COMMONWEALTH PARLIAMENTARY ASSOCIATION

PARLIAMENTARY SECURITY:
AN INTRODUCTORY GUIDE

CPA COMMONWEALTH PARLIAMENTARY ASSOCIATION

About the CPA

The Commonwealth Parliamentary Association (CPA) connects, develops, promotes and supports parliamentarians and their staff to identify benchmarks of good governance and the implementation of the enduring values of the Commonwealth. The CPA collaborates with parliaments and other organisations, including the intergovernmental community, to achieve its statement of purpose. It brings parliamentarians and parliamentary staff together to exchange ideas among themselves and with experts in various fields, to identify benchmarks of good practices and new policy options they can adopt or adapt in the governance of their societies.

About the Author

Dr Paul Martin CBE is a security practitioner with more than 30 years' experience in the UK national security arena. He is a former Director of Security for the UK Parliament and a former head of the UK Centre for the Protection of National Infrastructure (CPNI, now NPSA). He is currently Professor of Practice in Coventry University's London-based Protective Security Lab, a Distinguished Fellow of the Royal United Services Institute (RUSI), a member of the UK Police Science Council, an independent adviser to various public- and private-sector organisations, and the author of books including The Rules of Security (2019) and Insider Risk and Personnel Security (2024).

Acknowledgements

The author is grateful to the following people for their expert advice: Matthew Francis, Alison Giles, Mark Harbord, Oliver Hoare, Rupert Jones, Robert Kennedy, Peter Mason, Adam Smyth and Becky Thomson and to the Head of Physical Security and Head of Personnel and People Security at NPSA. Thanks is also given to the security teams based in the Parliaments of Canada, Cayman Islands, New Zealand and New South Wales for reviewing the Guide and contributing to its development.

Parliamentary Security: An Introductory Guide was edited by Matthew Salik, Head of Programmes on behalf of the CPA.

CONTENTS

Have you used this publication?
If you have, let us know as we are always keen to hear how our products are being used.

Views and opinions expressed in this publication are the responsibility of the Commonwealth Parliamentary Association Headquarters Secretariat and should not be attributed to any Parliament or Member of the Association.

Cover design and illustrations by Matthew Salik with elements from freepik.com and Shutterstock.

Foreword

Dear Colleagues,

As I am sure many of you are aware, the security of our Parliaments and Parliamentarians is a topic that I am absolutely passionate about. For we are not just talking about protecting individuals, data and IT, and securing buildings, but we are defending democracy itself, and there cannot be a more vital priority, or a more important time to do it.

We are confronted by an ever-evolving set of threat actors: terrorists, extremists, criminals and state actors, all using increasingly sophisticated methods to try and defeat our defences. The challenge can feel overwhelming, particularly when you have, like us, suffered a terrorist attack or if one of your friends and colleagues has been assassinated. This is why it is essential that we work together, and share our knowledge, experiences and best practice.

It is with great pleasure then, that I write the foreword to this excellent Guide. It is designed to be of use to anyone responsible for, or who is a stakeholder in the security of their parliament, providing a framework for thinking through the different angles of security. I hope it will be particularly useful for those of you who don't yet have a formal security function, or are reviewing what you do have in place. The Guide won't give you all the answers, but I hope it will ask you the right questions, so that you are able to apply its principles to your own circumstances.

A final request from me, please let us have your feedback and thoughts: I hope this will be an opportunity for all of us to share and learn.

With warmest wishes,

Rt Hon. Sir Lindsay Hoyle MP, Speaker of the House of Commons, UK Parliament

Parliamentary buildings are often seen as the symbolic heart of democracy. Places where elected representatives come together to make laws and shape policy. It is therefore no surprise that such vital institutions can be viewed as tempting targets for attack. Today, across the world, governance institutions are under threat; whether that be cyber, physical or technical in nature.

With these risks in mind, the Commonwealth Parliamentary Association has developed, for the first time, a valuable and timely resource for our members and broader stakeholders. ***Parliamentary Security: An Introductory Guide*** *is intended as a resource to guide best-practice approaches around parliamentary security. Our motivation is to aid Parliaments to meet the highest standards in parliamentary management and governance, especially in the light of the updated CPA Benchmarks:*

> *30.12. The Legislature shall have risk strategies and implementation procedures in place around security, resilience, and continuity planning which shall include the provision of physical and digital security for the legislature's infrastructure, as well as for Members, parliamentary staff (regardless of location) and visitors to the legislative precinct.*

Updated CPA Benchmarks for Democratic Legislatures 2025

This publication is not intended as an all-encompassing, detailed manual on parliamentary security. Parliaments and parliamentary structures across the globe are too diverse to provide a one-size-fits-all approach. Instead, the Introductory Guide is designed to provide a strategic-level overview and identify key considerations and actions that can be taken to minimise the risk to Parliaments and peripheral entities.

The Introductory Guide also includes a ***Parliamentary Security Checklist*** *which provides an invaluable, practical aide-memoire, listing key security questions for those responsible for parliamentary security to consider and to act upon where appropriate.*

On behalf of the CPA, I extend my thanks to Paul Martin for his impressive work developing this Introductory Guide and his long-serving commitment to the field. I also give special thanks to the UK Parliament and particularly the Parliamentary Security Department for their support and commitment to this endeavour. I offer my appreciation to all the Parliaments and their security experts who offered valuable insight and guidance towards the development of this publication. It once again highlights the shared importance of this issue and the collaborative ethos at the heart of the CPA and the Commonwealth.

In conclusion, I wish to dedicate this publication to all those parliamentary colleagues and security personnel who devote their professional lives to keeping us safe, including those who have sadly died at the hands of extremists. I hope this Introductory Guide can contribute in a small way to ending such violence.

Stephen Twigg, CPA Secretary-General

Introduction

Protest outside of the Parliament of Victoria in 2021.

Parliaments and legislatures around the world face potentially serious risks to their security and well-being. These risks arise from a diverse array of threat actors, including violent protesters, hostile foreign states, terrorists, criminals, and fixated individuals.

Security is essential for enabling parliaments and legislatures to continue performing their vital democratic functions. Parliamentarians and the people who work with them must be protected from intimidation, both at their place of work and elsewhere. In doing so, however, an unusually delicate and difficult balance must be struck between managing the security risks and maintaining the openness of democratic institutions.

The purpose of this brief guide is to provide a non-technical introduction to protecting democratic institutions, including the people working in them and for them, and the people visiting them. Its target audience is officers and Members of Commonwealth Parliaments with an interest in, or responsibility for, protective security – in particular, Speakers, Members, Clerks, Serjeants at Arms, security officials, police officers, risk owners, policymakers, and other stakeholders.

The content is intended to be relevant to small and medium-sized institutions, not just those with large security departments. In such a short document it would be impossible to cover the full range of protective security measures in technical detail; the aim therefore is to present key principles and guidelines which should enable readers to decide which technical details are most relevant to their circumstances

1. Current Risks to Parliamentary Security

Damage left to the National Assembly of Kenya following the storming of the Assembly building in 2024.

The security risks faced by Parliaments, legislatures, elected representatives, and the officials who support them, differ greatly according to their evolving national and local circumstances, among other things. For some, the biggest security risks may stem from disruptive protesters and cyber criminals, whereas terrorism and hostile foreign states may pose the most concerning risks for others.

Security risks arise from the actions of ***threat actors*** – individuals, groups, or other entities who have both the intention and the capability to cause harm. The main categories of threat actors that are most relevant here, in varying combinations and to varying degrees, are:

- Violent protesters and rioters
- Hostile foreign states
- Criminals (conventional, serious and organised)
- Disruptive non-violent protestors
- Terrorists
- Insiders
- Lone hackers
- Fixated individuals
- Single-issue activists
- Ideological extremists

Threat actors differ enormously in their intentions and capabilities, which also change over time. Some protective security measures can mitigate risks that are common to several types of threat actors; for example, physical access controls and cyber security measures should provide a degree of protection against a range of risks. However, other security risks are specific to particular threat actors and require specially tailored defensive measures. For example, vehicle-blocking security barriers are designed to protect buildings or public spaces against terrorists attacking with vehicle-borne explosive devices or using vehicles as weapons, but they have little effect on other security risks.

Security risks may materialise in the physical world (e.g. an unauthorised intrusion by a protester or a terrorist bomb attack) or in the virtual domain (e.g. theft of data in a cyber attack) or a combination of the two (e.g. a terrorist attack facilitated by prior cyber reconnaissance of the target). The targets of attack may be institutions, individuals associated with those institutions, or democratic processes more generally. Different threat actors use widely different methods to attack or disrupt their targets. The table below contains some examples. The list is not exhaustive.

TYPE OF THREAT ACTOR	EXAMPLES OF COMMONLY USED OR RELEVANT METHODS
TERRORISTS	**Bladed and blunt-force weapons**
	Firearms
	Person-borne, vehicle-borne, postal, placed or under-vehicle explosive devices
	Vehicles used as weapons
	Fire as a weapon
	Drones
	Chemical and biological agents
HOSTILE FOREIGN STATES	**Insiders (spies)**
	Cyber espionage
	Cyber sabotage
	Disinformation and misinformation[1]
	Election interference[2]
	Technical eavedropping
	Physical sabotage
	Criminal proxies
	Poisons
SERIOUS AND ORGANISED CRIMINALS	**Cyber attack (e.g. ransomeware and extortion)**
	Insiders
	Social engineering
	Forced entry

[1] Disinformation is conventionally defined as false or misleading information that is deliberately created or spread with the intent to deceive or mislead, whereas misinformation is false, inaccurate, or misleading information that is spread regardless of any intent to deceive.

[2] For a description of how the Canadian government responds to this threat, see https://www.elections.ca/content.aspx?section=vot&dir=int&document=index&lang=e

TYPE OF THREAT ACTOR	EXAMPLES OF COMMONLY USED METHODS
FIXATED INDIVIDUALS	**Social media stalking and trolling**
	Bladed weapons
	Firearms
NON-VIOLENT PROTESTERS	**Unauthorised intrusion**
	Paint, banners
	Chains, padlocks, glue
	Noise
VIOLENT PROTESTERS AND RIOTERS	**Disinformation and misinformation**
	Fire as a weapon
	Rocks and other projectiles
	Forced entry
	Fireworks
	Firearms

Parliaments and parliamentarians around the world have been subject to attacks for centuries, dating back at least as far as the 1605 Gunpowder Plot to blow up the Westminster Parliament. More recent examples (most, but not all, from Commonwealth nations) are listed below. The list is not exhaustive.

AUSTRALIA	**1996**	Protesters forced their way into Parliament House, causing damage.
	2019	Cyber attack on the Australian national parliament, reportedly attributed to China.
	2024	Person charged with planning a terrorist attack after allegedly entering a New South Wales MP's office with 'intention to kill'.
	2024	Protesters arrested after climbing onto the roof of Parliament House in Canberra and unfurling banners.
BANGLADESH	**2024**	Protesters stormed the parliament building.
CANADA	**1966**	A lone attacker died inside the parliament building while preparing a bomb.
	1970	Quebec Provincial Minister Pierre Laporte was kidnapped and killed.
	1984	A lone shooter entered the National Assembly of Quebec and killed three people.
	2012	A shooter attempted to assassinate the Quebec Premier Pauline Marois.
	2014	A lone gunman ran inside the parliament building after killing a soldier on sentry duty nearby. He was shot dead inside the building.
	2022	'Freedom Convoy' protesters demonstrated at Parliament Hill.
	2024	Government agencies discovered Chinese cyber espionage activity against parliamentarians, starting in 2021.
FIJI	**2000**	Insurgents seized the parliament building and took the prime minister hostage.

GABON	**2016**	Protesters set fire to the National Assembly building.
GERMANY	**2015 & 2021**	Russian state hackers conducted cyber attacks against the federal parliament, stealing large amounts of data and compromising email accounts.
GUERNSEY	**2024**	A cyber attack disrupted the States of Guernsey IT network and Members' accounts.
INDIA	**2001**	Armed terrorists attacked the parliament in New Delhi, killing ten people.
KENYA	**2024**	Protesters set fire to the parliament building.
NEW ZEALAND	**2022**	Violent protesters and extremists occupied the grounds of the parliament, causing damage.
	2023	Russian hackers conducted cyber attacks against parliament.
PAPUA NEW GUINEA	**2018**	Protesters stormed the national parliament building, injuring staff and damaging property.
SOLOMON ISLANDS	**2021**	Rioters attempting to depose the prime minister set fire to a building in the parliamentary precinct.
SOUTH AFRICA	**2022**	A man set fire to a parliamentary building, causing significant damage.
SWITZERLAND	**2001**	A fixated individual entered the Canton of Zug parliament and shot dead 15 people, including himself.
	2023	Pro-Russian hackers conducted cyber attacks against government and parliament websites.
TRINIDAD & TOBAGO	**1990**	Radical Islamists seized the parliament building and took the prime minister and most of his cabinet hostage.
UNITED KINGDOM	**1974**	Irish Republican terrorists bombed the Houses of Parliament, injuring 11 people.
	1979	Irish Republican terrorists killed Member of Parliament and government minister Airey Neave with a bomb under his car, which detonated as he exited the House of Commons car park.
	1984	Irish Republican terrorists bombed a hotel hosting a Conservative Party conference, killing five people, including one Member of Parliament, injuring more than 30, and narrowly missing the Prime Minister.
	1990	Irish Republican terrorists killed Member of Parliament Ian Gow with a bomb placed under his car at his home.
	2000	Member of Parliament Nigel Jones was attacked and severely injured in his constituency office by a fixated individual wielding a samurai sword. His colleague, a local councillor, was killed.
	2004	Protesters threw condoms full of purple powder onto the Prime Minister as he was speaking in the House of Commons.
	2004	Protesters invaded the House of Commons chamber during a debate, reportedly with inside help from a passholder.
	2010	Member of Parliament Stephen Timms was stabbed and severely injured by a lone Islamist extremist at his constituency surgery.
	2016	A lone right-wing extremist fatally stabbed and shot Member of Parliament Jo Cox in her constituency.
	2017	A sustained cyber attack on parliamentary email accounts was attributed to Iran.
	2017	A lone terrorist drove his car into pedestrians on Westminster Bridge, killing or injuring more than 50, before running into the grounds of the Houses of Parliament and fatally stabbing a police officer.
	2018	A man drove his car into cyclists and pedestrians in Parliament Square, injuring several, before crashing it at speed into vehicle security barriers outside the Houses of Parliament.
	2021	Member of Parliament Sir David Amess was stabbed to death in his constituency office by a lone Islamist terrorist.
	2024	A parliamentary researcher was charged with spying for China.
USA	**1971**	Far-left extremists detonated a bomb in the US Capitol, causing extensive damage.
	1998	A man entered the US Capitol and shot dead two police officers.
	2021	A crowd of violent rioters invaded the US Capitol, resulting in the deaths of a rioter and a police officer.

Scenes from the 6 January attack on the US Capitol Building in 2021.

Key points:

- Parliaments are subject to a wide range of security risks arising from a diverse array of threat actors including violent protesters, hostile foreign states, and terrorists.

- Attacks may be physical or virtual, and the targets may be institutions, premises, individuals, or information.

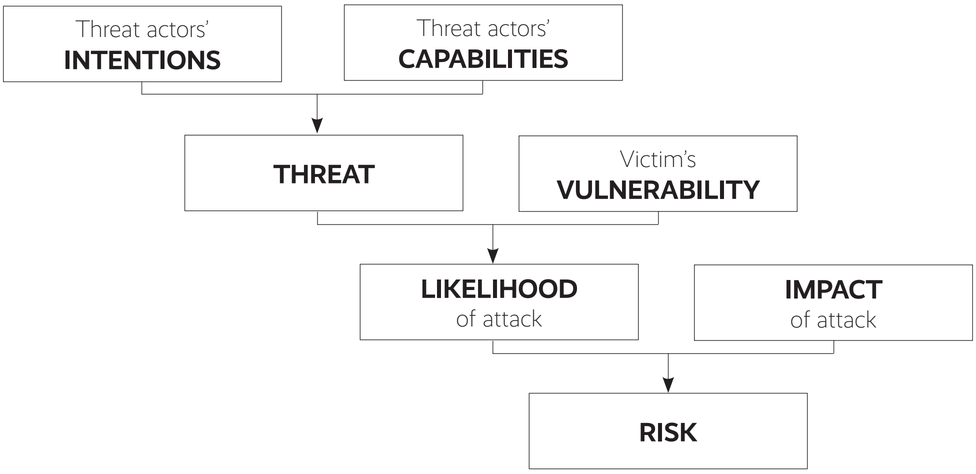
- Protective security should be designed to deal with the particular risks faced by the institution. These risks vary between institutions and change over time.

2. The Fundamentals of Protective Security

Protective security is the means of understanding and managing security risks arising from the actions of threat actors such as criminals, terrorists, hostile foreign states, and insiders. Good protective security reduces the risk of harm. It also helps to build trust and confidence, freeing people and organisations from the fear of harm and enabling them to go about their business.

Security risk is the amount of harm that is likely to arise if no further mitigating action is taken.[3] It is composed of three elements:

1. **Threat:** the capabilities and intentions of threat actors
2. **Vulnerability:** the gaps or weaknesses in the target's defences
3. **Impact:** the harm or consequences if the risk materialises



[3] Martin, P. (2019). The Rules of Security. (Oxford University Press).

The combination of threat and vulnerability is equivalent to the **likelihood** of the risk materialising – in other words, the probability of an attack or security incident taking place. The combination of likelihood and impact is equivalent to the risk – that is, the amount of harm (impact) that is likely to arise if no further action is taken to mitigate the risk. Thus:

Risk = Threat x Vulnerability x Impact
= Likelihood x Impact

The impact of a significant security breach or attack will have several disparate elements. For example, a major cyber attack might result in the loss of sensitive data, disruption to business, loss of stakeholder confidence, regulatory action, and reputational damage. A terrorist bombing might result in deaths, physical injuries, psychological injuries, damage to buildings and infrastructure, disruption to business, loss of public confidence, financial costs, societal fallout, and political turbulence. Impact cannot simply be reduced to a single metric like financial cost.

Given that risk is a product of threat, vulnerability, and impact, it follows that ultimately there are only **three ways to reduce security risk** – namely, by reducing the threat, reducing the vulnerability, or reducing the impact (or some combination thereof). Most conventional protective security measures, such as fences, alarms, guarding, and cyber firewalls, are designed mainly to reduce **vulnerability**.

Reducing the threat element of security risk is difficult, especially in the case of determined and capable threat actors like terrorists and hostile foreign states. Responsibility for reducing threats tends to lie mainly with national law enforcement, security, and intelligence agencies. That said, parliaments, legislatures and other organisations can contribute to threat reduction through deterrence – in other words, by influencing the intentions of threat actors. Carefully crafted **security-minded communications**[4] can convey a discouraging message to potential attackers, to the effect that they should expect to confront professional security measures and face a substantial risk of being caught. Security-minded communications can also create a perception that an attack will fail or not have the desired impact. For instance, a parliamentary website might advertise that visitors will undergo 'airport-style screening', without explaining precisely what that entails. The public should be reassured by such messages, whereas some threat actors might be deterred. More determined threat actors might still be deterred if they encounter a robust security regime which creates, for them, a hostile environment. Ultimately, parliaments and legislatures also have recourse to legislation as another means of influencing security threats.

EXAMPLES OF LEGISLATION PROTECTING PARLIAMENTARY PRECINCTS:

Australia
Parliamentary Precincts Act 1988: This legislation defines the boundaries of the parliamentary precincts and specifies that the management and control of these precincts are vested in the Presiding Officers of Parliament. It includes provisions about the role of security officers and gives police certain powers to ensure the security of the precincts.

Canada
Parliament of Canada Act (R.S.C., 1985, c. P-1): This Act outlines the administration of parliamentary precincts and gives the Speaker of each house responsibility for security within those areas. It also provides the legal framework for the jurisdiction of security services within Parliament.

South Africa
Powers, Privileges, and Immunities of Parliament and Provincial Legislatures Act, 2004: This Act outlines the powers, privileges, and immunities of Parliament and provincial legislatures, including provisions related to maintaining order within parliamentary precincts. It stipulates that security services, such as the police, may enter the parliamentary precincts to perform policing functions only with the permission and under the authority of the Speaker or the Chairperson.

National Key Points Act, 1980: While not specific to Parliament, this Act provides for the declaration and protection of sites of national strategic importance, which can include parliamentary buildings. It grants the government authority to implement security measures to safeguard such sites against sabotage.

[4] https://www.npsa.gov.uk/security-minded-communications-guidance

If security fails to deter or prevent an attack, the risk can still be mitigated to some extent by reducing the **impact**, or harm. A good way of achieving this is by responding rapidly to a developing incident and preventing further harm from being done. Other conventional means of reducing the immediate impact of an attack or security breach include secure backup of data and critical facilities, business continuity planning, physical and cyber incident detection and response, disaster recovery, and insurance (see Section 9 on resilience). Physical security measures such as vehicle security barriers and blast-resistant glazing may reduce the immediate impact of a physical attack. For example, the additional standoff distance created by vehicle security barriers (otherwise known as hostile vehicle mitigation, or HVM) can make a big difference to the blast damage from a vehicle bomb.

Other sorts of measures are needed to mitigate the **psychological, societal, and political impacts** of a major security incident. These measures are likely to include the provision of welfare support to victims, timely and accurate communication, and some form of investigation or inquiry to learn lessons and demonstrate accountability. Stakeholder confidence is likely to be further reduced if the accountable authorities do not demonstrably act on the lessons arising from a major incident. Regrettably, official promises to 'learn lessons' sometimes amount to little more than a process of merely *identifying* lessons.

Protective security measures should be designed to work in complementary combinations and achieve one or more of the following effects:

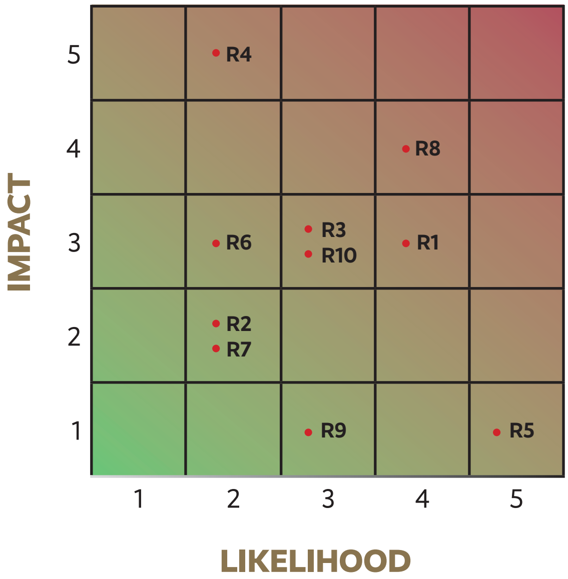
- **Deter** threat actors from targeting or attacking
- **Detect** attempts to target or attack
- **Delay** threat actors when mounting an attack
- **Disrupt** an attack
- **Detain** the attackers and bring them to justice
- **Mitigate** the impact of an attack

Security practitioners tend to divide themselves into professional **specialisms** – namely, physical, cyber, personnel, personal, and technical security. However, security *risks* do not divide neatly into these same categories. Security risks are usually **blended**, or hybrid. They require integrated responses that typically straddle two or more of the specialist domains. For instance, a well-placed insider can defeat most physical or cyber security measures, cyber-attacks can facilitate insider attacks, cyber security is required to protect networked physical security systems from hacking, and so on. Most cyber security breaches involve some form of intentional or unwitting human action within the target organisation.

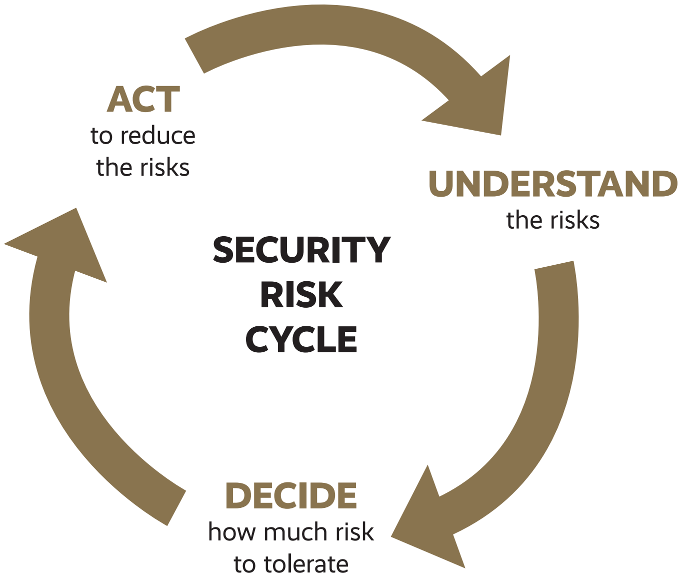
The blended nature of security risks means that protective security needs to be **holistic** (also known as integrated or convergent security). In other words, the physical, personnel, cyber, personal, and technical domains should be managed collectively as a coherent whole, and not as though they were independent of one another. In many organisations and businesses, however, the different security specialisms sit in separate organisational silos and do not converge. It is common for cyber security to sit within the IT or technology function, physical security within facilities management or building services, and personnel security within HR, with limited interplay between the different domains and no clear convergence at the senior leadership level. This is a recipe for sub-standard security. **Good governance** is vital. That means having, among other things, the right organisational structures, trustworthy communication, and collaborative relationships.

Security risks stem from the behaviour of intelligent human threat actors. Consequently, security risks are **dynamic and adaptive**, which means they change over time and adapt in response to the actions of defenders. In this sense, security risks are different from some other kinds of risk. In practical terms, it means that security practitioners are locked in a perpetual arms race with threat actors. Protective security must therefore continually adapt to the changing risks, as threat actors continually devise new ways of defeating existing defences. Protective security cannot afford to stand still. The pace of change is accelerating with the rapidly growing use of artificial intelligence (AI), both by attackers and defenders.

The standard way of comparing and communicating different security risks is with a simple **risk matrix**, in which each specific type of risk is plotted according to its likelihood and impact, as illustrated below (where R1 might be, say, the risk from a cyber-attack, R2 a disruptive protest, R3 a serious crime, R4 a terrorist attack, R5 an unauthorised intrusion, and so on). A particular type of risk, such as a terrorist attack, can encompass a wide range of potential scenarios that differ considerably in their impact. In recognition of this variability, it is conventional to represent each risk as the reasonable worst-case scenario – that is, the worst plausible manifestation of the risk, ignoring the most extreme but highly unlikely variations.



How are security risks managed? At its most basic, protective security involves a three-step cycle. The first step is to **understand** the risks the organisation or person is facing. Protective security should be shaped according to the particular risks it is likely to confront. The second step is to **decide** whether the current level of risk is tolerable. If it is not, then the third step is to **act** to reduce the risk to a tolerable level, provided that it is possible, affordable, and acceptable to do so. Security risks can rarely be eliminated, which means a degree of risk tolerance is unavoidable. Some organisations apply the principle of seeking to reduce safety and security risks to a level that is As Low As Reasonably Practicable, or ALARP. Security risks continually evolve, which means these steps must be repeated cyclically, as shown below.



Many organisations are inclined to focus mainly on action and fail to invest sufficient time in first understanding the risk. An organisation is unlikely to have optimal security defences if it does not understand the risks it is trying to manage. Organisations should continually learn from experience, especially incidents and near misses, so they can improve their understanding of the changing risks and adapt their defences accordingly.

A crucial first step in understanding security risks is to **identify the assets** that need protection. These are likely to include people, operational capabilities, buildings, digital systems, information, money, intellectual property, and reputations. Identifying assets is not always straightforward. It might be obvious, for example, that a business should protect its money, but perhaps less obvious that it must also protect the personal information of its customers and the infrastructure it relies on to function. A purist approach to identifying assets can be immensely time-consuming and inclined to focus on enumerating material assets like buildings and IT infrastructure, whereas parliaments and legislatures may place more weight on intangible assets like reputation and (crucially) their ability to continue functioning as democratic institutions.

Risk registers (see illustration below) are commonly used to catalogue the various risks facing an organisation and the actions it is taking to mitigate them. In practice, risk registers have an unfortunate tendency to fossilise – that is, the list of risks remains static even though the actual risks are changing, while attention is focused on actions and risk scores. The risk register consequently becomes increasingly detached from reality, representing risks that people worried about in the past rather than those they should be worrying about now. Another common problem with risk registers is their tendency to accumulate an excessive number of ill-defined and overlapping risks, resulting in confusion and loss of perspective. As with most things in protective security, it is best to keep things clear and concise.

Most organisations, including parliaments and legislatures, rely on a complicated network of suppliers, contractors, and other third parties. For example, security guarding, IT, or cleaning services might be outsourced to third-party suppliers, all of whom require access to perform their roles. Consequently, a significant proportion of security risk will sit in the supply chain, where the organisation may have less visibility of the risk and less ability to control it. A significant proportion of cyber security breaches involve a supplier or other third party.[5] **Supply chain risk** is inherently difficult to assess or manage, and therefore can be tempting to neglect. Organisations ignore it at their peril.

EXAMPLE OF A POSSIBLE BASIC RISK REGISTER[6]

Risk No.	Date Identified	Risk Category	Risk name and description	Impact description	Link to Strategic Aim	Impact Level	Likelihood level	Overall risk level/ score	Mitigations and controls
1.	*Date risk identified.*	*E.g. financial, reputational, legal. Can be more than one.*	*Name and brief summary of risk.*	*The possible outcomes if the risk is not mitigated or removed.*	*How does the risk relate to overall aims and strategy?*	*Rate from 1 to 5*	*Rate from 1 to 5*	*Impact x Likelihood*	*What can be done to lower the impact of the risk or eliminate it, where possible?*

[5] Verizon. 2024 Data Breach Investigations Report. www.verizon.com
[6] https://www.npsa.gov.uk/resources/tr-implementation-risk-register

Key points:

- Make sure you understand your security risks before rushing to mitigate them.
- Maintain awareness of current threats and vulnerabilities.
- Protective security should be holistic.
- Do not let your risk register fossilise.
- Pay attention to the security risks in your supply chain.

3. Personal Security

Personal security is the means of protecting individuals against risks to their own safety and security in their professional and private lives. It should not be confused with personnel security (see Section 5).

Parliaments are fundamentally about people, not buildings or IT systems, and the protection of people should be the centrepiece of any parliamentary security strategy. Sadly, Parliamentarians, officials, and other people in public life are facing a rising tide of abuse, intimidation, and violence. Parliamentarians are particularly vulnerable because their public-facing role requires them to be visible and accessible in both the physical and virtual domains.

The personal security risks to parliamentarians and other people in public life vary along a spectrum of severity, ranging from online abuse and trolling to physical intimidation, stalking, physical violence, and murder. The threats emanate from a disparate array of actors, including single-issue activists, fixated individuals, terrorists, hostile foreign states, violent protesters, and rioters (see Section 1). The psychological and physical impact on the individuals and their families can be severe. The cumulative impact can undermine the integrity of democratic processes, which is the intention of some hostile foreign state actors.

Threats to the personal security of people in public life tend to be systematically **under-reported**, creating an impression that the problem is not as serious as it truly is. Under-reporting occurs for various reasons, including the tendency of some experienced public figures to habituate to the persistent threats and regard them as somehow normal and part of the job. Another possible reason for under-reporting is a lack of confidence that anything will be done to alleviate the problem.

Historically, protective security has been predominantly about protecting organisations, infrastructure, and information, whereas personal security is about protecting individuals. The security risks arise from the work they do in the public interest and affect their private and family lives. Parliamentarians and others in public life may be most vulnerable when they are at home or travelling, rather than at their main place of work. Personal security therefore requires a different approach.

National governments may provide extensive security to senior government ministers and heads of state. In some cases, this includes close protection by specialist armed officers. However, armed close protection is expensive and limited in capacity, and only a small number of individuals receive it. Fortunately, other protective security measures are available that are more affordable and less intrusive. They can be effective when used in combination. The menu of options includes:

- **Open-source intelligence:** information from social media and other publicly available sources about possible threats to individuals.
- **Threat intelligence:** secret intelligence collected by intelligence or law enforcement agencies about covert threats to individuals.
- **Situational awareness training:** improving the ability of the potential victim to spot and avoid possible threats in their immediate environment.[7]
- **Dynamic risk assessment training:** improving the ability of the potential victim to read a potentially threatening situation – such as a physical confrontation with an aggressor – and decide how best to respond from moment to moment.
- **De-escalation training:** improving the ability of the potential victim to defuse a potentially threatening situation – for example, 'talking down' an aggressor who might be about to assault them.
- **Digital hygiene:** ensuring that personal information about the potential victim which could help threat actors to locate and target them – such as their home address, pattern of life, and current location – is not easily available online through social media and other sources.[8] As the world becomes more connected, the leakage of pattern-of-life data from smart infrastructure and vehicles is also a growing concern.
- **Travel advice:** equipping the potential victim with current advice about the particular security risks they might face, both when travelling and after arrival in other countries, and supporting them with robust planning.
- **Official transport:** enabling the potential victim to travel safely to and from higher-risk events.
- **Social media monitoring:** scanning the contents of social media platforms to detect possible threats to individuals and assessing the seriousness of any threatening messages they receive.
- **Portable devices:** equipping the potential victim with a suitably configured smartphone or specialist lone working device that enables them to summon emergency assistance.[9] Smart watches and modern vehicles have in-built facilities for summoning an emergency response.
- **Police liaison:** maintaining an official liaison relationship with local police to ensure they are aware of the at-risk person's circumstances, provide appropriate advice and support, and have contingency plans for responding to incidents.

No one measure by itself can provide robust protection. Some measures, such as open-source intelligence and social media monitoring, are not easy to operate effectively in practice and produce outputs that require careful interpretation.

Additional protective security measures may be applied to the **homes and constituency offices** of parliamentarians and officials. The menu of options includes:

- Neighbourhood Watch schemes
- High-grade door and window locks
- Security-minded workspace planning (e.g. positioning of desks in relation to entrances and escape routes)
- Defensive planting

[7] https://www.npsa.gov.uk/personal-situational-awareness
[8] https://www.npsa.gov.uk/security-campaigns/my-digital-footprint
[9] https://www.npsa.gov.uk/calling-help

- External lighting (triggered by infrared sensors)
- CCTV
- Intrusion detection systems
- Alarms
- Video entry phones
- External mailboxes
- Panic alarm buttons (PABs)
- Lockable garages
- Regular reviews and advice from protective security professionals
- Forcible-entry-resistant glazing and doors
- Perimeter fencing
- Guard dogs
- Under-vehicle explosive device detectors (if there is a significant threat from terrorists using this attack method)
- Ballistic-resistant glazing and doors (if there is a significant threat from shooting attack)
- Refuges ('safe rooms')
- Patrolling by police or private security personnel
- Hostile vehicle mitigation (if there is a significant threat from terrorists using vehicle-borne explosive devices or vehicles as weapons)

Technology can ease the problem of **scalability** – that is, protecting large numbers of people in ways that are affordable and acceptable. For example, AI-enabled open-source intelligence tools can help to uncover and triage security threats to individuals; intelligent internet-enabled CCTV can help to detect suspicious activity and hostile reconnaissance around the potential victim's home or office and provide remote early warning of possible threats; and standard smartphones can be easily configured as lone working devices. Digital tools like these must be adequately secured against hacking to prevent leakage of personal data and violation of privacy.

A common barrier to the provision of appropriate personal security is **poor governance** – that is, lack of clarity about who is accountable for the risk, who is responsible for doing something about it, and who has the authority and resources to act. One reason why public authorities do not always rush to own the problem of personal security is its daunting scale and potential cost. Another reason is risk aversion about potential legal liability in the event of something going wrong. While it may be true that giving specific security advice to an individual could in principle create a legal risk for the organisation, *not* helping someone at risk could also be legally and reputationally risky. Furthermore, whereas employers have a legal duty of care for the safety of their employees, the position may be less clear-cut in the case of elected representatives who do not have an employer as such.

Another potential problem is the difficulty of deciding which individuals should be given additional protection and precisely what sort of protection they should receive. Protective security measures can be expensive to install and maintain. Costs rise even further if private security or police personnel are deployed. Should everyone in a particular type of role be protected, or only those individuals who are known to have been threatened? Which security measures should then be applied? When is it proportionate, for example, to protect a person's home with perimeter fencing or bullet-resistant glass? Decisions like these should be based on an assessment of risk, as distinct from just threat. As noted in Section 2, security risk is a product of threat, vulnerability, and impact. People in public life may be at greater risk because they face a heightened threat from certain threat actors; they may also be more vulnerable because their work requires them to be accessible; and the impact of an attack may be greater because of its wider societal and political consequences. The most dangerous threat actors behave covertly, making it difficult to discover their specific intentions. The upshot is that specific and actionable intelligence about such threats is at best incomplete and may be completely absent. Therefore, judgements about the nature and scale of protective security should be based on risk rather than threat alone. Where specific threat intelligence *is* available, it should of course be heeded.

Personal security is more than just a technocratic problem with technocratic solutions. It depends on the perceptions and behaviour of those involved, including the potential victims and threat actors. Trustworthy and effective **communication**, based on sound behavioural science, is therefore a vital tool. When properly applied, it can improve the security behaviour of potential victims so that they actively contribute to their own protection. Communication and training should enable them to do the right things in situations of acute stress. It should also equip them with a balanced understanding of the risk, thereby helping to insulate them from the extremes of either reckless complacency or irrational fear. A person in public life may be less willing or able to perform their role without fear or favour if they are frightened about their safety or that of their family. Personal security should make individuals *feel* safer, as well as being objectively safer. Ultimately, there are two metrics of success: the risk is reduced to a tolerable level; and the protected person feels sufficiently confident about their security.

Key points:

- **Personal security measures should be based on an assessment of risk (not just threat).**
- **Poor governance may be a barrier to good personal security.**
- **Modern technology can provide solutions that are more scalable.**
- **Trustworthy and effective communication about the risks, and how they are managed, is vital.**

4. Physical Security

Physical security defences are intended to protect people, buildings, infrastructure, and information by helping to deter, detect, delay, disrupt, or detain threat actors, or mitigate the impact of their actions, by physical means – for example, by physically preventing threat actors from gaining access to assets, or by detecting unauthorised physical access to sensitive locations. The most commonly deployed tools of physical security, with their potential effects on threat actors, include the following:

MEASURE	EFFECTS
CCTV	Deter, Detect
Security lighting	Deter, Detect
Perimeter fencing	Deter, Detect (if alarmed), Delay, Disrupt
Armed or unarmed guarding and patrolling	Deter, Detect, Disrupt, Detain, Mitigate
Screening people, goods, and vehicles to detect concealed weapons, devices, explosives, or chemical agents	Deter, Detect, Detain
Physical access control systems	Deter, Detect, Disrupt
Intruder detection systems and alarms	Deter, Detect, Disrupt, Detain
High-security locks	Deter, Delay, Disrupt
Defensive planting	Deter, Delay
Anti-climb paint	Delay, Disrupt
Automatic number plate recognition (ANPR)	Deter (if overt), Detect, Detain
Automatic facial recognition	Deter (if overt), Detect, Detain
Hostile vehicle mitigation (HVM)	Deter, Delay, Disrupt, Mitigate
Forcible-entry-resistant doors and glazing	Delay, Disrupt, Mitigate

Blast-resistant glazing	Disrupt, Mitigate
Counter-UAS (Uncrewed Aerial Systems) measures	Deter (if overt), Detect, Disrupt
Gunshot detection systems	Detect
Security control rooms	Detect, Disrupt, Detain, Mitigate

The combination of measures that is right for a particular institution will depend on the nature and severity of the risks, the maturity of its security arrangements and security culture, and the inevitable practical constraints on affordability, feasibility, and acceptability. For example, hostile vehicle mitigation (HVM) barriers are expensive and may be unacceptable or physically impossible to install in some locations.

A basic physical security package for a sensitive site would typically include CCTV, perimeter fencing, guarding, visitor screening, access control, and intruder detection. Additional measures such as blast-resistant glazing and HVM might be applied if the risk of violent attack is judged to be significant. More complex and multi-layered physical security systems are of course more expensive to install and maintain and may be more difficult to manage.

Alarms, CCTV, and other security systems are normally monitored from a central **security control room**, which will often be operated by outsourced security staff or, possibly, police. The control room may also coordinate the immediate response to an incident, such as an alarm activation, unauthorised intrusion, or disruptive protest. Control room staff should have well-rehearsed plans for responding to serious incidents such as a violent protest or marauding terrorist attack; for example, by initiating a lockdown, issuing warning messages to occupants, and liaising with police and emergency services.

Physical security systems like CCTV and intruder alarms are typically connected to digital networks, making them potentially vulnerable to hacking and interference. They should therefore be protected with adequate levels of cyber security, both to maintain the integrity of the security and protect people's privacy.[10] CCTV and other surveillance technologies, such as automatic facial recognition, may be subject to legal constraints to protect the privacy of those being surveilled. Privacy legislation varies between jurisdictions. Physical security systems should also be protected by personnel security measures to prevent them being misused by insiders (see Section 5).

Uncrewed aerial systems (UAS), or drones, present a growing security risk, including for parliaments and legislatures. They may be fitted with cameras for intrusive surveillance or used as a weapon. The technology for countering UAS is developing but still far from perfect. Detecting the presence of a UAS in the airspace around a sensitive site is relatively straightforward, but neutralising one in flight is not, especially in an urban environment where falling debris could cause injuries. UAS can also be used defensively to patrol secure estates and assist in responding to emergencies.[11]

[10] https://www.npsa.gov.uk/cyber-assurance-physical-security-systems-capss
[11] https://www.npsa.gov.uk/uas-protective-security

In terms of the origins of UK parliamentary security in a physical security sense, the mace was historically carried by the monarch's bodyguards, the Serjeants at Arms. These weapons were the symbols of the crown's authority, as well as instruments to protect the crown and Parliament. To this day, across the Commonwealth, Serjeants at Arms, Marshalls of Parliament and Black Rods carry the mace for strictly ceremonial purposes.[12] (Image credit: UK Parliament Jessica Taylor)

Key points:

- **Physical security measures are designed to deter, detect, delay, disrupt, detain, or mitigate.**
- **The combination of physical security measures deployed at a site should depend on the risks.**
- **Physical security systems should be protected by cyber security and personnel security.**

[12] CPA Blogpost, Weapons of Mace Democracy, https://www.cpahq.org/knowledge-centre/blogs/blog-post-weapons-of-mace-democracy/

5. Personnel Security

Personnel security is the set of defensive measures by which an organisation protects itself against the security risks arising from the potentially harmful actions of insiders. It should not be confused with personal security (Section 3). An important caveat here is that democratically elected representatives are generally exempted from the personnel security 'vetting' processes that are normally applied to government officials and employees with access to sensitive assets.

Protective security is conventionally seen as defending organisations from harm originating in the world outside (i.e. from external threat actors). But serious security risks can also come from within. They stem from **insiders** – individuals who have been trusted with access to people, buildings, infrastructure, and information. An insider need not be a direct employee: suppliers, contractors, interns, partners, and other third parties who have been granted access are also potentially harmful insiders. So too are former employees, all of whom will retain knowledge of the organisation and some of whom may retain partial access.

Trust is the universal currency of insider risk and personnel security. An insider may be defined as **a person who betrays trust by behaving in potentially harmful ways**. They have been trusted by an organisation, which gave them access to its assets, but they abuse that trust by behaving badly and potentially causing harm, whether intentionally or unwittingly. The purpose of personnel security is to reduce insider risk and build trust, by ensuring that people who have been trusted with access are trustworthy and remain trustworthy. In an era of disinformation, deepfakes, and widespread public distrust of institutions, trustworthy people are even more valuable. Human behaviour lies at the heart of insider risk, making it arguably the most interesting of all security risks.

Active insiders have been found in every type and size of organisation, from small companies to multinational corporations, universities, government departments, and parliaments (see Section 1). Their actions might be limited to stealing information or money, but insiders can inflict harm in many other ways, including leaking, physical sabotage, violence, covert influencing and assisting external threat actors. Several political leaders and heads of state have been assassinated by trusted insiders; for example, Indian prime minister Indira Gandhi was killed by her own bodyguards and King Faisal of Saudi Arabia was shot dead by his nephew. At the time of writing, it remains a notable factoid that whereas hundreds of people have been murdered by insiders over the years, no one has (yet) been killed as a direct effect of a cyber attack, as far as we know.

Insiders have the potential to cause more harm than external threat actors because they already have legitimate access, know more about their target, and may have authority over others. With the exception of truly unwitting insiders, they also tend to behave covertly in order to avoid detection. The most capable insiders may remain undiscovered for years, and some may never be found. Potentially the most dangerous insiders are those working on behalf of a capable external threat actor, such as a hostile foreign intelligence agency or organised crime group, and who receive expert tuition in avoiding detection. The history of state espionage is littered with examples of hugely damaging spies who have operated in plain sight for decades within high-security organisations like intelligence services or government departments. The visible manifestations of insider risk are only the tip of an iceberg of unknown size. Consequently, the number of known insider cases is generally a bad metric of insider risk: what it really measures is not so much the size of the risk, as the organisation's ability to detect the risk. To put it another way, the absence of evidence of known insider cases is not evidence of absence of insider risk.

In common with other types of security risk, insider risk is dynamic and adaptive and therefore personnel security must also be dynamic and adaptive. This requires, among other things, agile mechanisms for discovering risks and genuinely learning lessons. The most efficient way of deploying limited resources may be to devote more attention to individuals who occupy so-called **high-risk positions** – that is, people in roles that give them the greatest legitimate access and therefore the greatest potential to cause harm, such as IT systems administrators and security personnel. It is worth bearing in mind, however, that even supposedly 'low-risk' positions may still provide potentially damaging access, and that determined insiders may acquire additional access extending well beyond what is legitimate for their role.

Insiders are sometimes portrayed as the few 'rotten apples' who lurk within an otherwise trustworthy workforce. However, the **rotten apple metaphor** is deeply misleading. It falsely implies that insider risk is an inherent property of the individual, ignoring the crucial influences of the workplace environment, home environment, opportunity, and other factors in the genesis of insider behaviour. A poor workplace culture or a toxic manager is often a significant contributor to the development of harmful insiders – hence the wise observation that rotten barrels make rotten apples. The rotten apple metaphor unhelpfully focuses attention on detection rather than prevention, while also encouraging a simplistic binary approach (*either* trusted worker *or* rotten apple) to a risk that varies along a spectrum. It is often exploited by marketeers selling technologies that purportedly identify the so-called rotten apples by automatically analysing their behaviour on digital networks.

The best way to manage any security risk is to stop it from materialising, rather than waiting for harm to occur and then dealing with the symptoms. **Prevention is better than cure**. The same is true for insider risk. Personnel security should be designed to detect the weak early signals of potential insider risk and stop it developing into full-blown insider behaviour. One way of doing this is through a welfare approach, in which the organisation seeks to help individuals resolve whatever personal problems might be nudging them onto a path towards harmful insider action. Most people are never going to become active insiders, and resorting to punitive action at the first sign of trouble is rarely the right answer.

As noted in Section 2, protective security should be managed holistically, with convergence between physical, cyber, and other specialist domains. Nonetheless, many organisations have organisational security structures that are far from holistic, with the personnel security function – if any – sitting apart from cyber and physical. Personnel security is also typically less well-resourced and commands less attention at leadership level. It is often the poor cousin of cyber security.

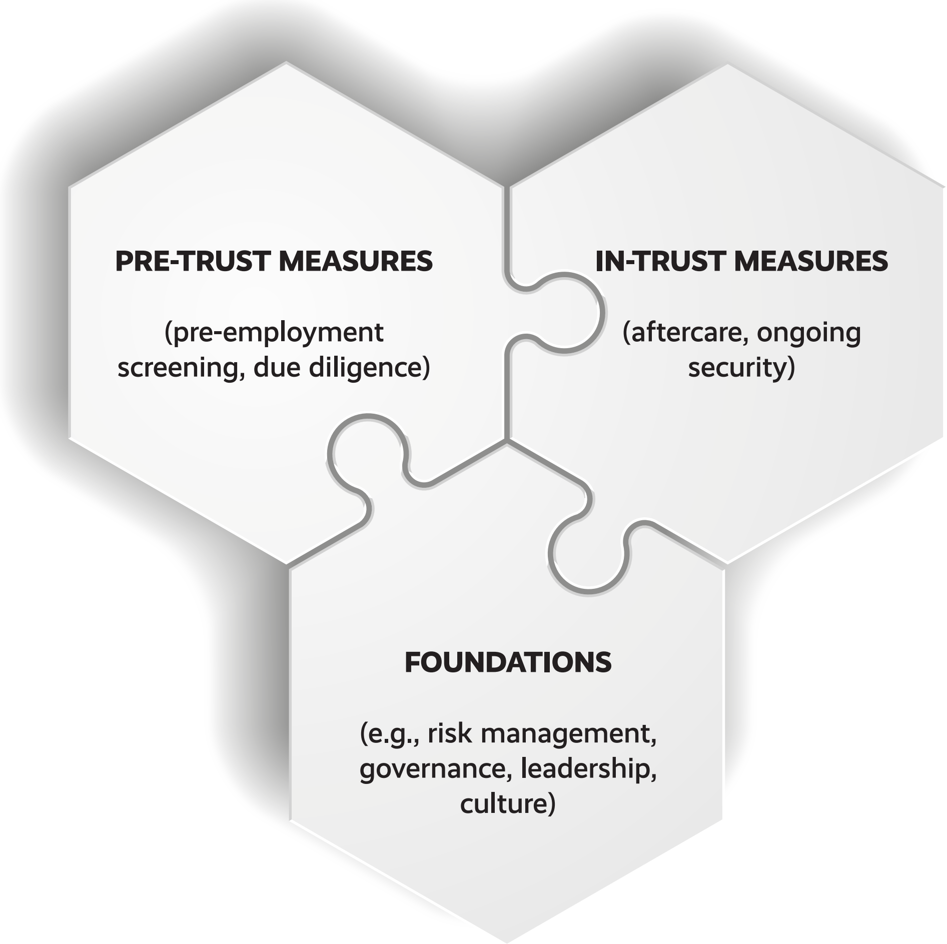
It can be tempting to believe that a single process or piece of technology, such as pre-employment screening or automated monitoring, can deal with insider risk. Tempting but wrong. Both in practice and in principle, no single process or technology by itself can ever provide robust protection against insider risk. Personnel security requires defence in depth from a system of complementary measures. The fundamental reason is that insider risk is a systems problem, and **systems problems require systems solutions**. There are no silver bullets.

The simplest model of a personnel security system[13] has three broad pillars:

Pre-trust measures (otherwise known as pre-employment screening, vetting, or due diligence) which are applied before deciding to trust an individual – for example, verifying identity, checking credentials, checking criminal records, checking national security records, and assessing trustworthiness by interviewing or psychometric testing.

In-trust measures (otherwise known as aftercare or ongoing security) which are applied after the individual has been trusted with access – for example, regular reviews of vetting status, internal physical and digital access controls, behavioural controls, automated monitoring of online behaviour, management oversight, investigation of leads, reporting and 'speak-up' channels, and exit procedures.

Foundations that underpin the pre- and in-trust measures, including good governance, ethical leadership, competent management, effective risk management, training and awareness, and a positive security culture.


PRE-TRUST MEASURES
(pre-employment screening, due diligence)
IN-TRUST MEASURES
(aftercare, ongoing security)
FOUNDATIONS
(e.g., risk management, governance, leadership, culture)

[13] Martin, P. (2024). Insider Risk and Personnel Security. (Routledge).

Many organisations rely too heavily on pre-trust measures, otherwise known as pre-employment screening or 'vetting'. However, the evidence from known cases clearly shows that a large majority of harmful insider cases develop *after* the individual has joined the organisation, often as a consequence of their experience of working there. It follows that pre-trust measures can only ever provide limited assurance. Personnel security will only work well if it also includes effective in-trust measures built on strong foundations. These should include trusted channels through which concerns and incidents can be reported.

In-trust measures that rely to a large extent on inter-personal interactions – notably management oversight and reporting of concerns by colleagues – may be more challenging to apply in **hybrid working** environments where people work mainly or wholly from home or remote locations. Remote working can make it harder for managers or colleagues to spot the early warning signs in a troubled individual if they rarely or never meet them in person. Nonetheless, traditional methods can be adapted to cope with remote working.

MENTAL HEALTH TOOLKIT FOR COMMONWEALTH PARLIAMENTS

In 2022, the CPA published its Mental Health Toolkit for Commonwealth Parliaments to guide, advise and educate parliaments on how to improve their response to mental health issues experienced by Members of Parliament and parliamentary staff. Depression, stress and anxiety can have a negative impact on staff mental health which can undermine personnel security. Download a copy here. https://www.cpahq.org/media/cczlingr/mentalhealth_toolkit_final_web.pdf

Key points:

- Insider risk is often neglected and poorly understood in comparison with cyber and physical security.
- Trust is the universal currency of insider risk and personnel security.
- Prevention is better than cure.
- A systems approach is required, involving a combination of pre-trust measures and in-trust measures supported by foundations including good governance.

6. Cyber Security

Cyber security is the means of protecting digital systems, the data on them, and the services they provide, from unauthorised access, harm, or misuse. In the current environment of ubiquitous digital technology, the terms cyber security and **information security** are often used interchangeably, although paper records still need to be protected.

Physical security measures such as access control systems, alarms, and CCTV, typically operate on digital networks, which means that cyber security is a crucial element of physical security.

The cyber security industry is huge and expanding, leaving its physical and personnel security cousins in the shadows. The global market in cyber security was valued at more than 170 billion dollars in 2023 and projected to reach more than 500 billion dollars a year by 2032.[14]

Cyber security risks can be divided into various categories. **Cyber espionage** and **cyber crime** involve attacks in which threat actors covertly and illicitly gain access to data over a digital network; for example, when foreign states or criminals steal sensitive data, intellectual property, or money from a victim's system. For instance, in 2015 and 2021 the German federal parliament was the victim of prolonged cyber attacks that were attributed to the Russian government (see Section 1). **Cyber sabotage** is the disruption of digital systems; for example, defacing a website or disabling a system by encrypting the data. A fourth category, which some call cyber subversion, is also relevant in this context. It refers to the misuse of the internet, social media, or other digital systems to distort or undermine democratic processes with disinformation and propaganda, tarnish the reputations of individuals and organisations, and sow division and mistrust.

[14] https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

The **malware** (malicious software) used in cyber attacks can be designed to cause a variety of harmful effects. These include stealing, deleting, or encrypting data; locking or preventing access to devices; taking control of devices and using them to attack other targets; stealing user credentials and using these to gain access to other systems or services; making money by accessing chargeable services (e.g. premium phone lines or pornography websites); hacking security systems for reconnaissance or as part of a coordinated attack; and mining cryptocurrency. Malware is readily available for sale on the dark web for anyone to use. It can be easily obtained through websites that provide malware-as-a-service in return for payment. You do not need to know much about computers to be a cyber criminal.

Artificial intelligence (AI) is increasingly being used by threat actors to identify vulnerabilities in software, generate disinformation, create new forms of malware, and conduct cyber attacks. Conversely, AI is also providing defenders with new tools for detecting and preventing cyber attacks. Some practitioners might argue that AI should become the sixth specialist domain of protective security, alongside physical, personnel, cyber, personal, and technical security.

Malware may be planted on a victim’s system by means of **phishing**. The unwitting recipient of a phishing email clicks on an innocent-looking attachment that contains malware. For more targeted attacks, hackers use phishing emails that are carefully tailored to look like the genuine article – a technique known as spear phishing. The practice of targeting high profile individuals, or those with greatest access, is sometimes referred to as whale phishing.

A well-constructed phishing email can deceive even the most vigilant recipients, including cyber security professionals. Phishing emails may be accompanied or preceded by scam texts or phone calls. They may direct the recipient to a website which looks genuine, but which covertly downloads malware onto the victim’s device or harvests their credentials. Some organisations unwittingly make it easier for the attackers by publishing seemingly innocuous information such as employees’ names, job titles, corporate email formats, internal phone numbers, and other details which can help threat actors to tailor their attacks and appear more plausible.

Another common attack method is known as **business email compromise (BEC)**, or pretexting, in which the attacker – often a criminal – uses apparently genuine emails to convince a well-intentioned recipient within the target organisation unwittingly to do something to the attacker’s benefit, such as transferring money to the attacker’s bank account. Phishing, BEC, and other types of social engineering attacks rely on exploiting human psychology, once again illustrating the importance of the human dimension in cyber security.

The prevalence of phishing and various forms of **social engineering** has fostered the dubious notion that ‘people are the weakest link’ in cyber security, even though a well-constructed phishing email can fool almost anyone. Everyone makes mistakes and it takes only one click to infect a network. An organisation cannot expect to prevent phishing attacks simply by instructing everyone not to click on suspicious links. Blaming people is sometimes an excuse for poor technology.

Cyber attacks are usually initiated remotely by gaining access to the victim’s system through methods like phishing or hacking. However, digital systems can also be attacked by **insiders** with authorised access, or by obtaining direct physical access to IT hardware. This underlines the importance of personnel security and physical security for cyber security – in particular, maintaining tight control over who has access to critical systems, hardware, and administration accounts.

Cyber sabotage is growing in prevalence. The classic form of cyber sabotage is the **denial of service (DoS)** attack, which involves trying to overwhelm a website with huge volumes of electronic requests. DoS attacks can be disruptive, although no one is likely to die because of a temporarily disabled public website.

Ransomware is a particularly harmful and widespread form of cyber sabotage malware, used mainly by criminals to obtain money.[15] Ransomware prevents users from accessing their digital systems or data. It does this by locking devices or by stealing or encrypting the data. The malware may also be designed to spread itself across networks, infecting other devices and machines. The anonymous attacker contacts the affected victim and offers to unlock the devices or data in return for a ransom payment in the form of a supposedly untraceable cryptocurrency like Bitcoin. The attacker may also threaten to publish the victim's sensitive data online unless they pay up. A 2024 report estimated that around a third of all cyber security breaches worldwide involved ransomware or some other extortion technique.[16]

Attackers often set the ransom at an amount they know the victim can afford, and the demand may seem bearable compared to the cost of losing critical services or data, prompting some victims to pay. However, ransomware attackers often fail to fulfil their promise to unlock the data. Indeed, some forms of ransomware are designed simply to delete data (so-called wiper malware). Moreover, experience shows that victims who pay a ransom are more likely to be attacked again. For these and other reasons, governments and law enforcement authorities generally advise against the payment of ransoms. The prevalence of ransomware attacks underlines the importance of maintaining secure backups of software and data and ensuring that systems are resilient (see Section 9).

An iconic example of cyber sabotage was the Stuxnet attack on the Iranian nuclear programme, which came to public attention in 2010. It employed sophisticated malware to subvert high-speed centrifuges which the Iranian authorities were using to refine uranium for nuclear weapons. The malware damaged the precision-engineered machines by altering the rate at which they spun. Stuxnet demonstrated how a cyber attack could be used to achieve physical effects that would previously have required military force. It also illustrates the human dimension of cyber security, as the attack depended on insider knowledge and, quite probably, insider action to install the malware. A further lesson from Stuxnet is that so-called 'air gapped' systems (i.e. systems that are supposedly isolated from the internet or other external networks) are still vulnerable to penetration.

The internet, social media, and other digital systems are being exploited by threat actors seeking to gain political, economic, or military advantage over adversaries by undermining their democratic and social systems, damaging the reputations of individuals and organisations, and fostering hatred and mistrust. With these ends in mind, hostile foreign states have attempted to influence democratic elections to their advantage – although whether these efforts have a decisive effect on electoral outcomes is a matter of debate. One well documented example was the Russian interference in the 2016 US presidential election. Russian hackers stole US Democratic Party emails and released them into the public domain, causing political fallout. More recently, in 2024, the US Department of Justice announced that it had disrupted Russian state disinformation operations intended, among other things, to influence the outcome of the 2024 US presidential election.[17] The US Attorney General pointed out that Russia was not the only foreign power trying to interfere in US elections.

A cruder but demonstrably effective approach is using **disinformation** to fuel social divisions and undermine belief in objective truth. Automated systems are used to generate fake news, hate speech, harassment, conspiracy theories, and other divisive information, which is transmitted in vast quantities through social media. Threat actors exploit the known existence of deepfakes and disinformation to encourage the public to doubt the authenticity of truthful information and distrust their politicians. An unfortunate side-effect of human psychology is that emotive lies spread much faster on social media, and reach much larger audiences, than the (often-unexciting) truth. When people no longer know what to believe, they lose trust, with damaging consequences for the integrity of society, including social unrest and violence. The World Economic Forum, in their 2024 report on global risks, assessed misinformation and disinformation to be the most severe risk currently facing the world – greater even than extreme weather events or interstate conflict.[18]

[15] https://www.ncsc.gov.uk/ransomware/home
[16] Verizon (2024). 2024 Data Breach Investigations Report. www.verizon.com
[17] https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence
[18] World Economic Forum. The Global Risks Report 2024. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

CPA PARLIAMENTARY HANDBOOK ON DISINFORMATION, AI AND SYNTHETIC MEDIA

COMMONWEALTH PARLIAMENTARY ASSOCIATION
PARLIAMENTARY HANDBOOK ON DISINFORMATION, AI AND SYNTHETIC MEDIA
Developed in partnership with
OAS
CPA COMMONWEALTH PARLIAMENTARY ASSOCIATION

In 2023, the CPA and OAS published the Parliamentary Handbook on Disinformation, AI and Synthetic Media. The Handbook contains effective strategies for combating disinformation and guidance on how parliamentarians can work with other stakeholders, including civil society, the media and technology companies, to develop effective policies and regulatory/legislative frameworks to address the challenges of disinformation. Download a copy here. https://www.cpahq.org/media/sphl0rft/handbook-on-disinformation-ai-and-synthetic-media.pdf

Russian hackers have generated vast amounts of false information and used fake accounts to pay for social media adverts dealing with divisive issues like immigration, race, and guns. Russian hackers have also interfered with political parties in France and Germany. The pernicious consequences of these and other abuses of social media have fuelled heated policy debates about whether and how to regulate the contents of social media platforms. The debates hinge on the tensions between combatting harmful dis- and misinformation and protecting freedom of expression.

How does cyber security work? A starting point, as noted in Section 2, is to identify the assets that need protection. When it comes to protecting digital data, this may not be straightforward, because it is common for multiple instances of an organisation's data to be scattered across different IT platforms and cloud services in ways that make it hard for systems administrators to catalogue comprehensively. It may be necessary to use specialised **data discovery** tools to locate an organisation's digital assets.

Some types of data are inherently more sensitive than others and require higher levels of protection. Obvious examples include certain types of personal, financial, and military data, and descriptions of an organisation's own security vulnerabilities and defences.

Most countries have legislation mandating the protection of personal data and privacy. Across the European Union, for example, the General Data Protection Regulation (GDPR), which came into effect in 2018, includes provisions to levy fines of up to 20 million euros or 4 per cent of an organisation's annual global turnover, whichever is the greater, for a serious breach of the regulations. GDPR provisions can apply extra-territorially to organisations that handle data belonging to EU citizens and residents, whether or not the organisations are based in the EU.

The broad aims of any cyber security strategy should be to achieve the following effects:
- **Protect** the organisation from attack
- **Detect** attempted attacks, including those that penetrate the defences
- **Respond** to any attack that has been detected
- **Prepare** to deal with the consequences of an attack

Most cyber security breaches are preventable; they are more a reflection of the victim's vulnerability than they are of the threat actor's capability. Basic cyber security precautions should prevent most (but not all) attacks from succeeding. The basic precautions that every organisation should take, regardless of its size or the perceived risk, are:
- **Updating and patching software** to strengthen security and plug known vulnerabilities.
- **Strong passwords** that are unique to each account. A strong password made from three randomly chosen words is easier to remember and use.[19]
- **Two-factor or multi-factor authentication** to ensure that only authorised users can gain access.
- **Correctly configured networks, devices, and cloud services** – for example, ensuring

[19] https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words

that the right security settings have been implemented on devices and configuring cloud services to provide end-to-end security.
- **Security awareness programmes** to improve the ability of users to recognise and respond correctly to potential cyber security issues.

Many organisations would also apply a range of other cyber security measures, including automated **network monitoring** to detect attempted or actual intrusions, and **data loss prevention** tools to block exfiltration (unauthorised removal) of data.

A crucial element of cyber security is controlling access to digital systems through technical measures like multi-factor authentication (MFA), which requires users to prove their credentials in at least two different ways. So-called **zero-trust** cyber security systems extend this principle by repeatedly requiring users and devices to re-authenticate their credentials as they access different services or parts of the network. This approach is analogous to a physical security regime in which people must use their security pass and associated PIN to gain physical access when moving around within a secure building or estate. In both cases, the aim is to make it harder for a threat actor to move freely and without challenge after they have passed through the external perimeter. However, this type of security by itself does not stop a trusted insider abusing their authorised access.

All but the smallest organisations should also consider seeking further assurance by:
- **Regularly testing** the effectiveness of their cyber security by employing a specialist provider to conduct penetration tests; and
- **Certification** against an appropriate cyber security standard (e.g. Cyber Essentials[20], Cyber Essentials Plus, or ISO/IEC 27001[21]). Certification by itself does not prove that the cyber security is fully effective, and at worst it can give false assurance; but it does at least constitute evidence that the key ingredients were in place at the time of certification.

The vast numbers of cyber threat actors, the ubiquity of vulnerabilities, and the often-substandard levels of cyber security mean that no organisation is immune from cyber risk. This reality is reflected in a catchphrase popular in the cyber security industry: 'It's not a matter of *if* you are breached, but when.' Or, as an unnamed head of cyber at MI5 once said: *'There are now three certainties in life – there's death, there's taxes, and there's a foreign intelligence service on your system.'*[22]

The near certainty of intrusion implies that organisations should invest in building **cyber resilience**. This can be achieved in various ways, including:
- **Data minimisation**: retaining only the data that is needed (including secure backups), because data cannot be lost or compromised if it is not held. When digital or paper-based information is no longer required it should be destroyed securely, so that it cannot be retrieved by an unauthorised person. Secure destruction means physically destroying digital storage devices and shredding papers. Simply pressing 'delete' or putting papers in a bin is not enough.
- **Secure backup** of files, software, and data to mitigate the consequences of an attack. Apply the **3-2-1 rule**: keep at least three copies (primary plus at least two backups); store the backup copies on at least two different devices (e.g. detachable hard drive and cloud); and keep at least one copy off-site. Ensure that backup devices are not permanently connected to the main platform.
- **Incident management**: well-practised procedures for responding to a cyber attack as soon as it is detected and then dealing with its consequences. Cyber security incidents may be managed from a cyber security operations centre (SOC), possibly run remotely by a supplier. Some organisations have contracts with specialist suppliers to provide expert support in responding to incidents.
- **Compartmentalising assets and systems**: dividing digital networks and data into separate compartments, or segments, such that an attacker who breaches one compartment does not immediately gain access to everything on the network; and maintaining tight controls over the management of access rights and systems administration.

[20] https://www.ncsc.gov.uk/cyberessentials/overview
[21] https://www.iso.org/standard/27001
[22] https://www.bbc.co.uk/news/uk-23098867

- **Encrypting data** so that it cannot be read without the key. Encryption protects data compromised by cyber attacks or by the accidental loss or theft of devices (which may be more likely). The effectiveness of encryption is sometimes undermined by procedural errors that enable threat actors to deduce the contents or get hold of the encryption key.
- **Anonymisation**: completely breaking the link between data and the identities of the people to whom it refers, such that losing the data would not compromise personal identities. True anonymisation is not easy to achieve, because it is often possible to deduce identities by cross-matching different types of anonymised data. Just deleting people's names is not enough. Data protection legislation like GDPR distinguishes between anonymisation and pseudonymisation, in which the data elements that could help to identify individuals are kept separate.

Parliaments and legislatures should consider seeking expert advice and technical support from their relevant national security agency, while of course respecting the constitutional boundaries between executive and legislature. A government agency with strong technical capabilities and access to secret intelligence might be able to warn of specific cyber threats and help to strengthen network defences against external attack.

Key points:

- **All organisations are subject to cyber attacks and should assume that some of those attacks will succeed.**
- **The human dimension is critical to cyber security.**
- **Given the inevitably of penetration, organisations should invest in building cyber resilience through measures such as testing and exercising, encryption, secure backup, and incident management.**

7. Technical Security

Technical security is the means of protecting organisations against electronic eavesdropping and other covert technical methods of espionage.[23] It is not the same as cyber security. Technical security, or 'sweeping for bugs', is generally most relevant to government agencies that handle highly classified information, embassies in countries where there is a high espionage threat, and organisations handling commercially sensitive information. However, parliaments and legislatures are vulnerable to technical attacks involving miniature cameras or microphones concealed in gifts or everyday objects.

Strong technical security, which may be referred to as **TSCM** (Technical Surveillance Counter Measures), involves systematically 'sweeping' a room or vehicle to detect any concealed eavesdropping devices, cameras, or other means of unauthorised technical surveillance. There is little point in painstakingly sweeping a room which is repeatedly used for sensitive conversations and then leaving the door unlocked for anyone to enter out of hours. To maintain its integrity, a swept room may be designated as a secure enclave, with strict access controls to ensure that only trusted and authorised people can enter. If the room has external windows, these may be covered in special anti-surveillance film to prevent technical eavesdropping from outside.

A more basic technical security measure is to instruct people to leave their phones and other electronic devices outside a room in which a sensitive discussion is to be held. It is always worth remembering that smartphones, smart watches, and other internet-enabled devices can be used as covert eavesdropping devices – with or without the knowledge of the owner.

[23] A more comprehensive definition of technical security, according to the UK Government, is: 'the practice of detecting the compromise of protective security systems, analysis and prevention of technical attack, mitigation of technology vulnerabilities and the deployment of countermeasures.' https://www.gov.uk/government/publications/government-functional-standard-govs-007-security

Key points:

- Meeting rooms and offices may be susceptible to surveillance from concealed miniature cameras or listening devices.
- If a room is technically swept to check for the presence of hidden bugging devices, it should subsequently be kept locked when not in use.
- Mitigating technical security risks must be balanced against the need to maintain the openness of parliamentary estates to the public and visitors.

8. How Good is Your Security?

PPS-SPP
PARLIAMENTARY PROTECTIVE SERVICE
SERVICE DE PROTECTION PARLEMENTAIRE
1305

A Parliamentary Protective Service patrol vehicle stationed outside of the Parliament of Canada.

Judgements about the adequacy and effectiveness of an organisation's protective security regime will depend on the nature and scale of the security risks it is facing. These risks will differ between organisations and change over time. Nonetheless, it is possible to assess security against a set of general design characteristics.[24] For a protective security regime to be maximally effective, it should be:

- Well governed
- Holistic
- Layered
- Risk-based and threat-informed
- Well implemented
- Understandable and understood
- Underpinned by strong relationships
- Supported by a positive security culture
- Professionally staffed
- Regularly tested

Well governed means being crystal clear about who is accountable for the security risks, who is responsible for understanding and managing those risks, and who has the authority and resources to take the necessary actions. For example, which senior leader is ultimately accountable for insider risk in the event of a serious security breach; who is responsible for ensuring that insider risk is properly understood and mitigated; and who has the authority and resources to make the day-to-day decisions and do the necessary personnel security work? Well governed also means setting clear expectations about security throughout the organisation and having leaders and organisational structures that promote rather than impede holistic security.

[24] For different but broadly complementary frameworks, see NPSA's Passport to Good Security: https://www.npsa.gov.uk/system/files/documents/npsa_passport_to_good_security.pdf and the New Zealand Government's Capability Maturity Model for Protective Security https://www.protectivesecurity.govt.nz/assets/protective-security-requirements/resources/psr-capability-maturity-model.pdf

In Parliaments and legislatures, political accountability for security would normally sit with a very senior elected representative – typically the Speaker or equivalent, possibly supported in this role by a commission or advisory board. Responsibility for managing and implementing security functions would be delegated to others, including officials, police, and private sector suppliers.

Holistic means that the various security specialisms (physical, cyber, personnel, personal, and technical) are managed collectively, so that they can be brought to bear on blended risks, rather than operating in separate silos as though they were independent of one another (see Section 2).

Layered means building defence in depth, rather than relying on a single line of defence, such that threat actors would have to penetrate two or more layers to succeed. Each layer of security provides an opportunity to detect the presence of threat actors, delay them, and respond before they have time to cause more harm. In physical security, for example, the outer layer would typically be a perimeter fence or vehicle barrier; in cyber security it would be perimeter firewall software; and in personnel security it would be pre-employment screening. Inner layers might comprise such things as internal physical and cyber access controls, internal CCTV, intruder detection systems, locked doors, protective monitoring of digital networks, and in-trust personnel security measures (see Section 5).

Risk-based and threat-informed means that judgements about the nature and scale of security measures are based on a solid understanding of the current and emerging security risks, taking account of the threats, vulnerabilities, and impacts. As noted in Section 2, capable threat actors typically act covertly, making it hard to discover their precise intentions. If threat intelligence is available, then the security should be modified accordingly. The key point here is that an absence of evidence of threat is not evidence of absence of risk.

Well implemented means having the capability to convert security policies and plans into functioning reality. There can be a tendency in some arenas for policymaking to be afforded a higher status than implementation, as though describing how to solve a problem were somehow tantamount to actually solving it. But there is little point in writing lengthy security policies unless they can be successfully implemented. Successful implementation requires, among other things, the ability to persuade stakeholders that the proposed security measures are necessary, proportionate, acceptable, and affordable. Stakeholders must be persuaded to stump up the money and put up with any inconvenience that may accompany the work. For larger-scale measures, implementation is likely to benefit from the judicious use of project and programme management (PPM) methodology. However, not everything in life is a formal programme, and the excessive use of over-complicated PPM processes is best avoided.

Understandable and understood means having security arrangements that are readily understandable, effectively communicated, and demonstrably understood by everyone. This is especially important during fast-moving incidents or crises. If a security regime becomes too complicated, there is a danger that people will fail to detect early warning signs, make poor decisions, or do the wrong things. Excessive complication can be especially problematic in cyber security and in technology-heavy security control rooms. The need for clarity and effective communication does not apply only to security professionals: the people who are being protected also need to understand what is required of them. Security is the responsibility of everyone in an organisation, from senior leaders to frontline staff. Setting clear expectations is crucial. Everyone, including officials and parliamentarians, should understand what is expected of them, both with regard to everyday security and in the event of a major incident. Understanding is also a prerequisite for a positive security culture in which people work together to create a safer and more secure environment (see below).

Underpinned by strong relationships means building and maintaining the personal and organisational relationships that are crucial for security in any organisation. Designing and operating an effective protective security regime will require cooperation between various internal functions such as security, IT, HR, and building services, with support and strategic direction from the leadership. Even large organisations with substantial in-house security departments will depend on external partners and suppliers, and smaller organisations may outsource most of their security functions. Having a strong relationship with the police is vital for Parliaments and legislatures.

Supported by a positive security culture means that everyone in the organisation has a sufficient understanding of the security risks, knows what is expected of them, and behaves accordingly. Security culture may be defined as an organisation's consistent tendency to behave in certain ways with regard to security, or 'the way we do security around here'. It is all about behaviour. A positive security culture is one in which people consistently do the right things, including reporting concerns and following the rules. The best type of security culture tends to be one in which people understand the risks, support the need for security, and actively want to do the right thing. This is sometimes referred to as a **concordance culture**. It compares favourably with the more traditional **compliance culture**, in which an auditing regime is used to enforce compliance with a set of prescriptive rules. Good security behaviour is more likely to be nurtured and sustained in a concordance culture.

Professionally staffed means having suitably qualified and experienced security personnel with the knowledge and confidence to challenge and intervene. Just having sufficient numbers of bodies on the payroll is not enough: those people will be unable to perform their roles effectively if they lack the necessary skills, experience, attitudes, and motivation. Organisations that wish to recruit and retain the right people, and maintain their motivation, should invest in their continuing professional development.

Regularly tested means conducting regular desktop and real-life tests of the security arrangements to verify that they actually work as intended. It often turns out that they do not. Regular testing also provides opportunities to practise making difficult decisions and performing procedures that might otherwise be rarely used. A third benefit is revealing ways of improving security, as tests often uncover imperfections. Some organisations make the mistake of relying solely on having written security policies and auditing for compliance with those policies. But written documentation is never enough; the only way to discover whether the security actually works (apart from waiting for a real attack) is to test it.

Particular elements of protective security can be assessed against recognised **standards**. Cyber security has many such standards to choose from, including Cyber Essentials and ISO/ IEC 27001 (see Section 6). Specific types of physical security equipment, like CCTV, locks, and barriers, can be assessed against detailed technical standards published by bodies such as the International Standards Organisation (ISO), the US National Institute of Standards and Technology (NIST), and the UK National Protective Security Authority (NPSA). However, there are very few recognised standards for personnel security. Arguably, the best (if not only) such standard is the NPSA's Personnel Security Maturity Model.[25]

The UK Parliamentary Security Department and NPSA have jointly developed a **parliamentary security checklist** to assess the security arrangements of parliaments and legislatures. The questions cover governance (e.g. 'Do you have a Senior Officer or equivalent accountable for security?'); physical security (e.g. 'Has your organisation implemented a risk management approach that enables a systematic evaluation of threats and risks?'); personnel security (e.g. 'Does your organisation perform pre-employment screening checks?'); incident management (e.g. 'Does your organisation have established processes for detecting, reporting, responding to and handling security incidents?'); and information security (e.g. 'Does your organisation understand how to protect sensitive data?'). The full checklist can be downloaded **here**.*

SAMPLE FROM THE CHECKLIST (SECTION ON GOVERNANCE)

Ref	Physical Questions	Guidance	Response	Comments *Use this column to provide context. If answer "No", "Partial" or "N/A", please expand where possible.*	Status
Organisation information					
G05	Are security roles and accountabilites clearly defined in the relevant governance and management framework?				Incomplete

[25] https://www.npsa.gov.uk/personnel-security-maturity-model
* https://www.cpahq.org/media/ahzl2y1l/parliamentary-security-checklist.xlsx

Key points:

- The adequacy of a protective security regime as a whole can be assessed by judging the extent to which it is well governed, holistic, layered, risk-based and threat-informed, well implemented, understandable and understood, underpinned by strong relationships, supported by a positive security culture, professionally staffed, and regularly tested.

- Aspects of cyber, physical, and personnel security can be assessed by comparing them against recognised standards.

9. Resilience

Even the best protective security cannot guarantee to prevent all security incidents or other disruptive events like fires or flooding. Bad things sometimes happen. Organisations should therefore invest in building resilience, which may be defined as **the ability to prepare for, absorb, respond to, and recover from disruptive events and adapt to new conditions**. Resilience is especially important for cyber security. Organisations may benefit from investing more in response and recovery, given the near inevitability of cyber breaches.

Resilient systems have built-in redundancy, fat supply chains, and an absence of single points of failure. These cost money and may create a trade-off between resilience and efficiency. Moreover, building resilience is about preparing for an uncertain future, whereas saving money and boosting efficiency bring immediate and tangible dividends. Add in the universal optimism bias of humans, and it is unsurprising that decision-makers often opt to avoid the cost of resilience and rely instead on hoping for the best. History shows this is usually a mistake. As the Covid-19 pandemic demonstrated, many nations and organisations discovered that they were less resilient than they thought and less resilient than they needed to be.

A useful distinction can be drawn between **passive resilience** and **active resilience**. Passive resilience is the ability to recover from a security incident or other disruptive event and return to normal functioning – in other words, to 'bounce back'. This is the traditional and narrow sense of resilience. The main building blocks of passive resilience include:

- **Rapid detection and response**: the ability to detect security incidents, attacks, or other disruptive events as soon as they start happening and respond quickly, before more harm is done.
- **Business continuity planning**: detailed prior planning and preparation to restore vital services quickly in the immediate aftermath of a disruptive event. Plans should be tested regularly.[26]

[26] The Legislative Assemblies Business Continuity Network (LABCoN) is relevant here. Its purpose is to share best practices for business continuity management (BCM) in a legislature. It does this through the documentation of benchmarks and the establishment of strong networks between participants from legislatures of different sizes from around the world. Members have produced a guide to BCM, which can be found at http://www.labcon.network

- **Incident management**: well-practised procedures for dealing with a wide variety of containable security incidents and disruptive events (e.g. a fire alarm or localised power failure).
- **Crisis management**: well-practised procedures for dealing with an acute and serious risk (e.g. a terrorist attack or major compromise of cyber security). Crisis management requires good governance, slick command and control arrangements, timely and effective communication, and teamwork based on strong relationships.
- **Secure backup** of data and IT services (see Section 6).
- **Disaster recovery**: fallback facilities for maintaining critical services if a major risk materialises and serious damage is done (e.g. following a terrorist attack, fire, or flood). For example, a vital building might have emergency generators, an alternative security control room, and off-site facilities where IT services and other business-critical functions can continue if the building is rendered unusable.
- **Sustainable staffing**: having sufficient people with the requisite capabilities, and deploying them in the right ways, to cope with demanding circumstances over a prolonged period.
- **Insurance** is one way of softening the financial impact of a major disruptive event.

If nothing else, an organisation should have a basic **emergency plan**, or protocol, for responding to the most likely types of disruptive events, including fire, flooding, bomb threat, violent incident, hazardous materials, loss of power or communications, and disruptive protest. The plan should be exercised periodically. Managing disruptive events can become more complicated if the organisation shares its physical or digital estate with one or more other organisations. Any ambiguity about who is responsible for making which sorts of decisions can be a huge problem in a fast-moving emergency.[27]

Active resilience, which includes passive resilience, is the ability to avoid disruptive events and grow progressively stronger by learning from adverse experiences and applying those lessons. Active resilience, or ‘bouncing forward’, is about avoiding crises where possible and coping better with the crises that cannot be avoided. To use an automotive metaphor, passive resilience may be likened to the crumple zone of a car, which protects its occupants in a crash, whereas active resilience provides the additional protection of advanced driving skills and crash-avoidance technology.

The key elements of active resilience include all of those required for passive resilience, plus well-developed capabilities to:

- learn from experience (your own and others’) and apply those lessons in practice;
- detect new and emerging security risks; and
- prepare for a wide range of foreseeable scenarios.

Active resilience is about thinking ahead and preparing to stay safe and secure in a changing risk environment.

Various techniques can help organisations to explore and prepare for possible future security risks. These include horizon scanning, wargaming, red teaming, modelling, computer simulation, scenario planning, exercising, and testing. It is impossible, both in principle and in practice, to make accurate and precise predictions about future security risks, but it is both possible and highly desirable to contemplate and prepare for a range of plausible potential futures.

If a serious security risk does materialise, and an organisation finds itself dealing with a crisis or a disaster, it will need help, both from within its own workforce and from external partners. Inter-personal and inter-organisational **relationships** are therefore a vital part of resilience. The best time to build such relationships is before a major risk materialises, not in the middle of a crisis. Resilient organisations invest in relationships

[27] Research by the Commonwealth Parliamentary Association in 2024 found that most, but not all, of the legislatures polled had an emergency protocol in place, and some legislatures shared a building with a non-parliamentary entity.

Key points:

- All organisations should invest in building resilience because even the best protective security cannot guarantee that a disruptive event will never happen.

- Passive resilience – the ability to bounce back – is necessary but not sufficient. Active resilience – the additional ability to prepare for and avoid crises – provides stronger protection.

- Active resilience should be developed by continually learning from experience, including applying the lessons from incidents and exercises, and learning from the experience of other organisations.

Further Reading

Australian Security Intelligence Organisation (ASIO). ***Protective Security Top 10***. https://www.asio.gov.au/protective-security-top-10

Australian Signals Directorate. ***Essential Eight***. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

Bereskin, C. (2023). ***Parliamentary Handbook on Disinformation, AI and Synthetic Media***. Commonwealth Parliamentary Association. www.cpahq.org

Campbell, G. K. (2015). ***Measuring and Communicating Security's Value.*** Elsevier.

Commonwealth Parliamentary Association (CPA). ***Parliamentary Security Checklist***. https://www.cpahq.org/media/ahzl2y1l/parliamentary-security-checklist.xlsx

Hoofnagle, C. J. and Richard, G. G. (2024). ***Cybersecurity in Context***. Wiley.

Martin, P. (2019). ***The Rules of Security***. Oxford University Press.

Martin, P. (2024). ***Insider Risk and Personnel Security***. Routledge.

New Zealand Government. ***Protective security requirements***. www.protectivesecurity.govt.nz

Sammons, J. & Cross, M. ***The Basics of Cyber Safety***. Syngress.

UK National Cyber Security Centre (NCSC). ***Authoritative advice on cyber security.*** www.ncsc.gov.uk

UK National Protective Security Authority (NPSA). ***Authoritative advice on physical and personnel security***. www.npsa.gov.uk

NOTES

NOTES

CPA COMMONWEALTH PARLIAMENTARY ASSOCIATION

Published by the Commonwealth Parliamentary Association (CPA).

CPA Headquarters Secretariat
Richmond House, Houses of Parliament
London SW1A 0AA
United Kingdom

Telephone: +44 (0)20 7799 1460
Email: hq.sec@cpahq.org
Website: www.cpahq.org