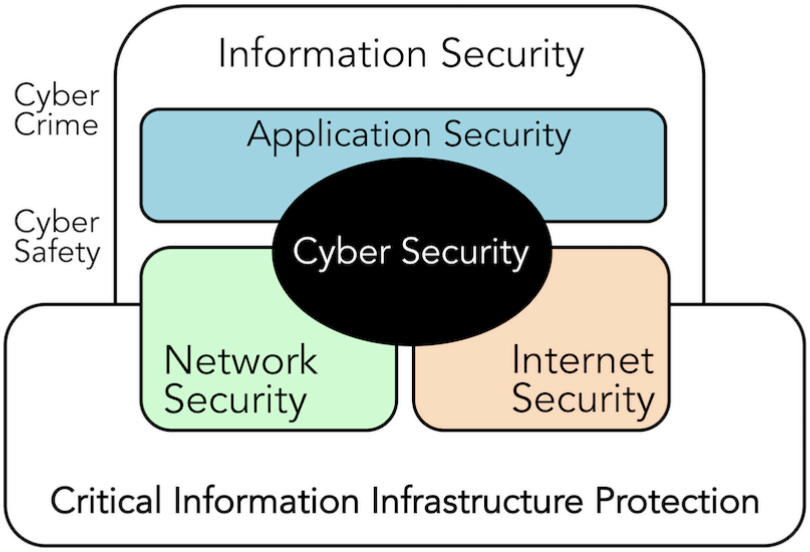
CYBERSECURITY FOR MANAGERS & BOARDS

B. von Solms, R. von Solms, K. Renaud



Boards of a (BoDs) and management teams are responsible and accountable for the well-being modern organizations. In recent times organizations have embraced cyber space, making them completely dependent on the ***confidentiality***, ***integrity*** and ***availability*** of their digitally-stored information. The GDPR regulations mandate protection of this information, and fines for not doing so are punitive.

Here we list some actions management teams should consider taking to embrace their cyber-related responsibilities.

Definitions

Information Security

"the preservation of the confidentiality, integrity and availability of information."
ISO/IEC 27000

Information Security Governance

"the governance of information security, regardless of its format"
Von Solms & Von Solms, 2018.

Cyber Security

"the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space."

Cyber Security Governance

"the process of directing and controlling the protection of a company's digital information assets from the risks that are related to using the Internet."

Examples

A company pays a contractor to destroy the hard drives of computers they want to dispose of. The company chooses, instead, to sell the hard drives on the black market. This is a breach of digital ***information security***.

A patient enters her Doctor's consulting room. Neither the doctor, nor the patient, realizes that the door is ajar, instead of being properly closed. The patient is given a cancer diagnosis and the entire waiting room hears it through the partially open door. This is a breach of non-digital ***information security*** i.e. confidentiality has been lost.

An employee works on a confidential contract on his home computer. He forgets to use the company's VPN when uploading the report. A hacker is sniffing the network traffic and is able to obtain the details of the contract. This is a breach of ***information security & cyber security*** i.e. confidentiality has been lost, *and the Internet enabled it.*

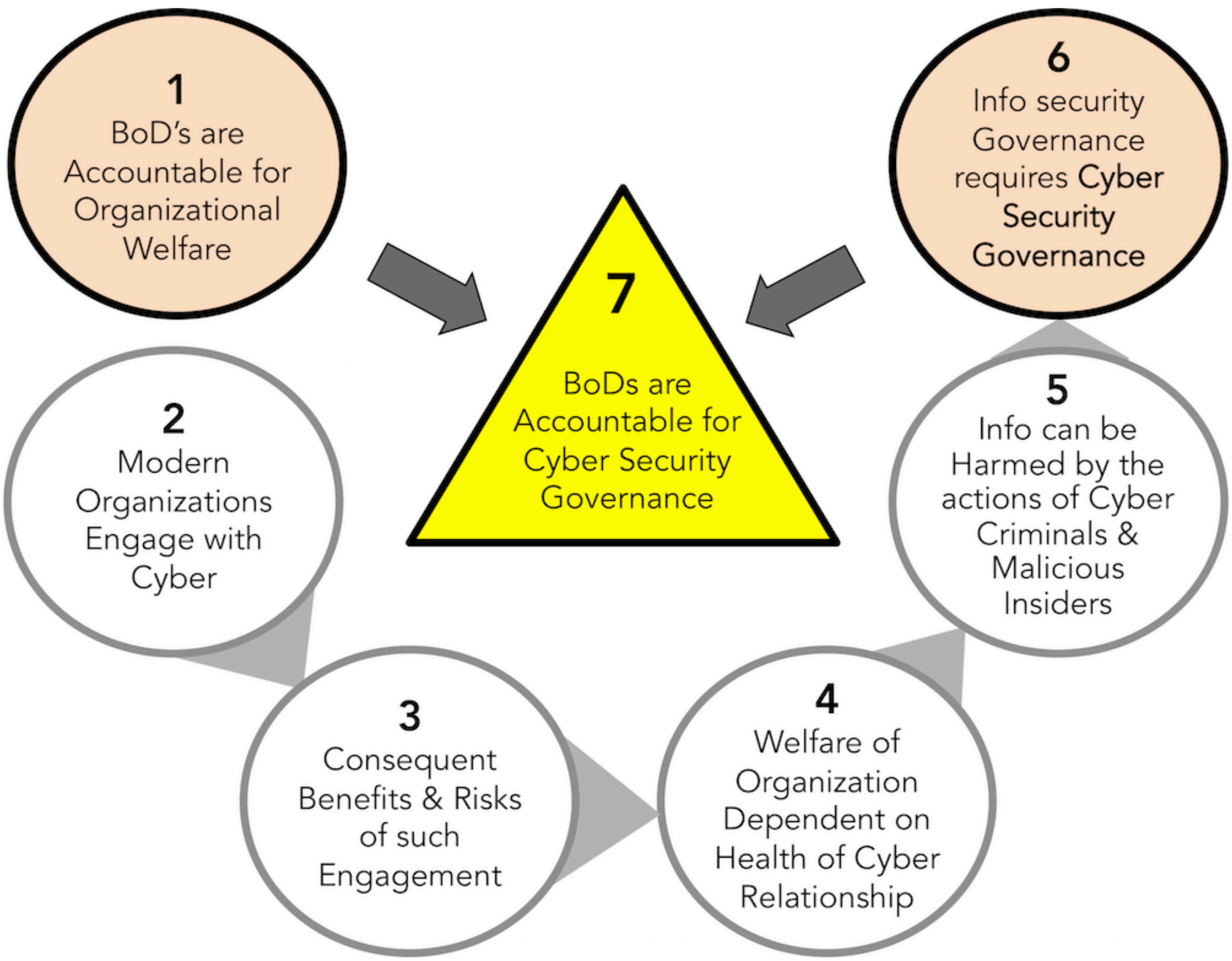
What Should Management Teams Do?

What decisions must be made to ensure effective cyber governance of information and who makes these decisions?

- Include a cyber expert on the management team.
- Establish an affiliated cyber security management committee with responsibility for overseeing and understanding the organization's cyber security state of play, and who reports to the board. They should:
  - ✓ Identify of all organizational assets, risks to the assets, and a recommendation to accept, avoid or mitigate these.
  - ✓ Monitor cyberspace for new risks.
  - ✓ Make recommendations on which standard cyber security mechanisms will be used to secure organizational information.
  - ✓ Make recommendations on actions that should be undertaken to pro-actively detect intrusions.
- Consider authorizing and paying for an annual penetration test by ethical hackers. Depending on the size of the organization, consider offering a bounty to hackers for finding vulnerabilities in the organization's cyber infrastructure.
- Consider taking out cyber insurance.
- Direct responsible bodies to formulate plans of action to address the risks, and refreshed annually:
  - ✓ A plan to direct breach responses and actions, should a breach occur, or retain an expert company to assist.
  - ✓ A business continuity plan to be implemented in the event of a natural disaster or cyber attack.

How will these decisions be made and monitored?

- Reports from the cyber committee should be a permanent agenda item.
- Ensure that the organization is spending adequately on cyber security; require such spending to be justified in terms of the risk that is being mitigated and the value of the protected asset.
- Oversee execution of plans of action: assign a board member to oversee each one, and to act as a board liaison to report on progress or to request and justify more resources if required.
- Due Diligence: stakeholder security practice:
  - ✓ Monitor the cyber security culture within the organization to ensure that the organization's employees understand that cyber security is not only a technology issue. Direct that regular awareness raising and training sessions be conducted within the organization.
  - ✓ Require reports from the organization's vendors (including software vendors) to ensure that their cyber and information security governance measures are adequate to protect the organization's information.



1
BoD's are Accountable for Organizational Welfare

2
Modern Organizations Engage with Cyber

3
Consequent Benefits & Risks of such Engagement

4
Welfare of Organization Dependent on Health of Cyber Relationship

5
Info can be Harmed by the actions of Cyber Criminals & Malicious Insiders

6
Info security Governance requires **Cyber Security Governance**

7
BoDs are Accountable for Cyber Security Governance

Boards and Management Teams are Accountable for Cyber Security Governance

ISO/IEC 27014. (2013), "ISO/IEC 27014:2013 (Information technology – Security techniques – Governance of Information Security)", available at: https://www.iso.org/standard/43754.html (accessed 11 April 2019).

Von Solms, B. and Von Solms, R. (2018), "Cybersecurity and information security – what goes where?", *Information and Computer Security*, Vol. 26 No. 1, pp. 2-9.

Renaud, K., Von Solms, B., Von Solms, R. (2019), "How does Intellectual Capital align with Cyber Security?" Journal of Intellectual Capital. To Appear

Prof Rossouw von Solms

Nelson Mandela
University, South Africa

Prof Basie von Solms

University of
Johannesburg
South Africa

Prof Karen Renaud

Abertay University,
Scotland

k.renaud@abertay,.ac.uk