Check Point Software Technologies (Australia) Pty. Ltd.

submission to

# Joint Committee of Public Accounts and Audit

# Management and Integrity of Electronic Information in the Commonwealth

# Index

# Executive Summary

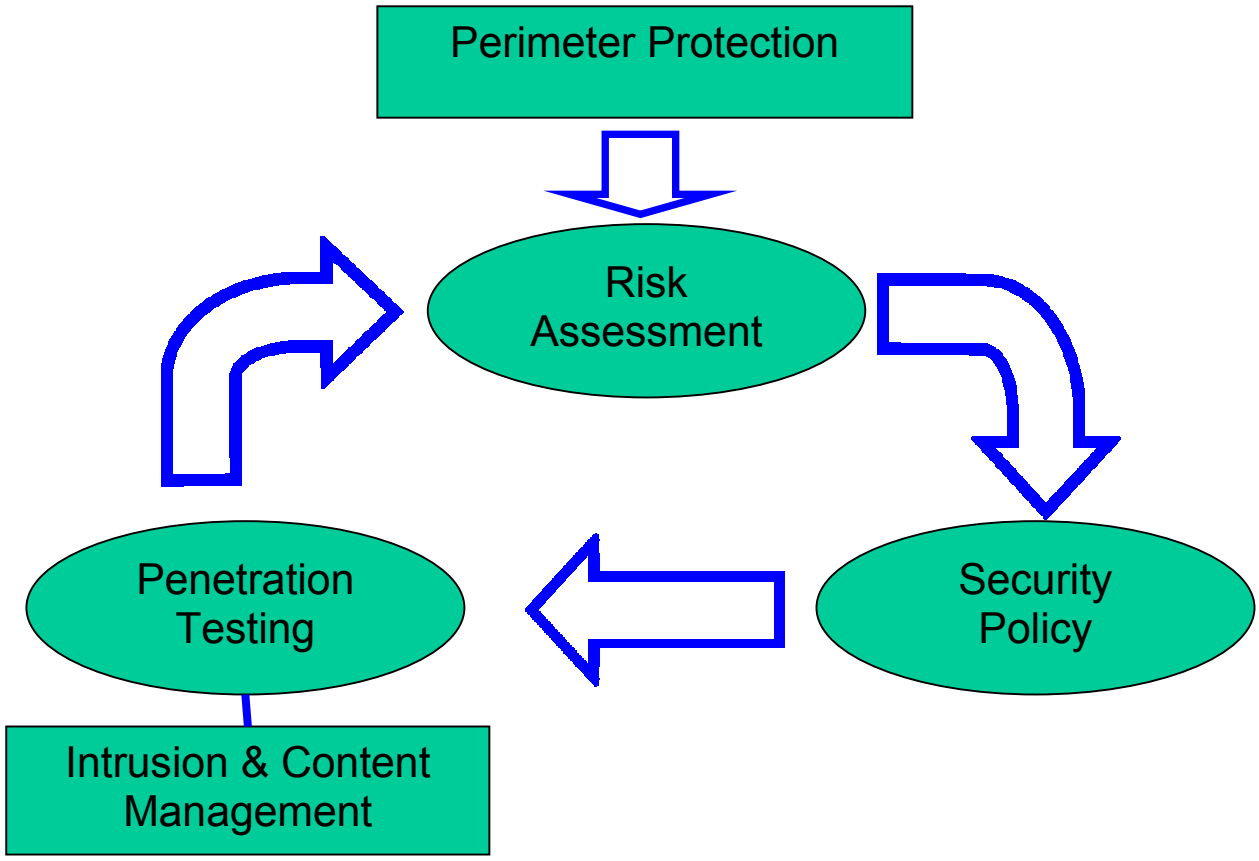
Check Point Software Technologies Limited is acknowledged as a global leader and an expert on information security. Drawing on that real life experience and expertise Check Point Software Technologies (Australia) Pty. Ltd. ('Check Point') has compiled this document to assist the Commonwealth in identifying potential security risks, and developing effective security measures – both corrective and preventative – to ensure the integrity of its electronic information – or as Check Point refers to it as 'information assets'.

To provide a detailed analysis of all the Commonwealth's electronic information would be impossible without a complete and thorough survey and study of each department, agency and private body that stores, transmits or receives any data. Therefore, in highlighting potential risks and suggesting effective security management measures, this submission focuses on **best practices** and **security strategies,** which the Commonwealth should recommend and adopt to ensure the integrity and adequate management of its electronic information.

Information assets are subject to a wide range of potential risks. The threats can be classified into six categories as follows:

- **Malicious Acts: 'Techno-Crime';** premeditated, planned, often with advance probing for weaknesses. As the Commonwealth Government is 'high profile', connected to the Internet, and has valuable information within its networks and systems this threat is very real - both from external persons (unknown) or from disgruntled employees.
- **Malicious Acts: 'Techno-Vandalism'**, opportunistic, random manipulation (theft, destruction, corruption) of data and / or systems. Again, the source may be external or internal.
- **Negligence:** Information Assets are placed at (unnecessary) risk because the organisation's personnel fail to exercise appropriate care and safety. This may be due to taking short cuts, inadequate training or not bothering to comply with procedures. The individuals are often unaware of the potential impact of their actions. Regardless, negligence is a genuine threat to organisations.
- **Human Error:** accidents are a major source of information security incidents. Unlike negligence, human error is normally a signal for additional training and / or review of procedures.
- **Systems Failure:** the sudden failure of a system can have a disastrous impact, not only upon that specific system, but also upon systems, which rely upon the failed system.
- **Environmental:** natural disasters are a serious threat; these include floods, lightning, heat, fire, earthquakes, tornadoes, etc. The only way to prepare for this threat is to ensure that a *Disaster Recovery Plan* and a *Business Continuity Plan* are both in place and tested.

The broad and ever-changing character of information, information technology (IT), information threats, and information/IT skills and users, determines that an effective security strategy **must be** an on going process not a one-off solution. The following diagram illustrates the perpetual process - of assessing, testing and implementing security measures - that is required to minimise risks and exposures effectively.




It might, on first inspection, seem odd to deploy security technology without first performing an assessment and planning a policy. But, without some type of perimeter protection in place your network is wide open, and a premature Risk Assessment would be misleading or redundant. Therefore, the very first step in the Security Life Cycle must be the installation of perimeter protection – in the form of a firewall . This will provide initial content for a Risk Assessment, and provide guidance in the development of the first security policy. It also has a valuable role to play in testing initial security measures.

The firewall implemented here needs to have the following characteristics (described in more detail in section 3 of this document):

- Form a closely integrated element of an overall open security platform (OPSEC certified)
- Easy to update and manage through an open management platform
- Software based
- Perform true Stateful Inspection of network traffic. (For more detailed description refer to section 3)

After the firewall is in place, a risk assessment study is required to understand the true risk to, and the value of, all your information,

The risk assessment process will identify the:

1. Nature and value of all your different information assets
2. Threats against those assets, both internal and external
3. Likelihood of those security incidents occurring
4. Impact upon the Government of such incidents.

The 'Key Information' Security Risk Analysis involves the following activities:

- Appoint a person to own security – e.g. a Chief Security Officer
- Prepare a list of the key information assets within the department/agency. Choose items which are the most important to the continued viability of the department/agencies
- Prepare a list of the **main** threats for each information asset identified above, together with a severity rating, potential frequency rating and probability rating
- Prepare a list of defences, both existing and required to protect against each threat
- Calculate a Risk Impact Rating for each information asset *(Initial Risk)*
- Determine priorities for identifying and implementing suitable defences, and prepare a Risk Management Strategy
- Prepare a revised Risk Impact Rating for affected information assets once the defences are implemented (*Residual Risk).*
- Regularly review the risk rating of each information asset.

A detailed explanation of a risk assessment process, which can be tailored to the needs of the Commonwealth, is outlined in the first section. Additional information on a suggested measurement model is also provided in Attachment 1.

Once the risk assessment has been carried out a set of security policies should be established to limit the risks identified. Every department/agency within the Commonwealth will share a standard set of foundation policies, but also have a set of policies supporting their individual departmental needs. These will define what are and are not accepted practices. An example policy and the recommended implementation strategy are explained in the section below entitled: “The management and security of electronic information transmitted by Commonwealth agencies.”

Once the policies are developed, and a written form of the policies are created and signed off, training should be conducted to all personnel where the Commonwealth should state its intentions from a security perspective. Because of the ever-changing environment, the Information Security Policy is a document that needs to be reviewed, and modified if necessary, on an annual basis, by every department, agency and private body within the Commonwealth.

To independently test the above, processed ‘penetration testing’ is needed to test how strong the security is - against attacks originating from both outside and inside the network. Without such a test, you may never find some of the real weaknesses in your security. Penetrating testing is usually performed as a zero-knowledge brute-force attempt to gain access into the information sources.

Typically, a hacker/cracker will gather information, in a process called profiling, about your operation before they try to launch an attack on your network. This exploratory activity is still detectable as an illegal intrusion – and can be detected in the same way as an actual security compromise, giving you the information needed to correct any outstanding weaknesses before an actual attempt at breaching your security is made.

Combined, penetration testing and intrusion detection are critical elements of security planning and management - providing an essential ‘real-world’ guide to improvements that should be made to policies and practices to minimise risk.

Among these practices is the implementation of a security technology solution. It is important that each of the components of the solution are not only best-in-class but have been independently proven to integrate seamlessly with the others, and with your overall IT infrastructure and management platform. Given the changeable nature of the electronic information environment, it is also important that your solution offers flexibility, scalability, upgradeability and manageability. These characteristics will optimise your security, while minimising ‘your total cost of ownership’ to protect your investment for the long term.

After making the changes suggested by these processes, a new risk assessment must be performed - and the cycle then starts again.

Following is a more detailed explanation of the processes and strategies explained above, with specific focus on the Terms of Reference document provided.

# Section 1 - The privacy, confidentiality and integrity of the Commonwealth's electronic data

A key goal of any security strategy is to protect the privacy/availability, confidentiality, and integrity of information and information assets. It is critical to understand here that *aspects* of information and information assets must be protected, not just the information or assets themselves. These fundamental principles are defined as follows:

- **Privacy / Availability** ensures the reliable and timely access to data or computing resources by the appropriate personnel or processes.
- **Confidentiality** attempts to prevent the intentional or unintentional unauthorised disclosure of information.
- **Integrity** ensures that unauthorised personnel or processes do not make modifications; authorised personnel or processes do not make unauthorised modifications to data; and data is internally and externally consistent.

These basic principles must cover all information, which could include data and information that is:

- Stored on databases
- Stored on computers
- Transmitted across internal and public networks
- Printed or hand written on paper, white boards etc.
- Sent by facsimile (fax), telex or other communications method
- Stored on removable media such as CD-ROMs, Zip DiskTM, hard disks, tapes and other similar media
- Stored on fixed media such as hard disks and disk sub-systems
- Held on film or microfiche
- Presented on slides, overhead projectors, using visual and audio media

As has been stated, there are a large number of departments, agencies and private bodies holding information: therefore it is impossible to give one broad-brush solution that will eradicate all risks to information stored electronically - and it is essential that all areas of the Government be treated on a case-by-case basis, hence the need for a risk assessment process that will identify the:

1. nature and value of the information assets
2. threats against those assets, both internal and external
3. likelihood of those security incidents occurring
4. impact upon the Government of such incidents.

**'Key Information' Risk Assessment**

The 'Key Information' Information Security Risk Analysis involves the following activities:

- Appoint person to own Security – e.g. Chief Security Officer
- Prepare a list of the key information assets within the department/agency. Choose items, which are the most important to the continued viability of the department/agencies.
- Prepare a list of the **main** threats for each information asset identified above, together with a severity rating, potential frequency rating and probability rating.
- Prepare a list of defences existing or needed to protect against each threat.
- Calculate a Risk Impact Rating for each information asset *(Initial Risk).*
- Determine priorities for identifying and implementing suitable defences, and prepare a Risk Management Strategy.
- Prepare a revised Risk Impact Rating for affected information assets once the defences are implemented. *[Residual Risk].*
- Regularly review the risk rating of each information asset.

**Potential Risks to Information Assets**

Having identified the information assets, which must be protected, it is important to identify the threats to these information assets. The threats can be classified into six categories as follows:

- **Malicious Acts: 'Techno-Crime';** premeditated, planned, often with advance probing for weaknesses. As the Commonwealth Government is 'high profile', connected to the Internet, and has valuable information within its networks and systems this threat is very real - both from external persons (unknown) or from disgruntled employees.
- **Malicious Acts: 'Techno-Vandalism'**, opportunistic, random manipulation (theft, destruction, corruption) of data and / or systems. Again, the source may be external or internal.
- **Negligence:** Information Assets are placed at (unnecessary) risk because the organisation's personnel fail to exercise appropriate care and safety. This may be due to taking short cuts, inadequate training or not bothering to comply with procedures. The individuals are often unaware of the potential impact of their actions. Regardless, negligence is a genuine threat to organisations.
- **Human Error:** accidents are a major source of information security incidents. Unlike negligence, human error is normally a signal for additional training and / or review of procedures.
- **Systems Failure:** the sudden failure of a system can have a disastrous impact, not only upon that specific system, but also upon systems, which rely upon the failed system.
- **Environmental:** natural disasters are a serious threat; these include floods, lightning, heat, fire, earthquakes, tornadoes, etc. The only way to prepare for this threat is to ensure that a *Disaster Recovery Plan* and a *Business Continuity Plan* are both in place and tested.

Examples:

| Types of Threat | Examples of Information Asset Impacted | Examples of Incidents |
|---|---|---|
| Techno-Crime | Customer Records<br>Taxpayer Records<br>Social Security information<br>Credit information | Stolen customer account details<br>Privacy violations |
| Techno-Vandalism | ATO Records | A virus destroys the data on the network's PCs |
| Negligence | Financial information | Financial accounts are modified by a user with an inappropriate access level |
| Human Error | Health records | Selecting the wrong email address discloses health details to the media |
| Systems Failure | Customer Records<br>Payment systems | The primary applications server fails, preventing access to both transaction process and client accounting systems |
| Environmental | All electronic information | Heavy rain results in a flooded data centre |

A full description of an example calculation model is included in Attachment 1 – part of a Confidential portion of the submission.

**Information Security Risk Assessment Review**

The risk the Commonwealth carries with regard to the threat to its information is the result of a combination of factors - changes to any one of which will alter the risk profile.

Information Security is concerned with the active management of, on the one hand, your exposure to the threats of (electronic) attack and, on the other, the threats of 'accidents' and opportunistic vandalism. For example, there is little point in safeguarding your valuable computer server from external attacks with all the latest technological tools if an employee is able to walk into the server room and remove the server from the rack. This may seem unlikely, but is a very common form of security breach!

The most common outcome from the risk assessment process is to define a clear set of information security policies.

**Information Security Policy**
Policies are one of the most critical elements of a proper security plan. Every department within the Commonwealth will have a standard set of foundation policies but also a set of policies depending on their departmental needs. These will define what are and are not accepted practices. The following is a partial list of areas for which usage policies are recommended. These policies could then be included in an Information Security Policy.

- Firewalls
- Electronic commerce
- Digital signatures
- Computer viruses
- Encryption
- Contingency planning
- Logging controls
- Internet
- Intranets
- Privacy issues
- Outsourcing security functions
- Computer emergency response teams
- Microcomputers
- Local area networks
- Password selection
- Electronic mail
- Data Classification
- Telecommuting
- Telephone systems
- Portable computers
- User training

Once the policies are developed, everyone within the Commonwealth department is required to review them, and acknowledge them with a signature. A "written" Information Security Policy is the document that describes the Commonwealth's intentions regarding security. Should there be a compromise, abuse or other violation, the Commonwealth is protected from possibly being held liable for loss of assets. Because of the ever-changing environment of most departments, the Information Security Policy is a document that needs to be reviewed, and modified if necessary, on a regular basis.

As this process is already underway in the Commonwealth departments a full review is required to assess the adequacy, and completeness of these procedures along with an audit of how far each departmental/agency has gone with policy adoption.

# Section 2 - The management and security of electronic information transmitted by Commonwealth agencies

In this case a policy that is specifically focussed on a “Secure Transmission Model” should be established. Writing the goal of secure data transmission as a security policy is simple:

- *Establish and ensure the appropriate level of security for data throughout its delivery*

Applying the actual appropriate level of security to data delivery is difficult, but with the help of data owners and risk models the definitive levels for protecting data are not impossible to set. Although there is a fine line between implementing a secure policy that is easy to use and implement, and a policy that is too complex to use and therefore not secure, a balance can be achieved with the right preparation and technology. The preparation ensures completeness and the technology ensures implementation.

**The preparation**

Appropriate levels of security may vary between departments, agencies and private bodies. There are also laws and contracts that can set the expected level of security. These should not be forgotten. Whether this means there are agreements between sender and recipient or regulations defined by government, the importance for managing to these definitions is the same as if set by government policy.

To assess the security level appropriate to the data being delivered there are three basic elements that need to be considered:

1. Payload
2. Destination
3. Transport.

Keeping up with these three elements separately and distinctly simplifies the overall management process so that any identified level of security can be evaluated with some confidence.

"Payload" refers to the information being delivered. Using "Payload" to describe the data flowing through the network breaks away from some current concepts about data. How to handle a payload does not mean the same as how to handle the data in a database. Static data can already meet the privacy, integrity or non-repudiation needs, so the answer to the question how to handle the payload can result in a different solution.

By definition, the second element "Destination" asks, ‘where is the payload headed at anytime during transit?’ This means that destination has a flexible character taking any number of different forms - an endpoint, hub, staging point, or a next hop down the line. It can even be defined as another site or as an arena of differing responsibilities. Destination can also refer to a legal entity, for example, another, co-operative department or agency. But, regardless of form, each of these destinations can be identified, rated, inventoried, and evaluated in terms of security. And since one destination can become nested within another, it is also important to not forget the enclosed destination’s attributes as well. Generally speaking, the purpose for including destination in this model is to reinforce the importance for security to be evaluated all the way to the end of the track.

The last element, referred to in this model as "Transport," is the most likely to have a technical definition, but it is often the hardest to confirm. Transport here refers to the data delivery protocols and other mechanisms. It is the engine behind the delivery process. Transport is easily quantified in security terms. Adequate privacy, integrity and non-repudiation can normally be proved mathematically. But its appropriate use in the security realm may not be clear-cut. Default configurations, changes in upgrades, a myriad number of patches, and a host of options, all make transport difficult to police. Only good review processes can meet the demand here.

Combined, payload, destination, and transport form a single functioning process for data delivery. Analysing them at first separately and then, as a whole is the purpose behind applying the model.

Each of these three features or elements in the model has various factors to consider and each of them must be analysed against the security policy's mandate to establish an appropriate level of security. In general, there are only two processes that actually need to be addressed for each element in the model:

1. Establish a standard for security requirements
2. Inventory the exceptions to standards.

The development of standards and the determination of their exceptions work hand-in-hand toward establishing a basic understanding of the security picture for any transport environment. Constructing these standards and exceptions inventories for each element - payload, transport, and destination - is the first step in the security process behind sound data deliveries.

**Payload**
Establishing the appropriate level of security for any data delivery payload means answering the question, 'how must the data be handled?' A first step to help answer this is creating a requirements document that explains security levels for payloads. An overly simplified example of "Payload Requirements" and their respective security levels is:

**Payload Requirements**

| Security Level | Types of Payload |
|---|---|
| Non-repudiation* | Transaction data |
| Privacy* | Secret classification, medical history, and credit history data |
| Integrity | Production and system data, internal email / correspondence |
| None | Public data |

*Includes ID/Authentication and Authorisation

An inventory of other payloads establishes the security requirement for specific payloads that are exceptions to the established standards. These can be found by checking existing databases, newsletters, web sites, etc.

**Individual Payload Inventory** [Exceptions to the Requirement Doc]

| Payload | Acceptable Security Level | Established by |
|---|---|---|
| Personnel Files | Privacy | HR Requirement |
| Contracts | Privacy | NDA w/ Departments |
| System Monitoring | Data Integrity | Engineering |

**Destination**
Building a table of security requirements for destinations is much the same as one for payload. However, some physical controls must be addressed as well. This helps answer questions like, 'how can the data be maintained?' And, 'how do you know the right payload is handled correctly?' An example of a table of destination requirements is:

**Destination Requirements**

| Security Level | Type of Destination | Mechanisms to have in place |
|---|---|---|
| Non-repudiation* | Co-operative department | Key Management |
| Privacy* | Production Host | Access Controls or Encryption |
| Integrity | Production Application | Server Access Controls |
| Authorisation | Production Staging Server | Access Controls |
| Integrity | Production Host | File checks or Hashing |
| Authorisation | Data Base | Permissions |
| Id/Authentication | Workstation | Authentication |
| Test Host | User Test Site | Open Code |
| Lab Server | Lab Only | Open System & Code |
| None | Public Web Server | Read Access Only |

*Includes ID/Authentication and Authorisation

The next step is to complete an inventory of any other destinations - both within and without the Commonwealth - that cannot be categorised.

**Individual Destination Inventory** (or Exceptions to the Requirements)

| Specific Destination | Acceptable Security Level | Established by |
|---|---|---|
| Person ABC | Privacy | Personal records |
| Person XYZ | None | Physical Site Review |

**Transport**
Getting a handle on the transport element is the final phase for establishing the baseline information in the roundhouse mode. This table of requirements addresses how the data is delivered. It also includes information showing how the right payload is picked up, how the right destination is in place, and how the delivery cannot be done any other way.

**Transport Requirements**

| Security Level | Type of Transport | Mechanisms to have in place |
|---|---|---|
| Non-repudiation* | VPN – full encryption | Contracts, Service Agreements. |
| Privacy* | SSH | Key Management, Directory Access |
| Privacy* | HTTPS | Web Resource Allocation |
| Integrity | VPN | Contracts, Service Agreements. |
| Authorisation | FTP | User Enrolment & Authorisation |
| Id/Authentication | NFS | System Controls |
| None | all the above | |

The most important task of all, and probably the most tedious, is the next step: complete an inventory of the specific delivery mechanisms on each platform.

**Individual Transport Inventory**

| Installed Transport | Expected Security Levels | Established by |
|---|---|---|
| Host1 FTP | Authorisation | Users |
| Host1 Connect Direct | Non-Repudiation | Operators |
| Server1 SSH | Privacy | Security Office |

This extensive list is necessary for the completion of the secure transmission model for data management. Having a good inventory of all the transport choices is mandatory before security can be ensured in the final phase.

**Ensuring the Appropriate Levels**
Once the requirements and inventories are completed, the next step is to ensure that the security levels across the board are consistent for each payload. That is, is the payload's security requirement being met by its respective destination and transport? A simple matrix drawn from the above requirements tables and exceptions lists should provide an example:

**The Secure Transmission Model**

| Payload/Security Level | Destination / Security Level | Transport/Security Level | Verify |
|---|---|---|---|
| Tax Records/Privacy | Prod App / Privacy | SSH / Privacy | Yes |
| System Data/Integrity | Prod Hosts/Integrity | FTP/Auth | No |

As to be expected, there will be exceptions that are acceptable because they have some other merit. Documenting these issues is critical, but they should be approved and inventoried individually. For example:

**The Exceptions Inventory**

| Payload | Destination | Transport | Conditions |
|---|---|---|---|
| Business Reports/Privacy | Web Server/Public | FTP/Authorisation | Special Approval |

**Administrating the Process**
Maintaining a complete list of standards and creating an inventory begins to address the security of data delivery. However, confirming that each payload is being handled appropriately does not address all of the security risks. There are also risks in *not* checking what else can be done. To cover this include activities that close "back doors." This will eliminate opportunities for breaches in security often overlooked. Complete the overall protection processes by including the following:

**Pro-active risk reduction**
Removing or eliminating the functions in hardware that cannot be secured is crucial. In essence, what is not being used should not be available:

- Turn off delivery options when not needed
- Isolate access to systems that do not protect the payloads appropriately
- Look at deliveries where special approval has been given. These must be monitored continually
- Close back doors or processes that can be used without proper administration.

**Pro-active Monitoring**
Use tools for verifying that processes are in place and being followed:

- Payload=> sniffers, access logging
- Transport=> trace route command, baseline, test deliveries
- Destination=> ping, IDS, physical site survey.

**Auditing**
Once the process is in place, there is still the verification that each element is correctly structured. For this assurance, provide an audit of:

- Payloads, destinations and transports
    - For payloads, drill down to specific files and confirm their actual status.

**Automating the Process**

Tools exist to automate the management of data delivery beyond the scope of individual delivery technologies. This secure transmission model can be used to systematically review the elements controlling data delivery throughout any department or agency. It does not replace the diligence of system administrators, operators and engineers, but it does present a well-outlined inventory of the security structure and a simpler format to address the question, ‘are all the Commonwealths departments and agencies in compliance with a data delivery policy?’

# Section 3 - The management and security of the Commonwealth's electronic information stored on a centralised computer architecture and in distributed networks

To address the management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks a continual security lifecycle needs to be created.

Daily, new attack signatures are being developed, viruses and worms being are written, natural disasters occur, changes take place in the workplace and technologies evolve. These all affect the security of Government departments and agencies. Any one piece of the lifecycle cannot be effective without the other. Identifying risks and correcting them are essential. Perhaps you have a solid Information Systems Security Policy, but can you be assured you are secure in an ever-fluid environment? Having a Policy is a good starting place, but the security process should not end there: it requires a continued effort – a continuous lifecycle - to keep abreast of changes in technology and weaknesses in security that are created as a result of these changes.

In this section, the security elements that make up a lifecycle will be discussed: what pieces are needed to address all aspects of security, and how often they should be addressed.

The security elements are categorised into three areas: *Prevention*, *Detection* and *Response*. Each category is discussed below, including what elements fit within these categories and how they address the overall security of the Government.

**Prevention** – As discussed in the earlier sections risk assessment is the first critical step in prioritising the risk associated with your information assets. Once that is completed then Penetration Testing addresses risk levels and "holes" that need to be corrected. Without an assessment, you may never find the weaknesses in security. The Risk Assessment will address not only Network & Host level risks, but also overall security risks that include Physical, Logical and Data. Penetration Testing is a great way to "test" the security strength once risks have been identified and corrected.

**Detection** – Intrusion Detection Systems (IDS) and Firewalls are both detection measures. The IDS monitors the network traffic for attack signatures, and reports any occurrence by risk levels that have been defined. Depending on where the IDS sensor is placed, inside or outside the Firewall, it can serve both as "detection" and "prevention". The Firewall itself acts as a detection measure, since all activity is logged and should be reviewed. Assuming your Firewall is blocking traffic defined in your rule base, it will write to a log file with all failed and successful attempts. By reviewing the log file, and observing the type of activity taking place, you can determine if someone is possibly looking for holes in your Firewall.

**Response** – What happens should there be a compromise? Keep in mind, a compromise can happen not only by a break into the Firewall, but by an internal employee, backdoor access into a network from a modem or even physical entrance to an area by someone pretending to be an authorised person (this is called Social Engineering). The Information Security Policy falls into the "response" category. The Information Security Policy is a written document defining Management's intentions on how Security should be addressed.

**Elements of the Lifecycle**

- Perimeter Protection
- Risk and Vulnerability Assessment
- Information Systems Security Policies
- Penetration Testing
- Intrusion Detection

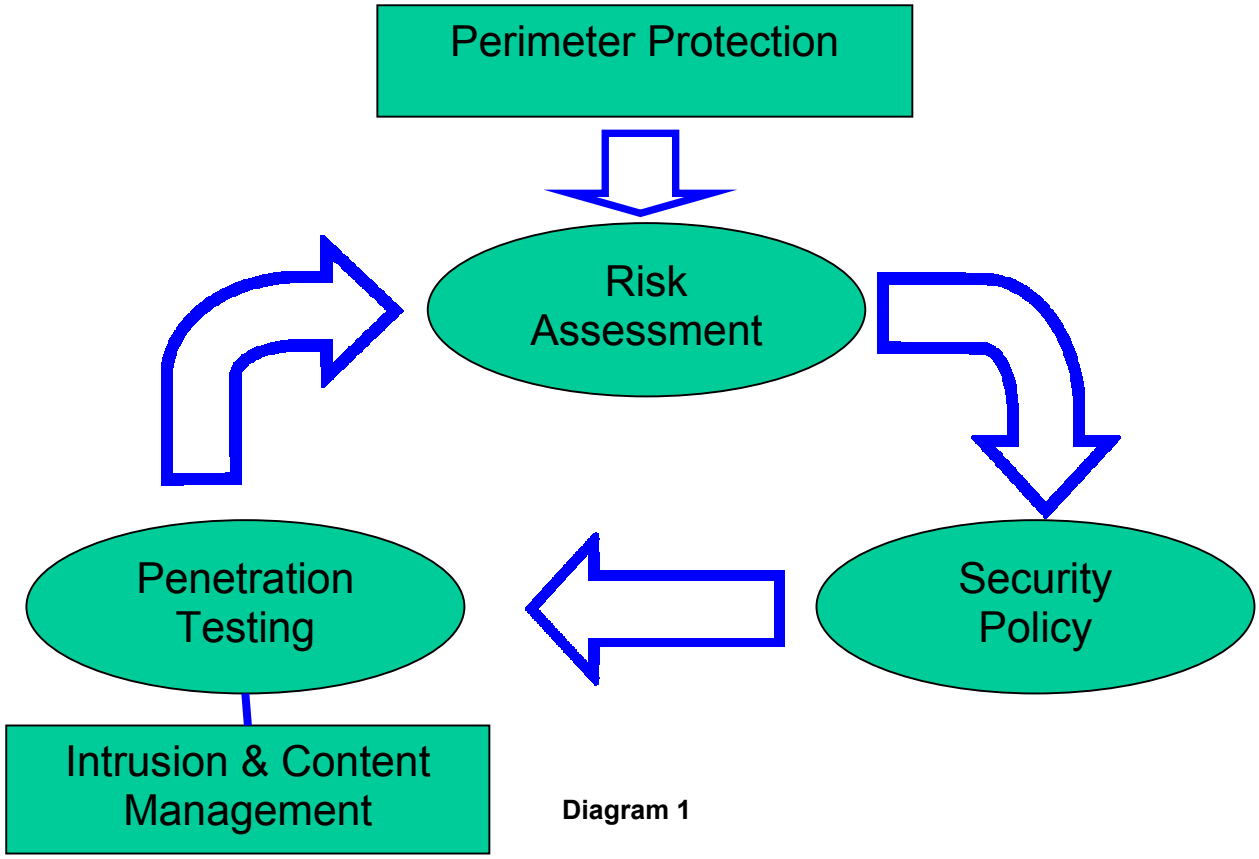



**Diagram 1**

**Perimeter Protection**

Most people think they are secure once they have a simple firewall in place. Firewalls are designed to protect the perimeter of a network. But just because a Firewall is in place it does not necessarily mean the network cannot be compromised. Firewalls come in different flavours. They can be a Packet Filter, Application Gateway, Circuit-level or State-full Inspection, and they all are designed to block different types of traffic. It is critical to build in a Firewall rule base that specifies what is and is not allowed to enter and exit the network. Even with these rules, there is always the possibility of an attack signature that can circumvent the Firewall. For instance, a fragmented attack, like a virus that has been broken into many packets may be able to pass through a Firewall that does not do State-full inspection. Remember, Firewalls "prevent" the possibility of a compromise by protecting the perimeter.

More detail about the different types of firewalls:

- **Packet Filter** – Packet filters are usually part of a router. The router will compare each packet to a set of rules, and depending on the rule, the Firewall can drop the packet or route it to its destination. The rules can include source and destination IP addresses, source and destination port numbers and protocols. The advantage of a Packet Filter Router is the low cost and low performance it puts on the network. The disadvantage is it only works at the Network layer and does not support Network Address Translation (NAT), to hide IP addresses behind the Firewall like the Circuit-based Firewall.

- **Application Gateway** – This is also referred to as a Proxy server. This type of Firewall is application specific, and works at the application layer of the OSI model. If there is no proxy defined, packets cannot access those services. The advantage of the application level gateway, or Proxy, is it can filter application specific commands like ftp, telnet and http. This cannot be accomplished with other Firewalls that are packet filtering or circuit-level because they do not filter at the application level. The disadvantage is the performance hit on the network as a result of the context switching that takes place.

- **Circuit-Level** – Circuit-level Firewalls work at the Session layer of the OSI model, and TCP layer of the TCP/IP model. They monitor the TCP negotiation between packets to verify the requested session is valid. The advantage of Circuit-level Firewalls is they can hide the information about the inside network using Network Address Translation (NAT), making the packet appear to originate from the Firewall. The disadvantage is they do not filter individual packets.

- **Stateful Inspection** –This Firewall combines the three other Firewalls into one. In order to provide robust security, a firewall must track and control the flow of communication passing through it. To reach control decisions for TCP/IP based services (e.g., whether to accept, reject, authenticate, encrypt and/or log communication attempts), a firewall must obtain, store, retrieve and manipulate information derived from all communication layers and from other applications.

  It is not sufficient to examine packets in isolation. State information - derived from past communications and other applications - is an essential factor in making the control decision for new communication attempts. Depending upon the communication attempt, both the communication state (derived from past communications) and the application state (derived from other applications) may be critical in the control decision.

  Thus, to ensure the highest level of security, a firewall must be capable of accessing, analysing and utilising the following:

  - **Communication Information** - information from all seven layers in the packet

  - **Communication-derived State** - the state derived from previous communications
    For example, the outgoing PORT command of an FTP session could be saved so that an incoming FTP data connection can be verified against it

  - **Application-derived State** - the state information derived from other applications
    For example, a previously authenticated user would be allowed access through the firewall for authorised services only

  - **Information Manipulation** - the evaluation of flexible expressions based on all the above factors. Fragmentation is an example of information manipulation. This can be applied to most types of information attacks. Therefore it is key that the "content" of the packets are examined and inspection of the full conversation that occurs to establish the integrity of the traffic.

The Firewall is the first part of securing your infrastructure. It does not make a lot of sense to perform a Risk Assessment without some type of perimeter protection in place. Without a Firewall, your entire network is wide open. But the Firewall is still considered part of the Security Lifecycle, and it should be. After all, once the Firewall is in place, you will at some time or another, add or change a policy rule. Perhaps, you will apply a new version, upgrade, or install patches. Changes to your Firewall will no doubt happen, often! So the Firewall needs to be reviewed and tested to make sure it is still doing what you are intending it to do. Much of this review will be addressed during the Risk Assessment. Perhaps you may decide not to do the Risk Assessment and go right for a Penetration Test. In this case, constant review of the Firewall is necessary to ensure nothing has been left open. Look at your rule sets and log files, review them regularly. This is the only way to be assured you are blocking everything you intend to.

Software based Firewall solutions are easier to manage, change and upgrade, than hardware-only solutions that are hard-coded in ASICS (Application Specific Integrated Circuits). There is also a total cost of ownership advantage with software-based solutions over hardware. The cost of change for hardware is excessively higher than for software, the initial entry cost may be cheaper for hardware but the total ownership cost is much higher.

OPSEC (Open Platform for Security) is another critical aspect of a firewall that needs to be considered. The OPSEC framework provides central configuration and management, while integrating third-party security applications. The resulting security system is composed of several components, each of which may be

provided by a different vendor and installed on a different machine. Therefore the departments and agencies can choose the security components that suite their specific requirements but still conform to the overall Commonwealth security strategy.

**Risk Assessment**

This is most often the first step in a security lifecycle. A thorough Risk Assessment will address risk at all levels within a department or agency to identify the Integrity, Confidentiality and Availability of the information assets. We all know there can be a loss of data if our networks are hacked from the outside. What about the inside? In reality there are a high percentage of compromises that have been caused from inside a company's network. For example, internal compromises can be caused from an employee with unrestricted access "playing" or, in the case of a new administrator, learning on the job and configuring software incorrectly, causing a denial-of-service (DOS) attack.

But there are many other logical and physical areas that also need to be reviewed during an assessment in addition to the networks and hosts. The following key areas should be addressed during an assessment:

- Exterior security – fencing, lighting, building location
- Secured dumpsters – disposal of confidential information
- Building security – key-locked doors, biometric authentication, physical guards, cameras
- Departments - logically broken up, kept secure
- Passwords - Post-It notes stuck under a keyboard or side of the monitor with user ID and password
- Computer/Data Centre – environmental controls, fire and cable management, secure consoles
- Data Classification – confidential, secret, need-to-know
- Access groups – assigned by user and/or group
- Human Resources and IT staff coordination
- Unauthorised modems
- Social Engineering – persons pretending to be an employee or maintenance worker to gain unauthorised access

The assessment will itemise all risk levels associated with the areas mentioned above. Should any of these areas become compromised, how will it effect the operation of the government? Will there be a loss of revenue, loss of reputation, possible lawsuits?

Information generated from the data gathering process will help the IT staff and Management to make logical decisions on how to better protect the company assets. This data will also serve as a reference to creating and/or updating the Information Security Policy.

The Risk assessment process is defined in more detail earlier in this submission, and a risk assessment calculator is included in Attachment 1.

**Information Systems Security Policy**
The Information Systems Security Policy is made up of a collection of individual documents called policies. Policies are one of the most critical elements of a proper security plan. Every organisation will have a different set of policies depending its specific needs. These will define what are and are not accepted practices. The following is a partial list of items for which policies could be included in an IS Security Policy.

- Firewalls
- Electronic commerce
- Digital signatures
- Computer viruses
- Encryption
- Contingency planning
- Logging controls
- Computer emergency response teams
- Microcomputers
- Local area networks
- Password selection
- Electronic mail
- Data Classification
- Telecommuting

- Internet
- Intranets
- Privacy issues
- Outsourcing security functions
- Telephone systems
- Portable computers
- User training

Once the policies are developed, training should be conducted to all personnel where management should state the Commonwealths intentions from a security perspective. Should there be a compromise, abuse or other violation, the Commonwealth is protected from possibly being held liable for loss of assets or privacy. Because of the ever-changing environment of most organisations, the Information Security Policy is a document that needs to be reviewed, and modified if necessary, on an annual basis.

So where do you start developing the Information Systems Security Policy? You could hire a Security Consultant to create these Policies for you. Or, if you have the resources, this can be done in-house.

**Penetration Testing**

Is this really necessary? Here are a few questions to ask:

- How vulnerable is my technology infrastructure to network attacks from outside the organisation?
- By what means can hackers / crackers gain unauthorised access to my technology and information resources?
- Are Firewalls, routers, modems, and other network devices configured correctly and managed correctly?
- How well does my Information Systems Security Policy support access barriers, rights, and privileges to my technology infrastructure?
- How many of my Internet Protocol (IP) addresses are visible/accessible to the "outside world" and what services are available on those addresses?
- How many "modems" does my organisation present to the "outside world" and how vulnerable are those modems to hackers?

Once a Risk Assessment has been performed and fixes have been applied, the Penetration Test is a good exercise to test how strong the security is from outside and inside the network. This is usually performed as a zero-knowledge brute-force attempt to gain access into the network. Typically, a hacker/cracker will gather information, called profiling, about your operation before they try to launch an attack on your network.
If you have the same team that performs the Risk Assessment performing the Penetration Test, you will not be emulating the same results of a hacker/cracker. A security person with zero-knowledge about your organisation would best emulate what a hacker/cracker does during the profiling stage. The idea is to use a person that has no knowledge of information that was gathered during the Risk Assessment about the organisation. This will result in the same outcome as if someone actually did compromise your network, giving you the information needed to correct the security weaknesses before an actual attempt is made.

**Intrusion & Content Management**

So you have a locked-down, tight Firewall, assessment looks good, a strong written Information Security Policy is in place, and everyone has gone through security awareness training. How do you monitor all those potential compromises, both inside and outside your network? You can review your Firewall logs, and hopefully there are rules in place that are blocking those attempts, and these should be reflected in your log files. But what about those attack signatures that are not defined in a rule? Intrusion Detection Systems (IDS) are designed to monitor all traffic destined for your network, or leaving your network. The IDS when configured properly will show all potential attack signatures at different risk levels. When these are noticed, a quick review of the Firewall rule policy will tell you if the source IPs, ports and signatures are being blocked. If not, this is a good time to add them to the rule base. The following are items that an Intrusion Detection System will address:

- Monitor system, event and security logs for a change in files, comparing the new log entry with attack signatures
- Check key system files and executables via checksums at regular intervals for unexpected changes
- Monitor of port activity and alerting administrators when specific ports are accessed
- Define type of attack
- Contain the Intrusion
- Identify the source
- Notify all interested parties
- Review/Repair systems
- Detail a post-mortem of the Intrusion

There are many choices for Intrusion Detection Systems. Most fall into two categories: host-based and network-based.

- Host-based – Host-based IDS are used to monitor the system itself for abuses and internal (system) attacks
- Network-based – Network-based IDS are used to monitor the network for TCP/IP type of external attacks.

It is important to understand the different type of attack signatures, and how they are used to launch an attack. You can easily determine when someone is ping flooding or port scanning you. But a good hacker/cracker will usually do a series of pinging, probing, DNS gathering, and any number data gathering techniques before an actual attack is launched. A seasoned security person should be able to monitor an Intrusion Detection System, and notice by the events that are taking place if someone is using an off-the-shelf port scan utility, or if they are actually gathering pre-attack information.

**Conclusion**
Remember, Security is a LIFE CYCLE. These elements need to be performed on a scheduled basis, at least annually. The following is a re-cap of the cycle in steps.

- Implement perimeter protection using a Firewall, review rule sets and log files regularly
- Perform a Risk Assessment at least once a year
- Develop a written Information Security Policy. Review and update the policy at least once a year
- Test the strength of security by performing a Penetration Test at least once a year
- Monitor all network traffic using an Intrusion Detection System
- Should there be a possible compromise, respond immediately

There is no guarantee that the Commonwealth will ever be 100% secure. As an example, take into consideration how a bank would secure its assets; can they be 100% safe from a possible loss? A bank can install state-of-the-art alarm systems, have security cameras throughout the building, install crack-proof safes, place security guards on the premises, but should a person really be determined to rob that bank, they probably will. This is also true for Information Security. The best any organisation can do is to deter the possible hacker by making it more difficult to gain access.

# Appendix 1 – Risk Assessment Model

See attached