OFFICIAL REPORT
AITHISG OIFIGEIL

Criminal Justice Committee

Wednesday 14 May 2025

Session 6

The Scottish Parliament
Pàrlamaid na h-Alba

Wednesday 14 May 2025

CONTENTS

CRIMINAL JUSTICE COMMITTEE
15th Meeting 2025, Session 6

CONVENER

*Audrey Nicoll (Aberdeen South and North Kincardine) (SNP)

DEPUTY CONVENER

*Liam Kerr (North East Scotland) (Con)

COMMITTEE MEMBERS

*Katy Clark (West Scotland) (Lab)
*Sharon Dowey (South Scotland) (Con)
*Fulton MacGregor (Coatbridge and Chryston) (SNP)
*Rona Mackay (Strathkelvin and Bearsden) (SNP)
*Ben Macpherson (Edinburgh Northern and Leith) (SNP)
*Pauline McNeill (Glasgow) (Lab)

*attended

THE FOLLOWING ALSO PARTICIPATED:

Miles Bonfield (National Crime Agency)
Assistant Chief Constable Stuart Houston (Police Scotland)
David Keenan (Arnold Clark)
Jude McCorry (Cyber and Fraud Centre Scotland)
Adam Stachura (Age Scotland)
Nicola Taylor (CyberScotland Partnership)
Chris Ulliott (NatWest)

CLERK TO THE COMMITTEE

Stephen Imrie

LOCATION

The David Livingstone Room (CR6)

Scottish Parliament

Criminal Justice Committee

Wednesday 14 May 2025

[The Convener opened the meeting at 10:01]

Decision on Taking Business in Private

The Convener (Audrey Nicoll): Good morning, and welcome to the 15th meeting in 2025 of the Criminal Justice Committee. We have received no apologies this morning, and Katy Clark joins us online.

Our first agenda item is to consider whether to take items 4 and 5, which are a review of evidence and consideration of a draft report, in private. Are we agreed to take those items in private?

Members *indicated agreement.*

Cybercrime

10:02

The Convener: Our main item of business is an evidence session on the challenges facing business and vulnerable individuals in Scotland from the threat of cybercrime. The session will not cover elements of child exploitation, as the focus will be on businesses and individuals that are at risk of being targeted by cybercriminals.

As we are all aware, cybercrime is becoming more prevalent and sophisticated every year. Its victims are across our society and range from vulnerable individuals to small, medium and large-scale business, as well as public and voluntary sector bodies. The aim of this session is to inform parliamentary debate on the issue by hearing from those who are at the coalface of responding to cybercrime. I hope that we will gain insights into the methods and impacts of cybercrime, what we are likely to face in the coming years, and what more the Parliament and Government can do to help to keep Scotland safe from that threat.

I am pleased to welcome our witnesses. We are joined by Adam Stachura, associate director of policy, communications and external affairs at Age Scotland; David Keenan, chief information officer at Arnold Clark; Jude McCorry, chief executive of the Cyber and Fraud Centre Scotland; Nicola Taylor, member of the CyberScotland Partnership; Miles Bonfield, deputy director at the National Crime Agency; Chris Ulliott, head of cybersecurity at NatWest; and Assistant Chief Constable Stuart Houston, who is with Police Scotland’s organised crime and counterterrorism intelligence division.

I refer members to papers 1 and 2 and thank all the organisations that provided us with written evidence in advance of our meeting. I intend to allow up to two hours for the session.

I begin with a general question to get us started. For ease, I will ask Jude McCorry to respond first. I will then go to Miles Bonfield and ACC Stuart Houston to set the scene. Cybercrime is a vast topic, and we probably all know someone who has been targeted or who works in an organisation that has been affected. What are the most significant risks facing individuals such as the elderly or vulnerable people? What are the most significant risks for businesses? How might cybercrime develop in the coming years?

Jude McCorry (Cyber and Fraud Centre Scotland): The first question is about older people. Some of the most vulnerable people in our society are being targeted, which is probably what pulls at our heart strings the most. Usually, those crimes are being committed by serious organised criminals. In the past two years, cyberattacks targeting older people have originated not in Scotland but from the rest of the United Kingdom and outside that. The biggest scams have involved investment fraud—such as gold investment fraud—and romance fraud. I have been talking about this with Adam Stachura. Sometimes, people are lonely, and older people can feel as though they have someone to speak to who will help them and take an interest in their finances.

Collectively, we are trying our best to reach out to as many people in the older generation as we can, but it is difficult to do that in the world of social media. We have to look at how we can reach individuals directly, as well as reaching their families, friends and neighbours. As we saw during Covid, many older people do not have any human interaction, so a lot of work needs to be done. There is no point in thinking that the criminals will not go near older people, because they are unscrupulous and will target anyone. Older people seem to be very susceptible and vulnerable to cybercrime.

Today's meeting is timely, but it was set up before the big hacks on businesses took place, so most of the papers for it do not include anything on Marks and Spencer or the Co-op. In the past two weeks, West Lothian Council and the City of Edinburgh Council have also been affected by cybercrime. I thank them for the work that they have done. I am a parent of a child who is at a school in the West Lothian Council area. She is very disappointed that the exams went ahead, but I am not, and neither is any other parent. Well done to those teams. It is very easy to judge organisations that have experienced cyberattacks, but the work and effort that the councils have put in and how well they have kept everything together over the past few weeks is admirable.

For larger companies, such as Marks and Spencer and the Co-op, people immediately look at the data aspects. Yesterday, Marks and Spencer announced that some customer data has been affected. We do not have further detail, but we know that it was not financial data. However, everyone is in an uproar about the data. I am not saying that data exfiltration is not harmful, but it happens every day. We are hearing about it only because Marks and Spencer and the Co-op are large organisations that have an impact on individuals in Scotland.

However, we need to think about the broader destruction and damage for organisations and not just the data element. Data exfiltration is very damaging, but we should also consider the broader impact of cybersecurity attacks. In Scotland, islanders have been left without food because Co-op stores have been empty. We are coming up to the high season for tourism in Scotland, so there will be further issues when people start to visit the islands and there is no food in the stores. We also have to consider the human impact of cybersecurity.

If we are looking for something positive from the attacks of the past few weeks, one thing is that I hope that everybody, not just us as a team and others who work in cybersecurity, will start to take the issue seriously. It has an impact on everybody in society, so I hope that people will start to take cybersecurity and personal resilience more seriously.

Miles Bonfield (National Crime Agency): I will give the threat vectors from an international and national perspective. That is captured in the national strategic assessment of serious organised crime that the National Crime Agency issues every year. It was most recently issued in March 2025, I believe.

Online connectivity underpins a wide variety of offending, including cybercrime and fraud, and enables almost all serious organised criminality in some form. SOC offenders are increasingly exploiting advances in technology to access victims. I am using particular language from the analytical product, but it is clear that the online nature of our lives means that extra-territorial offenders can access communities in Scotland very easily, and that is a threat vector that we need to recognise and respect.

Ransomware that is used for financial gain remains the foremost serious organised crime cyberthreat to the whole UK, including Scotland. What we mean by ransomware is what we have seen in the recent public discourse. It is a piece of malicious software that is placed on a system that either excludes the operation of that system and/or exfiltrates data. The motivation is financial gain for the criminals. It is almost certain that the threat from cybercriminals who are based in the UK, including in Scotland, and in other English-speaking countries such as the USA, has increased relative to 2023.

The infrastructure that we use to enable our lives, the commonality in the use of that technology and the commonality of language in our social interactions and in technology are enablers of wealth and business, but they also provide an opportunity that has been exploited by unscrupulous and immoral criminals for illicit gain.

The National Crime Agency's function, as given by the Parliament, is to provide the national strategic assessment and to lead and support the fight against serious organised crime for the United Kingdom, in partnership with others. In that space, it is important that we have a strong relationship with the police service in Scotland, and indeed we have that. If you wish, convener, in my later responses, I can talk a little bit more about how that manifests itself.

The Convener: On that note, I will bring in ACC Houston from Police Scotland to cover the enforcement role of Police Scotland.

Assistant Chief Constable Stuart Houston (Police Scotland): Good morning, convener, and thank you for the opportunity to speak about the issue. We have heard from colleagues about the change in perspective of cybercrime. It is useful to see the difference between cyber-enabled crime—95 per cent of fraud is now committed online, which means that it is cyber-enabled—and the cyber-dependent part, which covers attacks with malware and real efforts to attack and exfiltrate data.

The picture is changing. We will all have had various text messages from a well-known parcel company saying that they have missed a delivery—indeed, members have probably had one this week. That is very much the cyber-enabled aspect. It is important for us to follow the 4P mechanism—pursue, prevent, prepare and protect—and we have heard about various parts of that in what my colleagues have said.

To answer your question about the criminal justice outcomes, these crimes are often borderless and are, on occasion, perpetrated outwith the UK. We have had cases of denial-of-service attacks that have been orchestrated by individuals within Scotland. Someone was convicted of that as recently as last year.

Quite often, a network of people are involved in the larger ransomware attacks. In the past, organised crime groups would operate in networks of people who knew one another, but we need to be alive to the fact that people now often operate in networks where they have only seen someone through a screen. That is a different approach, and it is important for the first P in our methodology—pursue.

10:15

The action that we take is often to gather the threat intelligence and to find out the weaknesses in systems. If there is a text message that is being sent this week, is there a theme there, and can we push out a prevention message on the back of it to ensure that vulnerable people are not being taken in by anything that is happening or exploited in any way?

We have touched on the impact that there can be on businesses. We are there to investigate that and to get an outcome, but a big part of that involves helping businesses to recover.

The Convener: That is really helpful scene setting. We have two representatives with us who have been at the sharp end of cybercrime: Mr Keenan and Chris Ulliott. Before I open up to members' questions, I will bring both of them in. I am not necessarily asking you to talk about the detail of what happened, but I am interested in the impact on your respective organisations of being targeted.

Chris Ulliott (NatWest Bank): As a big bank in the UK, we are targeted all the time. Some facts and data can perhaps give a sense of scale. As a bank, we analyse every single email that enters our estate, and we process it, looking for malicious content. We block about a third of the emails—which is millions a month—because they are believed to be the start of an attack against our staff.

Looking outside our network at the attacks that are probing our estate, we average about 100 million attacks per month that try to break past the organisation's defences. As a result, we have to make a huge on-going investment. I am very fortunate in that our bank has resources that I can use to defend against those attacks. Hundreds of people, with costs of millions of pounds per year, are defending the bank and our customers' money. I am very alive to the fact that, when I look to my customers and other organisations across Scotland, they cannot make that scale of investment.

That is the scale of the problem that we are trying to handle and manage. You might then ask how everybody else is able to do that, particularly when we discuss individuals and some of the victims who we have talked about. We are seeing the advanced use of artificial intelligence to create fake documents that look very realistic. We are seeing advances in fraud, with fraudsters from overseas using artificial intelligence to change their appearance in real time. They can do a video call with a victim in the UK, appearing as an elderly British gent talking to an elderly lady, for instance, but the person behind it is not like that in reality; it could be a youngster or somebody elsewhere in the world.

The advances in technology are enabling what were traditional crimes but in new and very convincing ways, and that presents a set of problems, such that we are essentially in a continuous arms race, trying to protect the bank and our customers.

The Convener: Those are fascinating and eye-watering numbers.

David Keenan (Arnold Clark): Good morning, and thank you for the opportunity to come to the committee as a witness today. Arnold Clark was the victim of a serious cyberattack in December 2022. I do not want to downplay the theft of data, which occurs in many incidents, but the real impact for the public is ultimately the loss of services. Jude McCorry talked about the issues with the Co-op and the empty shelves in remote areas of the country.

In the days immediately after the attack on Arnold Clark, when we were unable to operate our systems for a period, more than 4,000 customers were expecting to come and make use of our services. More than 700 people who had bought a car were expecting to take delivery of that vehicle. Some 2,000 people who either had their car in for a service or had booked in to have their car serviced were unable to have that work done. We were unable to provide our rental service to more than 1,500 people who had planned to make use of it, many of whom were holidaymakers who were travelling from abroad. They expected to arrive at Glasgow or Edinburgh airport and to come to our local rental branch to collect the car that they had booked for rental.

That was the direct impact on customers. As a business, we were left without our systems for seven days immediately after the incident, and we got back to about 30 per cent capacity relatively quickly. However, the recovery from the attack was a multimonth effort for what is a significant information technology team. At the time of the incident, we had well over 200 members of staff in IT, with a multimillion-pound budget and 12 members of staff who were dedicated to cybersecurity, but that still was not enough to protect us.

The committee has heard the kind of numbers that Chris Ulliot is dealing with. What we face is not quite at that scale, but we are seeing similar things. Ultimately, a cybercriminal has to be lucky only once, but we have to be lucky against every single attack.

The Convener: Thank you. I am sure that members will be keen to come back to you to explore the human impact of cybercrime. I will bring in Rona Mackay.

Rona Mackay (Strathkelvin and Bearsden) (SNP): Good morning. My questions will really be for ACC Houston, but I will first say to Chris Ulliott that those numbers are absolutely staggering—would you mind repeating them?

Chris Ulliott: On the boundary of our technology estate, we block about 100 million attacks every month. We are very fortunate as a bank to have a dedicated intelligence team that talks to our peers, law enforcement and other industries. We exchange information on known criminal gangs and the people who are mounting those attacks, and we then put blocks in place to try to prevent them from getting anywhere near our estate.

Rona Mackay: Have you had to expand your workforce to deal with that?

Chris Ulliott: Yes.

Rona Mackay: Wow—that is amazing.

I want to ask ACC Houston and Miles Bonfield how accurate the recorded data on incidents of cybercrime is. I am pretty staggered to see the increase in the Police Scotland figures and the Scottish Government figures, which are similar. According to Police Scotland, the estimated number of cybercrimes in Scotland was 7,710 in 2020 and 18,280 in 2024. The data from the Scottish Government is similar. Those figures are estimates, and I suppose that, given the nature of the crime, it is hard to say how accurate they are. What is your take on whether those figures are underestimates or overestimates?

Assistant Chief Constable Houston: With any such crime, underreporting is massive. People might not want to come forward for a number of reasons. Vulnerable or exploited persons might feel a bit of embarrassment; they might think, “I’ve been taken in by something.” I think that that is a big factor. We have seen recent instances of big businesses coming out and saying, “We’ve been a victim here,” which is quite positive in that it might encourage others to come forward.

In my opening statement, I spoke about the need to obtain a threat intelligence picture. The more people tell us about the modus operandi, the tactics or the way in which criminals are playing the attacks out, the more we can build an understanding of the threat picture across the globe. What is happening here today could happen elsewhere in Europe or even further afield tomorrow.

The international collaboration that we have is a huge part of this. We have a lot of great link-in through the National Crime Agency and through some of our five eyes law enforcement group partners—particularly the Federal Bureau of Investigation, which does a lot of work in relation to online cyberattacks, whether they involve fraud or ransomware.

To get back to your question, the impact is and will always be underreported, until people have the opportunity to ask how they can deal with it. People might not report the attack to the police because they might not want to speak to us. However, if they report it to some of our partners—for example, the banks, which Chris Ulliott touched on—it is essential that those partners share that information with us, because we will then have a better understanding of the threat picture, which is more important than anything.

Rona Mackay: Are you confident that the public know that you are taking the issue seriously?

Somebody could say, "Well, the police won't do anything about that." How are you getting over to the public that you are taking it seriously?

Assistant Chief Constable Houston: Getting the cyberharm message out has always been a bit of a work in progress. In April, Police Scotland created a cyber and fraud unit, which sits under my command as part of the specialist crime division, so we have a dedicated unit that will deal with the issue. We are working towards a fraud report system, which the City of London Police will operate and which will cover all UK-reported fraud and cyber incidents. That is an opportunity for us to push the message that there is an avenue to report those incidents.

My personal message is that, although we might not get to the point where we get someone in the criminal justice process, people telling us about incidents means that we can help others to not fall foul of the same thing and ensures that we get that message across.

Rona Mackay: Dealing with the issue must be creating an awful lot more work for you as a force.

Assistant Chief Constable Houston: Absolutely. We are looking at where the opportunities are for us to keep pace with technology, but an important part is that there is also an opportunity for us to collaborate with partners that can support us in doing that. That is about co-ordination, because we are all making the same effort—we just need to bring it into the same place.

Rona Mackay: Can I have the view of Miles Bonfield on the accuracy of the recorded data and so on?

Miles Bonfield: I agree with ACC Houston that there is almost certainly underreporting. From our perspective, the element of shame is a hurdle for the victim to get over in order to report; a business might consider how it might damage its public image. The figure that is reported is almost certainly lower.

As ACC Houston said, it is really important that we get over that feeling and encourage as much reporting as possible, not only because that brings shared awareness and common purpose about how the threat is evolving but because it provides a first-touch opportunity with a victim to give them preventive advice so that they do not get revictimised in the same way. There is another opportunity to give preventive advice through Action Fraud, which is a really good thing.

We take public confidence communications very seriously in order to reach the public and get out the message that we have a competent and important response. That is as much a key part of the overall system response as pursuing offenders is.

Rona Mackay: Do you know of any false reporting? How easy is it to detect? For example, if somebody wants attention or whatever and phones up to say that they have been a victim, is that easy for you to detect? Do you ever get hoax calls?

Miles Bonfield: I am not aware of instances of false reporting. We run a triage system to support the system partners, through which initial reports are assessed and progressed to the appropriate action, such as a pursue response, prevent activity or advice to the victim. I am not aware that we have had false reporting through that triage system.

Rona Mackay: I would not have thought that people did that sort of thing, but you never know.

Miles Bonfield: No, indeed.

The Convener: Would Nicola Taylor like to come in?

Nicola Taylor (CyberScotland Partnership): I will add to one of Stuart Houston's points about collaborative working and touch on the CyberScotland Partnership, which has been designed to do exactly that. The partnership was established in 2021. Since 2020, the number of reports has almost doubled, which is testament to the fact that the message is getting out to the public by way of the CyberScotland Partnership.

Twenty-one organisations sit on the partnership, all of which have access to different networks. The CyberScotland Partnership website signposts people to the great work that Police Scotland and the Cyber and Fraud Centre are doing and to the resources that are available to the public.

10:30

Rona Mackay: You have quickly set up an impressive system to collaborate with each other.

Liam Kerr (North East Scotland) (Con): Good morning. ACC Houston, are traditional policing bodies able to effectively police the digital space, or do the police and, perhaps, justice agencies need to be structured, resourced and perhaps even trained differently to accommodate the new environment?

Assistant Chief Constable Houston: There is such a change in pace, and things move all the time. Law enforcement does not always have the answers to the issues so, for example, we work with the financial sector if money is being moved on the back of cybercrime, whether it relates to cryptocurrency, which we see a huge increase in, or other aspects that are not, as you said, a traditional policing threat that we would face.

The approach is about linking with our partners. We have good relationships with the National Cyber Security Centre and other intelligence organisations that can assist us in how we target that work. We can take different approaches, and I do not think that the criminal justice outcome is always the best answer. Disruption or prevention is sometimes more appropriate in making sure that we prevent such crime happening again.

We cannot lose sight of the fact that such crime is borderless, so how we are equipped for that is important. Police Scotland is fortunate to have officers embedded in Interpol and Europol, so we have the opportunity to collaborate quickly on cases internationally. We have had joint operations with the FBI in relation to cybercrimes in Scotland and America, including SIM swapping and various aspects of that.

There is probably a bit for us to learn about where we can go with academia, but we are in a strong position in Scotland. On Friday, I was fortunate to go to the cyberquarter in Dundee with Mr Dey, the Minister for Higher and Further Education, where we saw a showcase from students who are coming into their final year of cybersecurity and ethical hacking courses. They showcased work that they had done on managing large amounts of data and assessing data for threat, risk and harm. That is probably where we need to takes some ideas from in relation to how we reach in and tackle the issues.

Police Scotland has signed a partnership with the cyberquarter at Abertay University. We link in and liaise with it about how we can advance our thinking. Going forward, the approach will not be about the traditional policing that you spoke about; it will be about how else we can tackle the issue. We do not have all the ideas, but people in business and academia have ideas about how we can better detect things.

Liam Kerr: I am grateful for that. I should say that anyone else should try to catch my eye if they want to come in on any of my questions.

I have a subsidiary question for ACC Houston. Do you have any view on whether the legal framework is appropriate? Does it require looking at again? Do the crimes that are on the statute book need to be reconsidered in light of the developing situation?

Assistant Chief Constable Houston: That is a very good point. We are still working to the Computer Misuse Act 1990, which, I keep getting told, was passed a long time ago. It does not feel like it, but it was—it was even before I joined the police. However, there have been changes. I know that parts of the Online Safety Act 2023 will help the situation.

Given that a lot of this takes place elsewhere, it is interesting to look at the international situation. How do we block and take down the platforms that cause harm? That is a wider issue. I do not think that one country can legislate for that, so we need to take a more strategic look at it.

There is also a bit about how we treat those who are convicted of cybercrimes, and how we use serious crime prevention orders as a deterrent for people who might have been involved in such activity. They limit the access that people can have and how they can share information, and people subject to such orders have to allow their activity to be viewed by monitoring officers. That is something that could be looked at again. We could also look at strengthening the ability to deal with encrypted communications for those who might have been through the system. This is a moving feast. The technology changes monthly, so how do we keep pace with that?

Jude McCorry: In my submission, I raised the sharing of stolen data. When there are large-scale attacks, such as the one on NHS Dumfries and Galloway, how do we protect patient data and customer data? If the gangs are not paid the ransom, they dump the data. The laws to protect health data or customer data are not there, so the data is then free for anybody to download and share.

If someone handles stolen physical goods, they commit a crime, but someone can share data and it can be sold from the dark web. The victim is the company that has been the subject of the cyberattack, but it is also the victim again six months or a year later, because solicitors are chasing its customers to tell them that they might have a case against the company or organisation because their data has been leaked. It is not good that people’s data is out there, and another industry is thriving on that stolen data because it is not a criminal act to steal it. We need to look at things such as that.

In Dumfries and Galloway, we had discussions about whether to take out an injunction against the sharing of the data. The Health Service Executive in Ireland took out an injunction against the sharing of any data on any patient from the whole healthcare system in Ireland that could have been dumped. However, an injunction can be used only in the country where it was taken out, so that does not prevent people in other countries from sharing the data.

We have not seen evidence of the Dumfries and Galloway data being shared, but we have seen crimes that could be attributed to it. We need to look at that. I know that the law involved is not Scottish law, and we need to look at it from the UK’s perspective. It would be good if we had an adult conversation about how we protect organisations from data re-emerging all the time and being rehashed everywhere.

Liam Kerr: That is helpful. I will stick with you, Jude McCorry, if you do not mind. Your submission says:

> "More needs to be invested in proactive areas to prevent cybercrime, or around innovation."

For the committee's benefit, would you mind elaborating on what we, as politicians, need to think about to meet that aim?

Jude McCorry: I am an ex-employee of the Data Lab, which holds datafest—we have people from datafest here. We had the first datafest 10 years ago, and I am still hearing the same conversations about AI and how everything is great. I never hear a conversation about how we can use AI for good in cybersecurity and how we can join up data science and cybersecurity. As a nation, we are very good at pushing forward data excellence—Edinburgh is the city for data excellence—but we are not talking about how we protect that data. We are building data and innovating in data science and AI every single day, but we are not talking about how we are protecting them. I would like there to be more of a conversation about that.

On law enforcement, there is a big thing around "Computer says no," like in that programme, and how we cannot share data. We do not need to share data. As ACC Houston said, we should be sharing intelligence. We should be open. I am proud that the people who we have here share that intelligence and help to make Scotland safer, but a lot of other organisations could help us to do that.

We rely on a lot of organisations that are outside Scotland for innovation, but we need to start taking the lead on that ourselves. We have seen intelligence agencies in the US, such as the Cybersecurity and Infrastructure Security Agency, have their budgets slashed. We cannot therefore rely on others for innovation and the protection of our organisations.

We have spoken about the students at Abertay University. We have the brightest brains in this country coming out for ethical hacking. They are the good people in cyber. I shorten the term and call them "hackers" and some people get very afraid that I have hackers working for me. They are brilliant people and it is a brilliant university, but I would like to see organisations open up to work in different ways with those students.

Those individuals should not have to do two years on the beat. I know that Police Scotland is considering that, but a lot of them would shy away from having to go out and meet people, whereas they could start straight away in Police Scotland in different roles doing data science and cybersecurity and looking at the emergence of those.

To go back to your question about changing the law and the workforce and whether everybody should be skilled up in fraud and cyber, Police Scotland does very well on the streets, and it meets people who have had crimes committed against them. We are never going to be able to educate everybody in cyber and fraud, but Police Scotland is very good at signposting and making sure that the victims of such crimes get the support that they need.

What we need to get out into the public domain is that people should report as many crimes as possible, because Police Scotland will be there to support them. The ethical hackers and young people understand cybersecurity and fraud a lot better than us, and Police Scotland is very good at victim support, too.

David Keenan: I will pick up on a couple of points that Jude McCorry made. The first is about investment. Cybercriminals are becoming increasingly advanced, so the tools, techniques and technologies that are required for businesses to combat attacks are growing in complexity, and with that there is a growth in cost. That will have a massive impact on the Scottish and UK economies. All businesses have to purchase the tools to prevent such attacks. Most of those tools are built and sold by international companies, so that means that money is leaving the Scottish economy. More investment and innovation in the UK and in Scotland would be very useful.

Liam Kerr asked ACC Houston about changes of approach. As the victim of a cybercrime back in December 2022, we did the responsible thing—we reported the crime to the police and the Information Commissioner's Office. That immediately made us the subject of an investigation by the regulator. However, what was missing was an organisation for support. We were the victim of a crime, and we had little or no support, except through organisations such as Jude McCorry's. The change in approach that we need should involve support for businesses that are victims of cybercrimes.

Liam Kerr: That is fascinating—thank you. As no one else wants to respond, I will hand back to the convener.

The Convener: I will bring in Adam Stachura, who has been listening patiently to what we have been discussing. I am very interested in your organisation's perspective on the importance of support in the aftermath of a crime.

Adam Stachura (Age Scotland): This has been a fascinating discussion. I have been listening not only patiently but with great interest.

The human element is incredibly important. We have touched on that with regard to customers who might have been impacted by the incident at NatWest, and there are people who might have been impacted by the incident at Arnold Clark. Every serious organisation in the country will have cybercrime on its risk register. It is a case of knowing that such incidents will happen as opposed to hoping that they will not happen. I am sure that a lot of investment has been made in that area and that there has been a lot of good thinking on it.

For the past few years—probably since 2021—we have been undertaking research on the issue. Initially, the research was on older people's attitudes to scamming and fraud, but we have moved on to cybercrime as that has become more prevalent. Our latest research on that, which was published in 2023, showed that, between 2021 and 2023, there had been changes in the type of thing that people encountered. Being targeted through email or text message was the most common method, and there will now be a lot more cases in which, because of developments in AI, as we have touched on, people will not be able to understand that some things are not real, as they will look very convincing. A lot of older people have sensory impairment, such as sight loss or hearing loss, so, if there is a glitch in a system, it will be passive for them. Things can look very convincing.

The last time that we undertook research on the issue, we found that about 20 per cent of people who had been a victim of a fraud-related crime did not report it. They did not know where to go to report it, they did not think that it would be taken seriously and they did not think that anything could be done. I am not sure whether 20 per cent represents a lot of people or not very many, but, in the future, we will want people to become more confident in reporting what has happened to them.

10:45

There might not be a particularly good and easy resolution, because a lot of such cases involve people losing money. As has been touched on, that affects people's confidence and they might not want to tell anyone that such things have happened. It is quite hard to work out the degree of financial loss, which is perhaps due to how stats are collated and reported. Sorry, ACC Houston—I am not necessarily looking at you and Police Scotland in that regard, but having such information will help us to understand the scale of the problem out there. We know that there is a lot of underreporting, too.

Such crimes can result in financial destitution for people. They absolutely hit an individual's confidence and self-worth, but there are other detrimental impacts, too. There can be an effect on someone's health and wellbeing, on their trust in others and companies and even on their interactions with state institutions.

We have found that that is the case among people who are not particularly confident online. I can provide a couple of statistics. About three quarters of older people are online, but that does not necessarily mean that they are particularly comfortable in or skilled at navigating the internet. They can be plugged in but not necessarily able. About a quarter of those people who are online are not comfortable or safe operating online, so that means that a load of people—we are talking about between a quarter of a million and 300,000 over-65s in Scotland—are online but really unsafe. That pool of people are in a potentially difficult spot.

Being a victim of such crime can draw people into isolation, and they might move away from the internet. Some of the information that we have had relates to how we adopt digital technology throughout Scotland. If the only way that older people can interact with the state or services is digitally, and they have been a victim of or subject to digital-related incidents, they will mistrust such services. They will ask, "Is this thing legitimate? Who am I seeing?"

Committee members might have heard me say this repeatedly in different places over the past however many years, but we have to be very careful to ensure that our public services are open so that people can get support by seeing and speaking to real people.

There are two elements that are incredibly important for older people and for anyone who will, we hope, become older. Some issues might come with them, but how do we prevent such issues from happening and protect people in the first place? As a nation, how do we provide people who are online with better digital skills and with access to programmes and systems on their devices that keep them safe by blocking malicious attacks? Can we stop them from even being exposed to such issues in the first place? That would really help.

The Convener: Thank you for that. There was a lot in there.

Pauline McNeill (Glasgow) (Lab): I have a couple of questions. One is on the ransomware issue, and the other is on the evidence that ACC Stuart Houston has provided to the committee on exploitation, physical harm and so on.

I do not know whether this question is for Miles Bonfield—you can decide between you—but I am interested in the recent attacks on M&S. David Keenan quite rightly outlined the investment that is needed by companies, but, in the case of M&S, it was reported to be a simple breach. Somebody phoned up the IT help desk, as we are all used to doing, and that was a simple way in.

Jude McCorry: We do not know that. That has not been confirmed, and the case will still be subject to a criminal investigation. We need to be very careful not to trivialise that kind of thing. It is a criminal matter, and we do not know—

Pauline McNeill: I am not trivialising it. I am just saying that there are reports in which people say that that is what they think happened.

Jude McCorry: There are, but I would wait for any evidence, or people can share—

Pauline McNeill: Are you sceptical about that?

Jude McCorry: I am sceptical about what I read in the papers every day.

Pauline McNeill: That is fair enough.

Jude McCorry: We deal with facts, so I would wait. We do not know the full facts yet.

Pauline McNeill: Okay. Let us see what the full facts are.

With regard to ransomware, there is information out there about groups such as scattered spider. Who are these people? Do we know much about them? Are they highly trained individuals? What is attracting them to crime? It might be important to get behind that.

Chris Ulliott: The attack is currently being attributed to a group called scattered spider, but we need to wait for the outcome of a proper investigation to know whether it was that group. The people who are behind such crimes have very varied backgrounds. In the case of past attacks, it has ranged from individual youngsters who have just got bored at the weekend or loose collectives of individuals who might frequent the same online forums—for example, we believe that the group that we call scattered spider consists of youngsters, by which I mean people in their late teens to early 20s, from multiple countries who happen to collaborate and exchange ideas on an online forum, so they are loose collaborators—all the way through to very organised criminal gangs that build a huge dedicated infrastructure and have large amounts of funds available to build the support infrastructure that is needed to mount attacks.

It is really useful to take a step back from the people we are talking about, because there is a huge ecosystem behind such crimes. It is not always one group of people. You will find that there will be a group of people who write the software, which they will sell online. A different group of people will then use the software to mount the initial attack. They might gain access to a corporate network or to an individual's computer, but they might not do anything with that. They will then sell that access to another group of people, which might do the extortion or commit the visible crime. There is then the problem of how you launder the money, and there are different groups of people who specialise in taking cryptocurrency, anonymising the source and the destination and providing services to turn that into hard cash afterwards.

Therefore, it is very rare that it is just one group of people or one person throughout the entire chain of the attack; there is usually an entire ecosystem. There are many places where you can look to see how you disrupt such crime, but it will be an international process. The group that writes the software might be in one part of the world, and the people who carry out the attack might be in another part of the world. That is part of the problem. The scale and the number of people who are involved are huge, and there is an entire black market and ecosystem, which we are all trying to track, understand and interrupt, as they carry out attacks.

Pauline McNeill: It is really helpful to have that understanding. With the proper investment that is being talked about and with warnings and police resource, how easily could we shut down the scope for ransomware incidents?

Chris Ulliott: It is a really big and hard problem. The investment that the bank and I make in protecting against such attacks is huge. However, I might be with Jude McCorry talking to a charity, where there is a handful of individuals with computers that they have bought who are doing really valuable work, but they are not IT specialists. I do not have the answer, but we need to find a way. That is where research and work with academia and our industry partners can help. It is about how we take the knowledge and the capability that is available to very large enterprises, such as NatWest, and make a subset of that available to charities, health services, local councils and small companies that, in many cases, do not even have an IT department, never mind large investment in a security organisation in the way that we have. That is the challenge.

You have to pass a driving test before you can drive a car on the road, but you can just buy a computer, go online and hang out in some really suspicious neighbourhoods without any controls. I wish that we had an answer. I do not have one, but, working together, we can start to manage the impacts.

Jude McCorry: Chris Ulliott also works very hard on supply chains. You cannot just protect yourself; you have to try to make sure that the people with whom you are interacting are good custodians of your data and respect their cyber-relationship with you. NatWest, with Royal Bank of

Scotland, does a lot of work regarding its supply chain.

We always say to organisations that they will never be 100 per cent safe. Arnold Clark was a very secure company, but it still got attacked. I do not know what the budgets are for Marks and Spencer, but I am sure that it spends millions, too, and it still had an attack, as did the Co-op. Lots of other organisations are affected, but we might not hear about that—they might pay the ransom or, even if they do not, they might not want to talk about the attack for fear of retribution or losing public good will.

Pauline McNeill: ACC Stuart Houston, in your submission, you said that there has been a rise in cybercrime and

> "physical harm with online groups exploiting vulnerable individuals online to self-harm and share the content."

Will you say anything more about the profile of those people? Is it mainly children and young adults? Is it mainly girls? Do you have any information on the gender split for sextortion? Any of that information would be useful.

Assistant Chief Constable Houston: I will answer the first bit of the question. Sextortion is quite underreported, and I do not have the figures on the gender split to hand, but I can certainly provide them. However, we are seeing online-enabled violence—that is how it has been termed—through groups that encourage people to self-harm or to place marks on themselves and publish that online. That has been a trend, particularly across the US, for some time, and it is starting to leak into other groups. There are networks of people, who might be unknown to one another, on encrypted platforms that are quite difficult to see, and such networks causes harm.

I know that today's evidence session is not necessarily about the indecent images aspect of online crime—we would probably need another full day to speak about that subject—but that is quite prevalent. The National Crime Agency has placed online-enabled violence and how it will consider that in its control strategy for this year. Specifically, the com networks get mentioned a lot, and you will hear quite a lot about the 764 gang in the media. Those are also about exploiting the vulnerable.

The reason why I mention that is that, although money is not necessarily being made from some of the stuff that we have spoken about, the issue is about individuals having power over others and exploiting the vulnerability of other people for their own enjoyment. That is a challenge, and it fits in with the other challenges, such as underreporting and how we trace the individuals, given that they might be operating in other countries. There is legislation on the encouragement of people to do harm, and there could be specific common law crimes that we could libel for that. It is a challenge for us to trace people so that we are in a position to libel those, but we are looking at that.

Chris Ulliott: It might be useful to know or bear in mind that your view of the internet and the platforms that you interact with will be different from the view that I get, which will be different from the view that my teenage son gets.

I have some personal anecdotes. I have an elderly relative who was the victim of online fraud a few weeks ago. Even though she gets regular briefings from me on the things that she should and should not be doing, she still fell victim. When I looked at her social media feed, it was interesting to see that it was full of adverts, the majority of which looked suspicious to me but were targeted towards her, as a lady in her 70s. My social media feed is tailored to me, a middle-aged gent—there is lots of cycling, fine wine and that kind of stuff—and my son's social media feed is all about cats and the like.

The big social media platforms do a lot of heavy tailoring, and the people behind these crimes know that. If you want to target elderly people, you can build a profile and place an advert—it might be advertising a scam or something suspicious—that will hit only that community of people. If you want to target young females, you can create an advert for that demographic and only those people will see it.

On the one hand, it is great that the platforms are tailoring content—people get what they think that they want to see—but, on the other hand, that introduces risks, as a lot of the fraud, scams and attacks that we worry about can be targeted at specific populations, which increases the probability of the attacks being successful.

The Convener: That is fascinating. Thank you.

11:00

Ben Macpherson (Edinburgh Northern and Leith) (SNP): Good morning. Thank for your time and for all that you are doing for our constituents.

This is the criminal justice issue of our time, not just domestically but, in many ways, as you said, internationally. Recently, the fraud epidemic in the UK was deemed to be a national security threat and the issue seems only to have grown as a point of concern since then.

As you say, anyone can fall victim to it, and it is the responsibility of us all to raise awareness in our constituencies. In that spirit, I will say that we have all been targeted: somebody phoned me pretending to be from my bank and, thankfully, at the right point, I realised that they were not. I consider myself to be quite tech savvy and conscious of the issues, but that just shows that anyone can be a victim. We all have to have our wits about us, and raise awareness in our constituencies. I have had people impersonate me in contacting constituents.

We are grateful to have you here in our Parliament to enable us to consider what more we can do in this space. You have talked a lot about the collaboration between law enforcement, the National Crime Agency, commercial Scotland, local government, our devolved agencies and the third sector. Do you want to emphasise anything more about the importance of collaboration, both domestically and internationally?

You also talked about legal change. The UK Government has undertaken a number of reviews and one is on-going. Criminal justice law is devolved, however. Does more need to happen here as part of the UK-wide effort? How do we make it easier to trace, evidence and prosecute such crime? All of us in the Parliament have a responsibility to enable those of you who are trying to pursue the perpetrators and hold them to account to be more robust in that, and to work with commercial organisations and the public sector. The Scottish Environment Protection Agency has been a victim of such crime, and the British Library is still experiencing difficulties in that regard. How do we work together to do more for our constituents?

The Convener: Does Miles Bonfield want to kick off on that?

Miles Bonfield: Initially, as a positive point, I note that we do not need to prosecute offenders here, or have a criminal justice outcome in Scotland or in the United Kingdom, to ensure an adequate and robust response. As a system, we work with partners, in particular in the five eyes group—the US, the UK, Australia, Canada and New Zealand—in order to ensure that we have a moderated and appropriate response, and that we play to our strengths and take action wherever we possibly can.

Sometimes that action is to provide support for an FBI or Australian Federal Police investigation to take action in another jurisdiction, which would be hard for us to reach but is easier for them to reach. That is one of the things that we do.

Chris Ulliott articulated very well the threat and how it works. The increase in the threat has been driven by a loose association of online entities: the subculture of skilled people who work in a nefarious way. That threat is really hard to combat. As Stuart Houston said, a concerning and worrying point is that it is diversifying from fraud and financial motivation into power dynamics that can relate to perpetrating and encouraging violence against individuals and disrupting our services for the sake of it. That diversification adds a layer of complexity to what is already a complex piece.

I go back to Mr Kerr's point about whether or not the traditional response is working. I would say that our traditional response is for policing and law enforcement to work in partnership with other public bodies and the public themselves. That works for us, and we need to continue to do that in order to get the message out there. Just as it is important for you to put locks on your windows and doors, and to lock your car with an alarm, it is equally important to ensure that your passwords are changed regularly, that you keep up to date with your security patching and that you do two-factor authentication. That sort of thing will help us.

On the advances in the threat, I would say that artificial intelligence is a threat, but it is also an opportunity for us to process the information better and to tackle the threat. We are being more proactive so as to waste criminals' time, disrupt criminals online, stop that offending and change the circumstances so that that offending never gets close to NatWest, for example. We absolutely need to do more of that.

We enforce the laws that the Parliament makes, so I would not wish to make changes in relation to that.

Ben Macpherson: I appreciate that. There are lots of people like me in that space, in that fraudsters have tried to steal from us, but we managed to recognise something as a scam at the right point, so it did not happen. How important is it for someone who is not a victim of a fraud—who becomes aware that someone is not a genuine person calling from their bank or wherever—still to report it? Is that intelligence useful to you? Should people report such incidents, so that you are getting the widest availability of evidence from the public?

Miles Bonfield: Absolutely. Making our threshold reporting easier is a thing to do, because that will help with that shared awareness and common purpose of deflecting those threats. We look to intervene at every stage of that event chain that Chris Ulliott talked about to change the circumstances, so that it is even more difficult for criminals to exploit those events, from the beginning of a threat vector penetrating an individual or a system right through to how they may dispose of the proceeds of their crime using crypto. Making that even more difficult for criminals globally is an important part of the response on which we work together on a daily basis.

Chris Ulliott: A single fraud or scam might be hard to investigate in isolation, but it is valuable to get a big picture, and we suddenly start to see things that are common across those different events. That is when we start to take leads. We share intelligence with our peers in financial services, and it is not unusual that it is not until we talk to one of our peer banks and take its information that we start to see some commonality, with accounts or addresses in common. We can then pass on that information to law enforcement. That intelligence sharing is really important. We recognise that each case in isolation might not lead to a successful prosecution, but the value is found when we start to get the bigger picture.

Jude McCorry: We work with NatWest and some other banks, as well as Police Scotland and the NCA and the Met in London. On a Tuesday, we do a fraud call, which takes an hour of people's time. We try not to waste that time—we just share the intel. That is a group of people who trust each other from Barclays, NatWest and Metro—I cannot remember all the rest of them. We share the information and the intelligence during that hour, and people then say, "I've seen this," and "I've seen that."

We take that information back and share it on social media, saying what we have seen. This morning, I shared something about gold scams for high-net-worth older people. We are not just taking and sharing the intelligence; we have to get it out there. That is not just on social media; we need to reach the people who are not on social media and to speak in a language that people understand. I work in cyber, but I did not know what "2FA" or "MFA" were for a while. I hate such terms, but I know why we have to use them and why it is so important. I say to people that this is on all our internet banking, or our Marks and Spencer or Next accounts. People should go into their security settings. However, we have to be mindful that people are not security specialists. I think about how my mum or dad would understand it and try to get the message across in the right language, so that both older and younger people understand it. Younger people probably know more than we do, but some people may not be tech savvy. We should not look down on people for that—I could get caught by fraud tomorrow.

Ben Macpherson: I will bring in Nicola Taylor in just a moment. First, I want to add a point to the discussion, if anyone wants to say anything in response. Jude McCorry talked about young people being more savvy and the need for greater awareness among those in the population who are potentially more vulnerable. However, there is also—as David Keenan talked about—demand from businesses and public sector organisations for the capability within their workforce to be able to counter this type of crime. Do we need to do more to build skills and capacity in the population in order to have enough specialists to cover all the organisations that will need protection?

Jude McCorry: We have made the point that collaboration between people works, but it will only go so far. The Arnold Clark attack happened on Christmas eve; in the holiday season, it was very difficult to get the people that we needed and to get an instant response from organisations that had more people available.

My issue is that we need more investment just in case, but it is very hard to get just-in-case investment because we will not need it until we need it. If we had two attacks on the same level as the SEPA attack, at the same time, we would not have the people that we would need to manage something like that. If four councils had been attacked in the past few weeks, we would not have had the people, in any of the organisations, that we would have needed to deal with that.

We need to look at how, as a country, we address that. We cannot depend on law enforcement down south to help us when there are two attacks going on with the Co-op and Marks and Spencer; we need to be able to stand on our own two feet up here and support organisations when those attacks are happening.

Ben Macpherson: Are you saying that we have good resilience but we need to build more resilience in our capabilities?

Jude McCorry: I would not even say that we have good resilience. There is a preconception that organisations have instant response plans and board members who have the skills to talk about cybersecurity, but in a lot of businesses in Scotland, that does not happen—

Ben Macpherson: You are talking about the private sector, not the public sector.

Jude McCorry: Yes, the private sector.

Ben Macpherson: Do we have the resilience in the public sector?

Jude McCorry: Well, looking back at what happened with SEPA, I would say no. We do not have the resilience in-house—again, that is down to investment.

To go back to the point about West Lothian Council and City of Edinburgh Council, we have seen the councils announce budgetary cuts for everything in the past few months. There will probably now be millions added on for the clean-up operation after the cyberattack in West Lothian, so it will be us as residents, or the Government, who will have to pay for that.

I go back to the point that the investment has to be there. There is an on-going project with the Digital Office for Scottish Local Government to try to build a security operations centre and cybersecurity capability to enable all the councils to come together, rather than people operating on separate budgets. That is a really good way to go, because if we read the report on the SEPA attack, we see that a lot of people have said that SEPA needs a security operations centre. It is very difficult for us to say, however, that all public organisations should have a security operations centre, as there is no budget for that. As the Digital Office is doing, we can think about getting the councils together. NHS Dundee is also thinking about how organisations can support each other collaboratively.

Government needs to get on board with what types of technology and support are working, and test resilience, asking whether organisations will be able to operate if they have a security breach. All that has to be mandated from a Government perspective. How secure are we as a nation? I do not know the answer to that, because I am not employed in Government.

Ben Macpherson: What I take from that—correct me if I am interpreting you incorrectly—is that some business organisations have good resilience, but many could have better resilience—

Jude McCorry: Yes—I am not blaming people for not having better resilience, because that requires a huge budget. You should see what Chris Ulliott has to spend to do what he does.

Ben Macpherson: Some public sector organisations could have better resilience, in particular given the attacks that have happened in the examples that you cite, which include some local authorities and health boards.

I think that SEPA is the only national agency in Scotland that has been the victim of a major cyberattack, which would suggest that a number of the national agencies are secure. I just want to give the public that reassurance. We might want to ask the Government for that, as a follow-up to today's meeting, but I do not want to create undue alarm.

Jude McCorry: As I said, I am not causing alarm, but we are asking people to prepare for the worst to make sure that organisations are able to carry out their core purposes. West Lothian Council was a good example in that it was able to have children do their exams, but there will have been a cost to that, and no organisation will be 100 per cent safe.

11:15

The Convener: I suggest that we bring Nicola Taylor in before we go to Liam Kerr.

Nicola Taylor: I want to pick up on the collaboration point. We, around the table, have heard the numbers today. They are huge. They are frightening. It is certainly a bigger task than any one individual or organisation can tackle. That is exactly why the CyberScotland Partnership was formed in the first instance. It was to bring as many voices as possible around a table in order to help to address the challenge that we are facing as a nation.

It is important to recognise that the Scottish Government takes this issue very seriously and has been very supportive in terms of investment. There are always things that can be done, and more investment will always be needed in this area, because we will constantly be trying to keep up with the threat that exists out there. There are initiatives such as the public sector cyber upskilling fund, which has allowed public sector organisations to access funding for individual employees to train for cybersecurity qualifications. There is a huge shortage of those who have the specific skill set that is needed, but for the past three years, funding has been made available to public sector organisations to help to address that.

It is also important to recognise that, from a business perspective, the Scottish Government has been very good at recognising the need to get information out there and to get organisations to understand why it is important for them to look at their cybersecurity posture. For the past three or four years, funding for cyber essentials accreditation has been made available to such organisations. We are looking to get as many organisations as possible to that minimum standard or baseline.

Although there is always a need for further investment, it is important to recognise that the Scottish Government, in particular, already takes the issue seriously and has made investments to get us to where we need to be.

Chris Ulliott: It is probably worth adding to Jude McCorry's comments that there needs to be maturity around how you respond and protect cybersecurity. You can put all the defences and controls that are available to you in place, but, ultimately, something could eventually go wrong. The term that is used a lot nowadays is "operational resilience". Plan for the worst. How would you maintain service if your technology was disrupted? Your technology could be disrupted for many reasons. Cybercrime is one of those, but it could be a purely technical failure that leads to your technology being unavailable. Within financial services, both in the UK and internationally, we regularly use a set of scenarios and exercises to work through what we would do if we, or one of our peers, had a huge outage and how we would ensure that our customers continue to receive the service that they need.

I do not know the Scottish Government well enough to know whether it does that, but how it would exercise or model its response in the event of another SEPA-type incident is something to consider for the future. Having that muscle memory after having gone through those steps ensures that you can respond much more rapidly should the worst happen. Hopefully, the worst will never happen, but having preparation up front is really valuable and minimises the impact on customers and citizens should something go wrong.

Jude McCorry: The Scottish Government carries out such exercises, but whether to do so is up to individual agencies. We won a tender four years ago to deliver the National Cyber Security Centre's "Exercise in a Box". We delivered it to 2,500 organisations, including some in the public sector.

Organisations carry out fire testing and drills two or three times a year. They should be doing that for cybersecurity, too, rather than just doing one exercise every so often and then forgetting about it. Things change, such as your supply chain, your organisation and your people, so we need to make sure that we not only have an instant response planned but that we are carrying out testing.

The Convener: Liam Kerr has a follow-up question to one of Ben Macpherson's questions.

Liam Kerr: ACC Houston, unlike elsewhere in the UK, the proceeds of crime in Scotland, of which there have been some significant seizures, cannot be used for policing, as I understand it, or, for example, for agencies such as the Cyber and Fraud Centre, Victim Support Scotland, prevention or anything such as that. Do you have any idea why that is the case? I appreciate that Police Scotland is there to keep us safe rather than to make policy—that is our job—but do you take a view on whether the Parliament might look to change that?

Assistant Chief Constable Houston: We have seen that played out across other jurisdictions. For example, the regional organised crime unit network in England and Wales uses a lot of proceeds of crime money to fund various aspects of tackling serious and organised crime, which includes cybercrime. Again, that money could go into staffing or equipment. The main thing to say is that, with some of that extra money, it is able to enhance its capabilities, which is the big part of what is needed. That is what we need to do. At the moment, we build the capability with what we have in the organisation. We are funded through our block grant, so we fund the work from that. As you rightly said, we do not get access to the proceeds of crime that are seized.

That has become quite an interesting issue, given the value of some of the cryptocurrency involved in crime—to stick with the cyber theme. Since 2019, in Scotland, we have seen the involvement of cryptocurrency in criminality increase by 2,000 per cent. Cryptocurrency varies in value, and some parts of policing in other parts of the UK have seen the benefits, where they have set up dedicated teams to go after the crypto and to ensure that it is seized in the appropriate way. Therefore, it does benefit those parts of policing, and, without doubt, it would enhance our capability if we were able to access that additionality, with the understanding that it be used to deliver against organised crime—whether that is cybercrime or other types of crime.

The Police Service of Northern Ireland also has that capability. Previously, it has used that money to tackle financial crime and generated further enhancements in order to chase that type of crime for its particular version of asset recovery. It is a useful tool that is used quite effectively in other areas across the country. I see real benefit in being able to do that, because you can turn that money back to deal with the type of crime that you are facing.

The other aspect of being able to use the proceeds of crime relates to the criminals, because we can say to them, "The money that you've made through criminality is now going to directly fund people who will chase you or your colleagues," which must have a bit of an impact. I think that that is relevant. If possible, we would want to look at obtaining the proceeds of crime money in a slightly different way—probably on a par with our colleagues south of the border.

Liam Kerr: I am very grateful for that.

Fulton MacGregor (Coatbridge and Chryston) (SNP): Good morning. It has been a really interesting evidence session; thank you for your contributions. I was going to ask about protections for vulnerable people, but we have had quite a good discussion about that already. Adam Stachura, Jude McCorry and others have contributed with regard to older people in particular, which is what my question was going to focus on.

Instead, I would like to ask about increasing resilience in the population overall, which is possibly something for a wider discussion and not for today's witnesses. However, while we have been talking today—particularly in the exchanges with Ben Macpherson a few moments ago—I have been wondering whether there has been any discussion about that sort of internet safety awareness being brought in as almost a mandatory topic in schools, for example? If you can start to implement that awareness at a very young age, you can increase the population's resilience over time so that people are less vulnerable. I do not even know who would be best to answer that, but has that been discussed or thought about, and who would deliver it?

Jude McCorry: It is a hard issue to deal with, because, as I said, younger people are a lot more savvy than we are. I do not know whether anybody else watched the television series “Adolescence”. It was an eye-opener even for me, as someone who works in cybersecurity and as a parent of two kids. I did not want to believe that a young person would be involved in something like that.

My fear is that we, as parents, are putting too much on to schools. The purpose of organisations and schools is to educate our children. As parents in society, we should be aware of what our kids are doing—and of what they are doing online. How can they protect themselves? On the back of “Adolescence”, we have issued guidance for parents and carers about keeping children safe online, which we have shared with schools so that they can send it to parents to tell them in a softer way to please be aware of what their children are doing. It is also about the level of education that you go in with—we cannot go in at a basic level because children are a lot more tech-savvy than we are.

Fulton MacGregor: That is understandable. Given that the issue is here now—and here to stay—would it be any different than schools teaching about road safety, which they do very effectively? Is there also, perhaps, an element of postcode lottery? I know that my kids’ primary school does a wee bit of work on online safety. Is there an argument that there should be something more standard across the board?

Jude McCorry: Yes, but I think that schools do work on that—again, we probably need to hear from somebody from education. I know that my daughters get assemblies on the issue and on different current subjects. It would be unfair to think that schools do not do that work. However, my point is that we are asking them to educate our children and to raise attainment and so on, too, and it should not be left only to teachers and schools to work on the online safety issue, although I think that they do it really well. However, it is not only about online security. The harm bit is a big issue, too, as everything today is. I will hand over to Stuart Houston to talk about some of that.

Assistant Chief Constable Houston: Let me touch on that. Our cyberharm team, which sits in our cyberfraud unit, develops packages not only for education but also for volunteer groups and other clubs and associations—particularly those that relate to children, although we also have tailored packages in relation to older people. Those packages address safety from online harm and some of the stuff that we have spoken about around harmful social media, content that young people might be encouraged to go into and look at, and certain platforms that young people in particular might be dragged into. We do quite a bit of work on that.

It is a very difficult message. As Jude McCorry has touched on, younger people might have more knowledge of some of those apps than we do, so we need to try to keep pace with that, as well. In order to tailor that response and the prevention messaging, you need to know what is happening. I come back to Mr Macpherson’s question about what happens if we do not report: if we do not report, we do not know what harms we need to try to prevent. We need to take that holistic approach. For us to tailor and push our prevention messaging to the right area—which includes age, geography or whatever it might be—we need to know what is out there and what the harms are. That way, we can ensure that we are getting the message right.

Everything that we do is built on what is happening out there. We need to have an understanding of the true picture of the threat from cyber. For example, that could be social media groups that are encouraging kids to do things—in the past, we have seen pranks put online on social media that have fatal consequences for kids. We need to know about such things so that we can at least push the message in the right direction.

Fulton MacGregor: Okay, thanks. As I said earlier, the question came to me during the wide-ranging discussion that we were having.

The Convener: Nicola, would you like to come in?

Nicola Taylor: On the challenge for schools, I would like to add that the conversation is bigger than just internet safety because it is also about password authentication and all those other things, which makes it a more significant task and a bigger conversation than we have probably been able to have to date.

I stress that things are definitely happening in schools. For example, most schools now are big supporters of internet safety day, which is a whole day that is dedicated to online safety, during which assemblies and workshops are run throughout the schools. The information is disseminated from a group, so it does not add to the workload for the teachers—it is provided in packs that they can just deliver in the classrooms. Those schools where there are Chromebooks and iPads and so on, either in the classrooms or that are given to the individual pupils, get information on being safe online, ensuring that their passwords are not shared and those types of things.

There are also initiatives that allow the private sector to go into schools and share more information. For example, we run a digital critical friends programme, and there are science, technology, engineering and mathematics ambassadors and other initiatives as well. Should schools want additional information, they can certainly get access to it.

11:30

Adam Stachura: The question is a really good one, and it goes beyond schools. There is a considerable appetite on the part of the public to be as informed as they possibly can be about how to mitigate against threats and generally to be safe, live their lives and not be attacked online.

One of the most popular of our 70-plus information guides at Age Scotland is about scams and fraud. That is updated semi-regularly, because the nature of those issues will change a lot. The key elements that are required for good information are that it is not patronising and that it is simply written, without using jargon like “2FA” or “MFA” and all the rest of it, otherwise people will say, “I don’t know what that is,” and they might immediately switch off, so to speak.

There is a question of how people access free, low-cost systems to protect themselves. That might be built into certain digital devices, but if someone gets an approach via text message and clicks on a link, they might not be sure how secure their device is or whether they are protected from malware or ransomware. That may be especially true for those people who are no longer in the workplace, who are using their own personal devices. About 15 per cent of pensioners are in poverty, and half of Scottish pensioners have incomes lower than the threshold for paying income tax. It will be pretty tough for them to keep up with and pay for technology if we expect them to operate online.

There are some things that we could try to make available to people so that they know where to go to get good protections for themselves. A great example that Cyber Scotland put together a few years ago, to which we contributed to some degree, was the “Digi ken?” adverts. In those adverts, Fred MacAulay was the host of a game-show type thing, and the older person got all the questions right—they were not the person who was wrong. It was a great series of adverts, and it involved password updates, two-factor authentication and people updating their devices.

At the time, it seemed almost to be a new issue. Could we create a case to keep doing such things? It was obviously important, but it could have been a bit of a flash in the pan. It is an important responsibility for public services, the Government and other bodies to have regular discussions using smart and engaging ways to talk about how people can be safe online and protect themselves from cyber risks, and to fund that well enough. It should not just be something for cyberawareness week or scams awareness week; it has to be every blooming week if it is going to be helpful.

Jude McCorry: It was the Cyber and Fraud Centre that created those adverts, with Fred MacAulay. That was at a time when Fred was cheaper because of Covid—if he is listening or watching today. STV, as a partner, was a very good platform to help get that message out, and that collaboration worked, too.

Going back to the point about platforms, which I had forgotten about and we have all probably forgotten about, I note that we are talking about harm to kids and harm to older people as well, and the platforms that allow that are not carrying out their duty of care. It is quite difficult, as police and banks will tell you, for us in Scotland to contact the platforms and to get anything done when we find harmful content or if we find a way in which children or older people might engage in harmful content. It would be good if the Government could do anything to take the big platforms to task, pointing out that some people are paying for that—indeed, the platforms are getting paid per user. They have to carry out that duty of care to protect the people who use their platforms.

Rona Mackay: Adam, I am thinking about the number of bank closures in our communities. That genie is out the bottle; we are not going to go back to traditional banking now. Do you have evidence of some of your members or older people not wanting to use banks now because of the threat that they might lose their money? Are people going back to putting their money under the mattress or that sort of thing?

Adam Stachura: I do not necessarily think that it is going under the mattress, although there is certainly a level of concern about how to access banking systems, because people do not necessarily feel that they have the support. That is why people are so exercised about losing a bank branch. Without wanting to go over the old ground on that, footfall will change in bank branches, because people are not cashing in pay cheques and pensions every single week: that is not done in the same way as it was. The nature of what branches were doing changed over time. We have had a strong view for years that branches have an important role in supporting people to change how they bank and to help them, in person, to learn how to be safe online, how to access financial information and how to develop some degree of financial independence using different products.

Rona Mackay: Do you think banks have a role to do that?

Adam Stachura: I do. There has been an absolute move away from banks being on our high streets and in our communities. Of course, the default had been to use the Post Office for simple things, but it does not really do all the same things; it is for simple transactions. When the Post Office network is under threat or is fragile, there is no resilience there. We have been promoting shared banking hubs since 2016. That has been taking off, but there are parts of the country where that has not developed yet. I presume that members here have sometimes looked for such solutions in their constituencies or areas where that is not yet.

It is a challenge for people to be able to bank and have financial independence if they are wholly reliant on being online. There are a number of people who are not comfortable with that, and there is a risk that they might be left behind. Our financial lives are much more than simple cash-in, cash-out transactions. That is not really what branches were doing. They were fantastic places on high streets across the country where people were able to do something different to support customers.

I did not realise that NatWest was represented in the room, and this is not meant as a direct dig, but you will probably have seen Age Scotland comments and outcry over the years about the closure of bank branch networks. I have spoken to your colleagues about that. If you are moving everyone, broadly speaking, to digital use, there is a responsibility to consider what else you can do to support them. Chris Ulliott made a point about the proliferation of systems and the importance of making things available to customers. The system that you have at your end might be safe—sorry: I am referring to any bank, not just NatWest—but people's access point into it might not be.

To go back to your point, Mr Macpherson, we have seen lots of examples of callers purporting to be from someone's bank, and it is pretty convincing. It is possible to mask phone numbers, and the caller might say, "Just look at the back of your bank card: we have the same number. Of course you can tell us these things."

The ability to go into a branch, speak to a real person and get some security is invaluable. We will lose that, and we will have a hidden challenge of people who do not feel comfortable with interacting with society and having their own independence, without relying on a family member to do their online banking—which opens them up to financial harm and elder abuse.

Rona Mackay: There are much wider consequences.

Adam Stachura: Yes. That is at the extreme end but, if we want, as a country, to support people to live independently and live well, all those factors are important.

Rona Mackay: I have another question, for David Keenan. You might not be able to answer this, and you may not want to, but, when your organisation was attacked in 2022, what did it cost you? What did you lose in business? Do you have that figure?

David Keenan: It is difficult to put an exact figure on it, and it depends on exactly what you include, such as loss of revenue and legal fees, but we would put the figure in the tens of millions of pounds.

Rona Mackay: How long did that period last, when you were under attack?

David Keenan: The attack itself lasted a matter of hours. The recovery period was six months plus.

Rona Mackay: That is amazing.

Ben Macpherson: I am sure that you would want me to say this, convener, as would others. For anyone listening, if anyone phones you pretending to be your bank, hang up and then phone your bank back. That is a really important message to send out.

The Convener: We have carried out our crime prevention duty for the day. [*Laughter.*]

I will stay with David Keenan, and I might bring in Chris Ulliott. I made a point earlier about the emotional impact, particularly on your workforce, David, of the entire disruption, and not just on the service that you offer through your business. Was there a feeling across your staff body of being targeted, or of being a little bit vulnerable?

I am very interested in how being attacked in such a hard way impacted your workforce. It is something that we perhaps overlook—we talk about our older population and protecting young people but I am interested in how such attacks impact people who work in an organisation, including, for that matter, Marks and Spencer.

David Keenan: The immediate aftermath of the attack was almost pure shock at having experienced it; then, it quickly went into response and recovery. The efforts of the IT department teams to recover from it were absolutely heroic. It was long months of 12 and 14-hour days to restore the systems.

Outside of the IT team, the impact on employees across the wider organisation was very much around their inability to do their job day to day and the frustration of facing customers who were coming in and were not able to transact with us in the way that they expected to. Lots of members were not able to perform their roles or, in some cases, not able to perform them adequately—in the way that they expected—for months post-incident. That was very difficult.

The Convener: Chris, do you have a view on the emotional toll on victims and the impact on their wellbeing?

Chris Ulliott: Yes, that is when I get very superstitious and touch wood—as I just did. As a bank, NatWest has remained robust against the attacks that we are seeing but I have worked with peers in other industries who have fallen victim to them. They take a huge toll on the workforce; the recovery can involve many months of working around the clock to fix systems. That aspect of the impact should not be underestimated. I have huge sympathy for Marks and Spencer and the firms that are currently recovering from attacks, because I know what they are going through.

For the community of people who do my job in industries, one of the hot topics is how to prepare for that response—we talk about how to get food and water in and whether we would need to have sleeping accommodation in the office. There is a whole load of things that we do not think about, which companies must do to manage that recovery when those attacks happen for real. They take a huge toll on people, so we absolutely think about that.

Although it is fantastic—and I am glad—that Marks and Spencer is still here to talk about it, it is probably worth saying that a lot of companies around the world have gone out of business because the cost of recovery was too much. At that point, it is not only about the loss of a business but also about all the staff who have lost their jobs. The impact is quite wide. The attacks that we have been talking about have a real impact in a wide range of ways that we really need to be conscious of.

The Convener: Stuart, your police officers deal with victims every day. Are officers perhaps given some support, or even training, on how to interact with victims of cybercrime, and the advice and support that officers can offer them in the aftermath?

Assistant Chief Constable Houston: It is really important that the people who speak to the victims know about and understand the technical questions that we need to ask. That is important because we do not want to have to go back to somebody three or four times, with different people asking different things, which would only retraumatise. It is about getting that right in the first place.

From now on, as part of our approach, we will look to use the fraud, cybercrime, reporting and analysis service, which is administered by the City of London Police but covers all UK forces as part of Action Fraud.

It is also important that the first contact that someone has tells them what they need to do. We can advise them to stop immediately to ensure that they do not lose any more money—if the fraud involves money—or if some sort of harm is going on and they are still connected to the person. It is important to give the right advice from that first point of contact onwards. We have to ensure that we do that from that first engagement.

It is then about following through with aftercare opportunities. I pointed towards some of the third sector organisations that might help—Age Scotland and others. People could go back to their bank, too, and ask the right questions about the financial support that it might be able to offer through its different care packages. We cover victim care in a wide range of ways.

The Convener: We have a little bit of time in hand, so I will come in with a couple of questions on issues that we have already touched on. I am happy for other members to come in with final questions, too.

11:45

My question is about European Union co-operation. Coincidentally, last month, the committee heard evidence from academics on criminal justice co-operation with the European Union. We were told that access to the European Union Agency for Cybersecurity would be

> "relevant to co-ordinating cybersecurity positions and highlighting new cybersecurity threats that have emerged."—*[Official Report, Criminal Justice Committee*, 30 April 2025; c 7.]

Is the loss of access to Europol or the European Union Agency for Cybersecurity and to their databases impacting on or hampering our effectiveness in the UK in tackling cybercrime? Given that we are in the middle of the trade and co-operation agreement review, should anything be raised or discussed to address gaps in criminal justice co-operation, particularly in the cybercrime space that we have been discussing?

Miles Bonfield: The tech arrangements that were put in place are effective. They have been used very well by UK law enforcement, particularly by Police Scotland, in order to ensure continuity of co-operation and collaboration with European law enforcement and prosecuting agencies. Because of the extraterritorial nature of the threat, there is a need for shared awareness and common purpose across agencies.

I am talking for Stuart Houston here, but Police Scotland is an active member of the Europol joint cybercrime action task force and leads some of its work.

The National Crime Agency supports the wider Europol network and ethos, and we ensure that the UK is well represented, that forces such as Police Scotland have a place in that network and, most importantly, that we support that work and do not get in the way of it. We will seek to continue to do that and to strengthen that collaboration further if there is an opportunity to do so. However, that is a political discussion and an agreement to be made by those who are democratically elected to do so.

I hope that that answers your question.

The Convener: Does anybody want to come in on that—perhaps Stuart Houston or Chris Ulliott?

Assistant Chief Constable Houston: Police Scotland still has an officer at Europol and an officer at Interpol. Those officers strengthen our relationships and ensure that we are kept up to date on matters on a daily basis. We are an active member of the task force that Miles Bonfield commented on, and we engage regularly with it.

Cyberinvestigators across the world are a unique group of people. That group crosses into the private sector and other agencies really easily because there is a shared threat. It is important that we are part of the group that looks at that shared threat and that we collaborate as much as possible. Any improvement in terms of collaboration would be great.

On some of the challenges that lie ahead, we have the dark web and encrypted platforms that may operate outwith Europe or even outwith the remit of the United States. That may become more challenging, but we are all facing those challenges together, and countries are all working together.

The Convener: Rona Mackay, do you want to come in?

Rona Mackay: Not on that point.

The Convener: I will come back to you.

I have a follow-up question. Jude McCorry, your submission referred to EU-UK co-operation and to organisations facing

> "budgetary pressure or geo-political changes and challenges to keep supporting their own entities."

Do you want to say more about the issue of co-operation?

Jude McCorry: We have a dependence on other people helping Scotland. As an Irish person, I can say that everybody wants to help Scottish people, but we are seeing all these budgetary pressures in the US, Europe and in other countries, so we need to be mindful that those pressures could affect threat intelligence and other projects that we are doing. Things that happen outwith Scotland will affect us.

The Convener: Got you. Thank you.

Ben Macpherson: I have attended events during cyber Scotland week, which takes place in February or March each year. In 2020, one of the most powerful presentations that I saw was from colleagues from Estonia; conversations with them were also some of the most powerful. In that jurisdiction, they are right on the edge of Europe, and they spend a lot of time combating cybersecurity attacks from the Russian state. Are we learning from those countries, which are at the forefront of not just the battle but the expertise?

Jude McCorry: We have a good connection with Viljar Lubi, who is based in the UK. It was probably Viljar who you spoke to. He is the Estonian ambassador to the UK, and he regularly visits Scotland. I think that we also have an Estonian ambassador here. I cannot remember the name of the person who was appointed—it is a Scottish person.

Ben Macpherson: It will be a consul general.

Jude McCorry: Yes—a consul general. Those relationships exist. Estonia has huge budgets for that work, but it finds itself in a unique situation. The history of what it has had to go through has meant that it has invested very heavily in cybersecurity. There are conversations going on between Estonia and Scotland.

Ben Macpherson: We are aware of the countries that a lot of the organisations that undertake cyberattacks work from—Russia being one of them—taking money from law-abiding people in our democratic country out of our country to other places. Is there a wider concern about that finance being part of the build-up of power and abilities by organised crime groups or whatever groups there might be in other jurisdictions? Everyone is aware that there are organisations in Russia that carry out organised cyberattacks, but where else in the world does that happen?

Chris Ulliott: The money goes to many places and funds some regimes around the world that are not aligned to our interests. That is one of the reasons why the National Cyber Security Centre is heavily promoting the message not to pay a ransom, for example. The agency can see the money going out of the country to support either the development of further crime networks or, in some cases, nation states and regimes that are not aligned to our interests. We absolutely have to be aware that, in a large number of cases, that money is leaving the country, which is to our detriment on many fronts.

David Keenan: These are professional organisations—it is an industry—and they are doing it because they want to and can make money and because companies in the UK can and do pay ransoms. That is something that should be considered.

Jude McCorry: Companies can also be insured, and their insurance company pays the ransom.

Rona Mackay: This question is probably for you, Jude. I apologise if I missed this earlier, but when companies and retail organisations such as Arnold Clark or Marks and Spencer are attacked, how safe is our personal data? Like lots of people, I shop online with Marks and Spencer.

Jude McCorry: An announcement was made about that yesterday. At the beginning, Marks and Spencer announced that it did not think that any personal data had been taken, but yesterday it announced that customer data has been taken—not banking details, but customers' names, addresses and purchasing history.

Rona Mackay: Oops.

Jude McCorry: Yes, it is really bad.

I go back to what we were saying earlier. Everybody should check out the website haveibeenpwned.com and put in their email address, or email addresses, to see how many times the companies that they deal with have been attacked and where their data is.

Make sure that you change your password—

Rona Mackay: I was just going to ask what a person could do in that situation.

Jude McCorry: As Marks and Spencer customers, we should have changed our passwords when we knew that it had been attacked. We should ensure—I include myself in this, as a citizen—that we are not using the same passwords across different shopping sites. I also do not save my card details to shopping sites, because that information could be taken.

We should also build in extra security. We have two teenage girls and we verify all shopping from Amazon. They cannot order stuff until we see what they are ordering and ensure that it is them doing the ordering.

I know that, for online shopping from Next, you can use 2FA by ensuring that you have two-factor authentication set up in your security settings. There is an Irish saying, “to be sure to be sure”, which is the only way that I can describe two-factor authentication.

Make sure that you are following the guidance and advice, but be a few steps ahead once you know that there has been a data breach. I am not saying this to cause hysteria; I am saying that you should have a healthy paranoia all the time about your personal security as well as business security.

Rona Mackay: That is helpful, thank you.

Pauline McNeill: Over the past two hours, it has become apparent—as I think that Ben Macpherson was suggesting—that this is a much bigger area of criminal law and social concern than we realised at the beginning of the evidence session. I am clear about that.

Chris Ulliott, should the Government legislate to outlaw the payment of ransoms?

Chris Ulliott: Oh, that is a difficult question. My personal feeling is that I would not pay a ransom, but I am conscious that there might be some extreme circumstances in which, with the right support from law enforcement and the Government, paying a ransom might be the lesser of two evils. Ideally, we should never pay a ransom, but I can imagine some circumstances in which it would be really hard not to, so I would never say never.

Pauline McNeill: Should we have more regulation around whether or not to pay ransoms, given what has been said about where the money might be going?

Chris Ulliott: Yes, absolutely. I would encourage anyone in that situation to engage with law enforcement, the Government and the relevant agencies so that there is a combined decision on the best approach to take. I would discourage anyone from unilaterally paying a ransom.

Pauline McNeill: Stuart Houston, I think that you said that you have difficulty recruiting people to fight cybercrime. Is that correct?

Assistant Chief Constable Houston: It is more about finding the right people. Policing is built on the model of someone with a warrant card going out and doing the role, but we need a mixed workforce. A lot of the work that is done on cybercrime in particular does not need to be done by someone who has been a police officer for a number of years. We need to take a wider look at the skills that are available in some of the universities in Scotland. How can we bring those people into roles in policing as part of a mixed workforce to look at cybercrime, rather than just using police officers?

Pauline McNeill: Would that be done by the National Crime Agency or by Police Scotland?

Assistant Chief Constable Houston: It would be done by Police Scotland, although I know that the National Crime Agency also recruits people from different backgrounds. The people whom we recruit may not always be from a law enforcement background—they may be data scientists or ethical hackers, or anyone else with a more specialist skill set that would enhance our capabilities.

Pauline McNeill: Are you able to recruit people with those skills directly, if you decide that they are needed?

12:00

Assistant Chief Constable Houston: Absolutely. We are looking at how we can increase our police staff numbers through having a mixed workforce rather than just police officers. Again, however, that requires funding and an increase in capability with regard to how many people we can bring in to do those jobs. We need to ensure that we can still support the front line of policing while also having the right people with the right skills in what can be, at times, a more technical area of law enforcement.

Pauline McNeill: Given what we have just heard, including about the international aspect of cybercrime, fighting crime that is perpetrated by people who are clearly very skilled and intelligent may be a very attractive career to somebody who sees that they could use their skills to go after those people. Do you agree that a bit more discussion and public promotion of the need to resource this area might attract the people whom you need?

Assistant Chief Constable Houston: Definitely—again, that comes back to how we fund that resource and change police numbers into police staff numbers in certain areas. This area in particular is one in which I see the benefit of doing that. We have already had civilian investigators coming into roles for which a warrant card is not required. It is important that we get the right people in this area of business.

The Convener: Does Miles Bonfield want to come in on that?

Miles Bonfield: Just to cap that off, it is for Police Scotland to decide on the skills mix that it wants and how it wants to achieve that. The NCA has regular on-going conversations with Police Scotland, not just about cybercrime but across the piece, about where we can provide a national service once, and do it cheaply to get best value for the taxpayer, and where that is better delivered in Scotland.

At an industry level, we might want to bring in people such as data scientists, data engineers and data architects, so we have a conversation about whether it would be useful for the NCA to provide those people as a service to the law enforcement community or to UK plc, or whether Police Scotland requires to have those capabilities in-house. We have really strong relationships at command and operational level, and the conversation about the threat and those responsive roles is on-going.

The Convener: I know that we are just slightly over time, but we will probably not have the opportunity to have such a large amount of expertise in the room again, so I will shamelessly take advantage of that.

I have a final question, about ransomware; Pauline McNeill touched on that a moment ago. For a business, what are the pros and cons of paying a ransom versus not paying it? I note that David Keenan's business presumably had to ask itself that question—you may not wish to pick up on that, David. Nevertheless, are there things that businesses need to consider in dealing with that awful dilemma?

Chris Ulliott: Absolutely. From seeing a lot of countries around the globe face that dilemma, we have learned the lesson that, ultimately, we are dealing with criminals, and even if we pay, there is no guarantee that we will have a solution to the problem. We have seen instances where people have paid and then, at a later date, the criminals have come back and said, "We said we'd delete the data, but we didn't—this time we will, if you pay us again."

On the flipside, there are occasions when paying gives a business a tool to accelerate its ability to recover. Those occasions are quite rare, but if a business is in a very difficult situation, that is something that it would have to consider. However, the money is going to criminals and is possibly leaving the country, so we would not want to encourage that.

It is a really difficult dilemma, and I do not think that any two instances are the same, but evidence has shown that paying does not always—indeed, it frequently does not—solve the problem, and that needs to be a big factor in considering what to do.

The Convener: Yes, absolutely. Does anyone else want to come in on that?

Jude McCorry: We have seen it—as the police will have done—from both sides as well. We are not here to judge or critique people on why they make a certain decision. There are conversations, and those decisions are well thought through. I am sure that people who have not paid were tempted to pay during the process—I can say that with hand on heart.

One case that presented a moral dilemma—in which I agreed with the business on why it was going to pay—involved a legal firm that was attacked. The firm knew that some of the data that had been taken included witness statements and details on victims of rape and other crimes, and that, if that data got out into the public domain, it would be really harmful to those individuals.

The firm was put under pressure by the board to pay the ransom. It was not a huge amount of money—not the millions of pounds in ransoms that we hear about—and the firm was insured to pay that via its cyberinsurance, so it was paid. However, two days later, the data was still dumped on the dark web.

In that case, I tried to make the person from the firm feel better about it by saying, “If you hadn’t paid the ransom, the board would have said that you made a decision not to pay and the data was dumped, but you did pay it, and the data was dumped anyhow.” Sometimes, it is a case of damned if you do and damned if you don’t. Most organisations that we deal with do not pay the ransom, but there are a lot of unreported ransoms that we feel that organisations have probably paid.

The Convener: Does David Keenan want to add anything?

David Keenan: Payment of the ransom was discussed, of course, and we took the decision that we were absolutely not going to pay it. However, we were in the fortunate position of having robust back-ups in place, and we knew that we would be able to recover our systems and our data.

We initially completely refused to engage with the criminals, but we learned relatively quickly that the engagement with them, and the negotiating process, was a useful tool in being able to draw out the length of time that it took them to dump the data on the dark web. That allowed us to make contact with our customers and inform them of what had happened. The negotiating tool was useful for us as part of our response, but—as I said—there was never any intent to pay the ransom.

However, a lot of organisations would not have been in the fortunate position of having back-ups to enable them to recover from the situation, and I would not blame any organisation, when faced with that decision in those circumstances, for considering paying the ransom.

The Convener: Yes—it is a very difficult one.

I see that Miles Bonfield wants to come in.

Miles Bonfield: As we have heard, it involves a very nuanced threat from a loose association in a subculture involving individuals right through to criminals who are linked to the states that mean to do us harm, so it is really difficult to make a judgment, as individual circumstances are very different.

On the point about using it as an opportunity and contacting law enforcement as quickly as possible, that is an important message, along with “Don’t click on the link” and “Hang up if the call is suspicious”. The message is that if there is a ransomware attack, people should contact law enforcement, because of some of the issues that we have heard about from Chris Ulliott and David Keenan.

The Convener: We will draw the session to a close there. We have gone just a little bit over time; I am sure that we could spend another hour throwing questions at the witnesses. The session has been very interesting, and we are grateful to you all for your time. I thank you all for joining us this morning.

I suspend the meeting for 10 minutes.

12:08

Meeting suspended.

12:19

On resuming—

Secure Accommodation

The Convener: Our next item of business is consideration of the correspondence that we received on 29 April 2025 from the Minister for Children, Young People and The Promise, Natalie Don-Innes MSP.

The letter provided an update on the Scottish Government's work to restore secure care accommodation capacity for young people in Scotland. I refer members to paper 3, which contains the letter. We will discuss our views on what action, if any, we want to take in response to it.

Does any member want to come in with comments or observations on the correspondence?

Pauline McNeill: I am glad that the subject has come up. There is a crossover between our role and the role of the Education, Children and Young People Committee in relation to secure accommodation.

From our perspective, it is important to keep an eye on the matter to make sure that, in meeting the commitment that no young person under the age of 18 will be in custody but will instead be in secure accommodation, that does not give unfair disadvantage to the young people who are in secure accommodation on other grounds and that there is sufficient accommodation.

A rumour was circulating—although it was not confirmed—that a case was in court about a week ago for which secure accommodation was not available. That has not been confirmed. However, at the time of a statement on the issue, I asked the minister whether she was satisfied that there will be enough accommodation.

When it comes to court matters, the sheriff has no cause to ask whether accommodation is available; they can ask only whether the person will be detained. Previously, the sheriff would have asked about that and, if secure accommodation had not been available, some other arrangement would have been found. That is why people such as William Lindsay Brown ended up in Polmont prison. It is vital for the Criminal Justice Committee to monitor that area as the policy is embedded.

The Convener: The correspondence from the minister outlines an update on secure accommodation contingency planning and ensuring capacity, and details some of the work. You are right that that is one of the key areas for this committee—we should be provided with updates and follow the developments.

Rona Mackay: I agree 100 per cent with Pauline McNeill's comments. The situation is ongoing: St Mary's Kenmure in my constituency paused admissions, which caused a shortage of beds. That pause has been lifted, but there are still fewer beds than there were before. I see that Rossie up north has four new beds, but do they offset the ones that St Mary's has lost? There is an issue with capacity.

I am keen to ask for an update on the reform of the contractual model for the provision and financing of secure places. The Justice Committee tackled that question in the previous parliamentary session, and we are not in a different situation now. We should ask for an update on that model, although one may be coming.

The Convener: That is a good point to raise. Although there is an update on capacity at Rossie, what is it in addition to, and how does it affect the overall figures? I have made a note on the reform of the contractual model too—thank you.

Sharon Dowey (South Scotland) (Con): I share the same concerns about capacity. I am also interested in the processes when capacity is reached. When somebody needs to go into secure accommodation, and there is none because capacity has already been reached, what is the process? Where are the kids going and what are we doing about it?

The letter highlights the new post of a "dedicated professional lead". I would like to know more about what that is and what improvement it will give to the service. It also highlights a

"contingency plan with up to £2 million"

in funding. What will that additional funding achieve? Will it achieve extra numbers in accommodation and how will that impact the service?

Liam Kerr: I am musing on something based on what Rona Mackay said. It is hoped that St Mary's will go back to having 24 beds before the summer. The minister said that she will update us before the summer, which we may want to note in order to make sure that it comes through.

Let us say that St Mary's goes back to having 24 beds. As Rona Mackay pointed out, Rossie has added four contingency beds. As I understand it, those places need to operate at 90-plus per cent capacity in order to break even. If St Mary's goes back to having 24 beds and Rossie adds four, what impact does that have, given the capacity that Sharon Dowey talked about, on the 90 per cent break-even point? There might be nothing in that, but listening to the conversation I wondered whether we need to satisfy ourselves about it.

The Convener: Thank you for that—I have made a note of it.

I propose that we seek further information from the minister—which may be forthcoming in any case—on the points that we have covered: whether what is being proposed will be sufficient accommodation; clarity on capacity and reform of the contractual model; what happens when capacity is reached and what the arrangement is for that; and, as Liam Kerr said, the impact of restoring capacity at St Mary's, taking into account the four beds at Rossie, set against the 90 per cent capacity requirement.

Rona Mackay: There is a statement to the Parliament tomorrow about secure care. Some of those issues may be clarified.

The Convener: Thank you. Are members agreed that we will highlight those points? We are aware that a statement is forthcoming later this week, during which some of the points may be covered.

Members *indicated agreement.*

The Convener: Before we move into private session, I remind members that our next meeting will be on Wednesday 21 May and our main item of business will be to hear from a public petitioner, alongside other witnesses, on the issue of making non-fatal strangulation a standalone criminal offence in Scotland.

12:27

Meeting continued in private until 12:56.

Published in Edinburgh by the Scottish Parliamentary Corporate Body, the Scottish Parliament, Edinburgh, EH99 1SP

All documents are available on
the Scottish Parliament website at:

www.parliament.scot

Information on non-endorsed print suppliers
is available here:

www.parliament.scot/documents

For information on the Scottish Parliament contact
Public Information on:

Telephone: 0131 348 5000
Textphone: 0800 092 7100
Email: sp.info@parliament.scot

The Scottish Parliament
Pàrlamaid na h-Alba