are excessive will make it difficult to monitor what is going on and will distract you from making your profits. Hence, the situation requires a balanced approach.

On page 8. in **Figure 1.,** I supply a visualised breakdown which offers some suggestions of how to think about your priceless and prized

[4] Vu, A.V. et al. (2023). *Getting bored of cyberwar: Exploring the role of civilian participation in the Russia Ukraine cyber conflict*. University of Cambridge.
[5] *As per footnote 4.*

assets[6]. You do not need to see this as gospel. Indeed, please do adapt these to your situation. The key principle is knowing why these are important for your specific situation as opposed to following the canonical set, which I laid out.

[6] Finney, G. (2020). Well Aware: *(…)*. Adapted, elaborated and extended from p. 27.

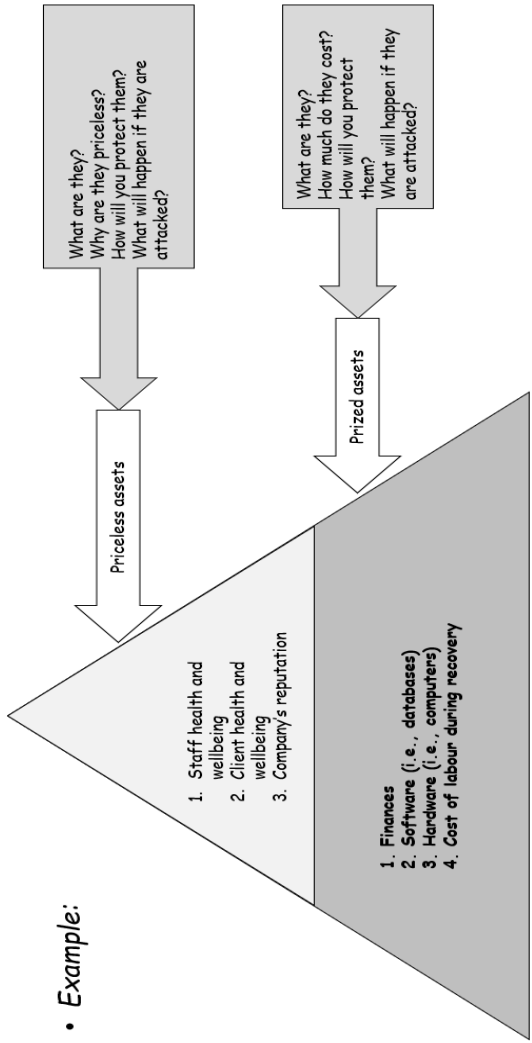

Figure 1. Example for analysing priceless and prized assets.

In **Figure 1.,** I breakdown my interpretation of priceless and prized assets.

Priceless assets are those that cannot be financially quantified. If a priceless asset is destroyed during a cyberattack, then there is a chance that the business will not recover and might have to close down. In many respects, the three priceless assets are interconnected. Priceless assets 1. and 2. pertain to staff and client health & wellbeing. If data are leaked during a cyberattack or if finances are misappropriated, then people's mental health and physical health will suffer. In fact, some people can become suicidal. Priceless asset 3. is the company's reputation. If a company falls into disrepute, which can happen if sensitive client data is leaked, then this can have terminal consequences for the SME.

Prized assets are those that can be financially quantified although in some cases the process might be very effortful. Prized asset 1. are finances. If say, you transfer a set amount of cash to a fraudulent invoice, then you will know precisely how much you lost. Prized asset 2. is software, which are usually databases. Whilst

the reinstallation of software can be very cheap and potentially free, the chaos caused to your business by losing track of clients' records can result in indirect harm in tens of thousands of pounds[7]. Prized asset 3. is hardware such as computers. These are easy to financially quantify and based on your turnover can be a cheap asset to replace. Prized asset 4. is the cost of labour required to restore the systems. People who have not been attacked readily discount this asset. In fact, if you were attacked, you will spend a significant amount of time and emotional resources to restore your business. Hence, time that could be devoted to making a profit, will be dedicated to getting back on track and simply surviving.

[7] Sikra, J. (2023). *Improving cybercrime reporting in Scotland: The victims' perspective.* DSMS, 14-16 June, Glasgow – United Kingdom. [in press]

Understanding harm to your assets

The following segment offers an indicative list of common cybercrimes that affect Scottish SMEs although this is not an exhaustive list as a lot of scams will be tailored to the specific business. Also, the boundaries between these are not clear cut and their definitions evolve somewhat as time goes by. Knowing the names of these cybercrimes can put you in a better position to report them accurately.

1. Phishing[8]: Spelt with a 'Ph' as opposed to an 'f' at the beginning. This cybercrime's modus operandi is that cybercriminals send out tons of hyperlinks to unsuspecting victims much like you would throw a net into the sea during a fishing expedition to see how much fish you can catch. Clicking on the link might result in the downloading of ransomware (discussed next) or it can take you to a cloned website, which might get you to engage by releasing your details.

[8] https://www.ncsc.gov.uk/guidance/phishing

2. Ransomware[9]**:** Much like taking somebody hostage and demanding a ransom, ransomware is a malevolent software that does just that to your computer by encrypting your systems and locking you out. Ransomware is usually downloaded via a phishing link, but there are ways it can get into the computer too. Most ransomware originates from organised crime gangs, who perform it using a modus operandi like that of the 1920s racketeers threatening to burn down restaurants refusing to pay up for "protection." Even if a victim pays the ransom, there is no guarantee they will receive their data.

3. Whaling[10]**:** This crime's name is derived from the principles of phishing. Except, unlike in phishing, where the aim is to cast the biggest net possible, during whaling the operation is specifically tailored to a concrete business/ business owner. Hence, it is more like going after a whale. The modus operandi is that the

[9] https://www.ncsc.gov.uk/blog-post/ransomware-taskforce-rtf-announce-framework-to-combat-ransomware
[10] https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it

cybercriminal will successfully impersonate either a business owner, an important stakeholder, or some other powerful function. After this, the cybercriminal will engage less powerful employees in an organisation and get them to transfer the company's funds under a legitimate pretext. When it comes to whaling, the less powerful employees are at risk for getting blamed by their employer.

4. Business e-mail compromise (BEC)[11]: This cybercrime can be connected to whaling, but its modus operandi varies somewhat. Whereas in whaling the cybercriminal is impersonating a powerful function with the use of deception, in BEC the cybercriminal creates the appearance of using company's boss' e-mail account and is using it to request that funds be transferred by employees similarly to whaling.

5. Spyware[12]: This is a form of malicious software that is often downloaded by clicking a

[11] https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf

[12] https://www.ncsc.gov.uk/news/cyber-experts-warn-of-rising-threat-from-commercial-hacking-tools-over-the-next-five-years

phishing link but can be transferred via a simple USB stick too. Its purpose is to monitor the users' behaviour and collect passwords as well as gain access to other sensitive data.

6. Malware: This is a generic term pertaining to malicious software. All forms of malicious software that we discussed thus far can be generically referred to as malware.

7. Data breach: This can constitute a separate cybercrime or is a consequence of a cybercrime. When a state employee looks up his ex-girlfriend on a national database, then this data breach is a form of cybercrime even though there was no financial incentive. On the other hand, if a ransomware gang publishes the details of a company's clients on the web, then technically this is a ransomware attack, but the accessing and release of the data is also a data breach. All financially motivated cybercrime entails data breaching.

Safeguarding your assets

To safeguard the SMEs priceless and prized assets effectively, we need to understand that harm can come from the physical world and

from the cyber world. The two are not separate, rather the cyber world originates from the physical world. The boundaries we should instil in the physical world will be similar in the cyber world although we may use some software tools to help with the latter. Please consider **Table 1**.on the following page, which explains the different types of threat to your assets and how to safeguard against them.

Physical world threat:	**Physical world safeguards:**
This is anybody who is not a formally designated recipient of data pertaining to assets including close acquaintances, family, and colleagues.	Restructuring the physical environment in a way that focuses information only towards designated recipients and *enforcing consistent boundaries*. e.g., files are kept in the office rather than a public area
Cyber world threat:	**Cyber world safeguards:**
This is anybody who is not a formally designated recipient of data pertaining to assets including close acquaintances, family, and colleagues.	Same as above. But it also includes cyber tools such as insurance, access controls, backups, VPNs, effective passwords, psychological techniques, the use of secure payment methods etc. e.g., customer financial details are not available to staff who don't need them.

Table 1. An analysis of threats and safeguards.

Notice how in **Table 1.** I have never identified cybercriminals as posing a threat to your assets. Can you guess why? The main reason is that most people only identify a cybercriminal once they were victimised and by that time it can be too late and their assets have come to serious harm. Therefore, it is better to engage

in securing your environment against any illegitimate forms of access regardless of whether they are motivated by negligence or cybercrime. Scottish SMEs that understand the value of a consistent and boundaried cyber-approach to their assets will be in a better position to safeguard them against harm.

Much like in the case of **Figure 1**.on page 8., where I have supplied an example of priceless and prized assets, **Table 1**. is indicative and you are welcome to adapt it to your situation.

Regardless, you should create an exhaustive list of the roles people in your SME can have and the circumstances in which people in those roles can access different company data[13]. It is okay to make a couple of discretionary exceptions to this rule but if you find yourself making exceptions all the time, then it is either a bad rule, or you need to reconsider your approach.

[13] Finney, G. (2020). Well Aware: *(…)*. Adapted from p. 76.

Safeguarding with psychology techniques

It is important to set time aside when you are doing work on the computer, particularly your e-mails. Ensure that you are focused on solely that task and do not multitask. Be prepared to tell people that are needlessly distracting you that you require the space and time to complete the task safely. Then:

1. **Slow down and frown**[14]**:** When we frown, we subconsciously activate a part of our brain called the amygdala, which enables us to focus attention more effectively.
2. **Look for red flags**[15]**:** E-mails that create a sense of urgency or ask you to bypass normal processes are all red flags that you might be targeted by a criminal.
3. Try to do tasks that require most focused attention in the morning, but no later than 15:00[16].

[14] Finney, G. (2020). *Well Aware: (…)*. Adapted from p.62 .
[15] Finney, G. (2020). *Well Aware: (…)*. Adapted from p.57.
[16] Finney, G. (2020). *Well Aware: (…)*. Adapted from p.65.

Safeguarding with effective passwords

Passwords[17]**:** Everyone should have a unique login name and password to enter the company's systems. Password sharing is unacceptable as it dilutes responsibility for the activity that takes place during a person's login. Crucially, it can make someone culpable for something they have not done. Never remain logged into the company's system if you are not working on it. Always logout or lock screen even if you're just going to get a glass of water.

Using strong passwords[18]**:** For a long time, it was suggested that people should use extremely complex passwords to secure their systems such as "XC45$%?@Qdfg1" to use an illustrative example. The problem was that whilst it kept the cybercriminals out, people often forgot them and got locked out too! Therefore, researchers recommend that you use a password that is made up of three or more random words (e.g. open a random book at a random page and pick a random word three

[17] Renaud, K. (2023). *Information Security [PowerPoint Presentation]*. Adapted from p. 30.
[18] Renaud, K. (2023). (…). Adapted from p. 31.

times). You should also use a two-factor authentication process.

Safeguarding with software

VPNs (Virtual Private Network): The purpose of a VPN is to encrypt your data as it travels between various internet sources. What kind of VPN is appropriate depends on the company's network structure and working practices. There are many VPN products out there from reputable brands so it is important to choose one that is established. Thanks to VPNs we minimise the chances of cybercriminals collecting intelligence about our behaviour, which they can use against us. It is like a smoke screen in military operations. There are many VPNs on the market with a varied price tag. Major software providers will also offer their own VPN products. Where appropriate the company should configure a VPN on applicable systems.

PayPal[19]**:** It is advisable to conduct online purchases via the PayPal service, which is a widely accepted free intermediary for online

[19] https://www.startupguys.net/pros-and-cons-of-paypal/

transactions due to its ability to safeguard clients' information. However, all solutions have some disadvantages as does PayPal. For example, withdrawing your balance takes time unless you pay an extra fee. Be sure to familiarise yourself with both pros and cons of this service.

Antivirus: An up-to-date version of antivirus is crucial as is running regular updates on it. Microsoft Windows comes with Windows Defender antivirus built in.

Safeguarding with the law

The Data Protection Officer (DPO)[20]: If you are unsure what data is safe to disclose and under what circumstances, then appoint a DPO who will be required to ensure the organisation's compliance with data protection regulations. If you are under pressure to disclose data and do not have access to a DPO, then it is advisable to safeguard it. Otherwise, you run the risk of committing a data breach and breaking the law.

[20] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/accountability-and-governance/data-protection-officers/

Cybertips for resolving personal data requests when you do not have access to the DPO. These requests can usually be of two types, which are business and personal related:

<u>Business requests:</u> For example, someone you have never heard of makes a legitimately sounding request for your colleague's or manager's details to follow up their query. If you don't know what to do, then take down their details and say you will pass on the query and either you or the sought person will get in touch within a specified timeframe. Then keep your promise and provide closure to the enquirer when you get the information.

<u>Personal requests:</u> For example, one of your clients requests the data of another client. Unless you are a networking agency, you must politely and resolutely refuse this and where it sounds logical respond by saying that: "We can neither confirm nor disconfirm whether the person you are looking for is our client."

At the end of the day, you are an SME, not the Wall Street stock exchange. So, take your time when somebody is pressuring you for a quick response!

Cyberinsurance: Fortunately, insurance companies offer cyberinsurance for cases where an organisation might suffer an attack. It may be helpful to enquire about this from a reputable insurer and take out insurance. The benefit of insurance, among other things, is that it can be used to pay for an elite private company that can help more effectively than the Police and will also be in a better position to advise on issues regarding reputation management post-attack. Reputation management can be especially useful in cases of ransomware where sensitive client data has been leaked onto the web.

Cybercrime affecting employees' lives

Whilst the bulk of information in this booklet is geared towards the needs of SMEs, the latter employ individuals who can also fall victim to cybercrime, which can result in various problems that could impact their job performance. Hence, I have compiled three examples of prevalent scams based on current intelligence that affect a wide population of Scots. These are by no means exhaustive; this is particularly the case because new scams are rolled out daily. Yet, it is my hope that by discussing three particularly prevalent ones, I can contribute to keeping the readers a little bit safer whilst online and hopefully transfer some of my scepticism towards online information along the way. It is the quality of scepticism that researchers see as being more preventative as opposed to carrying encyclopaedic knowledge of what cybercrimes are currently running rife[21].

The nature of various scams taps into people's most basic needs as well as major societal

[21] Finney, G. (2020). *Well Aware: (…)*. Adapted from p.62.

trends. Here are three examples to illustrate the point, with an explanatory note:

Investment scams[22]**:** It is a basic human need to want more money for less work. Cybercriminals know this very well which is why they populate social media with countless advertisements for a range of investment opportunities. In line with major societal trends, the cybercriminals frequently invite victims to invest in cryptocurrency. In reality, these are all scams carried out with various levels of marketing appeal. Do not be fooled by professionally sounding language, charts, graphs or even persuasive in-person meetings with flashy paper handouts and free promotional ballpoint pens. You are not on your way to becoming rich, you are being expertly groomed. There is no easy money. All money is hard and having more money than one's peers is extremely hard. It requires the mastering of a highly desirable skillset and then executing that skillset by working a lot more and potentially risking a lot more than everybody else. There may be a few exceptions to the rule, but they

[22] Sikra, J. (2023). *(…)*. Cambridge – UK.

will not come in the form of an investment opportunity via social media.

Romance scams[23]**:** It is a basic human need to pursue an idea of a perfect romantic and sexual relationship. Social media and the internet have made the pursuit of these opportunities more accessible than ever before. A lot of people have found love this way. However, be careful not to develop strong feelings for people you have not met in person. Instead, try to meet in person as soon as possible in a well-known central location during broad daylight. If a picture speaks a thousand words, then conversing with someone for an hour speaks novels about who they are. Before sharing any photos or videos of yourself consider: "If this was made public would I be okay with it?" If the answer is "No", then use an Emoji instead. That way you reduce the risks of becoming a victim of sextortion, which is the blackmailing of a person with intimate photos. Also, legitimate prospective partners would be embarrassed to ask for money or come across as needing it.

[23] Sikra, J., Thomas, D., Renaud, K. (2023) UK Cybercrime, victims and reporting: A systematic review. *CCJ*, 1(1), 28-59.

Therefore, if a person is starting to come across as financially needy or even requests money before you get to know one another properly, then it is safer to assume you are dealing with a romance scam.

Cyber-enabled sale of counterfeits[24]**:** It is a basic human need to want to look and dress cool. To address this need, people will frequently invest in designer clothes because it is simpler than cultivating one's own unique style. There is a societal trend that if a plain t-shirt has a miniature crocodile on it, then it is superior to most other plain t-shirts devoid of the symbol. Cybercriminals understand the basic human need to take fashion shortcuts. This is why they collaborate with expansive organised crime networks to flood social media with the sales of counterfeit goods, which a victim can purchase at a fraction of the price of the original. In reality, there are several victims. Firstly, the retailer, which is missing out on profit and possibly suffering disrepute if there are people running around with a miniature crocodile facing the wrong way. Secondly, the government is

[24] Sikra, J. (2023). *(…).* Cambridge – UK.

losing out on tax. Thirdly, the buyer was tricked into buying a fake, which may also result in an adverse skin reaction depending on the production techniques of the unknown manufacturer.

In summary, cybercriminals will have a very good grasp of people's needs and the issues that are most salient in society. They will combine the two to amplify their impact and make a victim more likely to engage. Money and relationships that are hard to come by in the real world, will be hard to come by online. Hence, be weary of online information and telephone calls which create a sense of positive excitement (e.g., a fantastic investment opportunity) but also a sense of frightening urgency such as the need to transfer finances by a governmental body who is accusing you of a serious crime, which is also a common scam.

Reserve your sovereign right to take your time. Slow down and frown. Legitimate people will not pressurise you. Speak to people you can trust before you decide to transfer finances. If you have already engaged with, who you think is a scammer, then overcome your feelings of

shame. Know that you are not to blame and seek help. Do not sit with what is happening to you alone because the modus operandi of cybercriminals is to isolate their victims so that they remain submissive.

Reporting cybercrime

Whilst Police Scotland may not assign you with a crime reference number if you report a cybercrime, there are things you can do to increase the chances of receiving a crime reference number, which will be helpful both for the investigation as well as claiming insurance after an attack. Under no circumstances should you start your own investigation by attempting to autopsy the attacked system. You must go completely hands off as soon as you are sure that an attack has started. Simply document what you are seeing as it is taking place and avoid interfering with the computer.

Here are some simple steps to follow if you get attacked. Do this before calling the non-emergency 101 number:

1. Take a note of the date and time when you noticed an incident unravelling such as your systems becoming locked.

2. Make photographs using your mobile phone of any information that comes up on the computer evidencing that you are being victimised (e.g., a ransom note or randomly looking code that obstructs your access to files).

3. Make a list of your priceless and prized assets that are threatened by the attack. You should prepare this during or after the training not after you get attacked. When you get attacked, these should be readily available. They will not have changed massively since you wrote them down.

4. Write down how you are feeling. Reports to the Police that emphasise your personal distress are likely to elicit a quicker response than impersonal interactions.

5. When you have everything ready, pick up the phone and make the report to 101. Supply them with all the evidence. Also, retain the evidence for your insurer, so that they can process your claims. If you can show you've collected

evidence during the crime, then this can carry a bit more weight as evidence collected after the crime. But as I said, do not start investigating or interfering with the system when you are sure it has come under attack because if it transpires that you were trying to fix what you knew was an attack, then that can count against you before the Police and the insurer.

Lastly, if the Police come and investigate, they are likely to interview staff under caution. Whilst this may feel like you are getting blamed, remain aware that this is a matter of standard procedure[25].

Conclusion

This short booklet offered a condensed view for the Scottish SMEs in terms of the key issues surrounding cybercrime and cybersecurity to reduce their chances of being attacked but also so that they know how to correctly report an attack.

[25]Sikra, J. (2023). *(…).* Cambridge – UK.

Acknowledgements

The **'Client-centred cybercrime training'** which this booklet relates to is part of my broader national PhD research project into:

'Improving cybercrime reporting in Scotland.'

I wish to thank Dr D Thomas and Prof K Renaud of the University of Strathclyde for showing me the ropes of this exciting sphere as well as Dr J Carletta of the University of St Andrews for our work into the new Scottish cyber-resilience curriculum from which I have gained so much.

The information within, if not otherwise referenced, is directly tied to the precious knowledge these people have shared with me during their lectures, seminars, supervisions, and informal conversation.

Funding:
The University of Strathclyde £56,154.89.
Scottish Institute for Policing Research (SIPR) £38,154.92.
University of St Andrews £2,559.06