CREST

CMAGE
Cyber Security Maturity Assessment Global Ecosystem

Good Practice Guide

Establishing an Effective Law Enforcement Cybercrime Unit

August 2022

Government

Establishing an Effective Law Enforcement Cybercrime Unit

Contents

Foreword

This guide aims to assist countries in assessing their own needs and requirements regarding law enforcement capabilities required to address cybercrime. It is part of a wider programme of support to help countries strengthen and improve their overall financial services.

Many steps may have already been taken, so this guide is designed to complement those steps and help countries identify gaps or areas that could benefit from additional development.

The guide is compiled from research and engagement with organisations that have experienced the issues described here.

Whether you are starting out on a developmental journey or have already put some capabilities in place – and are looking to strengthen or add to these – this guide will assist you.

The document is guidance, it is not prescriptive.

It aims to act as an off-the-shelf guide for establishing cybercrime capabilities as part of a National Cyber Security Strategy or equivalent policy. The guidance delivers a generic overview of the component parts that could, or should, be considered when introducing an effective law enforcement response to cybercrime threats.

It is based on the author's knowledge, skills and many years of experience working as a senior police office and consultant, building and delivering these capabilities in the United Kingdom.

It is hoped that this guide, taken together with the other elements of this support programme, can be used to develop capabilities to combat the threat from cybercrime and help citizens build more prosperous and secure lives for themselves, their families, and their communities.

Author Profile

Rob Harris
Cybercrime Subject Matter Expert and Consultant

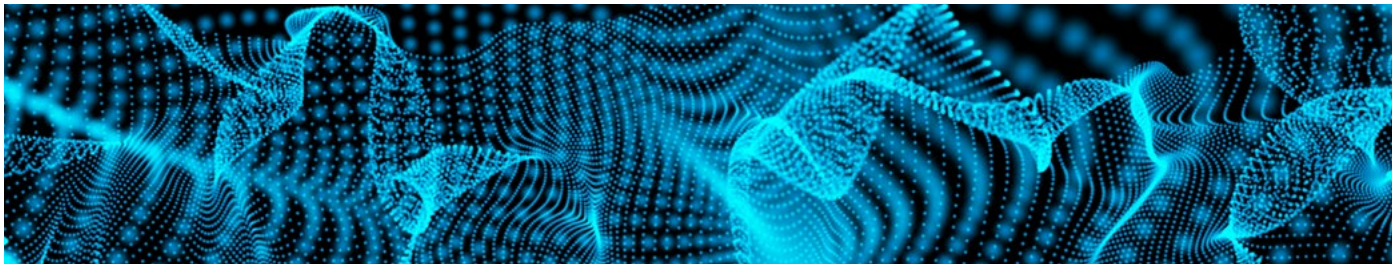
Rob has over 30 years' experience of law enforcement, becoming a police officer in 1989 and spending much of his career in criminal investigation. Rob gained extensive experience in serious and organised crime, as well as financial investigation, fraud, Digital Forensics, and towards the end of his service, cybercrime.

In 2013 he was involved in developing the UK's Regional and National Cybercrime Network. Since 2018, Rob has been part of the UK's National Police Chiefs Council (NPCC) Cybercrime Programme Team. As part of this role, he helped deliver the recent uplift of local police force based cyber capabilities, which saw the introduction of local police cybercrime teams across all 43 police forces in England and Wales.

Now retired from the police, he has continued in the NPCC role and provides services as a consultant and subject matter expert.

Introduction and Requirements for an Effective Cybercrime Unit

Technology is transforming the world, opening up a global community and paving the way for innovation and development in all aspects of society. This has enabled greater access to the online world, bringing products such as shopping, entertainment, news, media and social networking to more and more people.



Meanwhile, business has evolved. Whole industries rely on the internet to trade and provide services. This has created greater opportunity for improving the quality of life for a significant number of people. People who, for the first time, can access banking and financial services, as well as important social support mechanisms such as health care, education and employment.

Our lives are becoming more entwined with the digital world. As this reliance grows, so does the threat from hostile actors, looking for new ways to exploit victims, steal property, infiltrate organisations and attack governments.

Essential services now rely on technology and the integrity of systems, structures and data required to function. A breakdown in systems, structures and data can have catastrophic impact, undermining confidence in the integrity of those systems, and in the ability of government to function correctly. Ultimately, this can impact a country's wider economy.

At individual level, a breakdown in essential services will restrict access to those services and degrade the ability to improve quality of life. Just as in traditional crime, cybercrime victims can be massively impacted, with far reaching effects.

Any internet search will provide several estimates of the economic impact of cybercrime, which most agree runs into many trillions of dollars globally each year. However, the damage is not just monetary.

In many countries, the most common crime is now a cybercrime of some description.

This introduces a new challenge to law enforcement, which not only involves a threat to national security, but also creates an environment where everyone and everything is potentially vulnerable.

There are many documented examples of incidents that bring this into sharp focus, including:

- Terrorism
- Large scale theft
- Theft of intellectual property and research material, and
- Crippling of critical national infrastructures – grinding an entire nation's functions to a halt.

Introduction and Requirements for an Effective Cybercrime Unit

This does not just stop at state and industry level. Some attacks can have significant impact on an individual, including a loss of opportunity, and in the worst cases, threat to life. The effects of a single successful cybercrime attack can prove devastating and have wide-reaching impact on society.

One of the main responsibilities of government is to protect and safeguard its citizens, which includes national security, law and order, and administration of justice. Citizens must have trust in this protection, including the effectiveness of its structures and its ability to keep pace with emerging threats.

National policy, effective strategies and infrastructure, and investment in combating cybercrime is now vital in helping establish trust and should feature prominently in a country's approach to discharging these duties. Government must play a clear leadership role in combating cybercrime and demonstrate genuine commitment to tackling threats.

However, no one group, organisation or section of government can do this in isolation. The approach needs to be inclusive and involve strategies which bring together effective partnerships with a shared vision of tackling the threat beyond simple criminal justice.

This includes looking at the root of the problem and introducing ways to help individuals and organisations to protect themselves and better recover when an attack happens. Any approach to tackling cybercrime must also include ways of identifying and diverting people (who may be vulnerable to engaging in unlawful activity) away from a life in cybercrime. Everyone has a part to play in this. Any solution needs to have joint initiatives with a cross society and cross government approach, where everyone understands and acknowledges their own digital responsibility.

Cybercrime does not respect geographical boundaries, meaning threats can come from anywhere and impact otherwise unconnected areas or regions in a country. This presents two issues:

i Threats can originate from territories outside of a country's control or influence. Furthermore, some of those threats could come from within uncooperative regions in the world, or even from rogue nation states.

ii Any local or parochial response in isolation is likely to be compromised and inefficient, as what may appear to be a single incident could in fact be far reaching and affect other locations within the country, as well as other nations. Therefore, any structure and response also needs to address the geographic threat and have elements capable of protecting national interests globally through work with international partners. This also requires consideration around national security, domestic interests, and a network that covers national, regional and local law enforcement responses. These must all be sufficiently joined up to share intelligence, assess the various threat landscapes and work together when required.

In considering law enforcement responses, there needs to be acknowledgement that this may present new challenges. The traditional investigative approach to crime becomes difficult as, unlike other crimes, such as theft, assault or house burglary, the relationship between victim, offender and location is not as evident within cybercrime and often does not exist.

Material evidence presents in different ways. Suspects can appear anonymous, and tactics used to track, trace and trap suspects require new tools. Also, methods used to commit cybercrimes are by nature often very technical, which many may find difficult to understand.

Introduction and Requirements for an Effective Cybercrime Unit

A fresh approach is required, and staff skills involved in responding to cybercrime incidents can be different to those usually found within policing. It is also important to recognise that policing will not have all the answers, and that a strong relationship with industry and academia is required.

A police or law enforcement cybercrime unit needs a careful blend of skills, as well as access to relevant training in technical matters, and the ability to procure and use technical equipment within the legal frameworks of their respective country.

Another part of a state's responsibility to its citizens includes developing and maintaining economic growth, fostering social mobility, and providing equality of opportunity. In the UK, it is now recognised that fraud and cybercrime make up more than half all recorded crime, and technology features in some way in the majority of offences.

Other countries will have similar results, demonstrating the necessity for action and a requirement for some form of law enforcement cyber capability, underpinned by a host of national policies. This must include due diligence to technology and cyber space.

An effective cybercrime unit requires sufficient investment to not only build, but also sustain, a blended response to the problem that keeps pace with the threat, nurtures a resilient cyber ecosystem that supports communities and is a deterrent to those looking to try and exploit it.

Experiences from International Partners

1.0 Experiences from International Partners

Introduction

Law enforcement and policing have been around for hundreds of years. Over this time, successive generations have honed their skills, with new tactics and advances in evidence gathering improving the way we do business.

The development of forensic capabilities such as fingerprint identification, fibre comparison and DNA analysis gave us new tools. But in the last few decades, technology has transformed society and created new investigative opportunities that break away from methods our predecessors relied upon.

Of course, with new technology comes new opportunity, which also means new ways for criminals to take advantage and develop their own tactics to exploit new opportunities.

This has resulted in brand new types of crime, as well as some existing crime becoming transformed and industrialised, capable of being committed on a scale never before possible. This challenges law enforcement. Across the globe, a race to catch up is underway, with police officers and staff having to learn new investigative methods and develop fresh tactics.

In this section, we will look at some of the challenges teams and organisations face, consider fresh opportunities, and examine some of the more challenging aspects of this new requirement to combat cyber threats.

To begin with, agencies may need to identify new threats, requiring a dedicated specialist response; and what are simply old crimes, being committed in a new way. This can help with investment and resourcing decisions.

Clearly, trying to train and equip every police officer, security services agent, prosecutor and judge to the level of an ethical hacker or tech industry expert is impossible. But by understanding the differences in cyber threats faced, governments and agencies can make informed decisions on how to approach threats in the most efficient way. They can channel investment and resources into areas of greatest impact, such as new specialist cybercrime teams, while maintaining a level of service that addresses the needs of all citizens.

“Of course, with new technology comes new opportunity, which also means new ways for criminals to take advantage and develop their own tactics to exploit new opportunities.”

1.0 Experiences from International Partners

1.2 What is Cybercrime?

How do you define "cybercrime"? It's an important consideration when you take into account the potential volume of offences capable of being committed using technology.

Consider two friends falling out, where one embarks on a campaign of threats and harassment over social media. Is this a "cybercrime"?

If offences such as this were to be categorised inappropriately and allocated to specialist, highly trained cybercrime teams, those teams would soon become overrun with the sheer volume of offences and be inefficient in their approach.

To manage cybercrime threats, consideration should be given to setting criteria of what will and won't fall to the specialist resources, with their appropriate levels of training and technical capability.

Of course, this highlights the need for all elements of a law enforcement organisation to have sufficient general levels of cyber awareness and the abilities to deal with everyday demand where technology plays a part – a topic we will consider later in this guide.

We suggest an approach that looks at crimes directed at computers, such as hacking or denial of service (DoS) attacks. The approach may also need to include crimes in which technology and cyber tactics are an integral part of the offence, such as online fraud, identity theft and extortion using malware. No universal definition of cybercrime exists, however various countries have attempted to define it.

Example definitions include:

In Australia, the term 'cybercrime' is used to describe both:

Crimes directed at computers or other Information Communications Technologies (ICTs) (such as computer intrusions and Denial of Service attacks).

Crimes where computers or ICTs are an integral part of an offence (such as online fraud).

South Africa has the following comment within its legislation: "Cybercrime" means any criminal or other offence facilitated by, or involving the use of, electronic communications or information systems, including any device or the Internet or any one or more of them.

In the UK the National Cyber Security Strategy[1] defines the distinction as:

Cyber-dependent crimes – crimes that can be committed only through the use of Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g., developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity)

Cyber-enabled crimes – traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft)

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

1.0 Experiences from International Partners

1.3 Legislation

The next consideration is around domestic law. Various aspects of a country's laws may already contain a link to technology and its use in crime. However, due to the creation of new crimes, it is recommended that specific laws relating to cybercrime are considered, covering the following:

- Unauthorised access to computers and digital material
- Unauthorised modification of data, including destruction of data
- Unauthorised access with intent to commit a further offence
- Unauthorised acts with intent to impair the operation of a computer or other digital device
- Unauthorised acts causing or creating risk of serious damage
- Unauthorised interference with computer programmes or data

Other considerations could include creating specific cyber offences relating to other crime types such as cyber fraud or cyber extortion, and further ancillary offences such as 'creation, possession or distribution of malicious software', or 'possession of stolen data'.

Caution is required around specific wording, as due to the exponential advancement of technology, terminology can become dated very quickly.

Connected to this is the ability for law enforcement organisations, police agencies, and security services to undertake investigation of these offences.

Such organisations must consider what activities they will carry out during an investigation that may have to be regulated or have judicial oversight. For example:

- What access should they have to communications data?
- To what extent should they be permitted to interfere with digital equipment for lawful surveillance activity? and
- How can they effectively secure and preserve data that may be needed as evidence?

Legislation with technology references will probably already exist, but it is recommended these are reviewed for compatibility, with consideration of the new activity investigating cybercrime will bring.

You may also need to consider how law enforcement can access and gather evidence effectively. For example, are there sufficient powers for police forces to compel relevant organisations – such as Internet Service Providers (ISPs) or communications companies – to hand over data required in an investigation?

1.0 Experiences from International Partners

1.4 Geographic Challenges

The international element of both the offending and investigative process have additional challenges.

More than just about any other type of crime, cybercrime will undoubtedly bring a number of international considerations to the fore. These include how to deal with suspects from foreign territories; evidence held in, or transmitted through, other countries' infrastructures, and victims or witnesses located outside a country's legal boundaries.

This requires several approaches to engage and influence international relationships and exploit all available international legal avenues to bring offenders to justice, protect domestic interests, and ensure the country remains resilient – and unattractive – to cyber criminals.

Areas to consider include diplomatic relationships through posts such as International Liaison Officers, bilateral and multilateral cooperation treaties, membership of international organisations (such as Interpol), and inclusion in wider regional or global treaties.

Examples include the African Union Convention on Cyber Security & Personal Data Protection[2], and The EU Budapest Convention on Cybercrime[3].

Another obvious consideration is collaboration with other countries in your region to develop joint working practices and build training opportunities.

We will cover training in more depth later, but developing a collaborated framework provides a common approach and helps build working relationships.

Such a framework assists with identifying and engaging suitable training providers, making it more cost effective. Help from organisations such as the Global Forum on Cyber Expertise[4] is also available.

[2] https://au.int/en/treaties/african-union-convention-cyber-security-and personal-data-protection

[3] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[4] https://thegfce.org/

1.0 Experiences from International Partners

1.5 Crime Reporting & Records

To understand and monitor the threat, adequate crime reporting, recording and oversight is needed. A majority of cybercrimes have no geographical focal point, often affecting numerous victims, regions and police force areas. A view of the bigger picture is needed.

> Trying to deal with apparent singular reports in isolation is likely to duplicate effort, reduce effectiveness of the overall response, and lead to missed opportunities to intervene and stop attacks.

Where possible, a national tasking process is also desirable, empowering a single body to assess, categorise, and allocate reports and incidents effectively. Unconnected national, regional and local structures can sometimes impede this.

Law enforcement partners should work together to look at ways to breakdown these barriers, encourage a networked response across the whole of the country, and provide a capability that can be flexed and called upon in response to various incidents.

Later in this guidance we will discuss options around how to set up these structures.

1.0 Experiences from International Partners

1.6 Incident Categorisation

Effective incident categorisation and tasking will assist with crime reporting and records.

Using your country's chosen structures, incidents and reports of cybercrime can be assessed and given an appropriate tasking decision to ensure the report is allocated to the most appropriate agency or team.

This assists with the efficient use of what will be a limited resource of specialist staff and helps to provide a more targeted service to victims.

To categorise an incident, we can use information such as:

i **Victim status –** are they an individual, a local business, government agency, or national infrastructure, for example?

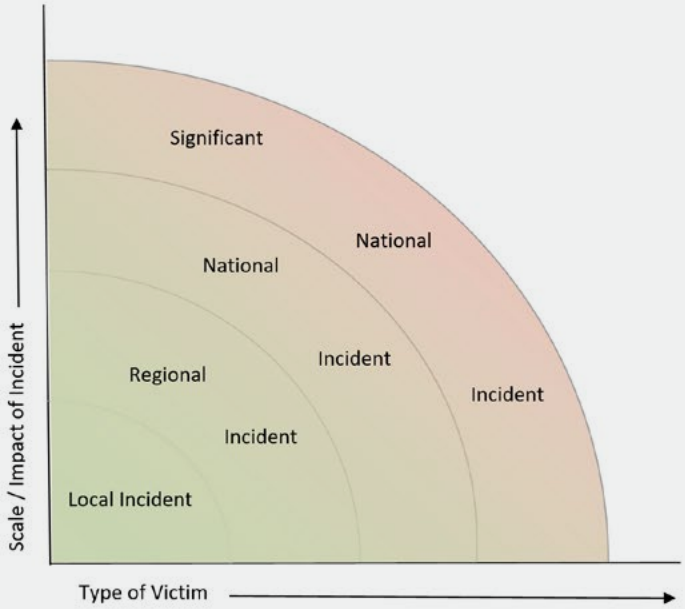
ii **The scale of the incident –** is it local, is it affecting more than one area or region, is it impacting multiple locations, or is it national/ international?

iii **By estimating likely impact –** low, moderate, severe, for example – it is possible to assign a category and make a decision around allocation. This could include categories such as local or regional incident, significant regional incident, or national threat, for example.

Such an impact estimate can then be sent to the most appropriate team or organisation best placed to respond to it.

This central assessment and tasking process is the best method to recognise emerging events and call upon the network if a larger incident needs a full network response.

Example of an Incident Categorisation Matrix



1.0 Experiences from International Partners

1.7 Collaborative Approach

This approach will still only let you understand part of the overall threat.
It is important to acknowledge that the police and law enforcement agencies will not have all the answers.

Many people and organisations may not fully report attacks or incidents for a number of reasons. This could be down to corporations looking to protect their reputation or business interests, or individuals not fully understanding what has happened to them, or even how they can then report incidents.

Public awareness campaigns can assist with this, to some extent.

> *"Nurturing strong working relationships with key partners and industry sectors is vital."*

But more deep rooted reasons – such as confidence in law enforcement, properly understanding very technical attacks, or perceptions about whether police have the correct structures in place to handle the incident – can also influence decisions around reporting.

If you also consider that up-to-date understanding of the threat is likely to come only from industry experts, this means police and law enforcement will only see part of the picture.

This is where a partnership approach becomes important. Nurturing strong working relationships with key partners and industry sectors is vital. This is also an important relationship when you add in the sheer scale of some incidents, with some attacks now being committed on an 'industrial' scale.

Traditionally, law enforcement has struggled to deal with such 'industrialised' high-volume, potentially low-impact attacks, so involving relevant industry sectors as part of the solution may be required.

This has proved difficult to address. Early considerations around how these high-volume incidents could be reported and responded to within your specific processes will be required.

Initiatives such as CERT (Computer Emergency Response Teams) collaborations are a good start, but deeper partnerships, including trusted information sharing alliances are also needed.

There are examples from countries which have explored various options around this, such as the Cyber Task Force model in the USA[5], and the Cyber Information Sharing Partnerships (CiSPs)[6] and Cyber Resilience Centres in the UK[7].

These partnerships can support activity such as:

- Information sharing
- Development of specialist training
- Greater understanding of the current threat picture
- Horizon scanning for emerging threats
- Intelligence analysis, and
- Secondment opportunities between public and private sectors

There is also a busy cyber incident response sector, with organisations which have first-hand experience of the impact of cyber offences on a daily basis. Meanwhile, organisations such as CREST work to represent and support the technical information security markets.

5 https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

6 https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

7 https://www.brimcentre.com/

1.0 Experiences from International Partners

1.8 Wider Approach

Add in the reality that you will not be able to identify every single offender, (even the ones you can identify may be located in uncooperative regions or countries, or lack domestic capability to support your investigations), and it becomes clear that you cannot simply arrest or legislate your way out of the problem.

This is where a much wider approach becomes important. We must look at ways of reducing the number of people who become victims. We must make society more resilient to the threat. We must develop ways to respond and recover when an attack occurs, and create opportunities for people who may be at risk of moving into a life of cybercrime that can divert them into more productive and rewarding pathways, such as careers in the cyber security industry.

At state level, this requires innovative approaches, involving strategies including:

- Security
- Business
- National infrastructure
- Education
- Public awareness campaigns
- Research and development
- Training and career pathways, and
- Appropriate law enforcement capabilities.

1.9 Structured Response

To support this wider approach, it is useful to define how various components of law enforcement can be structured to deliver an effective response as a cybercrime unit and interconnected network.

Developing the topics we covered in the previous paragraphs we can identify four key aspects to this:

i The ability to understand the threat, respond to incidents, and investigate, identify, arrest and prosecute suspects.

ii Develop and deliver strategies to help people and organisations become more resilient to the threats and not become victims in the first place.

iii Develop and deliver strategies to help people and organisations respond more effectively to an incident when it does occur, recover more quickly from it, and reduce its impact.

iv Develop and deliver a strategy that identifies people vulnerable to becoming involved in cybercrime, helps divert them, and provides greater opportunities for them to follow a cyber security industry career. Or where individuals have taken the path of cybercrime, develop strategies that will degrade and disrupt their activities.

1.0 Experiences from International Partners

1.10 Four Ps Strategy

The 'Four Ps' strategy is a ground-breaking law enforcement concept devised primarily for counter terrorism and used for serious and organised crime threats and now adapted for use in cybercrime by the UK's National Crime Agency.

It can be summed up as follows:

Pursue individuals, groups and larger organisations involved in creating the most serious cyber threats.

Prevent individuals becoming involved in cybercrime, deter and divert those on the periphery of cybercrime, and degrade and disrupt those committed to cybercrime.

Protect businesses and the public from cybercrime.

Prepare business and other organisations to respond effectively to major cyberattacks, and to mitigate their impact.

Of course, countries may wish to structure and set their strategies in accordance with local and regional landscapes. But in this guide, we will follow the 4Ps, which we believe provides a comprehensive approach to the problem.

The 4P approach introduces tools and strategies that assist with combatting threats and supports countries and law enforcement agencies in setting up an effective response.

Outline of 4P Approach (UK College of Policing, 2020)

* SOC: Serious and Organised Crime

The following sections explore the 4P approach in greater depth and provide guidance on how to establish an effective cybercrime unit.

1.0 Experiences from International Partners

1.11 Necessity

A final point to make here is the necessity for this type of strategy. For many years, the threat from cybercrime has been seen as a technical issue.

Law enforcement has been slow to react and fully understand the impact of cybercrime offences. Cybercrime is like any other crime. Implementing wider strategies to tackle the causes of crime, as well as making participation less attractive and riskier is as relevant here as with any other type of crime.

> *"Cybercrime has an impact throughout society from the individual, through business and up to government and state level."*

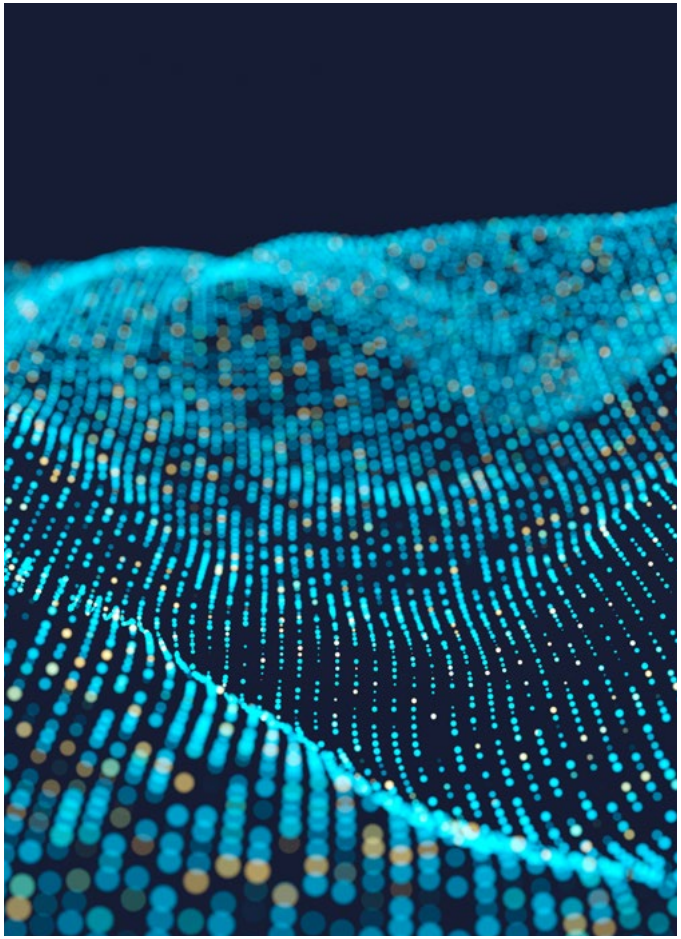
Closed thinking by senior officials – without due regard to the harm that can come from just a single successful cyberattack – has compounded the problem, often resulting in reluctance to invest in adequate capabilities, or support programmes of change.

This is not just a virtual threat; it is very real with real world consequences.

Cybercrime has an impact throughout society from the individual, through business and up to government and state level. People have lost their lives, business and companies have collapsed, and governments have been weakened.

Cybercrime must attract the same attention as any other form of crime, and appropriate capabilities should be in place.

Equally, real world experience has proved that focusing purely on technology has limited impact. CyberCrime Units must adopt a holistic approach, understanding and addressing the plethora of criminal functions that support technical attacks, such as the use of **'mules'** to launder money. Simply put, if we can make cybercrime less lucrative, the threat would be reduced. New approaches in recruiting people into cybercrime focus on lifestyle and income. Coordinating a structured approach to halting money laundering would impact these recruitment messages, and dilute cybercrime.



Constituent Parts of a Cybercrime Unit

2.0 Constituent Parts of a Cybercrime Unit

Introduction

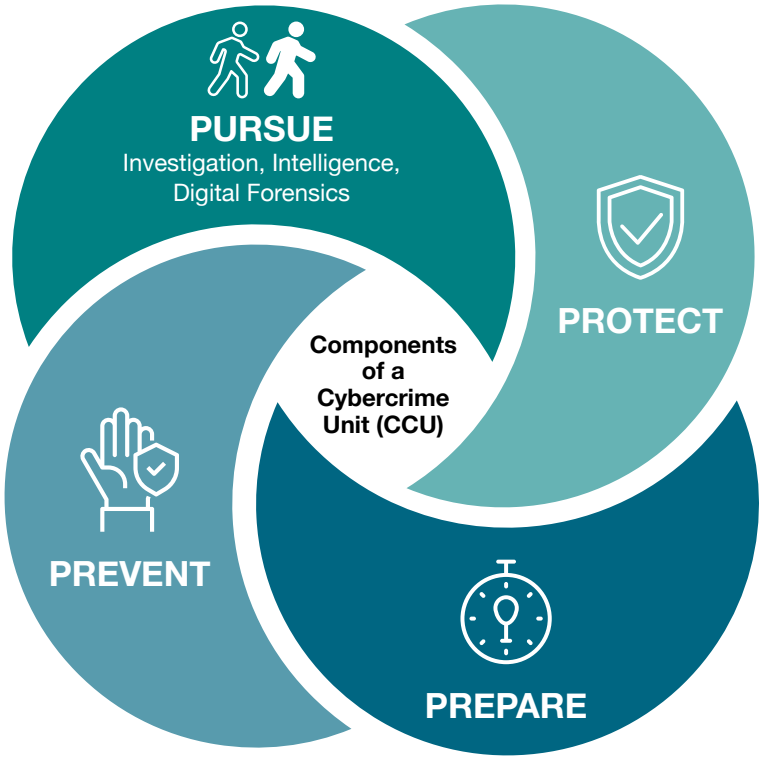
This section explores the components recommended to develop a cybercrime unit. We will examine a whole network solution, including assets and capability at national, regional and local levels.

Different countries may be at various stages of development or may not have the capacity to undertake a singular large uplift programme all at once.

Where possible, we have provided this guidance to be used in a modular way, allowing aspects of it be used separately or as part of a wider development programme. However, we encourage all elements to be considered. Taken together, they will give the best levels of protection and provide greater levels of resilience.

A further dimension to this will be any interface with state-level capabilities, which this guide does not cover in detail. Different countries will have differing approaches, depending on their constitutional approach and criminal justice model. This may include control over national policy, links into government, critical national infrastructure governance, departments within security services and the like. There are other pieces of research and guidance covering the development and implementation of a national cyber security strategy which will assist further with this aspect. We would recommend considering these alongside this guide.

2.2 Components of a CyberCrime Unit



A CyberCrime Unit (CCU) needs a number of disciplines to function appropriately. Some may need to be embedded within the team, while others may be located elsewhere but available for tasking and deployment by the CyberCrime Unit. Broken down, a CyberCrime Unit should include capabilities under the rough headings of Operational, Technical, and Intelligence. The 4P approach needs to be considered alongside this. Each 4P element will have interdependencies with these capabilities to function effectively.

For example, staff delivering Protect messages and services need to understand the latest technical issues to comprehend current threats and tailor their material appropriately.

2.0 Constituent Parts of a Cybercrime Unit

2.2 Components of a Cybercrime Unit (CCU)

Staff running 'Prevent' interventions need access to the latest intelligence to ensure people they are engaging with are suitable for those programmes. All their work must feedback into the overall understanding of the cyber threat, so needs to be an integral part of the team's work. For these reasons, we recommend 4P capabilities are colocated and contained within the CyberCrime Unit structures, and staff should work together.

There will be various ways of setting up networks and governance structures to oversee this, which we will explore in more detail later. This can include different ways of setting up teams or networks and involve staff working at various levels such as national units, regional hubs, and local teams. Whatever the structures decided upon, composition of each CyberCrime Unit needs careful consideration.

Putting some of the unique challenges aside, this is still law enforcement, and at its core units need to have the ability to investigate crime, disrupt offenders, arrest suspects, bring offenders to justice and protect citizens.

As with any other type of crime, some of it is complex, some is committed by organised groups, some has the potential to cause great harm, some can be seen as petty and more of a nuisance, and some is nothing more than 'digital graffiti'. CyberCrime Unit structures should have the ability to meet cybercrime at all levels and gauge its response appropriately.

As we discuss the elements required, we will take a relatively neutral, generic approach without commenting on the size or final composition of the team. This will need to be a decision made by each country and agency to reflect specific demand, geographical coverage of the unit, and available investment.

Clearly, not all capabilities will be required for all investigations, so we leave you to make your own judgement around the level and extent of each capability within your CyberCrime Units.

Additional considerations that will assist with this are explored later on.

2.0 Constituent Parts of a Cybercrime Unit

2.3 Pursue

Pursue

‘Pursue’ is seen as the traditional element of the 4P approach, and in essence is a police team, like many others, which is directed at a specific threat, such as robbery or car crime. Pursue requires much the same approach, with a team comprising motivated, experienced staff working to understand the nature of the crime, then implementing tactics to combat it and disrupt criminals.

As discussed previously, cybercrime brings its own challenges, so the structure of a CCU Pursue capability needs specific elements, as well as access to other support capabilities which can be called upon when needed.

2.0 Constituent Parts of a Cybercrime Unit

2.4 Investigation

This must include a team of detectives or experienced investigators. These investigators do not need to be trained to the highest levels of technical capability, rather a foundation level to provide them with enough of an understanding and appreciation of the concepts and language used in cyber offending.

For more technical aspects of investigation, we recommend a close relationship between investigators and technical staff, where regular contact and appraisal of the latest updates on an investigation from both parties will prove invaluable.

The approach must include the ability to conduct both ***reactive*** investigations, where you are responding to a report of a specific incident, and the skills required to undertake ***proactive*** work, specifically targeting offenders and crime groups.

To get ahead of criminals, this ability to take the fight back to them is a vital tactic, keeping pace with the changing nature of cyberthreats, and sending a message that law enforcement operates effectively in the cyber world.

"A missed opportunity to secure some volatile evidence or capture the content of a particular web page might prove costly."

Similarly to other areas of criminal investigation, it is important that staff develop and follow appropriate strategies which are thoroughly considered and created specifically for each case. A missed opportunity to secure some volatile evidence or capture the content of a particular web page might prove costly and lose an opportunity to prosecute an offender.

Without stating the obvious, cybercrime investigation requires the ability to operate in the digital world. Evidence and vital lines of an investigation will be out in cyber space, may be protected behind hidden services, and could be volatile in nature, only existing or visible for a limited time before it could be completely lost. Some of the ability to find, capture and secure evidence for use in the investigation will no doubt be within the role of the Digital Forensics team. But sometimes, the investigator may need to take initial actions to capture and preserve evidence.

This introduces an important consideration, where staff that are not necessarily fully trained digital forensic operatives are handling the capture and preservation of evidence.

This is a tricky area. If not approached correctly, this practice could lead to legal challenge, see evidence excluded from criminal trials, and potentially result in cases collapsing.

We will explore the need for policy and processes to support this in greater detail later.

But, as a minimum:

- There should be controls in place to ensure the integrity of evidence is preserved as much as possible
- A record of the steps taken to access data should be made, and
- The person in charge of investigation should record their reasoning behind any actions and show due regard for any legal and regulatory conditions.

2.0 Constituent Parts of a Cybercrime Unit

2.4 Investigation

CyberCrime Units will access tools and services not normally considered by law enforcement.

The technology and availability of such tools and services changes regularly, so staff should frequently assess their particular needs, engaging with the tech industry to encourage innovation and keep abreast of what's available to them.

This includes scanning and assessing domains, capturing and preserving web content, and accessing areas of the internet beyond the 'surface' web, (such as the dark web), and networks like TOR.

Search and analysis tools to identify connections, establish provenance and ownership of services and map networks will also be needed.

This list is almost endless and constantly evolving, so the relationship with partners and the wider tech industry is important to maintain a CyberCrime Unit that is up to date and remains fit for purpose.

We have covered overt and visible tactics, but the ability to operate in an undercover, covert way is also necessary. Infiltration or monitoring of criminal marketplaces and chat rooms is a tactic that can prove very effective, but a traditional law enforcement undercover operative is unlikely to understand technical terms and struggle to be effective in this environment.

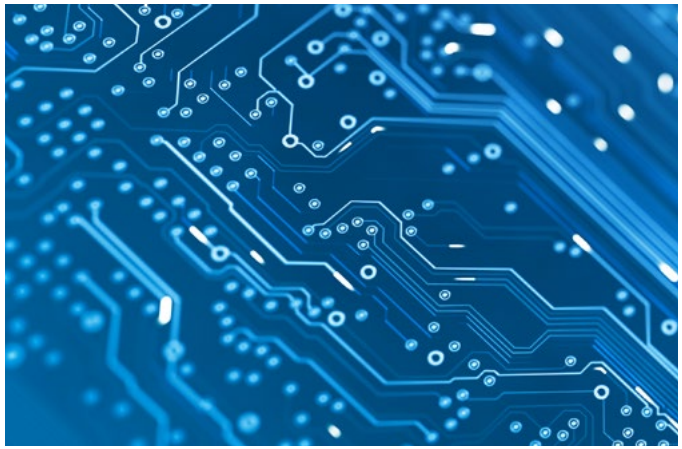
Cyber criminals and hackers will be cautious of new people, will speak in technical terms and test 'newbies' to probe their credentials. Any chat room exchange will happen in real time, giving no time to conduct research to find the answer. Operatives will need to have a degree of technical knowledge to come across as credible. Where responsibility for undercover work may sit in other parts of an organisation, special consideration should be given to ensuring online undercover operatives have sufficient experience and training for the challenges cybercrime brings.

Another element of covert tactics includes targeted interference of equipment by law enforcement.

Many aspects of this will depend on the particular laws of a country, so while it is not possible to go into all of them, parts link in with covert tactics, so are worth mentioning here.

Targeted interference could work in two ways:

i Gaining access to otherwise restricted or private locations to identify and secure evidence or intelligence, or



A lot of covert tactics are sensitive, so inappropriate to discuss in great detail in an open forum. But working with partners and organisations with experience of targeted interference will help identify appropriate methods and develop your team's skills in this area.

ii Offensives designed to target a criminal, take over an online account, or seize domains.

2.0 Constituent Parts of a Cybercrime Unit

2.5 Intelligence

A fundamental part of tackling cybercrime is understanding the threat. While there appears to be a consistent pattern to much of it, the way cybercrime is committed, who is doing it, and the motivations behind it constantly evolve and change. Different countries may face different threats.

So it is important for law enforcement to track and understand what current threats looks like, and which emerging cyberthreats could create future problems.

Effective intelligence capability must work holistically – internally within the law enforcement agency, and externally with the technology industry and trusted expert partners.

As previously stated, law enforcement does not have all the answers, so keeping a 'finger on the pulse' of what is impacting different sectors is necessary. CREST has many years' experience in mapping, identifying and developing Threat Intelligence, and **other guides and reports** are available to assist here.

As well as understanding the threat assessment, intelligence staff need to support the investigation team's work. Each investigation should have an intelligence plan within its investigative strategy. The interplay between the two disciplines will identify lines of enquiry, track down evidence and assets, and most importantly, help put real word identities to 'anonymous' figures on the internet.

The tools discussed earlier will be required to undertake this, as well as other law enforcement systems and traditional ways of gathering intelligence and information used in other forms of investigation.

Work by intelligence teams can bring order to apparent chaos – setting priorities, identifying targets, and feeding the pipeline of activity for CyberCrime Units. Using this approach can demonstrate a focused effort, provide proportionate and reasonable justifications for undertaking particular pieces of work, and ensures any activity is aimed at the overall goals of reducing the threat and protecting people.

Intelligence products can help set national strategy, guide institutional thinking, and provide tools for assessing the impact and effectiveness of the law enforcement response.

Another aspect of intelligence that needs considering is that during operational activity, CyberCrime Units are likely to gather and seize large amounts of data and information. This will come from a variety of sources, including data from seized databases, compromised credentials, victim information, suspect information, and evidence from seized devices that have been subjected to forensic examination.

Taken together, the data will produce a large pool of information that can be a powerful tool. However, this information will need storing appropriately and requires tools to effectively manage it.

This is where collaboration with analysts and data scientists has been used very successfully to form the basis of large enforcement operations, as well as interconnected diversion programmes.

Examples include large databases, often containing many thousands of entries, seized when providers of illicit services were arrested.

Data was then analysed, developed into 'suspect packages' and used to target users of those unlawful services. Using this sort of tactic – where investigations feed the intelligence function, which then uses big data analytics to form tangible connections and provide further investigative opportunities – can prove extremely effective.

2.0 Constituent Parts of a Cybercrime Unit

2.6 Digital Forensics & Technical Support

Digital Forensics (DF) is the main technical function of the 'Pursue' team, requiring the most specialist training and equipment to maintain a functioning capability. There are a few approaches to this, which include having the Digital Forensics team fully embedded within the CyberCrime Unit, to having it as a separate support function elsewhere in the organisation, or a collaborated approach, where a number of CyberCrime Units use a single Digital Forensics team.

As Digital Forensics will be the most technical aspect of investigations, there is a potential further option, to look at outsourcing some or all of it. This will need careful consideration, balanced against security requirements, internal capability, or other available options as mentioned above.

Outsourcing could present a good opportunity to build partnerships through private industry collaboration but will need to be considered against your individual circumstances and available capabilities.

You may also need to consider if outsourced providers are approved and capable of delivering the services required. Each country may have different rules or policies around how to do this, but examples of the UK approach include products and services that have been independently assessed against the National Cyber Security Centre standards[8], and compliance in a scheme called Cyber Essentials[9], which demonstrates an organisation's commitment to cyber security.

We will explore these options more later in this guide. But, whatever your preferred setup, there will be some fundamental requirements that a Digital Forensics function needs to deliver. During the next section we will explore some of these requirements, with guidance and suggestions on how to deliver and enhance the Digital Forensics function to provide the best support for CyberCrime Units and their particular requirements.

8 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

9 https://www.ncsc.gov.uk/cyberessentials/overview

2.0 Constituent parts of a cybercrime unit

2.6 Digital Forensics & Technical Support

Traditionally Digital Forensics is split into two functions, often described as ‘dead box’ and ‘live box’. As the names suggest, dead box considers powered-off devices with no ability to alter data or connecting to other devices or networks. When handled and examined correctly, ‘dead box’ data is preserved in the state it was in when last powered on, and an image (or digital copy) of that can be created for later examination.

‘Live box’ Digital Forensics work involves looking at a device in a powered-on state, which may be actively performing functions and could be connected to other devices and networks. This means the data is in constant change, so the device must be handled appropriately to capture and secure the best evidence possible.

Digital Forensics teams will need the skills and capabilities to deal with both. While ‘dead box’ capabilities have been the more traditional approach, ‘live box’ is now a vital capability that every CyberCrime Unit will need support with.

There are many reasons for this, including:

- How to secure volatile data, like RAM
- How to handle encrypted volumes that could be difficult to access later if shut down
- How to deal with remote connections to devices that may not be physically present, but need to be accessed later by an examiner in a lab.

These connections could lead to equipment located outside of the country and in areas of the world that may be hard to engage with.

So, devices in a live state may be the only opportunity you have to secure evidence.

In developing this approach, it becomes clear Digital Forensics teams and CyberCrime Units need to have a physical laboratory, and a degree of mobile capability, where forensic tools can be taken to a location as required. This could be for both suspect and victim examinations. Such equipment can be used reactively to respond to an incident or during the arrest of a suspect, and as an intelligence or evidence gathering exercise during proactive investigations.

When used appropriately, Digital Forensics can be a powerful tactic which can secure damning evidence and catch criminals in the act, leaving them no options but to admit their crimes.

A third element of Digital Forensics, network forensics, involves examination and monitoring of a network, its architecture, connections and live traffic. This data is used to gather intelligence or secure evidence for use in an investigation. Network forensics can be a useful tactic to locate and target suspects, ensure search warrants and arrests are carried out at the most productive times, and help secure the best possible evidence from a victim (particularly when the victim is a company or large organisation).

2.0 Constituent Parts of a Cybercrime Unit

2.6 Digital Forensics & Technical Support

Of course, undertaking network forensics requires specialist tools.

If you are creating a CyberCrime Unit 'in house', then Digital Forensics is where you will need to invest the most, not just in equipment and training, but also in longer-term development to keep pace with changing technology and the shifting nature of cyberattacks.

While listing a series of tools required to undertake these activities could be useful, given the rapidly changing nature of the cybercrime and technology environments, what we may recommend as a useful tool today is likely to be replaced tomorrow. Rather, we recommend regular engagement with the technology industry to keep track of the most up-to-date and effective tools available, as well as partners and other cyber teams within your networks.

To provide some guidance around key Digital Forensics elements, teams and organisations should develop and maintain capability in the following points, which are not exhaustive but should be considered as a minimum *(where appropriate the solution to acquire data should include all forms of devices, including mobile telephones and other smart devices, which may mean more than one tool for each is necessary):*

- Write blockers to ensure forensically sound examination of devices
- Tools to support forensic acquisition of data from a powered-on device
- Tools to support forensic acquisition of volatile data from a powered-on device (such as RAM)
- Tools to support the collection and analysis of network traffic (packet capture)
- Consideration of triage tools to assist examinations of larger scenes
- Virtual environments to recreate machines or networks
- Virtual environments to safely test and examine attack vectors
- Tools to conduct safe analysis of malware (or access to a malware analysis service)
- Tools to support the analysis of data, including big data and multiple data sets
- Password cracking (or access to a cracking capability)
- WiFi sniffing and mapping
- Tools for network analysis and mapping
- Faraday bags/boxes to block network signals from a powered-on device
- Sufficient storage solutions, including 'on-scene' use
- Capability to seize and securely store cryptocurrency
- Cameras to record and catalogue actions and stages of examinations.

2.0 Constituent Parts of a Cybercrime Unit

2.7 PROTECT and PREPARE

PROTECT

'PROTECT' and 'PREPARE' are often interconnected and can utilise similar tools and approaches.

Because of this, we will cover them together here. However, they are two distinct tactics aimed at differing elements of the model, so should be considered as such and have appropriate operating models in place.

The 'PROTECT' part of a 4P response is designed to deliver messaging, tools and tactics to make all targets more resilient and less likely to fall victim to an attack.

In simple terms, the more successful this is, the less victims there will be. Less victims means a reduction in reports of incidents to law enforcement, and an increase in confidence in the service. This will contribute to making the country much more resilient to the overall cyber threat.

Many of the tools and tactics across the whole 4P approach are interlinked and work best if developed and delivered together. 'Protect' is no exception, and the starting point is understanding the threat. This links back to many of the topics we have discussed and becomes a key interdependency between the various teams.

Technology has become more embedded within our lives with ubiquitous smart devices and the **'Internet of Everything (IoE)'** creating increased vulnerabilities.

As more people become reliant on technology, threats are ever increasing, with issues such as:

- Poorly designed technology
- Old and legacy systems not being updated or patched adequately
- Lack of training or understanding of the issues, and
- The ease in which criminals can equip themselves with the tools and guidance to undertake an attack.

A majority of attacks could be prevented using simple steps and good practice. This is true for both general citizens and businesses alike.

Developing these good practices into a tangible strategy with deliverable outcomes is key.

Working alongside partners to understand appropriate approaches to meeting cyberthreats is a priority. From this starting point, it is then possible to develop a 'Protect' strategy aimed at all levels, from national policy right down to messaging the whole population.

We will cover wider national policy and some ideas around what those strategies could look like later. This section concentrates on what the 'Protect' element of a CyberCrime Unit should look like.

'Protect' good practice messaging should include:

- Advice on creating strong, secure passwords
- Using two-factor authentication
- Antivirus protection
- How to spot common scams and phishing attempts
- Installing updates
- Setting devices to automatically backup
- Where to go for help and advice

2.0 Constituent Parts of a Cybercrime Unit

2.7 PROTECT and PREPARE

Staff will need to demonstrate credibility, so need training to appropriate standards to understand cybercrime and grasp the latest threats.

Consider industry recognised qualifications or certifications for staff. As qualifications may differ from country to country or region to region, we suggest regular engagement with industry and training partners will guide you around what may be the most appropriate for your needs.

For example, other countries have used schemes such as CISSP[10] or CompTIA Sec+[11]. CREST International, of course, offers a range of **professional development** opportunities and **individual certifications.**

Delivering presentations and undertaking public engagements to promote this messaging, staff will need to engage with a variety of audiences and be able to explain technical issues at a level non-technical people can understand.

Working with industry, initiatives to develop partnership groups and encourage support networks will help facilitate change and build a vibrant cyber defence community.

Once strategies have been developed, nationally agreed and supported messaging can be delivered as a network, producing consistency across the country. This will ensure all aspects are aimed at reducing the identified threat.

We recommend a disruptive approach to national cyber security awareness programmes, taking full advantage of online and offline-influencers and helping to generate community-contributed content.

This community approach is important, providing opportunities for community-driven and community-contributed content, and providing a platform for relevant influencers to promote good practice.

Once partnerships have been established, staff can work with community contributors to keep messaging current, respond to emerging issues, and work on producing support material such as cyber alerts and social media campaigns.

"We recommend a disruptive approach to national cyber security awareness programmes, taking full advantage of on and offline influencers and helping to generate community contributed content."

[10] https://www.isc2.org/Certifications/CISSP

[11] https://www.comptia.org/certifications/security

2.0 Constituent Parts of a Cybercrime Unit

2.7 PROTECT and PREPARE

PREPARE

'PREPARE' is similar in many respects to 'PROTECT', using strategies and tactics to improve the resilience of the population. However, the distinct difference is that this messaging is aimed at what to do if and when you fall victim to a cyberattack.

Unfortunately, it is almost impossible to completely protect a network or device from a well resourced, determined attacker.

Facing this reality and preparing for when it does happen will help victims be less impacted by an incident and assist in developing practices that can be used to recover more quickly. Prepare strategies can have common messaging across all technology users, but business is where the biggest impact can be achieved.

Some simple steps and straightforward policies can, however, have a significant effect, and Prepare staff will need similar knowledge and experience to Protect staff.

Prepare staff require sufficient understanding of the current threat, and adequate training to be credible in their messaging.

Examples of prepare messaging include:

- Exercising and testing as if an attack has occurred
- Advice on how to close down an attack and recover from it
- Using offline and cloud services for backups
- Staff training and awareness for businesses
- Advice on secure configurations
- Reminders around patching and software updates
- Signposting to education and assistance guides
- Understanding where and how to **procure accredited professional services** to assist with recovery
- **Assessing the level of maturity** of the organisation's incident response processes

Working alongside the networks and partnerships previously discussed, cyber recovery and continuity planning adds to the overall result and improves a country's cyber resilience. Cyber should be seen as an event to plan for, just as people prepare for things like flooding or power cuts.

Adding cyber incidents into this ethos will begin to make it more visible and encourage people to consider what their own particular cyber related risks and vulnerabilities look like, creating plans to protect their most valuable assets and recover better.

Working to nationally agreed messaging and set around common tactics, the network should work together in planning and delivering exercises for the most common or dangerous threats.

2.0 Constituent Parts of a Cybercrime Unit

2.8 PREVENT

PREVENT

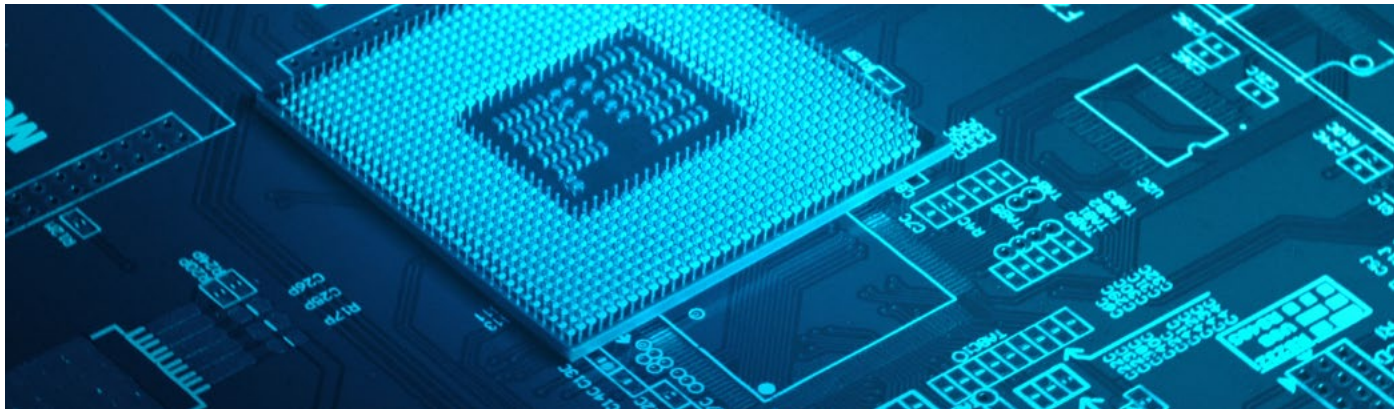
To complete the 4P approach, we recommend a Prevent strategy is adopted into the CyberCrime Unit network. Using different tactics and approaches to bring in a 'whole-system' solution to reduce the threat cannot be stated enough.

In simple terms, the more successful this is, the less victims there will be. Less victims means a reduction in reports of incidents to law enforcement, and an increase in confidence in the service. This will contribute to making the country much more resilient to the overall cyber threat.

A whole-system approach uses collaboration between partners across law enforcement, public, private and third-party sectors, both within the country and internationally, all with clearly defined roles and responsibilities to maximise the impact on organised crime[12].

We believe one of the most innovative approaches to this will come from an effective Prevent strategy that looks to identify young and vulnerable people who may be in danger of moving into a life of cybercrime, or inadvertently start on a path of unlawful behaviour. A Prevent strategy should produce options to divert them away from it, as well as introducing tactics to target those already involved in cybercrime to reduce their effectiveness or impact. This can be summed up as the 4D approach – Deter, Divert, Degrade, Disrupt. To Deter and Divert those on the periphery of cybercrime, and Degrade and Disrupt those committed to cybercrime.

We consider this such an important aspect of the 4P strategy, we have produced a separate guide to specifically cover this. To reduce duplication, this guide will not cover the Prevent strategy in any further detail. Rather, we encourage you to use the more detailed Prevent guidance reports available via CREST – **"Introduction to Intervention and Prevent Activities To Reduce the level of Grooming into Cybercrime" and "How to Establish a Cybercrime Intervention Programme".**



[12] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/289-nca-annual-plan-2019-20/file

2.0 Constituent Parts of a Cybercrime Unit

2.9 Management & Supervision

The last section of the constituent parts of the cybercrime model is ensuring appropriate governance and management structures are in place. It is sometimes difficult to get the size or potential impact of the threat across to everyone, and misconceptions can be held.

This can mean that not every decision maker will see the requirement for a dedicated CyberCrime Unit, let alone agree to the investment needed to make it happen.

It is imperative that senior staff have the right understanding of how impactive cybercrime can be and are able to educate and influence at all levels.

This should follow through the organisation and adequate management structures must be in place to oversee the CyberCrime Unit department, which will work best with innovative and free-thinking staff, supportive of the desire to meet the challenge head on.

While they may not require the level of training other staff will undertake, they should have a basic level of knowledge to better understand the work and ensure a proportionate and focused use of assets.

2.10 Staff and Organisational Safety

A final consideration is the very real danger that CyberCrime Unit teams and staff will attract attention and could be targeted by the very criminals they are trying to combat.

Not only should the above approach be used to improve the public's resilience, but there should also be some consideration about the CyberCrime Unit's own digital security, as well as within the wider organisation. Working to the same strategies as above and having awareness of staff's digital footprint will assist.

3.0

Team Requirements & Team Recruitment

3.0 Team Requirements & Team Recruitment

Introduction

The make-up of a CyberCrime Unit requires diverse elements to work together. It is not simply a case of employing a number of technical staff and pointing them at the problem.

A successful, high functioning CyberCrime Unit needs a blend of skills from traditional law enforcement expertise to brand new cutting edge capabilities.

Getting this mix right, and ultimately having the right people in place to deliver the CyberCrime Unit functions, will create the right ingredients to build and develop a successful team.

You may decide not to have all of the capabilities contained within a single unit.

Whatever the most appropriate structures for your organisation are, the following section will help you decide on the best approach to defining the team and selecting the most suitable staff.

3.2 Organisational Structures

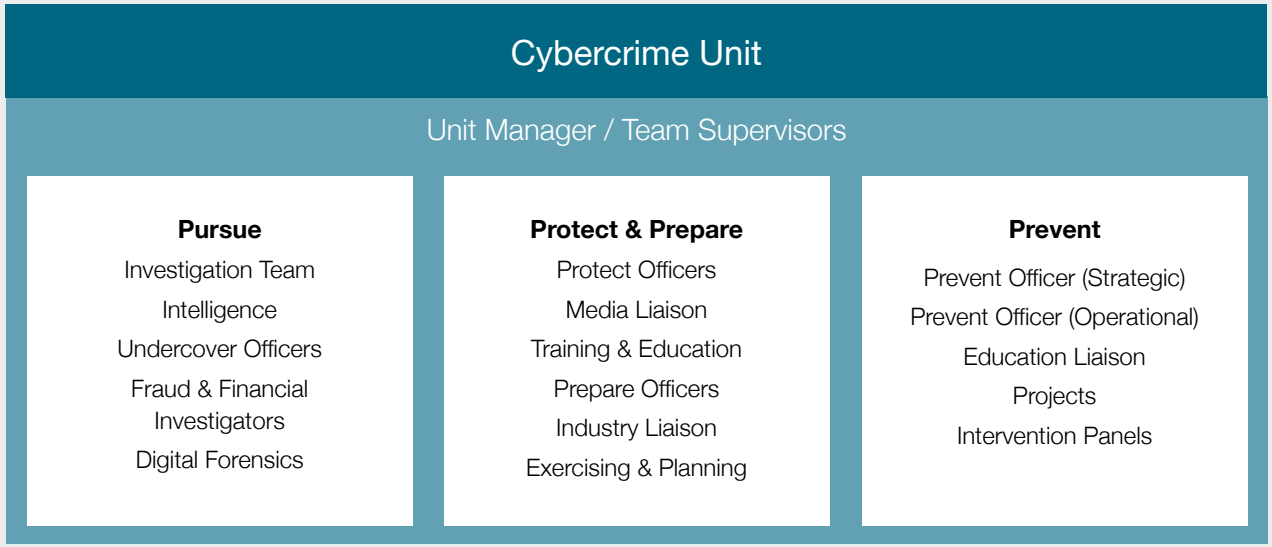
To begin, you will need to identify the structure of your CyberCrime Unit, along with any interconnected network and the key roles within it.

It may help to visualise this with a structure chart, which can also assist in defining where in the organisation the CyberCrime Unit team will sit.

For example:

3.0 Team Requirements & Team Recruitment

3.2 Organisational Structures



Creating a structure chart is a useful exercise, and a good way of highlighting connected capabilities, identifying areas of common service delivery to reduce duplication, and establishing senior oversight and reporting agreements.

If your CyberCrime Unit includes a number of agencies and is looking at a whole network response at various levels, this planning chart becomes even more useful in helping staff understand how all the different elements fit together and interact with each other. An organisational structure chart also ensures there are defined roles around who does what, and what responsibilities each part of the network has.

When considering the individual units, you will need to clearly define the roles and responsibilities of each team member. We recommend compiling job specifications and role profiles, which will assist when undertaking recruitment processes, defining training requirements, and aid with staff development later on. These profiles should set out key aspects of the role, detail what is expected of the position, list essential experience requirements and any other desirable experience.

To assist with development of these profiles, we have included suggestions and example documents in Appendix A. On the next page are some key points you may consider for each role.

3.0 Team Requirements & Team Recruitment

3.3 Staff Selection

Roles within a CyberCrime Unit are likely to be very sought after, so you should attract a variety of candidates, giving the best possible pool of talent to draw from.

However, they are also challenging roles, which need carefully considered selection. Employing the wrong person can prove costly, wasting time and money on training and development. All roles within the team will need some level of technical understanding.

While training will be necessary to give staff the right tools to undertake their work, they will still need to have the ability to undertake that training. We recommend your recruitment process involves some form of basic technical knowledge check. For a majority of CyberCrime Unit roles, this does not have to be very in-depth or detailed, but sufficient to ensure the candidate has an interest in this sort of work and would be able to understand training.

Examples of this could be basic questions about terms or phrases, such as “What does http mean?” or “What does the acronym RAM stand for?” Some roles will require more technical ability than others, so the level of these questions can be adjusted accordingly, and for roles in areas such as the Digital Forensics teams more probing and challenging subject matter can be used.

CREST, of course, offers a range of tangible, recognised courses and professional specialist certifications that bring clarity to a candidate’s experience, or offer employees the chance to enhance and codify their knowledge at a later date.

CREST is also working on a new Foundation course for those keen to enhance and underline their knowledge.

Some sections of society are underrepresented within the cyber security sector, most notably women. We encourage strategies to address this gender disparity and you might wish to take steps to encourage underrepresented groups to apply for the roles.

A final question – where should you look for the required skillset? Clearly some elements of the unit will need to have proven law enforcement experience. In particular, an Investigation team would normally include staff with experience of working within general law enforcement, with sufficient legal powers to undertake their duties.

There may already be staff within your organisation who have previously worked in a relevant industry or have skills they have developed through personal interest or hobbies.

Sometimes, candidates can come from surprising areas. That said, drawing a mix of candidates via internal and external recruitment will provide the team with a fresh outlook and bring in talent that encourages innovative and free thinking. This is where relationships with academia and industry can prove fruitful.

Programmes such as internships and volunteerships open up new career pathways and assists with staff development and retention. We will explore elements of this in more detail later.

3.0 Team Requirements & Team Recruitment

3.4 Governance

Any team, unit or organisation needs to have defined, appropriate line management. Depending on the setup you choose for your particular organisation, the CyberCrime Unit structures will be no different and need appropriate oversight. In some respects, they may require more attention than other areas to provide an environment where they are supported and able to operate.

This is not just a case of making sure there is management in place and individuals within the organisation with senior leadership responsibilities.

To succeed, a CyberCrime Unit requires support and vision, with leaders that understand the issues. CyberCrime Unit leaders need to be powerful, passionate advocates for the unit's creation, development and sustainment.

Using a traditional approach to risk, law enforcement agencies can easily fail to properly grasp the dangers associated with cybercrime.

This can create a culture that does not consider or assess cyber threat and risk as seriously as other forms of crime. Having senior staff that fully understand the issues in positions of influence, with the ability to shape policy, will assist with embedding the mindset required to meet the challenges of cybercrime.

Managers directly working with the CyberCrime Unit teams require appropriate training to be able to fulfil their roles. Of course, some direct line managers will be a part of the unit and, depending on setup, will be undertaking tasks and investigations themselves. Role profiles should reflect this, and an appropriate number of managers and first line supervisors should be included in the structures.

"To succeed, a CyberCrime Unit requires support and vision, with leaders that understand the issues. CyberCrime Unit leaders need to be powerful, passionate advocates for the unit's creation, development and sustainment."

3.0 Team Requirements & Team Recruitment

3.5 Investigation

Above all else, a desire to work within a cybercrime unit and willingness to learn and develop are key. It is no good having an experienced investigator who has little or no interest in technology, as they are unlikely to develop the basic level of understanding required to operate within this environment.

For the investigation aspect of the unit, we are not looking for in-depth knowledge of computer science. But, if candidates are unable to engage appropriately with specialist training, struggling to understand what suspects in interviews say, or get to grips with advanced persistent intrusion on a company's systems, then they may not be the right person for a CyberCrime Unit role.

CREST can help with understanding via its self learning modules available.

In the previous chapter, we covered the need to conduct both reactive investigations, (responding to specific incidents), and the skills required to underrate proactive work (targeting offenders and crime groups), being essential. You will need staff that can demonstrate previous experience in undertaking similar work, a strong desire to take a fresh and innovative approach to criminal investigation, and a willingness to develop and undertake new ways of working.

Some people that staff are likely to come into contact with may also have different challenges than experienced in other forms of law enforcement. Suspects and crime scenes will present differently, and witnesses may provide technical, complex evidence, difficult to explain in simple terms.

Generally, cases will sometimes feel difficult to compile in a way that can be understood by others and taken successfully through the criminal justice process. Investigators must demonstrate an ability to engage effectively with a variety of people; to explain complex issues in a straightforward and understandable way and have the vision to adapt and develop the way they investigate.

Selection and recruitment should test for these skills, probing candidates to draw out their experiences and appropriately assess their ability to undertake the role.

"Generally, cases will sometimes feel difficult to compile in a way that can be understood by others and taken successfully through the criminal justice process."

3.0 Team Requirements & Team Recruitment

3.6 Technical and Digital Forensics

Staff delivering technical and digital forensics functions to the CyberCrime Unit team will need to be the most technically competent. Again, careful consideration of staff employed here is vital.

It is no good employing a team of really experienced computer scientists if they do not have an investigative mind set. These experienced candidates may struggle to explain complex issues in a way others can understand or lack the flare to develop and test new ways of targeting difficult-to-infiltrate crime groups.

Technical and digital forensics staff need to interact with, and work alongside, investigators, assisting with drafting and evolving digital forensic strategies. Where appropriate, they must also be able to engage with suspects and witnesses to deliver the best possible strategy for that particular investigation. While certain skills required may be technical, you will also be looking for other abilities, such as communication and assessment skills that set potential candidates out from the rest.

The decision to look internally or externally will need consideration. Your organisation may already have staff with some of the skills required here. There may even be an established digital forensics function in place, providing forensic services to other parts of the organisation, with trained and experienced people available for redeployment.

It is worth looking at both external and internal recruitment for this team, which can bring out some surprising candidates who might have previously worked in the tech industry or have an interest in technology from their private lives.

Experience of this process suggests it can be difficult to compete with private sector organisations in terms of salary levels. Finding people with a public service mind set can help, and of course trading on the unique experiences that working with law enforcement brings also helps attract the right people.

"Where appropriate, they must also be able to engage with suspects and witnesses to deliver the best possible strategy for that particular investigation."

3.0 Team Requirements & Team Recruitment

3.7 Intelligence

Intelligence needs be at the heart of everything the CyberCrime Units will do. Intelligence should be used as a solid base on which to build and develop a structured and reasoned response to the threat from cybercrime.

"The ability to engage partners and work collaboratively to solve problems – and develop new techniques and ways of gathering intelligence – is paramount."

Staff undertaking intelligence roles must understand the unique nature of intelligence and ideally have previous training and experience in an intelligence role.

As with the other roles discussed, intelligence staff should be seen as part of the team and a close working relationship throughout the lifecycle of an investigation must be maintained. Intelligence section candidates must display an ability to interact with other team members, negotiating and influencing some of the decision making around the direction and focus of activity. They will need to make judgements based upon sound research and evidenced findings.

Over and above the standard law enforcement expectations of an intelligence role, the CyberCrime Unit role will need to operate in the digital world. This brings a fresh set of requirements to be considered when looking for the best candidate.

The need to assess and make use of a set of specific tools is also a key part of the role, requiring technical capability and an interest in the subject matter.

As with the other roles, if a person doesn't understand what intelligence opportunities there may be in online chat rooms, or how to safely access and navigate the TOR network, for example, they will struggle to operate in this environment.

This area of law enforcement is relatively new and is constantly evolving under the influence of staff working in the arena.

The ability to engage partners and work collaboratively to solve problems – and develop new techniques and ways of gathering intelligence – is paramount. A good working relationship with the wider cyber industry is crucial.

Candidates with previous experience of these areas are likely to have the right skills for intelligence roles.

3.0 Team Requirements & Team Recruitment

3.8 Analysts

Within general law enforcement it is common to see data and information analysis fall to the staff working within the intelligence roles.

A key difference in cybercrime investigation is the sheer volume and diversity of information, evidence and data generated by just a single investigation. More than any other type of investigation, the volume of information and the ability to effectively assess and analyse it creates issues, as well as the problem of how to securely store and manage it.

Some forward–thinking organisations have started to create specific roles to manage data analysis, enabling more efficient use of it.

Some have given this role the title of Data Scientist, others Cybercrime Analyst or Researcher.

Whatever the title, having staff who can implement data analytics methodologies and techniques, and develop processes to combine disparate data feeds to visualise, transform, model and exploit multiple open and closed data sources is helpful.

This approach can translate data into valuable insights, which can inform tactical and strategic decision making, connect seemingly unconnected matters and provide a rich pool of evidence for pursue and prevent campaigns.

Similarly to the intelligence role, analysts must be capable of working with the CyberCrime Unit team and be able to negotiate and influence people at all levels.

Use of specific tools will be required, alongside the ability to consider a problem from a fresh and innovative angle. Seeking candidates that demonstrate previous experience in this type of role, as well as interest in the subject matter, will assist with recruitment.

Technical training will be necessary to operate in the digital world, so some competency with existing tools or tactics should also be explored.

“More than any other type of investigation, the volume of information and the ability to effectively assess and analyse it creates issues, as well as the problem of how to securely store and manage it.”

3.0 Team Requirements & Team Recruitment

3.9 Protect & Prepare

While acknowledging Protect and Prepare roles are aimed at slightly different parts of the wider strategy, the skills and knowledge of staff employed in these areas are closely matched, and therefore dealt with in this single section.

Protect and Prepare staff will be at the forefront of delivering key messaging and strategies aimed at making everyone and everything much harder to target and a lot more resilient if and when an incident occurs. They need to be credible and require specific training to undertake their roles.

This requires two equally important skills: the knowledge and ability to track and understand the threat, and the skill to engage and educate various audiences while delivering a variety of physical and virtual campaigns.

More than any of the other roles in the CyberCrime Unit, it is important that Protect & Prepare staff can present technical concepts in an accessible way. Skills in building relationships and developing, producing and delivering engaging content are needed.

To maintain credibility, the roles should be supported with industry recognised training and accreditation, such as that provided by CREST. It's vital to employ staff who can undertake such training and who hold an interest in the subject matter.

Another consideration is the method of content delivery. The roles will need to be able to reach audiences of all ages and abilities, including hard to reach communities, so a variety of interpersonal skills are required.

Highlighted by the global pandemic in 2020-21, the ability to operate virtually using social media platforms and develop engaging content should also be an important consideration when selecting suitable candidates.

> *"Skills in building relationships and developing, producing and delivering engaging content are needed."*

3.10 Prevent

Although Prevent is focused on a different aspect of the model, it is still an integral part of the overall team.

A lot of the skills discussed above, along with the ability to engage and understand people in and around the online world, are needed for this role. As separate guides are available, specifically covering Prevent strategy, we do not need to go into further detail here, rather point you to those guides for a more in-depth view of what is required around the **Prevent and intervention roles.** (Report coming soon)

However, for completeness, we have included a role profile in **Appendix A** to assist. A more comprehensive summary of these role profiles can be found in the Prevent guidance documents linked above.

3.0 Team Requirements & Team Recruitment

3.11 Other Roles and Considerations

Apart from the main elements of the unit covered above, there are other interconnected roles. Covert or undercover requirements should form part of your wider capabilities.

Depending on the setup of your unit and organisation, these could be embedded in the main CyberCrime Unit or located elsewhere but connected into the unit. You may also want to extend undercover activity to operate and undertake activity in the deep and dark web.

This may include intelligence gathering or criminal marketplace takedowns, undertaking offensive operations to target offenders, infiltrating criminal infrastructures or taking out botnets used to deliver malware or criminal operations. All these covert activities require staff with appropriate skills and training.

As well as your main team, there is value in looking at what partnerships and support programmes such as a volunteer network might add. We have already discussed an approach which includes links into academia and industry; this could be an extension to that.

Creating opportunities for experienced external staff to assist and support the work within your organisation can bring great value.

It also helps develop those relationships, including things such as a volunteer programme, apprenticeships, internships, staff exchange schemes, training collaboration and development, and joint exercising.

Partnerships provide access to skills and capabilities that you may not normally have access to, or that may otherwise be too costly to have as a permanent option. Partnerships open up new possibilities and extend the range of capabilities you are able to call upon, as well as assisting with your own staff development. It does come with risks though – having security clearance policies is always recommended.

Such policies are relevant for both employed staff and any partners or volunteers you may have undertaken joint activity with.

It is also good practice to have different levels of clearance, which can be role-specific, depending on the level of information the staff member has access to.

For example, staff working regularly with security services or accessing top secret information should undergo the most rigorous checks. General staff could have quicker and less intrusive processes.

Your clearance policies should ensure the integrity of your operations, keep out staff that may be vulnerable to corruption, and provide a level of confidence to your partners that the unit is safe to do business with.

3.0 Team Requirements & Team Recruitment

3.12 Staff Retention

As you develop teams, you will want to consider appropriate training and development opportunities for the roles. Using a structured approach to ensure each role has a defined training pathway is a good way of approaching this – details of training pathways are covered in more detail in the next section.

But as the staff become better trained and qualified, so does the ability for them to move away from your organisation to other roles. In some respects, this can be seen as a healthy and positive thing.

This could mean staff move around gaining skills and experience they may not get from remaining with one organisation. As you employ external candidates, they will bring this experience back in. However, private sector organisations can often pay better in the short term, and the temptation of higher salaries may draw staff away. Using appropriate tactics to try and manage this can help.

Contractual tie-in clauses connected to training, such as stipulating if they leave within so many months or years of a particular training course, they must pay back a portion of the costs, can influence this.

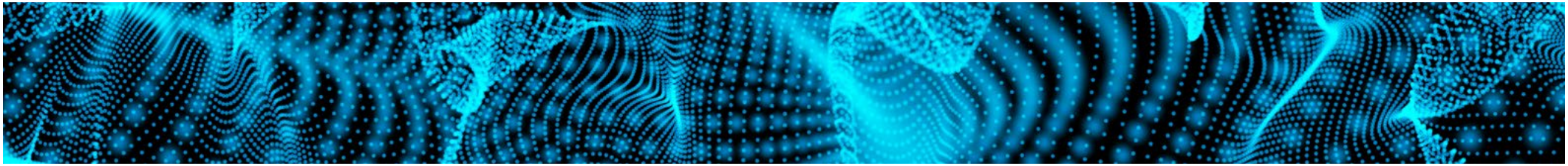
"Where possible, define and identify opportunities to keep your trained and talented staff with-in the cyber structures."

However, softer approaches, like allowing membership of professional bodies or accreditation schemes, or using internships and apprenticeship programmes to attract a regular cohort of fresh talent will help.

Another big factor we have seen is the lack of career pathways within the specialism of cybercrime.

All too often, officers and staff become well trained, experienced cyber investigators, but then have to move if they want to progress through the ranks or move up the organisational structures.

This can be very destructive and lead to staff being pushed away and becoming disillusioned. We encourage open debate. Where possible, define and identify opportunities to keep your trained and talented staff within the cyber structures. Law enforcement will always be an attractive employment option, so whatever your approach, be aware of these potential issues and create strategies to manage them.



Training Requirements & Availability

4.0 Training Requirements & Availability

Introduction

It is clear that specialist training is required to set up and develop all aspects of a CyberCrime Unit. Law enforcement must navigate and engage within unfamiliar environments to access training, qualification and accreditation services that it has not previously used.

A quick look at the market reveals a multitude of training service providers offering training, cyber security courses, accreditation and certified qualifications and all manner of useful courses to develop your staff.

Alongside equipment purchases, training will be one of your most significant costs. It needs a cautious and structured approach to prevent wasted expenditure and lost time and effort undertaking activities that may prove to be unnecessary.

Early research will help you (Report coming soon) establish what training is available in your region or country and begin to highlight which opportunities you can take advantage of. Relevant courses may have already been developed within your own organisation, such as elements of digital forensic training or digital intelligence collection. A review of internal or established training frameworks is a good place to start.

It is unlikely that your own training programmes will be sufficient to cover all the required development. You will have to look to external providers for some of the more specialist elements.

"Relevant courses may have already been developed within your own organisation, such as elements of digital forensic training or digital intelligence collection. A review of internal or established training frameworks is a good place to start."

Local or national requirements may also influence what you need to consider. For example, if there are directives that prohibit unregulated activity, or any legal framework that has specific restrictions around who can carry out certain activities, these will also need considering.

This could mean specific training, accreditation, or qualifications may be required for sections of your staff to legally operate. This is an opportunity to partner with other countries in your region around areas such as training, which can assist when engaging providers and help build consistent working practices.

4.0 Training Requirements & Availability

Introduction

The next sections will help. But you must address which qualifications framework should you use, which provider(s) deliver the best options for your particular needs, and which organisations have the most credible set of standards.

Credibility is important here, too. There will be members of your team who regularly interact with industry, which means they will need to (a) understand what they are being told, and (b) have professional credibility so others have confidence in their ability to deliver a competent service.

Industry recognised qualifications that mirror those held by professionals in the private sector will assist in proving credibility. There is also a need for tool-specific training, required to operate certain equipment. Specialist software often requires certification, which again could be a requirement under regulations to ensure staff competence.

Generally, there is a lack of consistent approach in establishing a law enforcement training programme, leaving each country or region to set their own.

Using initiatives such as collaborations with other countries will help, but you will also have to think about exactly what a good training programme comprises.

To our knowledge, there isn't a particular national or international qualification specific to policing or law enforcement.

In the UK, the College of Policing helped develop a professional accreditation alongside the Charted Institute of Information Security (CIISec) called 'The Institute of Cyber Digital Investigation Professionals' (ICDIP)[13]. This accreditation was introduced to professionalise and upskill law enforcement staff involved in cyber and digital investigations. We encourage countries to explore options of delivering a similar approach through collaboration frameworks with others in your region.

[13] https://www.ciisec.org/icdip

4.0 Training Requirements & Availability

4.2 Training Pathways

Using the above approach, and tools such as the role profiles in Chapter Three, it is possible to build a clear picture of the different skill sets each element of your CyberCrime Unit requires.

This will set out a structure to manage and control training and development. It will help focus effort and ensure staff has the correct skills to undertake their roles without unnecessary expenditure.

Having defined the various levels of training each role requires, you can identify clear training pathways for staff to follow. Such clear pathways provide organisations with reassurance that investment in training is appropriate, controlled and cost effective.

"Training must evolve to keep pace with changes in technology. What might be an appropriate course today may not fit your future requirements."

Training pathways help identify gaps and assist with development of possible further training requirements. Future law enforcement-specific training may not be currently available and require developing from scratch.

Engagement with the training industry is vital as you may need to create a specific course, as yet unconsidered. There are very few industry training providers that have ever designed or delivered cyber-themed courses specifically aimed at law enforcement and the unique skills they need, let alone a single course that turns police officers into *cyber* police officers.

Developing close relationships with trusted training providers gives you the opportunity to develop new and innovative courses. Such a close relationship also creates the chance to build and deliver bespoke training to your staff.

Training must evolve to keep pace with changes in technology. What might be an appropriate course today may not fit your future requirements. Considering the array of training options, and the plethora of providers (which will change over time), it is not possible to cover everything here,

or point you to a specific set of courses or singular provider.

We must take a relatively generic approach in this document, helping inform and guide you in your decision making, giving examples where we can.

Approach training with regular reviews and reassessment of needs, and you will ensure your particular training pathways remain fit for purpose and relevant to organisational requirements.

Feeding off your relationships with the technology industry, incident response companies and academia will help inform choices concerning what may or may not be right for your organisation.

4.0 Training Requirements & Availability

4.2 Training Pathways

Examine the Skillsets

Not every role requires the same level of training. A manager overseeing work will not need to attend crime scenes and forensically recover volatile RAM data.

A digital forensics specialist will not necessarily need to present intelligence reports formulated from pools of big data.

Certain skills may be beneficial for all (or to at least have a working understanding of) for roles to operate efficiently.

For example, an Investigator might not need to be fully trained in network analytics and live packet capture, but an understanding and overview of the value of the process would help when they are running cases and planning strategies.

So, the next step in your training plan must identify what the various levels of training might be.

These can then be mapped across different courses identified, and the level required for each role established. The processes outlined below concentrate primarily on the cyber and technical elements of training. Clearly, there will be crossovers with other investigative specialisms, such as fraud, money laundering and financial investigation.

To keep focused on cyber, we will not stray into these here. We will discuss this again later in *Other Investigative Skills*. However, depending on your team composition, you may also want to consider training options that cover those skills. Further advice can be sought from your Fraud or Economic Crime departments around what training provisions in these areas are available.

As a first step, break your training plan into different levels, such as:

Foundation – An introduction to the basic concepts around computers and how they are used to commit crime

Intermediate – Building on the foundation training, these courses will develop student's knowledge further and provide some of the specialist skills required for the roles

Advanced – As the student becomes experienced, this training will build them up towards more advanced concepts and capabilities, providing them with the most up to date skills

Specialist or Role Specific – more bespoke training aimed at the different specific roles within the CyberCrime Units

We recommend foundation level caters for all roles, providing a basic level of knowledge that all staff in the CyberCrime Unit need. Subsequent levels can then build on this and become more bespoke to cater for different roles and include more specialist or role-specific courses.

4.0 Training Requirements & Availability

4.2 Training Pathways

Identifying key or 'must have' components will assist in mapping out what is required from each level. This will provide clear reference material when searching for the most appropriate training, or engaging providers to establish what they can develop for you. It could include some of the following elements: ***(these can change regularly and should be defined by your specific set up and needs. The subjects here should not be taken as a comprehensive list, rather a guide to assist in mapping).***

FOUNDATIONS
An Introduction to Digital Devices and Computers
An Introduction to Computers, Operating Systems and Networking Protocols
An Introduction to Wireless Networking and Wireless Surveys
Threats, Attack Vectors and Common Cyber Vulnerabilities
Concepts of Digital Currency
Principles of Digital Forensics and Digital Evidence Preservation
IT Security Principles

INTERMEDIATE
Encryption, Obfuscation and Steganography
Digital Footprints and Traces
Introductory Digital Forensics
Principles of Digital Evidence
Router Examination
Cloud and Remote Storage
Cryptocurrency
Use of VPNs and the Dark Web
Introduction to Open-Source Tools
Identification and Preservation of Volatile Live Data
Incident Response and Scene Management
Virtual Machines
Networking (Including Physical and Logical Systems)
An Introduction to Hacking

ADVANCED
Digital Forensics (Including Live, Mobile Devices and 'At Scene')
Malware Forensics (Including Reverse Engineering)
Ethical Hacking
Open-Source Security/Hacking Tools
Packet Capture and Analysis
Network Intrusion Analysis
Computer Science (consider structured modules aligned to academic courses)
Triage and Screening Tools
Programming and Scripting
Wireless Networks
Password Cracking

SPECIALIST / ROLE SPECIFIC
Open-Source Intelligence (Including specific tools)
Linux Operating Systems
Mac and iOS Operating Systems
Games Consoles and Other Digital Devices
Analysis and Analytics of Large Data/Data Science
Tracing Cryptocurrency Transactions
An Understanding of Neurodiversity
Presentation and Training Skills
Information Security (Including any relevant accreditations)
Offender Management and Debriefing
Business Continuity and Incident Management
Wi-Fi Sniffing and Radio Frequency Detection
Equipment Interference
Informant/Covert Source Handling
Covert and Undercover Skills

4.0 Training Requirements & Availability

4.2 Training Pathways

Developing this a stage further – and cross matching roles against skills – you can then map out basic training pathways, which could evolve as the CyberCrime Unit matures.

An example of how this can be done is as follows: *(this contains example subjects so should not be taken as a definitive list; rather a guide for illustrative purposes and to assist with mapping)*

As you develop this approach, you will need to research what courses and providers are available, to identify where relevant courses sit within the training pathway. If your organisation has a Training and Development Unit, involve them in the exercise. They will be able to assist with creating skills and training profiles and build organisational memory for the future.

A Training and Development Unit will have previous experience in developing new courses and experience in engaging and negotiating with external providers. It is also worth considering at this stage what training other digital and cyber entities in your country have put in place.

For example, there may be teams at state level that require similar skills and have already undertaken some of this research.

Undertaking the same or similar training as others, who you may ultimately have to work with, will also help introduce consistency and common working practices. These other units may also have established minimum requirements and introduced restrictions around who may or may not be engaged to provide specialist training such as cyber and digital skills, which you may have to follow.

	Foundation					Intermediate					Advanced					Specialist Role				
	Digital Devices	Protocols	Networking	Wireless	Cyber Attacks	Encryption	Forensics (Intro)	VPNs/Dark web	Obfuscation	Incident Response	Digital Forensics	Malware Forensics	Logs & Registry	Live/Volatile Data	Packet Capture	Open-Source Intel	Linux OS	Big Data Analysis	Neurodiversity	Presentation Skills
Manager	✓	○	○	○	✓	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Supervisor	✓	✓	✓	✓	✓	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Investigation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	○	○	○	○	○	✓	○	○	○	○
Digital Forensics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	○	○	○
Intelligence	✓	○	✓	○	✓	○	○	○	○	○	○	○	○	○	○	✓	○	○	○	○
Analyst	✓	○	✓		✓	✓	○	✓	✓	○	○	○	✓	○	○	✓	○	✓	○	○
Protect/Prepare	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	○	○	○	○	○	○	○	○	○	✓
Prevent	✓	✓	✓	✓	✓	✓		✓	✓	○	○	○	○	○	○	✓	○	○	✓	✓

✓ Required ○ Optional

4.0 Training Requirements & Availability

4.3 Training Providers

While you start to map out courses and providers, you will also need to assess what methods, tactics and skills are being acquired. This is important as there may be laws or regulatory restrictions within your country that prohibit particular behaviour or activity which could render the newly-acquired skills unlawful, meaning staff cannot use them.

Just because you can find a training provider willing or able to teach you a skill, or provide you with specialist equipment, doesn't mean it is possible to legally use it. We have seen examples where considerable amounts of time and money have been spent on an apparently groundbreaking skill or new technical tool that was then unable to be deployed. Our advice here is to keep cross checking that courses and skills are compatible with your domestic laws and regulations.

Support networks – such as regional and national CERTS, regulatory bodies or accreditation organisations – are another good resource. Such support network bodies should be aware of the current training landscape in your country or region, and aware of which training providers are suitable, or which academic organisations would be best to approach. Examples include organisations like NITA Uganda whose functions include the certification of IT products, services and training[14]. On the NITA Uganda website you can find a list of approved and certified organisations. In Indonesia Id-SERTII/CC has similar lists[15], and Pakistan Information Security Association (PISA) offers training advice as part of its services[16].

Universities and academic establishments may offer off-the-shelf training or may be excellent partners to collaborate with in developing relevant courses.

International training providers are likely to offer suitable courses and relevant training. Companies like SANS Institute offer a comprehensive array of cyber related courses[17], and cover a wide number of relevant subjects, and popular accreditation providers, such as Infosec[18] or GIAC[19], can identify relevant pathways.

This is another area where you could look to other regional countries for joint initiatives and collaborations.

Some international providers request premium rates, so many of their courses could be prohibitive due to cost or geographical locations.

CREST International provides a list of approved training providers, which we recommend as your first port of call.

Taking a flexible approach could assist with selecting training providers and looking at options to introduce distance and online learning may be a more cost-effective solution. However, some development will inevitably need to include practical application and may involve examinations, so this is probably not a complete option, and some classroom time will need to be factored in.

14 https://www.nita.go.ug/sites/default/files/newsfiles/NITA.pdf

15 https://idsirtii.or.id/en/page/training.html

16 https://www.pisa.org.pk/public/Services/services

17 https://www.sans.org/cyber-security-skills-roadmap?msc=course-list-lp

18 https://resources.infosecinstitute.com/

19 https://www.giac.org/

4.0 Training Requirements & Availability

4.4 Wider needs of the Organisation

You must consider the wider training needs of your organisation and connected partners. This includes other law enforcement agents or police officers in your organisation. They will undoubtedly be coming in to contact with digital and cyber-related issues on a daily basis – and may also be the first staff to respond to developing cyber incidents.

They will need some form of knowledge and understanding of how to approach these cyber issues, so general or mainstream cybercrime training will need introducing.

This could include subjects such as:

- Understanding of digital communications, social media, cybercrime and law enforcement
- The initial response to cybercrime and digital policing
- Supporting victims of cybercrime
- Initial steps in an investigation, to include using data such as IP addresses and open-source information, and investigative opportunities on the deep and dark web
- Common online crimes, and how to secure and seize electronic evidence for an investigation
- Case preparation and prosecutions

4.5 Partners

The same is true for other support or partner organisations that play a part in the criminal justice landscape.

It is no good upskilling law enforcement if the teams involved in prosecution can't understand the case, or the judge in a hacking case is unsure of the terminology or concepts of the attack. This is also relevant for senior law enforcement officers, government officials and any staff that needs to understand cybercrime. A much wider training programme will assist in uplifting the overall cybercrime knowledge and skills of more generalist roles – benefitting your organisation, your network and society at large.

4.0 Training Requirements & Availability

4.6 Continual Professional Development

Continual professional development, or CPD, is good practice.

More than most other areas, cybercrime constantly changes. Technology improves and criminals learn new tactics to try and stay ahead of law enforcement. It is imperative that staff capabilities are continually developed.

CPD offers a chance for elements of the establishment, and partners, to hold joint events and exercises. Part of the CyberCrime Unit's ongoing responsibilities should be towards activity such as horizon scanning and research and development.

Aim to build a healthy and vibrant CPD programme, in conjunction with service providers, academia and the tech industry.

4.7 Conclusion

Taking this approach will:

- Help design a comprehensive training programme
- Keep control of what training each role requires
- Help identify and monitor which staff have undertaken which course, and what's next
- Standardise your approach to define what skills each role needs, and
- Allow you to offer the most appropriate development pathways for staff.

A structured, planned approach to continual training needs will provide financial control and return better value for money, giving senior staff confidence that a well-reasoned approach has been taken, and public money has been spent appropriately.

5.0

Requirements for Supporting Policies & Process

- 5.1 Introduction
- 5.2 Mission Statement
- 5.3 Linking to your strategy
- 5.4 Minimum Standards
- 5.5 Performance Indicators
- 5.6 Support from other teams
- 5.7 General Policies
  - *Equipment*
  - *Location, Security and Environment of the CyberCrime Unit*
  - *Procurement*
  - *Digital Evidence*
  - *Cryptocurrency*
  - *Covert Activity, Offensive Tactics and Targeted Equipment Interference*
  - *Assets Seizure, Confiscation and Compensation*

5.0 Requirements for Supporting Policies & Process

Introduction

Most countries will have some form of overarching cyber and information security strategy, such as a defined National Cyber Security Strategy. Before looking at what your organisational policies should cover, it is advisable to understand the existing national approach.

Using this as a basis to create your own complimentary frameworks will assist with integration across other elements of the wider law enforcement landscape, as well as garnering support for your development programmes.

If you are in a position to influence this at state level, then looking to develop a common set of themes to use across a number of strategies will assist in the national approach, mirroring and complimenting it at all levels.

In turn, understanding the existing national approach will provide consistency and develop a stronger and more cohesive response to the threat.

Of course, looking beyond your own geographical borders may also be beneficial, and some consistency with regional or international approaches will help with interoperability as and when you need to cooperate on bi-lateral or multi-lateral activity.

Engagement with international law enforcement organisations such as Interpol[20] is undoubtedly useful here, facilitating the exchange of working practices and helping understand how others are approaching cybercrime. Other international agencies, such as the United Nations also have cyber-specific support available[21].

[20] https://www.interpol.int/

[21] https://www.unodc.org/unodc/en/cybercrime/index.html

5.0 Requirements for Supporting Policies & Process

5.2 Mission Statement

Within these national strategies there will be vision and mission statements. These are likely to include sentences such as "To create a secure, dependable, reliable and safe cyber environment", or "Build a safe and secure trusted cyber community to provide opportunities for citizens and safeguard national assets and interests."

The vision will outline what the strategy aims to deliver, as well as the direction the country intends to take to improve cyber and digital resilience, capability and overall security. Using this as a starting point, policies and processes you subsequently introduce should support this. When drafting policies and processes, highlighting how they link back to, and underpin, the national vision will assist with introducing it and provide reassurance that your CyberCrime Units and structures are an integrated part of your nation's wider drive to improve cybercrime capability.

Taking this approach ensures the main vision of your country's cyber strategy is woven through every decision you make on how to set up and develop your particular CyberCrime Unit, organisational response and capability development.

In this section, we examine how you can identify policies necessary to support your activity and how they can map across the constituent parts of a CyberCrime Unit. You may also decide your CyberCrime Unit or organisation needs to define its own vision statement. We would encourage this, as it is an important first step in setting out commitment to developing and investing in a cyber capability. It also sends a message that these issues are a priority which your organisation takes seriously. **It demonstrates commitment from senior staff and supports subsequent decision making while undertaking development needed.**

5.3 Linking to your strategy

At the highest level, you will want to set out your approach to the main strategy. As we have used the 4P approach, we will again use it here to stimulate ideas and generate guidance.

Each 'P' can present a number of subjects that shape policies and the overall method on how you intend to deliver them, some of which may have common themes or interests and will mature over time. Generating a policy document that defines your approach will provide a base to support subsequent decisions and processes. An opening statement may look something like:

"Our Cybercrime Unit will support the national vision to create a secure, dependable, reliable and safe cyber environment, providing opportunities for citizens, and safeguarding national assets and interests.

Through partnerships with industry and academia, it aims to deliver a strategy that will:

Pursue suspects involved in committing cybercrime.

Protect businesses and citizens from cybercrime.

Prepare business and citizens to respond effectively to cyber attacks.

Prevent individuals becoming involved in cybercrime, deter and divert those on the periphery of cybercrime, and degrade and disrupt those committed to cybercrime.

5.0 Requirements for Supporting Policies & Process

5.4 Minimum Standards

You should outline the minimum capability and expectations around each element of the Unit. Drafting different outputs (which can be developed into agreed standards) will define service delivery expectations and act as a benchmark to assess development and hold staff to account on delivery.

You will need to decide what constitutes good performance; what you are expecting each part of the unit or network to deliver, and how you can measure that activity. In turn, this will enable you to set key performance indicators (KPIs) which can then be collected, analysed and monitored regularly, producing a framework to regularly assess performance and check progress.

Later on, this will help in assessing the effectiveness and impact of particular elements of your strategy, identify gaps in capability and steer future development and investment decisions.

Suggested capability minimum standards could include:
(please note this is not an exhaustive or complete list, rather examples and suggestions to assist with the process).

PURSUE

- Minimum staffing levels to maintain capability in investigation, intelligence and analysis
- Access to adequate digital forensics capability
- Creation of relevant training pathways for staff
- Expected standards of investigation and victim support
- Equipment required to undertake the role

PROTECT & PREPARE

- Minimum staffing levels to maintain capability
- Responsibility to develop and run relevant education and awareness campaigns
- Responsibility to build resilience to cybercrime through collaborative exercising
- Support internal staff to improve organisational resilience
- Coordinate wider messaging and campaigns

PREVENT

- Must have dedicated staff with set minimum levels to maintain capability
- Responsibility to develop and run Prevent campaigns, awareness and training
- Engage with agreed Prevent programmes and strategies
- Work with partners to promote Prevent messaging and publicise the programme
- Develop and run Prevent Offender Management strategies

5.0 Requirements for Supporting Policies & Process

5.5 Performance Indicators

Performance Metrics are a good method of assessing progress during development. Once matured, such metrics can be used to provide data on both quality and quantity around how a strategy is both delivering against its objects, and also what impact it has had on the problem.

Here, we mainly quote quantity metrics, as these are often more useful during a development programme.

However, it should be acknowledged that like other crime, the effectiveness of a cybercrime strategy should not just be measured on the number of arrests, but on reduction in the amount of offending – Impact over volume.

As your capabilities mature, we encourage you to develop these metrics, introducing ways to assess the impact and gauge the effectiveness of your overall approach. Initial metrics could include (please note this is not an exhaustive or complete list, rather examples and suggestions to assist with the process):

PURSUE	Number of cases allocated
	Number of live investigations
	Number of operations
	Number of warrants / searches
	Number of arrests / suspects interviewed
	Number of criminal justice outcomes
	Number of new intelligence products
	Number of criminal domains taken offline
	Number of threat assessment reports
	Number of international operations led or supported

PROTECT & PREPARE	Number of new projects / campaigns developed
	Number of Protect / Prepare campaigns undertaken
	Number of engagements with industry and partners
	Number of awareness exercises undertaken
	Number of events and presentations undertaken
	Number of workshops or training sessions delivered to law enforcement
	Number of workshops or training sessions delivered to partners
	Number of operational debriefs conducted to ID emerging threats

PREVENT	Number of new Prevent subjects identified
	Number of new Prevent subjects accepted into the programme
	Number of new diversionary pathways developed
	Number of new diversionary pathways delivered
	Number of subject debriefs undertaken
	Number of Prevent disruptions undertaken
	Number of Prevent campaigns developed and delivered
	Number of Prevent campaigns to degrade reputations/ products/platforms
	Number of Prevent contacts with suspects (cease & desist)
	Number of Prevent subjects that reoffend

5.0 Requirements for Supporting Policies & Process

5.5 Performance Indicators

You should also consider what wider strategies could be included in your own processes, covered by a defined policy. Include activity that supports national strategy, such as adopting nationally agreed messaging around matters like password advice, guidance on keeping regular backups, operating system updates and general cyber hygiene.

It could go a stage further by introducing a mandate requiring membership of appropriate schemes or accreditation bodies to organisations delivering particular services.

For example, a requirement for all companies doing business with law enforcement to have attained a particular accreditation or regulated standard, which could be extended to include their supply chain.

Encouraging your own organisation to take this approach shows commitment to leading by example. If you are in a position to develop this even further, then encouraging other national departments, government organisations and professional bodies to join you will prove beneficial. Such policies can help drive up standards around cyber security – and reinforce your Protect and Prepare messaging.

5.6 Support from other teams

As your CyberCrime Units begin to embed themselves within wider law enforcement structures, there will be a need to interact and cooperate with other teams and capabilities.

This could be to undertake searches, give a surge of officer numbers during operations, or provide surveillance capability during an investigation.

Whatever the reason, we suggest you consider what this additional support and interaction needs to include and ensure suitable Service Level Agreements (SLAs) are in place to a manage any additional requirements. SLAs can also be used to set expectations around partnership and collaborative work. They can form the basis of any joint investigation agreements when operating with other forms of law enforcement, or during international investigations. We will explore interaction with other teams and wider departments in more detail later.

5.0 Requirements for Supporting Policies & Process

5.7 General Policies

More generally, there are several processes and activities we recommend developing and maintaining policies around, to define and regulate delivery. Listed below are some we think you should consider. Again, this is not a complete or exhaustive list, but the below topics are a good start.

Equipment

Technical equipment required to perform CyberCrime Unit duties will include specialist and high-end capabilities. **There will need to be policies in place concerning procurement, management and usage of the equipment for a number of reasons:**

- It is unlikely teams within your general establishment will have had access to, or a need to use, these sorts of tools previously. There may be organisational restrictions in place around what ICT equipment can be purchased and how it can be used. This will need consideration to make sure CyberCrime Units can freely access appropriate equipment, while overseeing what it is to be used for.
- Regulatory or legal controls around particular types of equipment or tactics may restrict how it can be deployed, or who can use certain items. Intended use will need documenting and justifiable decisions recorded, to provide transparency and an auditable process should it need to be examined at a later date. For example, during a court trial.
- Some equipment will be high end and expensive. It is prudent to have security measures around it, including physical storage, transportation and auditing. Introducing controls such as asset lists, which record allocation, movement and usage history will help, along with adopting a regular auditing process to periodically check everything is as it should be.

Location, Security and Environment of the CyberCrime Unit

Some of the work the CyberCrime Unit will undertake will require additional security measures over and above those normally considered for general law enforcement activity. We covered the need for secure storage of the equipment above, but this extends to other infrastructure elements. Using security-controlled access to offices or premises is a start. However, depending on preferred set up, you may need to consider the digital architecture, such as servers and secure digital storage.

This could be part of a bespoke CyberCrime Unit network, which will need appropriate controls as well as specialist security protocols such as regular penetration testing and administrator-controlled access and usage policies.

Broadband internet access will need to be obfuscated and non-attributable to law enforcement. It is no good trying to run intelligence gathering tactics on a criminal marketplace if your IP address is traceable to a police organisation, or have an undercover officer deployed in child abuse chat rooms with equipment revealing they are from a government agency.

Such matters need careful consideration and planning. Any weakness here could compromise an entire operation.

5.0 Requirements for Supporting Policies & Process

5.7 General Policies

Procurement

There is benefit in keeping central control of procurement processes. This can deliver financial savings when purchasing large amounts of equipment - by doing it once and negotiating better prices for teams. It can also control setup of each unit or team to maintain consistency across networks, ensuring compliance with conditions you may need to adhere to. Larger scale procurement also delivers better interoperability between units, when called upon to collaboratively work on an incident. This extends out to training provisions, as well as other common processes or tactics you would want to see delivered in a similar way across different teams, networks or organisations.

Digital Evidence

In Chapter 2, we examined issues surrounding staff handling digital evidence and the need to have policies and processes in place to control this activity.

During an investigation, there are four phases involved in the initial handling of digital evidence: **Identification, collection, acquisition, and preservation.**

Each phase must be undertaken with due regard to the integrity and admissibility of evidence.

Digital evidence presents different challenges to physical evidence. A clear and consistent process should be developed, and steps taken to ensure staff follow these principles when dealing with evidence.

As a starting point, suggested elements could include the following:

- Where possible no action taken should alter the data. However, where it is necessary to access data, the person accessing it should be competent to do so and able to explain or justify their actions
- A record should be made of steps taken, which could be followed and recreated by an independent party at a later time.
- The person in charge of investigation should retain overall control of the process and give due regard to compliance with any laws or regulations.

Having a nationally supported and published process to underpin this procedure will help, which could be further supported by adoption of industry standards and processes that mirror those already in existence in other areas. Examples include standards developed by organisations such as The International Organization for Standardization (ISO), adopted into regulatory frameworks under the control of a government agency.

Taking this approach to digital evidence gathering will build confidence in the validity and integrity of digital evidence, allow courts to draw proper conclusions from such evidence and guard against inadvertent miscarriages of justice. Clear methods, practices and procedures concerning digital evidence helps partners and other countries gain greater confidence in your processes.

Cryptocurrency

During the course of a CyberCrime Unit investigation, it may well come into contact with cryptocurrency and is likely to encounter digital wallets and online storage facilities holding digital currencies.

5.7 General Policies

These funds may be connected to unlawful activity, may have been stolen, or represent proceeds of crime in some other way. Like any currency or criminal asset, your investigators are going to need to assess, transport and securely store these funds.

As we know, when dealing with money and other forms of currency, there are inherent dangers when seizing and handling what can sometimes be large or valuable amounts. It is imperative that you carefully consider this process and the security required around it. If not properly handled, there is a danger of data being corrupted or lost.

Poor security practices can create a risk of theft and staff accessing it, as well as the risk of someone hacking in to wherever you have stored it – and transferring it elsewhere.

At the most basic level, you will need to have appropriate digital capability to seize and transport the cryptocurrency, and then a long-term secure solution to store and manage it, while any criminal justice process is followed. We recommend exploring the option of working with a trusted partner, making use of long-established industry solutions through the network of cryptocurrency exchanges and storage companies.

Your cryptocurrency policies will need to be underwritten and supported through appropriate policies – and be regularly reviewed and audited.

Covert Activity, Offensive Tactics and Targeted Equipment Interference

We previously covered some considerations regarding introducing and deploying covert tactics, which can be a powerful tool in the online world.

You may also want to deploy offensive activity to target particular criminality, which could include accessing, and interference with, specific infrastructure or equipment.

It is likely that if these actions were undertaken by an ordinary citizen, then a significant number of them would be contrary to criminal law in your country. Some covert activities may even be unlawful for police or law enforcement to undertake. There may be regulatory restrictions, as well as internal policy or procedural guidance that would prohibit the use of certain tactics within traditional law enforcement structures.

As you consider each potential option available in this section, you should assess each of them against your particular laws, rules and regulations to ensure compliance, and consider new legislation, if required.

There are moral dilemmas here too; just because you can do something, is it ethically or morally right to do it? Introducing ways to sense check proposed activity may be necessary.

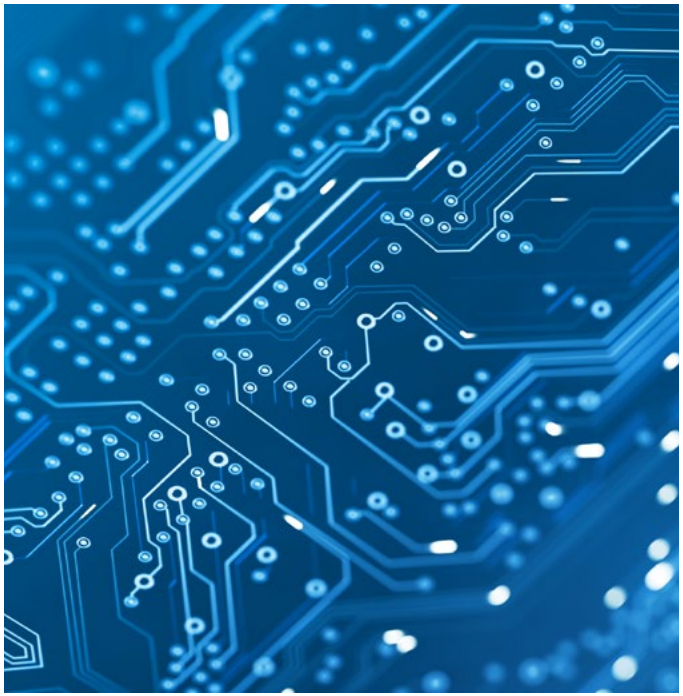
5.7 General Policies

This could include some form of judicial oversight, independent review, or use of trusted partners to provide an ethics board to examine the moral and ethical application of a tactic where appropriate. Strong, carefully considered policy and working processes will be required to protect staff engaged in covert activity and support its lawful use in your organisation.

Assets Seizure, Confiscation and Compensation

A significant proportion of cybercrimes result in theft of money, or other form of misappropriation of a victim's property. It should follow that your response to tackling cybercrime includes the ability to seize assets from offenders, allowing the courts to issue confiscation orders and compensate victims.

It is likely that your country already has existing legislation to support this approach in other forms of criminal investigations. Checking to ensure compatibility with existing legislation will help shape a complimentary cybercriminal assets seizure, confiscation and victim compensation policy. Subject to those regulations, it may also be possible to apply for confiscation of equipment used in the commission of crimes, allowing them



to be either sold for compensation or repurposed and used in the fight to combat crime. This repurposing of confiscated equipment can be used to great effect as criminals often have powerful, high-end hardware which could be used to boost law enforcement's capability. This has double impact – not only depriving criminals of tools to commit crimes but also providing equipment at no cost to your organisation. This sends a very powerful message that crime does not pay. Used in the correct way, seizure, confiscation and compensation activity can support very effective media campaigns.

There will be a multitude of general supporting policies and processes you will need to consider embedding to support the work of CyberCrime Units. These include human resources policies, staff security clearance requirements, staff retention, volunteers and partnership agreements, digital lab management and ongoing equipment and licencing needs, for example.

Wider planning will be similar to other teams or departments in your organisation, so where possible you should mirror or complement existing structures, taking advantage of previously developed relationships and working practices.

The most important aspect when undertaking this exercise is to ensure you methodically address all the new or specific policies or processes required for CyberCrime Units, while ascertaining how the teams will fit into your existing structures. In the next section, we examine the wider picture and explore what other parts of the organisation, law enforcement landscape and interconnected parts of the criminal justice system CyberCrime Units will need to work with.

6.0

Links with other parts of Law Enforcement & Judicial System

6.0 Links with other parts of Law Enforcement and Judicial System

Introduction

Just like other departments in large organisations, you must think how your CyberCrime Unit will need to interact with other teams and capabilities, assess which of functions may provide support to other units, and conversely, what support the CyberCrime Unit requires to fully discharge its own duties.

We have already touched on some of the more general considerations such as human resources support, physical locations and procurement processes. In this section we look at more specific connections into other parts of your structures and the wider system, to understand how they need to interplay with each other. We provide suggestions to help you map out your own particular needs.

6.0 Links with other parts of Law Enforcement and Judicial System

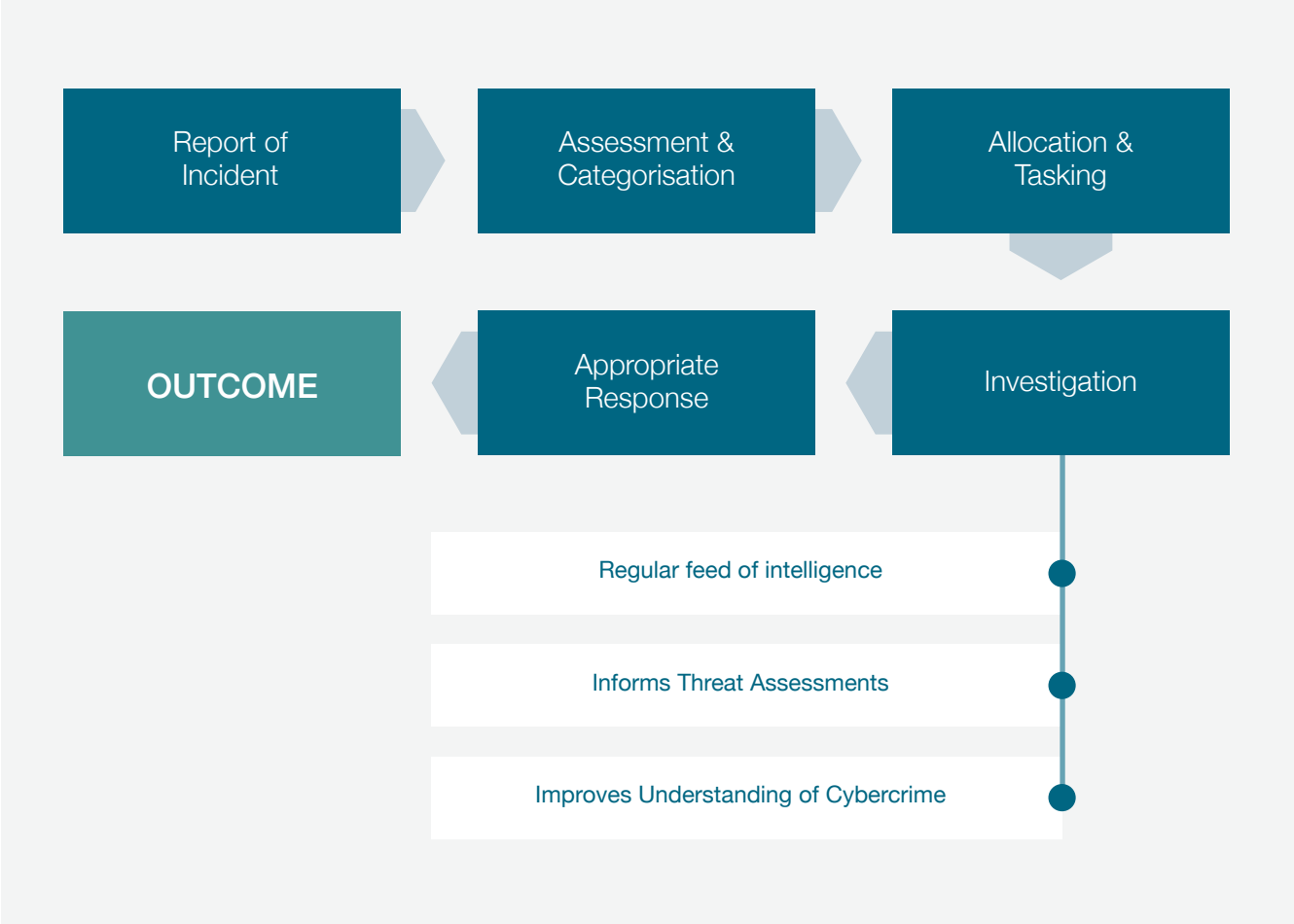
6.2 Case Assessment & Referral Processes

Let's look at the life cycle of cases and activity flow – from inception of an investigation to conclusion, as well as the other 4P activity that sits around it, beginning with reporting an offence.

Crime reporting, collection, assessment and allocation processes will already exist for traditional crime reports, which could just be adopted for cybercrime. However, cybercrime presents some unique challenges that may require additional measures.

To begin with, the threat is global. In your country, oversight across all reports is required to prevent multiple teams investigating the same incident without realising. The nature of many cybercrime offences can be very technical, so staff taking reports and assessing response required must understand the methods and technology used.

We recommend the proposed process of crime reporting and allocation is assessed for compatibility with cybercrime reporting, and adjustments made where necessary. This may include report compilation training, introduction of a Fraud and Cybercrime Reporting Centre, or a central processing and allocation team authorised to task the cases out to the most appropriate teams. Linking these processes into your daily activity will also support matters such as intelligence gathering, provide a regular flow of information to maintain an up-to-date threat picture, and keeping check on current methods and tools criminals are using.



6.0 Links with other parts of Law Enforcement and Judicial System

6.3 Other Investigative Skills

Once an investigation has been received and allocated, you will need to understand the skill sets required from your investigators. There are many other crime types intertwined with cybercrime, and some have their own specialisms with dedicated units to investigate them.

Obvious examples include fraud and money laundering, so ways to work with these other crime units should be explored. While contemplating particular departmental structures, you could include specialist investigators within the CyberCrime Unit to cater for different aspects, or have agreements with other departments on what aspects of an investigation will be led by particular teams.

For example, If a CyberCrime Unit is investigating a case of the theft of money where money mules are being used to move the funds, access to a financial crime investigator's skill, or traditional surveillance teams to follow suspects cashing out the proceeds, may prove beneficial.

However you decide to structure your investigative teams, there will always be links to other crime types, and an open approach to working with other units will assist investigations.

The services of other support departments will also need to be part of your service level agreements. Because of the specialist nature of the threat and training required, cybercrime units are likely to be relatively small in terms of staff numbers.

6.0 Links with other parts of Law Enforcement and Judicial System

6.3 Other Investigative Skills

However, some cases may involve multiple offenders (we have seen examples where many hundreds of suspects have been identified during a single investigation), so additional resources may be needed at particular stages of an investigation, such as during arrest operations or significant Prevent activity to engage with a potentially large number of subjects on the peripheries of offending.

There will also be particular skills or services required that you don't have in the CyberCrime Units. This might include skills like those above, such as surveillance or search teams, which may need to be deployed as part of your investigative strategy.

We have emphasised the international and global footprint of cybercrime. This will need to be borne in mind when looking at the support you will need. How are your teams going to undertake an investigation that has a main suspect in central Europe, additional offenders in South America, digital storage (with your victims compromised data on it) in Southeast Asia and a crew of money mules working their way across the USA to cash out the proceeds?

Your country is likely to have pre-negotiated and have existing treaties around how they will cooperate with international partners over such investigations.

"Both units, partners or teams must be aware of the unique challenges around cyber investigations, CyberCrime Units must understand how to trigger various elements of it, and most importantly, there needs to be an understanding of expectations and likely outcomes from particular countries."

You will need to understand these and ensure you have engaged with relevant staff and departments to access and make best use of these processes.

CyberCrime Units, more than any other crime teams, will need to regularly use other skills and services, so we recommend negotiating and agreeing a cybercrime-specific procedure to ensure your investigators can readily engage the appropriate networks.

Both units, partners or teams must be aware of the unique challenges around cyber investigations and CyberCrime Units must understand how to trigger various elements of it. Most importantly, there needs to be an understanding of expectations and likely outcomes from particular countries.

Existing processes may already have defined legal routes to follow – this will save time trying to figure things out separately. This interaction with other nations and jurisdictions may also impact on your ability to pursue a particular suspect.

The country they reside in may be uncooperative with your nation, may have disparate or non-functioning central government, or is simply reluctant to assist with your investigation.

You must, therefore, develop a strategy for when this occurs. Such a strategy could include utilising international arrest warrants (which can be put in place ready for if or when the suspects travel outside of the protection of that country), or seeking assistance from international law enforcement organisations such as Interpol, to help you progress the matter.

6.0 Links with other parts of Law Enforcement and Judicial System

6.4 Criminal Justice Process

The above interactions are likely to involve legal processes undertaken by an appropriately authorised department. This brings us on to that relationship and how your CyberCrime Units will interact with the criminal justice system.

Depending on the particular framework your country has, you will need to consider how your CyberCrime Units will access and work with prosecutors and the departments responsible for public prosecution.

In general terms, your system will fall into one of three structures:

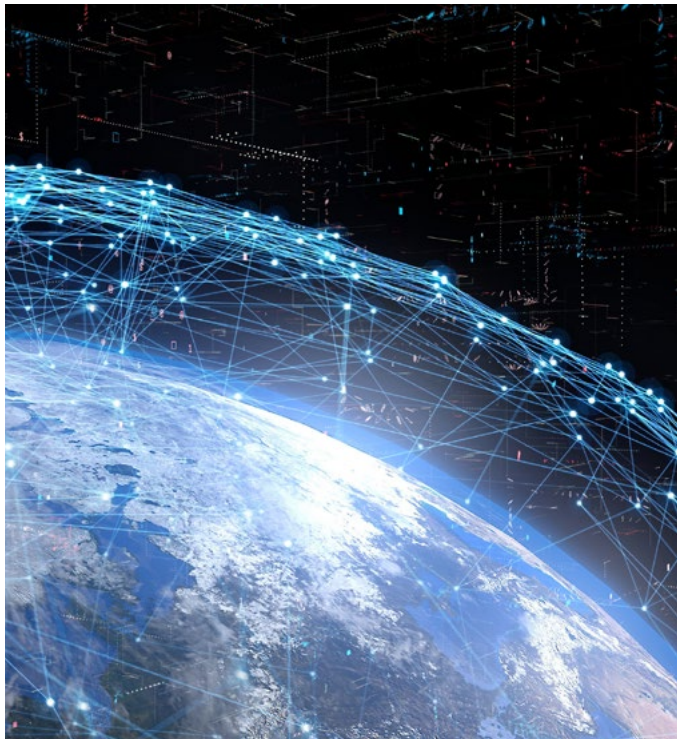
i Police/law enforcement agency-led
ii Prosecutor-led, or
iii Judge- or magistrate-led

In all cases, there is a requirement for interaction with those responsible for bringing about the prosecution of offenders, and the knowledge of those staff will need to be considered in your overall response.

Whether it is at an investigative stage, preparing a case for prosecution, applying for legal process such as warrants, or taking matters through the courts as part of a trial, these staff will need sufficient knowledge to understand the evidence and follow what may be technical submissions from your teams.

Experience shows that some of the most senior people, such as judges and solicitors, have the least knowledge about cybercrime. This can cause issues when attempting to run cases with the people expected to present the evidence or pass judgement on issues having little comprehension of the matters put before them, or even understand the language used by key witnesses.

We recommend introducing a programme of support for these roles, providing similar elements as previously discussed for the CyberCrime Unit staff such as specialist training and CPD type events. It would also be advantageous to complete training jointly with your staff, which will help to introduce consistency and build working practices that support the overall objectives. Such training sessions can present the opportunity to address gaps in legislation that may become apparent when running cybercrime cases. This could include outdated language, incompatible pieces of law, sentencing guidance that doesn't sufficiently cover these new crimes, or just a need to refresh the general legislative approach for cyber matters. Working with departments and staff that make up the criminal justice framework will make this much easier to address.



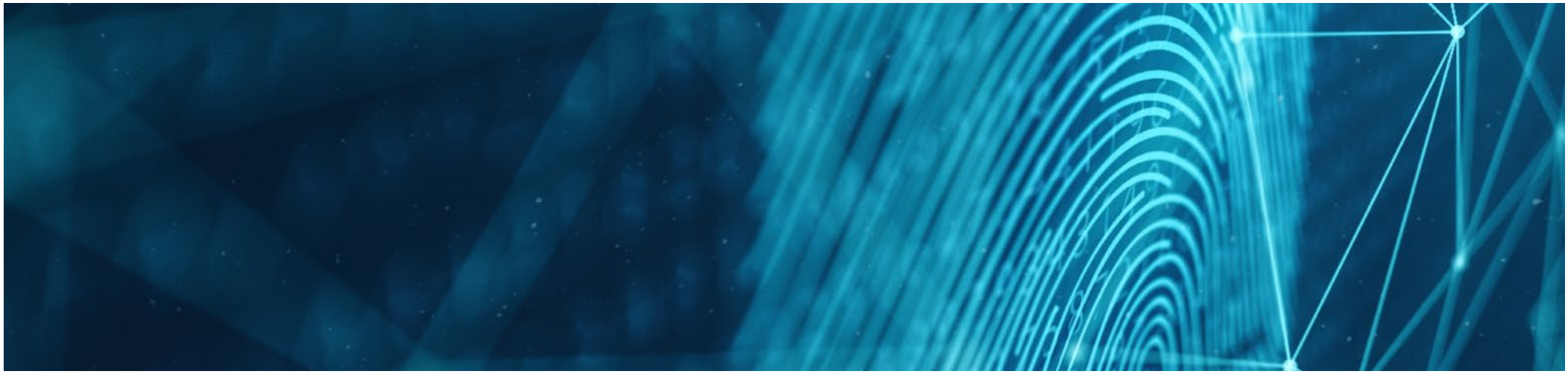
6.0 Links with other parts of Law Enforcement and Judicial System

6.5 Inter-Agency Cooperation

Cases or investigations may cross over multiple agencies and different sections of your own organisation. A case could involve higher level capabilities such as the security services, or even teams within the military or central government. Consider this element while creating your own capabilities, as you will need to establish appropriate links and agree accepted working practices.

Joint training, exercises and CPD activity are recommended, as are mutually agreed and documented protocols covering working together. For example, the USA's National Cyber Investigative Joint Task Force[22], includes more than 30 government, intelligence and military agencies working collaboratively in a colocated department. Such mutually agreed protocols could also be used in private working partnerships with organisations that, while not part of the law enforcement landscape, are providing services to your teams, or evidence gathering on your behalf.

Clearly, care is required here. You must ensure the integrity of your investigations, tactics and security of your staff, so more stringent controls and measures may have to be in place. This could be done on a case-by-case basis, depending on the threat being addressed, or longer term by introducing some trusted working groups which could be used across identified sectors such as banking or information security.



[22] https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

6.0 Links with other parts of Law Enforcement and Judicial System

6.6 Private & Third Party Organisations

There will be sectors that you will want to specifically assess when you are looking at this. These are likely to include:

Finance and the Banking sector

You will need to regularly interact with various establishments in this sector. It is likely they will have confidentiality regulations around their data and information.

Understanding how to engage them and access their data is required. Earlier, we discussed having access to financial crime specialists. This is where that structure will support your investigations.

Internet Service Providers

This sounds like an obvious and straight forward sector. However, depending on your country, there may be a multitude of providers, from small independent companies to multinational and state-owned organisations. Of course, this does not just cover fixed or traditional line to premises services anymore, but also mobile and satellite options. Some form of regulation is likely to be in place. Understanding the provision landscape and establishing processes to preserve and access data will be needed.

Data/Cloud Storage Companies

Similar to ISPs, there is a large industry which caters to the need for server space, data and cloud storage.

These include small independent businesses up to very large multinationals, running enormous warehouses full of servers and digital storage solutions.

Often data and cloud storage companies appear little more than industrial buildings from the outside – but contain huge amounts of equipment.

Understanding where the relevant companies are located, and having working practices around how you will engage and work with them, will help with preservation of evidence and access to relevant material.

Cryptocurrency Exchanges

Similar to the finance sector, you need to establish how you will engage with crypto exchanges. They are different to the traditional financial sector, mainly unregulated and not subject to the same rules as banks and card companies. There are, however, some excellent examples of good practice, and as a sector, the better exchanges are keen to be seen as cooperative and will have self-regulated codes of practice. These will include how they intend to interact with law enforcement. Understanding this will help you establish operating procedures when tracking or tracing crypto transactions and assets.

6.0 Links with other parts of Law Enforcement and Judicial System

6.7 Regulation & Legal Restrictions

As wider engagement is established, you may wish to ascertain which regulations or standards the CCUs will need to adhere to. Adding in partnerships and joint activities makes it even more crucial to get this right, as you will be sharing information and potentially asking other departments, organisations or even private businesses to undertake activity on your behalf.

You need to know and understand the legal or regulatory conditions, and what impact they might have on your activity. Forming a relationship and working with the regulatory body early on will prove beneficial, especially if you are introducing new practices and activities. Through this relationship, you can explore how your methods and tactics fit into regulations, what is or isn't permissible, and what processes need to be followed to undertake particular tasks.

Experience tells us that working with these bodies from an early stage is better than trying to fight against them later. A strong working relationship with regulators affords the opportunity to influence and negotiate how rules might be applied.

6.8 Courts

You should examine whether existing court structures are capable of supporting cybercrime cases.

How will you be able to present digital evidence?

Will a jury or court staff be able to follow complex and technical evidence?

What methods or tools could be used to assist in presenting a case and explaining an issue?

Working with the courts, you might prepare some generic material to explain things such as the most common types of cybercrime, methods of attack, or concepts of cryptocurrency.

Think about compiling aids, like a glossary of cyber community terms or phrases, and explanations of computing terms (like RAM), basic information on how a computer stores and transfers data, or simple network structures.

Using short films and preparing information packs will help provide a bank of reference material and guidance notes for juries or court officials to refer to.

It may be useful here to provide a short explanation of the organisation or structures that are often involved in committing these offences.

Your explanation of the environment could include:

- Malware coders
- Hackers
- Dark market and carding traders
- Deployment and victim contact
- Collection and trade of compromised data
- Botnet management
- Fraudsters
- Financial services and gateway corruption
- Money muling and cashout crews.

This is also an opportunity to explain how cybercrime feeds into wider criminality and is used by more traditional organised crime groups to access new ways of making money.

6.0 Links with other parts of Law Enforcement and Judicial System

6.9 Post-Conviction

Post-court and post-conviction considerations are necessary. While engaging with the Prevent programme, individuals may have been diverted into alternative options to a criminal conviction, or an offender has been given specific conditions as part of sentencing. These conditions might include limited internet access, or a requirement to produce devices to the authorities for regular examination.

Understanding who will take responsibility for managing these conditions and establishing a process to engage and support this will ensure the lifecycle of cases are adequately managed and best outcomes achieved.

Other aspects could include confiscation of assets or equipment, payment of compensation to victims, or debriefing of offenders to assist with the intelligence picture of cybercrime offending. There are likely to be similar processes already in place for traditional crime through departments such as Probation Services.

However, staff undertaking these duties are unlikely to fully understand or appreciate the various aspects of cybercrime or have the skills to undertake visits or examine digital devices.

Creating links to support their work, or even undertaking some aspects of it on their behalf, will help put the final piece in place to support a 'cradle to grave' approach to your investigations and ensure your teams play a significant part in providing a modern, digitally aware justice system.

Although briefly touched on above, it is worth specifically mentioning opportunities the Prevent programme and its innovative approach to tackling cybercrime presents.

Those suitable to take part in any intervention program such as the Prevent programme will be engaged through all phases of the criminal justice process. This presents numerous opportunities to implement these strategies. Post-conviction is an obvious area in which to build suitable intervention activity. We recommend reading the CMAGE guide to establishing a cybercrime intervention program (coming soon).

"While engaging with the Prevent programme, individuals may have been diverted into alternative options to a criminal conviction."

7.0

Programme Development & Implementation Planning

- 7.1 Introduction
- 7.2 Alternative Structures
  - *National*
  - *Regional*
  - *Local*
  - *Single National Structure taking complete control of the threat*
  - *National CyberCrime Unit and Regional only teams*
  - *Independent CyberCrime Units at different levels*
  - *Blended collaboration using various agencies to create National, Regional, and Local CyberCrime Units*
- 7.3 Approaching the Programme of Development
  - *People*
  - *Training*
  - *Equipment*
  - *Tools/Software*
  - *Licencing*
  - *Transport*
  - *Buildings*
  - *Infrastructure*
  - *Travel & Accommodation*
  - *Professional Subscriptions*
  - *Research & Development*
  - *Timescales*
- 7.4 Benefit Realisation
- 7.4 Final Thoughts
- 7.5 Capturing and Recording your Success

7.0 Programme Development & Implementation Planning

Introduction

Having explored a range of options throughout this guide, it's now time to make a decision on what you need to develop to support your particular cybercrime programme, and how to implement it.

Whether it is a full build of comprehensive capabilities from scratch, just adding to existing structures, or improving a particular aspect of your network, this section will help you organise your approach and offers advice on how to undertake it.

Any level of development is likely to involve additional investment and a new approach to ways of working that might seem different or challenge traditional methods that have been in place for decades.

Change can seem threatening, and some will resist it.

If you are just starting on this journey, it is likely that your programme will involve wide ranging developments that include the following:

Strategic – Introduction of new strategies and focus on new threats.

Structural – Building of new teams, departments or organisations.

Human – New skill sets and roles that look or feel different to previous ones.

Tactical – New technical tools and previously unused methods to target and combat the threats.

Cultural – Different way of thinking and approaching the issues.

It is important to have a process which will help promote the need for change, provide a structured and controlled implementation and produce a lasting, robust cybercrime capability.

This falls roughly into four stages:

i Adapting to the need to change and agreeing the way forward

ii Introducing control around the way change is managed

iii Having an implementation programme to oversee and introduce the changes, and

iv Maintenance of the capabilities once they have been delivered.

There are various options around how to develop your particular programme and what additional considerations may help. Where possible, we will provide examples. However, your own country's political structure, culture, and societal makeup will need to be considered when adapting your programme to your particular needs. Any lists or references to material will be for demonstration purposes, and should not be considered complete or exhaustive.

7.0 Programme Development & Implementation Planning

7.2 Alternative Structures

Throughout this guide, we have discussed various options around how wider structures could be set up and made numerous references to three basic levels: national, regional and local.

Below is a more detailed look at what each of these could be responsible for, as well as discussion around the advantages or drawbacks of how it could be approached. This should help with making a decision around how extensive your programme will need to be. Ask yourself whether you are intending to do a full national, regional and local capability uplift, or adding to existing structures to improve on previously established capabilities. Whichever way you are intending to go, the following descriptions should help shape the next stages of your development.

National

These capabilities are directed at the national response to cybercrime and will sit alongside other national law enforcement capabilities. Responsibilities include setting national policy and direction, linking into government, international liaison and relationships, and oversight of the country's response to threats.

Having links to functions such as critical national infrastructure, banking and financial services, and working relationships with security services, a national CyberCrime Unit takes responsibility for the response to significant national incidents and manages the most dangerous individuals and groups. It can also assess and monitor the country's overall threat assessment and can produce intelligence products to assist and guide other sections of the network.

"Ask yourself whether you are intending to do a full national, regional and local capability uplift, or adding to existing structures to improve on previously established capabilities. Whichever way you are intending to go, the following descriptions should help shape the next stages of your development."

Regional

These capabilities are located across regional areas and may cover a number of jurisdictional districts or police force areas. Depending on the composition of the country's law enforcement landscape, regional CyberCrime Units could include seconded staff from a number of forces or agencies. Such units operate across geographical boundaries, helping provide a collaborated and flexible capability, able to respond to significant incidents and support the national CyberCrime Unit where required.

Regional structures can also provide coordination of police forces or agencies in their area, ensuring a common approach to threats and making most efficient use of specialist assets. This could also involve providing collaborated capabilities where that is the most efficient way of providing a service. For example, one regional Digital Forensics laboratory, or regional governance and control over all CCU assets in the area.

Local

These capabilities normally sit within a local police force or agency, covering a specific geographical location. Providing a local response to issues effecting individuals, communities and local businesses, these CyberCrime Units have a more directed approach, responding to calls for assistance and working with local government or municipal structures.

Local CyberCrime Units provide support to local policing departments, helping them respond to incidents that may not fall to the specialist teams, but still contain an element of technology or investigation that could require CyberCrime Unit support.

The overall response to technology and a general understanding of cyber issues is an important factor for all law enforcement staff. A responsibility to 'mainstream' knowledge around cybercrime to the rest of the organisation is a good idea.

Our recommendation is that however you decide to approach this, overall, it should be seen as a network. Each CyberCrime Unit, police force and agency has formally agreed to operate together against any cyber threats. This does not necessarily mean forging just a singular body with overall responsibility for everything cyber related. It can include a number of forces or agencies taking responsibility for their own respective parts of the structure, while having working practices and agreements to share and collaborate over common issues.

Single National Structure taking complete control of the threat

This involves creation of a single National Cybercrime Force or large CyberCrime Unit sitting within a national agency and taking complete control of national cyber threat response, as well as all the responsibilities at state and international level.

There are positive and negative aspects with any approach, as follows:

Positives	Negatives
✓ Able to see the threat across all levels	✗ Singular approach likely to cause gaps at some levels
✓ Easy to control the response and flex staff levels where needed	✗ Could be seen as an extension to government
✓ Easy to set and control national strategy and national policy	✗ Requires considerable resource and investment
✓ No conflict with competing agencies or police CCUs	✗ May need to create supporting infrastructure to cope with their demand
	✗ Large recruitment required to establish
	✗ Leaves other levels of law enforcement to cover cyber issues not in remit of national CCUs

7.2 Alternative Structures

National CyberCrime Unit and Regional-only teams

To give wider reach, this would not only introduce a CyberCrime Unit with national responsibility, but also include creation of several regional CyberCrime Units to complement the national CyberCrime Unit. The national team could be either part of a National Cybercrime Force or be created as part of existing national law enforcement structures.

Positives	Negatives
✓ Still allows national control as above	✗ Could be a compromise not addressing all gaps
✓ More reach, helping to bridge geographical locations	✗ May still leave local issues unresolved
✓ Joining up of services across regions	✗ Some agencies or forces may feel unsupported
✓ More efficient use of resources, allowing the setting up of a network of services	✗ Local police forces may not have sufficient support or skills to cope with their demand

Independent CyberCrime Units at different levels

In this scenario, each agency and police service is left to decide how to set up their own CyberCrime Units under some national guidance, but allowing independent governance with no formal cooperation between them.

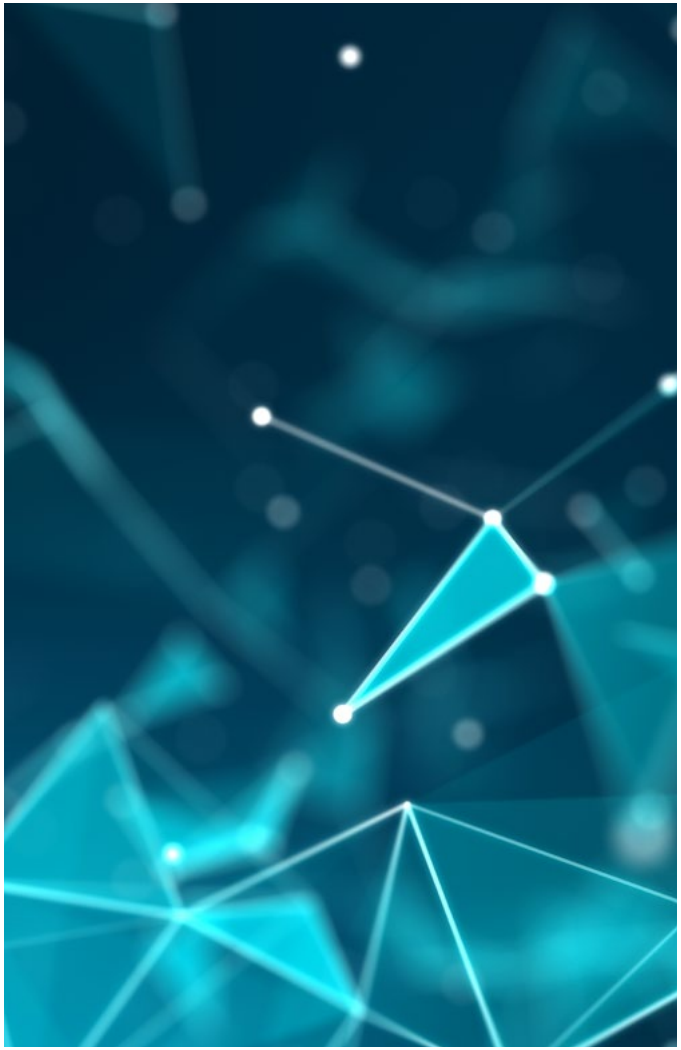
Positives	Negatives
✓ Does not require much central oversight	✗ Much less control over national strategy or policy
✓ Each agency or police force is able to decide their own response and set staffing levels	✗ Fractured response giving differing levels of capability
✓ Each agency or police force retains absolute control over their own assets	✗ Inconsistency in service delivery and variable outcomes
✓ No need to negotiate collaboration	✗ Likely to be higher cost overall as each agency has to set up their own complete set of capabilities and support structures
	✗ Inefficient as unable to see wider threats, or respond as a network to larger incidents
	✗ Unable to collaborate on common needs such as training or procurement of equipment
	✗ Considerable duplication of effort
	✗ Increased risk of agencies investigating the same incidents or suspects

7.2 Alternative Structures

Blended collaboration using various agencies to create national, regional, and local CyberCrime Units

Under national oversight and guidance and taking a collaborative approach, this scenario allows various agencies and police forces to set up CyberCrime Units at national, regional and local levels, with common aims and working as a network.

Positives	Negatives
✓ Collaborated approach to still provide national oversight, and support national strategy and policy	× Requires collaboration and agreement to operate as a network
✓ Each section of the network takes responsibility to support, develop and maintain their own CyberCrime Unit	× If your country has many levels of law enforcement, with a competitive culture, it may be difficult to introduce
✓ Whole system approach providing assets at all levels, allowing for flexing of response depending on the incident	× Depending on starting point, can take time to develop
✓ Greater sharing of intelligence and linking of crimes	× Some parts of the network may try to inappropriately exert authority, causing disquiet
✓ Greater consistency in service delivery and outcomes	
✓ Easier to share learning and development across force, agencies and regions	



7.0 Programme Development & Implementation Planning

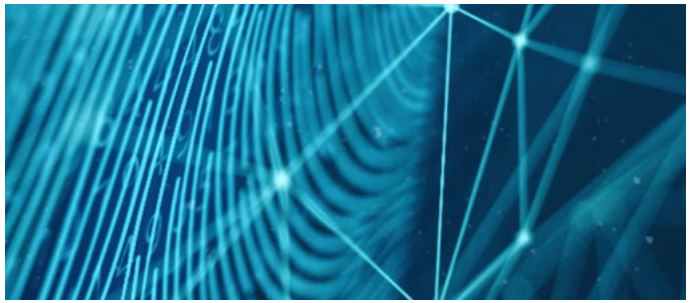
7.3 Approaching the Programme of Development

Once you are clear on the scale of your programme, you can make a decision on how significant that development will be and what support is required to undertake it.

It involves a large programme of work, overall control through a project team to oversee the implementation may be needed. All this development will require investment, with the initial outlay likely to be significant and careful management.

However, you must ascertain what the longer term and future legacy costs will be – and ensure these are permanently factored into relevant budgets to prevent a situation where the capability is left to fail as it is not adequately funded year on year.

Getting money and budgets agreed and set here will save you time and complications later on and will underpin the various stages of your development.



Key areas to think about include:

People

Agree and set your staffing numbers and ensure all costs are included. Hidden costs can sometimes be overlooked, such as regular overtime payments, or additional tax or employment costs. When thinking of future costs, you will need to factor in any likely rises in pay and effects of inflation.

Training

Once you understand your staffing profile, you will be able to establish your immediate and ongoing training needs. The training pathways you have previously set will guide this and help with future training decisions. One factor that can be missed here is staff turnover. New staff is likely to require training from scratch, so it is wise to see this as a regular cycle. Experience from other units would suggest a turnover rate of around 20% per year can be expected.

Equipment

As stated above, initial outlay on equipment will be considerable, and due to the specialist nature of the items required, some will be expensive. Taking time to agree and create a list of items required will assist in controlling equipment expenditure and prevent teams from purchasing unnecessary things. It is easy to see this as just an initial cost, but you will need to factor in regular ongoing costs. There will be a churn of equipment required to run these teams, including peripherals such as HDDs/SDDs, USB drives and various daily use items like cables, for example. It is also important to understand that equipment will have a ‘shelf life’ and need upgrading or replacing in future.

Tools/Software

To run various tactics, specialist tools and software are required. These are ever changing, so although you will have an idea of what your initial outlay may involve, you should keep some contingency to support regular review and refreshing of your tools and software.

Licencing

Once you have purchased your tools and software, it is likely they are supplied under some form of licencing agreement. Again, this is easy to overlook, and each year you will need to review and renew these. If you are deploying a tool or programme across a high number of staff/teams, renewal costs can be significant, and should be factored into future costs.

7.3 Approaching the Programme of Development

Transport

CyberCrime Units will need regular access to appropriate vehicles.

Premise searches are likely to involve taking mobile forensic equipment to locations, and removal and transport of often large amounts of seized equipment. So over and above general use cars, consideration of a larger van or similar vehicle may be necessary. You may also want to consider whether you want (or need) a 'mobile digital lab' capability. We have seen examples of bespoke vans with a Digital Forensics lab constructed in the rear. These can be used for 'at scene' work, and where it may be necessary to spend some time at a location. Such mobile Digital Forensics labs can be expensive, so may not suit everyone's needs. This is another area where collaboration could prove more cost effective, via introduction of a single shared resource for joint use by a number of teams or organisations.

Buildings

As covered in previous sections, CyberCrime Unit teams require secure, bespoke office space. Both physical and virtual security will need to be considered. Some construction or alteration to existing builds may be required. Upgrading of power supplies and the addition of uninterrupted or emergency power may well be required. Of course, the usual ongoing costs such as rent, power and water, for example, will need to be included. However, you should be mindful of the power requirements as these spaces are likely to consume more electricity than normal offices, especially if you are running servers and other digital equipment 24/7 (see below).

Infrastrcture

Digital infrastructure includes building an internal CyberCrime Unit network, servers, digital storage and security measures. You will also need strong, reliable internet connections that are not attributable to police or law enforcement, along with a mobile connection option such as a dongle or MiFi type device. If your preferred set up involves a number of teams spread across wide geographical locations, do you want to join them all up with a singular secure network so they can share tools, have common file and data storage and which could also include cloud options?

Travel and Accommodation

It is likely that your teams will have to regularly travel and stay in locations for a number of days while undertaking their duties. It is also likely that physical locations for the training courses will be some distance away. Add in regular CPD events and conferencing, and it is clear you must include these costs in budgets.

Professional Subscriptions

If you have decided to incorporate any form of professional qualifications, membership of industry groups, or subscription to relevant organisations or products, then these may carry annual or regular membership costs.

Research and Development

There is a need to keep tools, tactics and skill levels up to date and relevant, which requires some commitment to research and development. This will take additional investment and ongoing support but is necessary if you want to stay relevant and effective.

7.0 Programme Development & Implementation Planning

7.3 Approaching the Programme of Development

Timescales

Once you have agreed all your requirements as above, development can begin. As with any large project, you should set key milestones with realistic timescales. Depending on the scale of your build, you may want to break sections of it down and deliver certain capabilities at different times.

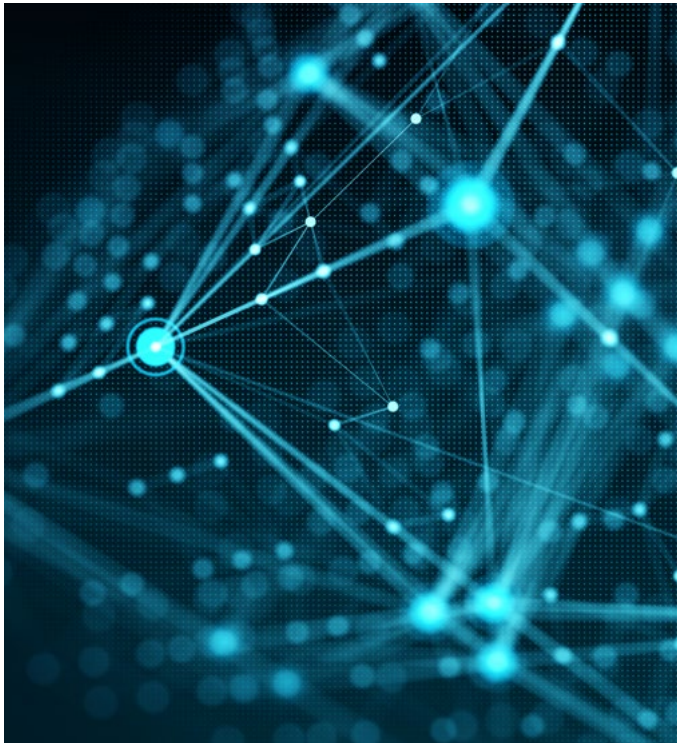
Of course, available funding and recruiting delays can have an impact. If these are factors restricting the scale or pace of your programme, look at ways of staggering the introduction of various elements.

For example, if your programme is introducing a full capability at national, regional and local levels, you may want to start with a national team first, then move on to the next stages a piece at a time as circumstances dictate.

You need to be realistic around the pace of the programme, as a lot of the elements can take time to achieve. Do not expect to run a three-month project and have a fully functioning CyberCrime Unit with trained and capable staff at the end of it!

See this as a rolling programme that will achieve results over a longer period, which you can continually review and amend as you go. Other countries that have undergone large capability build have spread the development over a number of years, and in reality, an initial time frame of six months to one year to get the first stages in place is not unusual.

Experience also tells us that from recruiting a person to getting them trained and experienced in this field can take a minimum of 12 to 18 months. Be realistic around the pace of development and manage others' expectations around the delivery timescales.



"See this as a rolling programme that will achieve results over a longer period, which you can continually review and amend as you go."

7.0 Programme Development & Implementation Planning

7.4 Benefit Realisation

In previous chapters we wrote about drafting strategic aims and linking your activity back into those aims. Here is now a good place to reflect on your plans to make sure your particular build is going to deliver on those requirements. Having a project plan that details what it is you will deliver and mapping those against the strategic aims and objects will help demonstrate success and show senior governance that you have done what you set out to achieve.

This can be presented in a document like a Benefits Realisation Report. Examples could include:

Benefit 1
Introduction of Cyber Crime Capabilities

Through a comprehensive development programme we have introduced structures and capabilities at national, regional and local levels that can address the issues of cybercrime through a 4P plan that will:

Pursue suspects involved in committing cybercrime,

Protect businesses and citizens from the impact of cybercrime,

Prepare business and citizens to respond effectively to cyber-attacks, and

Prevent individuals becoming involved in cybercrime, deter and divert those on the periphery of cybercrime, and degrade and disrupt those committed to cybercrime.

Benefit 2
Improved Level and Quality of Service to the Public

Through the assets and capabilities we have introduced, we can now offer a greater service to victims and members of the public, pursue offenders more effectively and deliver a comprehensive set of services to combat cybercrime. Dedicated staff are able to engage industry more efficiently and work more collaboratively with partners on joint initiatives.

Benefit 3
More Consistent Service Levels Across the Country

Taking a networked approach and ensuring joint training and exercises and cross discipline CPD events are undertaken, we have provided a consistent level of service across our country/region/state. This means that no matter where you live you will receive a high level of service from our teams, which in turn will raise confidence in our organisation.

Benefit 4
State/Region/Country is More Resilient to Cyber Threats

The introduction of specialist assets, training and tactics has contributed to making the State/Region/County more resilient to cyber threats. Businesses are better protected, the public can be confident in our ability to combat the threats, and overall, our society will be more prosperous and confident within the region and across the globe.

Tailoring tools like Key Performance Indicators provides a robust performance regime that can provide evidence of the delivery of these benefits, which can then be matured or amended as and when other demands arise, or operational focus needs to change. These will also act as a ‘temperature gauge’ against your development programme, providing an indication of how well the capabilities are functioning, and stage of development.

7.0 Programme Development & Implementation Planning

7.5 Final Thoughts

As we near the end of this guide there are a few final thoughts. As your teams go live, begin to deliver on the various strategies and gain experience in running cases, it could also be beneficial to introduce assistance guides.

These can include documents such as Standard Operating Procedures, Investigation Guides, Incident Response Guides and things like check lists to help staff gain confidence in responding to incidents, as well introducing consistency in how teams approach matters.

Basing content on best practice and 'what works' from incident debriefs and previous experiences, these can be living documents, constantly improving and maturing as the experience across the networks grows.

A few examples could include the following:

Victim Contact Check List: To ensure all relevant information is captured during initial contact and report. This ensures the most relevant information is captured, providing sufficient detail to make a reasonable assessment of what happened and how best to respond.

This approach will produce consistency in reports, ensure key information is not missed, and provide a chance to assess whether there are other investigative opportunities to explore or highlight other options to disrupt the criminals.

It is also a chance to provide victim support and direct them to places that can help them recover from the incident, as well as protect them from future attacks.

Organisations such as No More Ransom[23] and security providers like McAfee[24] offer advice and guidance on how to protect against some of the most common threats. If your particular country has developed a national strategy that includes authorised advice or guidance, then this can be referenced and used here.

Crime type specific guides can also be developed. Referring to your threat assessments, you will be able to identify issues that affect your country the most, and then tailor guides to fit these.

Guides could include Ransomware, Denial of Service attacks, Banking Malware, or Hacking/ Network Intrusion. Working through each methodically you can detail key staff required; list what evidence is likely to be present and requires preserving; provide information on how best to advise and support the victim, and assess extent of impact on them or their business. The guides could also include incident response plans and suggested Investigation strategies, laying out the operation's aims and objectives.

Standard Operating Procedures bring consistency and provide guidance to staff around how to approach an issue and what is expected from them. SOPs set out policy around how your organisation will tackle an issue. It is also useful to seek ways to spread this experience and help others develop.

Taking time to present at events – such as CPD training or conferences – on how incidents developed, how a team responded to them, what went well, what didn't go well, and any learning points will start to develop a supportive community all working together to help each grow and improve.

[23] https://www.nomoreransom.org/

[24] https://www.mcafee.com/

7.0 Programme Development & Implementation Planning

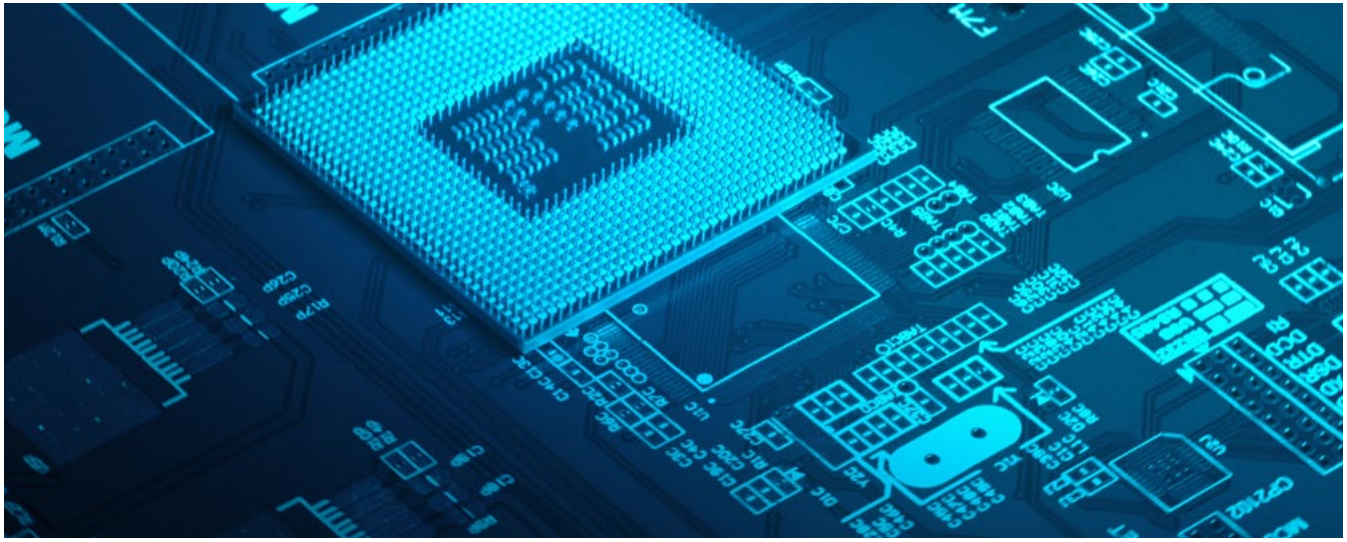
7.6 Capturing and Recording your Success

Over time this professional practice will develop and mature, and your cyber staff will become adept and expert in it. Recording and preserving this to add to your organisational memory is important.

Once you have reached a level of confidence that you have sufficient cybercrime policy and process in place, consider compiling a comprehensive document that captures all the details. The introduction of an overarching Cybercrime Investigation Manual can help with this process and provide a ‘go to’ document for both cybercrime teams and general staff.

Conclusion

Whatever your requirements or starting position, taking the steps outlined here should assist you with the introduction or further development of your Cybercrime Units. Wherever you are on this path, we wish you well with your development programmes.



What may work today may not work tomorrow, so continual review and reassessment is healthy. We advise horizon scanning and research and development is adopted to keep pace with technology. Relationships you have built with industry, academia and partners will help. All this puts you in a position where you can feel confident in the digital world.

We hope this guide helps you provide a safer and more resilient society where citizens can build more prosperous and secure lives for themselves, their families, and their communities.

You should see this as a continual journey. Cybercrime and technology are constantly evolving, as are tools and tactics used. There is a constant arms race going on between the security world and criminals.

Appendix

- Example Job & Role Profiles
  - *Cybercrime Unit – Manager*
  - *Cybercrime Unit – Supervisor*
  - *Cybercrime Unit – Investigator*
  - *Cybercrime Unit – Technical/Digital Forensics*
  - *Cybercrime Unit – Intelligence*
  - *Cybercrime Unit – Analyst*
  - *Cybercrime Unit – Protect & Prepare*
  - *Cybercrime Unit – Prevent Officer (Strategy)*
  - *Cybercrime Unit – Prevent Officer (Operational)*

EXAMPLE

Jane Briggs

Cybercrime Unit – Manager

Manage the Cybercrime Unit, where appropriate acting as Senior Investigating Officer, conducting reactive and proactive investigations and targeting suspects and organised groups that are committing cybercrimes. Manage and monitor the deployment of specialist capabilities and assets, ensuring ethical and most appropriate use of available resources. Lead on the development of partnerships with academia and industry.

Essential Criteria

- Experience of managing complex reactive and proactive investigations, demonstrating a sound awareness of intelligence and evidential gathering techniques
- The ability to communicate confidently at all levels including the ability to convey technical matters to a non-technical audience
- Experience of negotiating and influencing discussions, decisions and change with internal and external partners and organisations
- Able to develop and maintain effective partnerships and productive relationships with a range of internal and external units and organisations
- Able to develop and motivate a team to create strong performance against organisational and team objectives and strategic priorities
- Understanding of current technologies and display the ability to understand often complex technical issues

Core Responsibilities

- Manage reactive and proactive investigations and operations within cybercrime, acting as a Senior Investigating Officer for the most complex of cases
- Setting and/or approval of investigation strategies
- Setting and/or approval of appropriate digital forensic strategies
- Plan, manage and monitor operational activity, managing competing demands and priorities to make informed deployment decisions and ensure best use of available resources
- Set, monitor and assess key performance indicators in alignment with wider objectives
- Develop and maintain relationships with colleagues, communities and partners to drive collaboration across teams and organisations

Desirable Criteria

- Academic or Industry qualifications in cyber security, computer science or digital forensics
- An understanding and experience of surveillance and other covert tactics

EXAMPLE

John Briggs

Cybercrime Unit – Supervisor

Supervise staff conducting reactive and proactive investigations and operations against cybercrime, targeting suspects and emerging cyber threats. Develop and maintain partnerships with suitable business and industry sectors, promoting strategies to reduce the impact of cybercrime. Develop and support the staff in the CyberCrime Unit monitoring performance and making the most appropriate use of resources.

Essential Criteria

- Experience of supervising and running complex reactive and proactive investigations, demonstrating a sound awareness of intelligence and evidential gathering techniques
- The ability to communicate confidently at all levels including conveying technical matters to a non-technical audience
- Able to develop and motivate staff to contribute to performance against organisational and team objectives
- Understanding of current technologies and often complex technical issues

Core Responsibilities

- Supervise reactive and proactive investigations and operations within cybercrime
- Setting and/or approval of investigation strategies
- Setting and/or approval of appropriate digital forensic strategies
- Supervise operational activity, making informed deployment decisions and ensure best use of available resources
- Contribute to an enhanced threat picture, ensuring the gathering, development and dissemination of intelligence
- Develop partnerships with business, industry, education and third sector partners to promote cyber campaigns, increasing their resilience to cyber threats, and improving their cyber security
- Provide specialist technical advice and assistance, when required, to officers engaged in non-cyber investigations

Desirable Criteria

- Academic or Industry qualifications in cyber security, computer science or Digital Forensics
- An understanding and experience of surveillance and other covert tactics

EXAMPLE

Jane Briggs

Cybercrime Unit – Investigator

To undertake reactive and proactive investigations and operations against cybercrime, targeting suspects and emerging cyber threats. Act as case officer for investigations, using every available resource to bring offenders to justice, coordinating a number of capabilities and linking in with partners and relevant support networks. Offer cyber security advice to victims of cybercrime to reduce the risk of repeat victimisation.

Essential Criteria

- Proven recent experience of conducting complex reactive and proactive investigations, demonstrating a sound awareness of intelligence and evidential gathering techniques
- Demonstrate an ability to communicate confidently at all levels, including conveying technical matters to a non-technical audience
- Demonstrate the ability to work with limited supervision as part of a small team, being able to prioritise workloads
- Demonstrate an understanding of current technologies and ability to understand complex technical issues

Core Responsibilities

- Undertake proactive cybercrime investigations and operations
- Working with CyberCrime Unit Supervisors to set and implement investigation strategies
- Working with digital forensic specialists, set and monitor digital forensic strategies
- Organise and participate in planned operations, arresting suspects and conducting searches of premises
- Liaise with victims and witnesses to gather the best evidence when investigating offences, including technical and digital material
- Liaise with Prosecutors to present relevant cases
- Offer cyber security advice to victims of cyber-dependant crime to reduce the risk of repeat victimisation

Desirable Criteria

- Academic or Industry qualifications in cyber security, computer science or Digital Forensics
- Demonstrate a broad understanding and experience of surveillance and other covert tactics

EXAMPLE

John Briggs

Cybercrime Unit – Technical/Digital Forensics

Support the CyberCrime Unit investigations into cybercrime, agreeing and delivering Digital Forensics strategies, working with staff to provide technical knowledge and investigative skills in all aspects of Digital Forensics, network and technical investigations. Work with industry and partners to develop and maintain suitable capabilities and technical tools, as well as new methods and tactics to counter the latest threats.

Essential Criteria

- Good knowledge and expertise of common operating systems and applications
- Relevant qualifications in a computer-based discipline
- Demonstrate the ability to work with limited supervision as part of a small team, being able to prioritise workloads
- Demonstrate the ability to convey technical matters to a non-technical audience
- Identify opportunities to develop and improved the Digital Forensics capabilities and services provided

Core Responsibilities

- Support the CyberCrime Unit investigations by leading delivery of Digital Forensics and relevant technical capabilities
- Forensically secure and gather computer and digital-based material from both volatile and non-volatile environments using specialist tools and techniques
- Examine processed data in accordance with criteria set by investigators, and to produce relevant evidence in a form that can be readily understood and evaluated by others
- Where required attend scenes to secure, preserve and obtain digital evidence from victims, witnesses and suspects
- Undertake research for new investigation techniques, tools, software and technologies that will keep capabilities relevant and up-to-date

Desirable Criteria

- Support the CyberCrime Unit investigations by leading on the delivery of Digital Forensics and relevant technical capabilities
- Forensically secure and gather computer and digital-based material from both volatile and non-volatile environments using specialist tools and techniques
- Examine processed data in accordance with criteria set by investigators, and to produce relevant evidence in a form that can be readily understood and evaluated by others
- Where required attend scenes to secure, preserve and obtain digital evidence from victims, witnesses and suspects
- Undertake research for new investigation techniques, tools, software and technologies that will keep capabilities relevant and up to date

EXAMPLE

Jane Briggs

Cybercrime Unit – Intelligence

To develop and evaluate intelligence, making an assessment of the threat, risk, and harm from cybercrime, as well as assessing vulnerabilities and opportunities within the cyber and digital environment. Manage the production and circulation of relevant intelligence products, supporting reactive and proactive investigations and provide advice on appropriate digital tactical options.

Essential Criteria

- Experience of researching information from a variety of sources
- Experience of interrogating, maintaining and utilising data on a variety of computerised systems and operating systems
- Experience of preparing detailed reports and presenting information in a variety of formats
- Able to communicate with a range of partners to provide information and intelligence and ensure understanding of the current threat
- Able to break down a problem and determine appropriate action

Core Responsibilities

- Receive and assess information, and circulate to relevant parties ensuring intelligence is processed correctly
- Working to agreed strategies, gather, research and evaluate information to identify gaps and patterns, and inform briefing and tasking processes
- Develop and evaluate intelligence / information from open and closed sources and research various databases to enable the production of an accurate intelligence assessment
- Prepare and deliver intelligence products to inform decision making clearly and accurately, and provide advice on tactical options
- Use and evaluate specialist tools for intelligence collection and analysis
- Establish and maintain networks with relevant partners to assist with appropriate information sharing in support of shared objectives
- Maintain awareness of innovation within intelligence to ensure implementation of latest techniques and tactics, best practice, and information relevant to cybercrime

Desirable Criteria

- Experience of working in a previous intelligence role
- Experience of working with online or digital subject matter
- Experience in using specialised software tools and programmes to extract, analyse and report on activity
- Academic or industry qualification in a relevant discipline

EXAMPLE

John Briggs

Cybercrime Unit – Analyst

Support proactive and reactive investigation of cybercrime through implementation of data analytics methodologies and techniques, translating data into valuable insights that inform tactical and strategic decision making. Develop processes to combine numerous data feeds, including to visualise, transform, model and exploit multiple open and closed data sources. Work with the CyberCrime Unit investigators to inform and direct their investigations, show online connections, and expose real world connections.

Essential Criteria

- Experience of data collection or research skills in a statistical or information-based environment
- Experience of researching information from a variety of sources
- Experience of interrogating, maintaining and utilising data on a variety of computerised systems and operating systems
- Experience of working with large amounts of data
- Experience of preparing detailed reports and presenting information in a variety of formats
- An understanding of current technologies and ability to understand complex technical issues

Core Responsibilities

- Participate in operations and investigations, researching data, digital systems and providing information and reports from both open and closed sources, targeting offenders involved in cybercrime
- Working with the Intelligence staff, produce analytical products and reports about cybercrime activity, trends and patterns
- Identify and exploit numerous data sources, including large amounts of seized and downloaded digital data to establish patterns and links
- Support non-technical staff to understand their requirements, providing advice and guidance, helping to embed data analytic techniques in wider investigations

Desirable Criteria

- Experience of working in a previous analyst or intelligence role
- Experience of working with online or digital subject matter
- Experience in using specialised software tools and programmes to extract, analyse and report on relevant activity
- Academic or industry qualification in a relevant discipline

EXAMPLE

Jane Briggs

Cybercrime Unit – Protect & Prepare

Delivering cyber security advice to businesses and citizens. Offer cyber security advice to victims of cybercrime to reduce the risk of repeat victimisation. Deliver cyber resilience advice and exercising to businesses to enable them to better secure themselves against the threat from cybercrime, reduce the impact of incidents, and help them recover better if they become a victim.

Essential Criteria

- A knowledge of cybercrime threats and an interest in technology
- Demonstrate an ability to communicate confidently at all levels including the ability to convey technical matters to a non-technical audience
- Experience of delivering presentations or other means of promoting messaging
- Ability to engage and influence audiences in a variety of ways, including online, social media, and face to face
- Excellent verbal communication skills, the ability to adjust communication style to meet the needs of the audience
- Able to produce high quality and well-presented presentations and documentation

Core Responsibilities

- Identify and build partnerships with local business, industry, education and partners to promote cyber security, increasing their resilience to cyber threats, and improving their cyber security
- Provide cyber security advice to victims of cybercrime
- Develop and deliver cyber security exercising to public, private and voluntary organisations to help organisations to protect themselves increasing cyber resilience
- Develop and deliver cyber security events, raising awareness around cybercrime and cyber security to allow people and organisations to better defend themselves
- Engage with online and harder to reach communities promoting cyber security
- Work with industry partners and academia to better understand the threat from cybercrime, improve cyber security advice and develop protect and prepare strategies to keep pace with the evolving nature of cyber security

Desirable Criteria

- Academic or Industry qualifications in cyber security or computer science discipline
- Experience in delivering public events and meetings, maintaining professional relationships with a variety of partners
- Information security qualifications

EXAMPLE

John Briggs

Cybercrime Unit – Prevent Officer (Strategy)

The Prevent Officer's primary role is to work towards the Cyber Prevention aims and objectives within the National Cyber Security Strategy. They will work with primarily the Ministry of Justice, Ministry of Education and Ministry of Employment to develop mechanisms for progressing the Prevent agenda. They will establish the relevant Prevent working groups and identify the respective civil servants and representatives needed to attend. The Strategic Prevent Officer will work closely with their Operational Prevent counterpart to ensure they are continually aligned to the practical manifestation of Cyber Prevent and the Prevent Network.

They will be responsible for drafting Policy for Cyber Prevention, ensuring a template founded on good governance is established to enable clarity and focus of this developmental project.

One of their key roles is to forge and maintain relationships with representatives from the private sector. They will promote the benefits of primarily the Digital and Financial sectors engaging with the Prevent programme. They will also work with academia to identify the areas within Prevent that require further research and empirical evidence to help clarify the local difference of pathways into cybercrime, if any.

The Strategic Prevent Officer will be based within the national cybercrime structures. They will be expected to report directly to the Senior Police officer who holds the Cyber Prevent portfolio.

Essential Criteria

- Experience of working with government departments
- Extensive public speaking ability and experience
- Excellent report/policy writing and interpersonal skills
- Comprehensive understanding of Cybercrime and current threats
- Willingness to travel domestically and internationally to fulfil duties

Continued...

Cybercrime Unit – Prevent Officer (Strategy) continued...

Core Responsibilities

- Work with government representatives to assist with the departmental development of Cyber Prevention Strategy and Policy
- Forge relationships with representatives from the private sector to develop Cyber Prevent initiatives and interventions
- Develop innovative and targeted national campaigns that raise societal awareness of pathways into cybercrime and digital opportunities in the legitimate world
- Draft Law enforcement protocols, policies and procedures which ensure delivery against the objectives of the Police Cyber Prevent strategy
- Forge and maintain relationships with key stakeholders i.e., gaming, academia, tech industry and on/off-line media to progress Prevent
- Assist in the development and consolidation of an international Cyber Prevent Network
- Work with the Operational Prevent Officer to focus contributions to National Prevent policies and to develop Law Enforcement processes and protocols.

International Prevent Network: The Prevent Officer will act as the Single Point of Contact (SPOC) for Prevent Officers established around the globe. They will focus on building a network within the countries in their region without compromise to ferment relationships with Prevent Officers on other continents

Desirable Criteria

- Work with government representatives to assist with experience of working within the finance, gaming and/or digital industry
- Comprehensive understanding of cybercrime legislation
- Experience or understanding of neurodiversity
- Degree in Information Technology or similar subject, or Social Science (Criminology, Psychology etc)
- Understanding of cybercriminal career pathways
- Interest in gaming and related online forums

EXAMPLE

Jane Briggs

Cybercrime Unit – Prevent Officer (Operational)

The Prevent Officer's primary role is to work towards the Cyber Prevention aims and objectives within the National Cyber Security Strategy. They will raise public awareness of cybercrime in all its forms and identify opportunities for early intervention. They will identify vulnerable individuals at risk or involved in cybercrime. The officer, together with private and public sector partners, will be responsible for formulating strategies to amplify the impact of operations against the cybercrime fraternity.

The Prevent Officer will be based within the national cybercrime structures. They will be expected to identify operations in which Prevent intervention would amplify effectiveness by impacting on as many criminal actors as possible.

Essential Criteria

- Extensive public speaking ability and experience
- Excellent report writing and interpersonal skills
- Comprehensive understanding of cybercrime and current threats
- Comprehensive understanding of cybercrime legislation
- Willingness to travel domestically and internationally to fulfil duties

Continued...

Cybercrime Unit – Prevent Officer (Operational) continued...

Core Responsibilities

- Identify individuals subject to a Prevent or criminal justice intervention to debrief and inform cybercriminal career pathways
- Analyse intelligence and open-source information to identify and report on thematic trends
- Develop innovative and targeted campaigns that raise societal awareness of pathways into cybercrime and digital opportunities in the legitimate world
- Draft protocols, policies and procedures which ensure delivery against the objectives of the Cyber Prevent strategy
- Forge and maintain relationships with key stakeholders i.e., gaming, academia, tech industry and on/off-line media to progress Prevent
- Identify opportunities for Prevent interventions as part of all Cybercrime operations undertaken by the cybercrime unit
- Promote Prevent through publicity material and presentations to key target audiences and stakeholders
- Engage and upskill with established National Prevent Teams and Subject Matter Experts
- **Prevent Network:** The Prevent Officer will coordinate Single Points of Contact (SPOC) situated around Police Districts in-country, who will act as satellites for Prevent activities. This Prevent Network will comprise police officers who hold a Cyber Prevent portfolio that they manage alongside their normal duties.

Desirable Criteria

- Experience of managing offenders
- Experience or understanding of neurodiversity
- Degree in Information Technology or similar subject, or Social Science (Criminology, Psychology etc)
- Understanding of criminal career pathways
- Interest in gaming and related online forums