INFS 5115 Security Principles

Roles & Responsibilities

University of South Australia

School of
Information Technology
and Mathematical Sciences

Roles & Responsibilities

- In this module, we will discuss various aspects relating to being a cybersecurity professional, including examples of roles, duties and accountabilities.
- We will also briefly discuss ethics within the context of the six core ethical values in the ACS Code of Professional Conduct.

The Cybersecurity Officer

- The first security officers responsible for computers would have been guards who physically protected the machine and ensured that only authorised users had access.
- This was possible due to the fact that the machines could only be used by a single local user at any one time.
- With the evolution of multi-user and networked computer systems came a need for consideration of computer security, both at-rest on a computer system, and in-transit between computer systems.

Kovacich, GL 2016, The information systems security officer's guide : establishing and managing a cyber security program, 3rd edn, Butterworth-Heinemann, Waltham, MA.

The Cybersecurity Officer

- Information is often one of an organisation's most valuable assets.
- Cybersecurity has evolved to be recognised as a distinct profession, rather than a part-time responsibility for IT staff.
- Some organisations (particularly smaller organisations) may choose to outsource this function to external entities or make it a part-time responsibility for a member of their IT staff.

Kovacich, GL 2016, The information systems security officer's guide : establishing and managing a cyber security program, 3rd edn, Butterworth-Heinemann, Waltham, MA.

The Cybersecurity Officer

Role

Protect, Shield, Defend, and Prevent
Ensure that the organization's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the enterprise from cyber threats

Monitor, Detect, and Hunt
Ensure that the organization's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries and report instances of suspicious and unauthorized events as expeditiously as possible.

Respond, Recover, and Sustain
When a cybersecurity incident occurs, minimize its impact and ensure that the organization's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible.

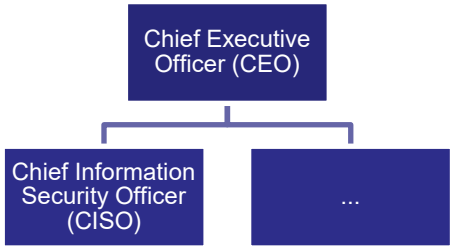
Govern, Manage, Comply, Educate, and Manage Risk
Ensure that the organization's leadership, staff, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement, and course correction of all cybersecurity activities

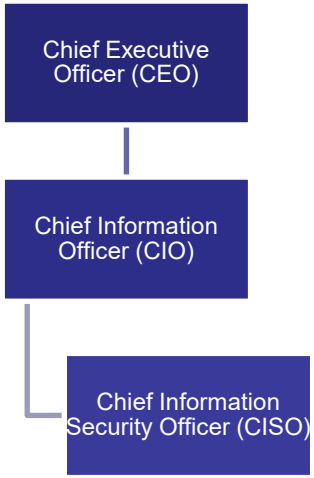
Software Engineering Institute, 2015, 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

The Cybersecurity Officer

Structure

Depending on the size of the business will depend at what level the Cybersecurity Officer sits.



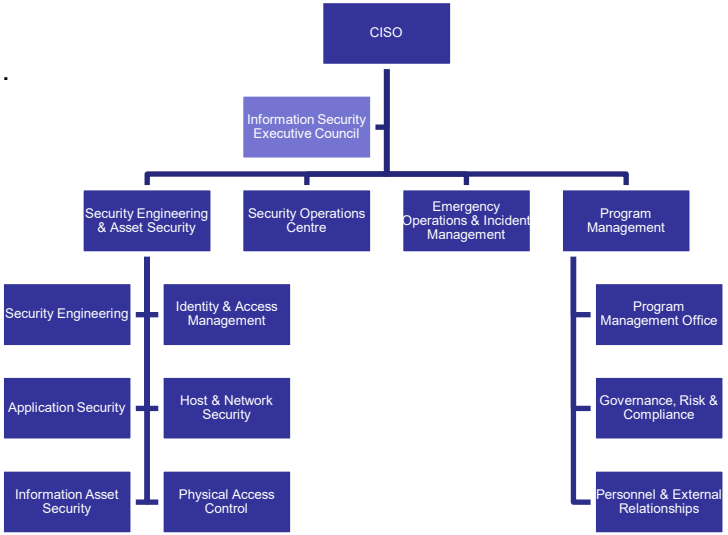


The Cybersecurity Officer

Structure

The following organisational chart lists the departments, subfunctions, and activities that are covered by a high-level Cybersecurity Officer.

Let's break down some of the sub functions..



Software Engineering Institute 2015, 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

The Cybersecurity Officer

Structure

Security Engineering & Asset Security

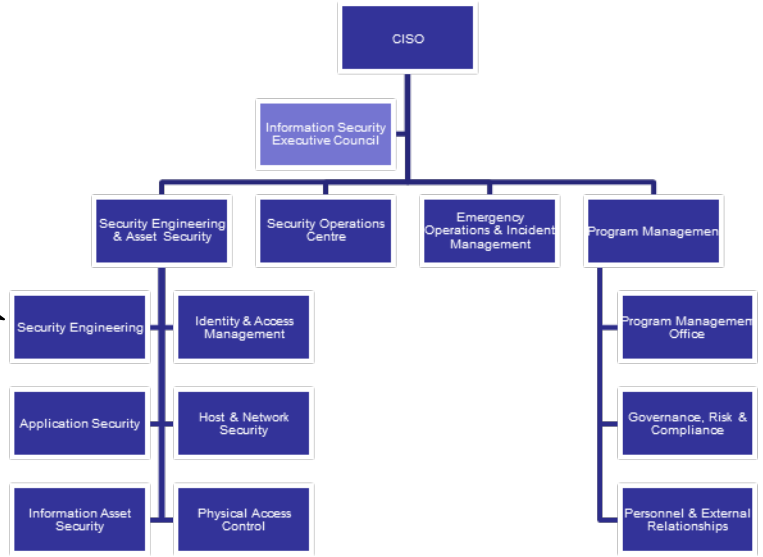
Security engineering:

Requirements - Specify and allocate/assign confidentiality, integrity, and availability requirements.

Architecture - Develop and maintain a security architecture

Secure lifecycle - Address security throughout the acquisition and development lifecycle

Certification & accreditation - Perform certification and accreditation prior to releasing new systems to production.

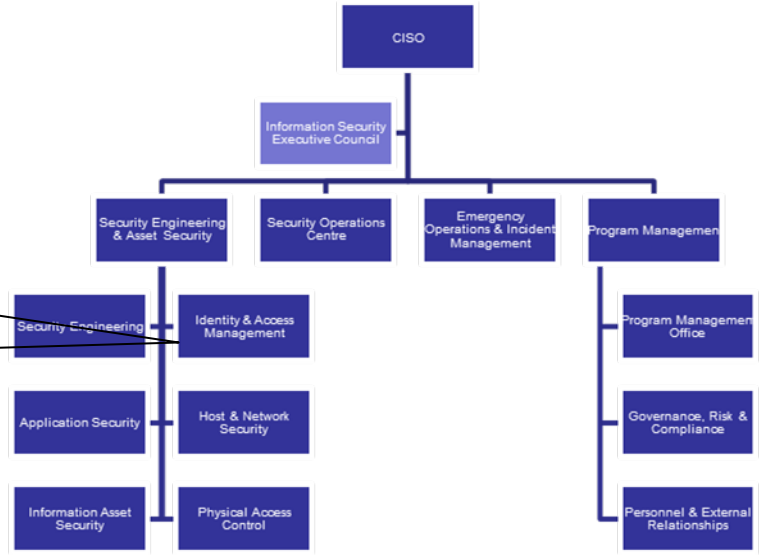


Software Engineering Institute, 2015 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

The Cybersecurity Officer

Identity & access management:

Define and manage identities and access controls based on identities (password management, single sign on, two-factor authentication, PIN management, digital signatures, smart cards, biometrics, Active Directory, etc.)



The Cybersecurity Officer

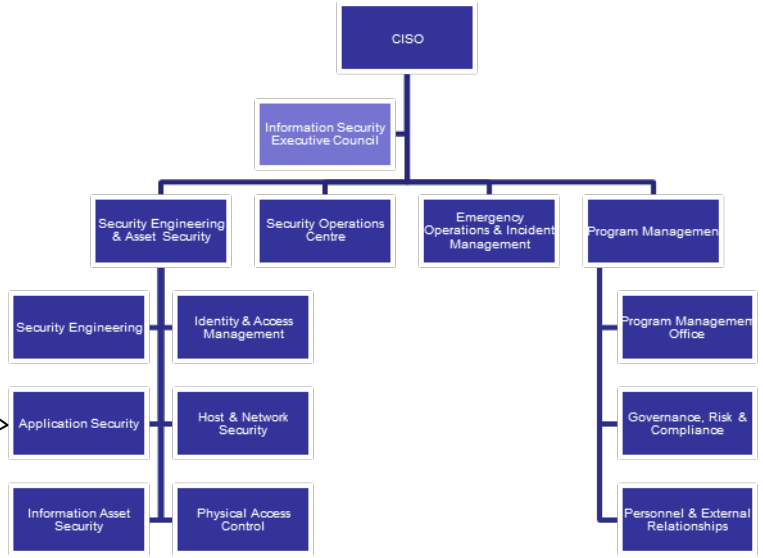
Application security:

Inventory software & assets - Develop and maintain software and application inventories

Controls to protect software and applications - Define, implement, assess, and maintain controls necessary to protect software and applications in accordance with security requirements (operating systems, applications etc

Configuration Management - Manage configuration for software and applications

Network perimeter controls - Define, implement, assess, and maintain controls necessary to protect the network/Internet perimeter in accordance with security requirements (firewalls, DMZ, network connections, third-party connectivity, remote access, VPNs)

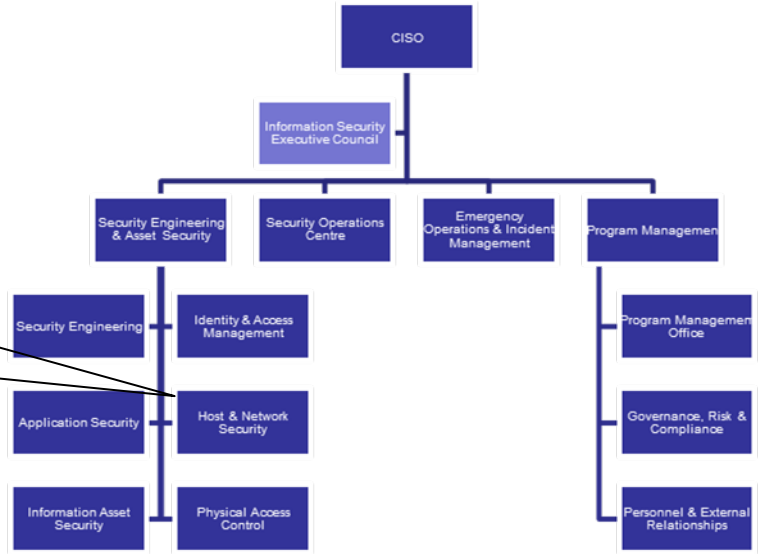


The Cybersecurity Officer

Structure

Host and network security:

Define, implement, assess, and maintain controls necessary to protect networks, hardware, and systems in accordance with security requirements (intrusion prevention/detection)



Software Engineering Institute, 2015 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

The Cybersecurity Officer

Information asset security:

Information asset categorization

Designate and categorize information and vital assets (including PII) (includes privacy requirements)

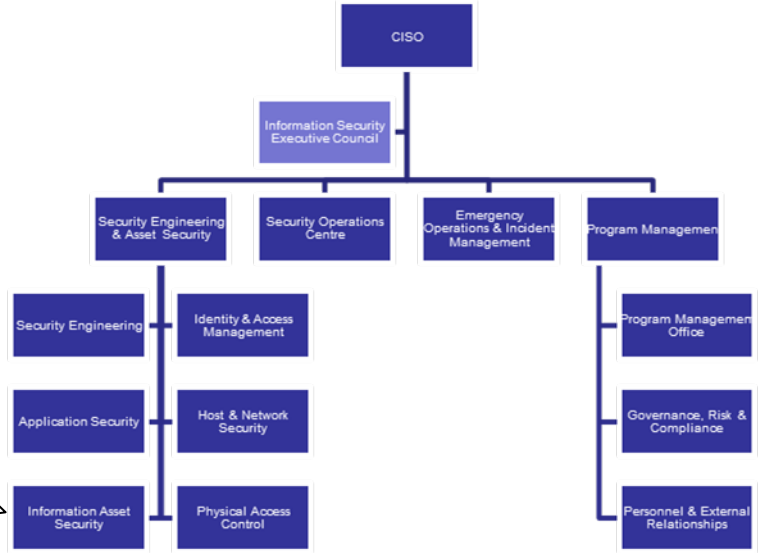
Information asset inventories

Develop and maintain information asset inventories

Information asset controls

Define, implement, assess, and maintain controls necessary to protect information and vital assets (including media) in accordance with security requirements (includes privacy requirements, PII, encryption, PKI, backups, DLP, data retention/destruction)

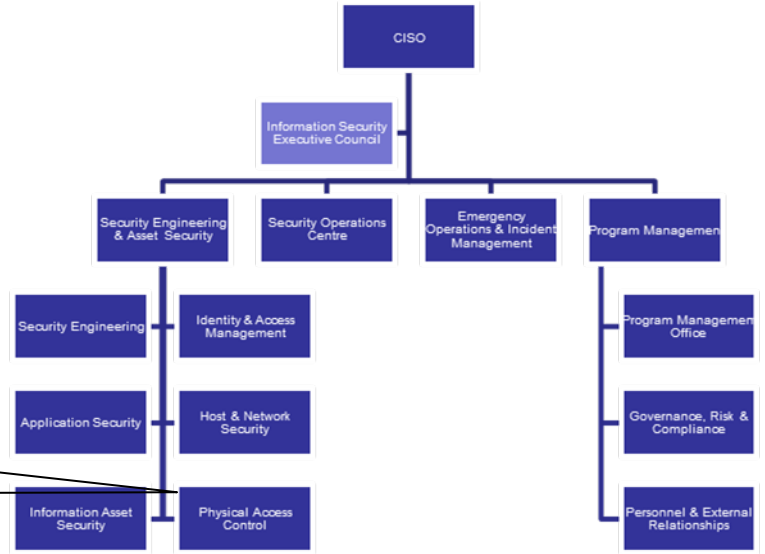
Structure



Software Engineering Institute, 2015 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

The Cybersecurity Officer

Structure



Physical access control:

Define and enforce access controls for facilities and other physical assets (such as networks and hosts)

Software Engineering Institute, 2015 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

The Cybersecurity Officer

- Security Operations Centre
  - Intelligence collection
  - Analysing & managing threats
  - Situational awareness & reporting
  - Collecting & monitoring logs
  - Managing vulnerabilities & malware
  - Responsible information security help desk (Computer Security Incident Response Team or CSIRT)
  - Managing security incidents
  - Communicating with external stakeholders

Software Engineering Institute 2015, 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

The Cybersecurity Officer

- Emergency Operations & Incident Command
  - Works closely with SOC to mobilise staff, activate response plans & manage time-critical incident management & response activities when a high-impact incident is declared
  - Planning for incidents, business continuity & IT disaster recovery
  - Tests, exercises & drills of response plans
  - Problem management, root cause analysis & post mortems
  - Forensic investigations

Software Engineering Institute 2015, 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

The Cybersecurity Officer

- Program Management
  - **PMO:** Develop & implement information security plan, allocate & manage funding for information security activities, organisational change management
  - **Governance, risk & compliance:** Oversight, risk management & compliance with legal, regulatory, policy & other requirements
  - **Personnel & external relationships:** Manage relationships with third parties, external stakeholders & wider ecosystem; manage employment lifecycle and people capabilities

Software Engineering Institute 2015, 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

The Cybersecurity Officer

- Information Security Executive Council
  - Advising CISO to help ensure
    - information security objectives & requirements are met
    - policies, programs & plans are implemented
    - externally imposed compliance obligations are met
  - May include members from key internal stakeholder organisational units and external experts

Software Engineering Institute 2015, 'Structuring the Chief Information Security Officer Organization', Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

Cybersecurity Related Roles

- *Chief Information Officer (CIO)*
- *Chief Information Security Officer (CISO)*
- *Legal Counsel*
- *Human Resources*
- *Corporate Communications*
- *Incident Commander*
- *Internal Investigator*
- *IT Security Manager*
- *Security Operations Centre (SOC) Analyst*
- *Endpoint Detection and Response (EDR) Technician*

Verizon 2017, 'Data Breach Digest: Perspective is Reality', http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf

Cybersecurity Related Roles

External

- *Lead Investigator*
- *Endpoint Forensics Examiner*
- *Malware Reverse Engineer*
- *Network Forensics Specialist*
- *Critical Infrastructure Protection / Cybersecurity Specialist (CIP/CS)*
- *Payments Forensic Investigator (PFI)*

Verizon 2017, 'Data Breach Digest: Perspective is Reality', http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf

Cybersecurity Roles

Indirectly Related

Beyond the roles specifically related to information security, relevant information security responsibilities and authorities should be included within other roles. For example, information security responsibilities can be incorporated in the roles of:

- *information owners;*
- *process owners;*
- *asset owners (e.g. application or infrastructure owners);*
- *risk owners;*
- *information security coordinating functions or persons (supporting role);*
- *project managers;*
- *line managers; and*
- *information users.*

Standards Australia 2017, *Information technology – Security techniques – Information security management systems – Guidance*. ISO/IEC 27003:2017, Vernier, Geneva, p. 10-11.

Ethics Issues

- Ethics
  - The *study of morality's effect on conduct: the study of moral standards and how they affect conduct* […][1].
- Ethical conduct is integral to any position of trust, certainly including that of a cybersecurity officer.
- There are differing views of the link between law and ethics.
- Some view any action which breaks a law as unethical, whereas others hold a range of broader and more narrow views.

Kovacich, GL 2016, The information systems security officer's guide : establishing and managing a cyber security program, 3rd edn, Butterworth-Heinemann, Waltham, MA.

[1] Encarta World English Dictionary as citied in *ibid.* p. 275.

Ethics Issues

- The Australian Computer Society publishes a ‘Code of Professional Conduct’.
- We will use the six core ethical values in this code as the basis for our discussion of ethics.
  - The Primacy of Public Interest
  - The Enhancement of Quality of Life
  - Honesty
  - Competence
  - Professional Development
  - Professionalism

Australian Computer Society 2014, ‘ACS Code of Professional Conduct‘, https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional-Conduct_v2.1.pdf

Ethics Issues

- **Primacy of Public Interest**
  - *In the context of this Code, the public interest takes precedence over personal, private and sectional interests, and any conflicts should be resolved in favour of the public interest.*
  - *In your work, you should safeguard the interests of your immediate stakeholders, provided that these interests do not conflict with the duty and loyalty you owe to the public.*
  - *The public interest is taken to include matters of public health, safety and the environment.*

Source: Australian Computer Society 2014, 'ACS Code of Professional Conduct', https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional-Conduct_v2.1.pdf, p.6.

Ethics Issues

- **The Enhancement of Quality of Life**
  - *The development of ICT has had a significant impact on our society and way of life.*
  - *Whilst this impact has been beneficial to a very great extent, like all technologies, ICT has also had some negative effects, and will continue to do so.*
  - *An ethical approach to your work will help to recognise and minimise these adverse effects.*
  - *You should promote equal access to the benefits of ICT by all members of society.*

Source: Australian Computer Society 2014, 'ACS Code of Professional Conduct', https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional-Conduct_v2.1.pdf, p.6.

Ethics Issues

- **Honesty**
  - *Do not breach public trust in the profession or the specific trust of your stakeholders.*
  - *Observance of utmost honesty and integrity must underlie all your professional decisions and actions.*
  - *Circumstances will undoubtedly arise during the course of your professional career where it may appear to be beneficial for you to be deceptive in some way. This type of behaviour is not acceptable professional conduct.*

Source: Australian Computer Society 2014, 'ACS Code of Professional Conduct', https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional-Conduct_v2.1.pdf, p.7.

Ethics Issues

- **Competence**
  - *Accept only such work as you believe you are competent to perform, and do not hesitate to obtain additional expertise from appropriately qualified individuals where advisable.*
  - *You should always be aware of your own limitations and not knowingly imply that you have competence you do not possess.*
  - *This is distinct from accepting a task of which the successful completion requires expertise additional to your own.*
  - *You cannot possibly be knowledgeable on all facets of ICT but you should be able to recognise when you need additional expertise and information.*

Source: Australian Computer Society 2014, 'ACS Code of Professional Conduct', https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional-Conduct_v2.1.pdf, p.7.

Ethics Issues

- **Professional Development**
  - *Keep yourself informed of such new technologies, practices and standards as are relevant to your work.*
  - *Others will expect you to provide special skills and advice; and in order to do so, you must keep your knowledge up-to-date.*
  - *You should encourage your staff and colleagues to do the same.*
  - *Take action to ensure that your hard-won knowledge and experience are passed on in such a way that the recipients not only improve their own effectiveness in their present work but also become keen to advance their capabilities and take on additional responsibilities.*

Source: Australian Computer Society 2014, 'ACS Code of Professional Conduct', https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional-Conduct_v2.1.pdf, p.7.

Ethics Issues

- **Professionalism**
  - *The ICT industry is relatively new and characterised by rapid change. It has not had the opportunity to evolve over many years and acquire its own standards and legislation.*
  - *The ACS is endeavouring to improve public confidence in the ICT industry.*
  - *It is imperative that members of the Society maintain professional standards that improve and enhance the industry's image, especially in the workplace.*
  - *All people have a right to be treated with dignity and respect.*
  - *Discrimination is unprofessional behaviour, as is any form of harassment. Members should be aware that the ACS can help them resolve ethical dilemmas.*
  - *It can also provide support for taking appropriate action, including whistle-blowing, if you discover an ACS member engaging in unethical behaviour.*

Source: Australian Computer Society 2014, 'ACS Code of Professional Conduct', https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional-Conduct_v2.1.pdf, p.7.

Discussion

- In response to the Bureau of Meteorology cybersecurity incident in 2016, the Prime Minister announced that Australia had developed an offensive cyber capability. Discuss the ethical issues associated with the development of this capability.