Top of Form

Bottom of Form

**Unit 6: The Future of Information Risk Management**

**In this unit we shall:**

* + Discuss the trends that could contribute or determine the future of the information risk management (IRM) field.
  + Review the NSA ‘hard problems’ and discuss what contribution IRM has to them.
  + Create a wiki that contains answers to key questions about the future of IRM.

**On completion of this unit, you will be able to:**

* + Describe the major trends driving the future of IRM.
  + Enumerate the NSA hard problems and argue which are affected by IRM.
  + Contribute to the argument supporting your preferred influencing factor.

**Reflection:**

Information Risk Management, often known as IRM, is a technique of risk mitigation that uses policies, procedures, and technology to reduce the risk of cyber-attacks caused by vulnerabilities and poor data security, as well as those created by third-party vendors. Frequently, inadequate data security is the root cause of data breaches, which have major and negative effects on enterprises (Tayas Tunggal, et. al., (2022).

Information technology risk management programs are gaining importance as a component of an organization's overall risk management. This is true regardless of your level of risk tolerance. Several governments, notably the United States, have formed government organizations with the main aim of advocating for enhanced cybersecurity policy (Marks, et. al., (2019). The National Institute of Standards and Technology's (NIST) Cybersecurity Framework "provides a high-level taxonomy of cybersecurity goals and a methodology to assess and manage those outcomes." Due to new regulatory obligations, such as the General Data Protection Regulation (GDPR) and APRA's CPS 234, your company operations must include the proper administration of your information systems (Balbix (2020).

In collaboration with NSA Research, the Principal Investigators (PIs) of the Science of Security Lablets established the 5 Hard Problems as a means of establishing a common language and measuring progress in cyber security. These five were selected based on their level of technical complexity, their potential operational importance, and the prospect that they might benefit from a stronger emphasis on scientific research procedures and enhanced measurement capabilities (AdamT (2015). All these five problems are discussed below.

1. **Scalability and Composability:** Develop methods that enable the construction of safe systems with known security qualities from components with known security characteristics, without the need to re-analyze the constituent components in depth.
2. **Policy-Governed Secure Collaboration:** Develop approaches for describing and enforcing normative norms and regulations for managing data with diverse usage requirements and among users from different authority domains.
3. **Security Metrics Driven Evaluation, Design, Development, and Deployment:** Develop security metrics and models capable of predicting or validating that a given cyber system respects a certain set of security properties (deterministically or probabilistically), in each situation.
4. **Resilient Designs:** Develop methods for designing and evaluating system designs that can continue to provide critical services despite compromised components.
5. **Understanding and Taking into Account Human Behavior:** Develop models of human behavior (of both users and adversaries) that enable the design, modeling, and analysis of systems with specified security characteristics.

The future of risk management depends on the effective incorporation of such efforts into risk management to the point when comments such as the one above are no longer alarming (Martin, et. al., (2021)..

With data, analytics, and digital technologies, risk information is becoming more complicated and available to almost all businesses today. Despite this, it seems that the future contains something of far greater significance (Vashistha, (2021).

**References**

AdamT (2015). *Science of Security 5 Hard Problems | CPS-VO*. [online] cps-vo.org. Available at: <https://cps-vo.org/group/sos/hardproblems>. [Accessed 7 July. 2022].

Balbix (2020). *What is the NIST Cybersecurity Framework?* [online] Balbix. Available at: https://www.balbix.com/insights/nist-cybersecurity-framework/#:~:text=The%20NIST%20cybersecurity%20framework%20is [Accessed 7 July. 2022].

Marks, L. (2019). *The Optimal Risk Management Framework: Identifying the Requirements and Selecting the Framework*. [online] www.isaca.org. Available at: <https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-optimal-risk-management-framework-identifying-the-requirements-and-selecting-the-framework>.

Martin, D. and Koenig, D. (2021). *The Future of Risk Management*. [online] Available at: https://centerforfinancialstability.org/research/Risk\_Future\_022221.pdf [Accessed 7 July. 2022].

Tayas Tunggal, A. (2022). *What is Information Risk Management? | UpGuard*. [online] www.upguard.com. Available at: <https://www.upguard.com/blog/information-risk-management>. [Accessed 7 July. 2022].

Vashistha, A. (2021). *Council Post: The Future Of Risk Management Is Automated*. [online] Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2021/02/25/the-future-of-risk-management-is-automated/?sh=4c01da8f4ed0 [Accessed 7 July. 2022].