ACICE Issue 09/23 (September)

ACICE Monthly Digest

A monthly roundup of significant news around the world

ADMM Cybersecurity and Information Centre of Excellence

Cognitive Operations

Navigating Cyber Security with Decision-Making Models

- The increasing use of advanced technologies has led to a surge in cyberattacks, affecting both Information Technology (IT) and Operational Technology (OT) environments. Cyberattacks can result in dire consequences, including financial losses and severe reputational damage. Major cyber security risks include:

  A. Malware and Phishing Attacks

  Malware, which stands for malicious software, encompasses a wide range of harmful programs designed to infiltrate computer systems, steal data, or cause damage. Phishing attacks, on the other hand, involve deceptive emails or messages aimed at tricking recipients into revealing confidential information or downloading malicious attachments.

  B. Distributed Denial of Service (DDoS) Attacks

  DDoS attacks involve overwhelming a target system or network with a flood of traffic, rendering it inaccessible to legitimate users. These attacks disrupt online services and can result in financial losses and reputational damage.

  C. Insider Threats

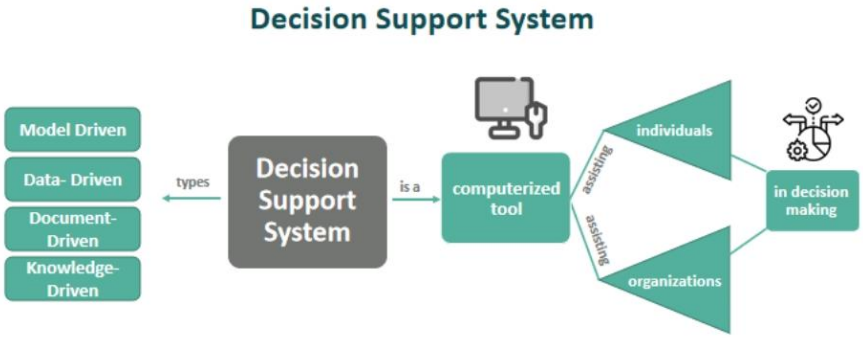
  Insider threats involve individuals misusing their access rights for activities which may harm the organisation's data integrity or confidentiality. These threats can be intentional through actions such as espionage or sabotage, or unintentional through individual negligence.

- To mitigate the damage caused by cyberattacks, it is important for incident responses to be based on timely and well-informed decisions using accurate data.

- Decision-making models in response to a cyberattack can be categorised into two main types: traditional methodologies and AI-based models. Traditional methodologies provide structured and systematic approaches to decision-making based on pre-defined rules and standard operating procedures (SOPs). Examples include signature-based anti-virus or rule-based intrusion detection systems, which rely on known patterns and signatures to detect threats. As such, they are less effective to counter zero-day exploits as these new vulnerabilities have not been previously configured in the detection systems.

- AI-based cybersecurity models, on the other hand, can identify behaviourial patterns rather than rely on predefined signatures. Examples include machine learning-based intrusion detection systems which analyse network traffic and detect anomalies, and threat intelligence models which analyse threat intelligence feeds. While AI-based models can provide a more proactive defence in detecting anomalies, they are also not immune to zero-day exploits. These cyberattacks may be designed to evade patterns that machine learning models are trained to pick up.

- Decision Support Systems (DSS) can address some of the limitations of AI-based and traditional decision-making models. DSS is a computerised information system designed to assist individuals and organisations in making decisions in complex and unstructured situations. It leverages the capabilities of AI-enabled techniques such as Bayesian Networks (BNs),[1] decision trees,[2] and neural networks[3], to merge the strengths of AI-based and traditional decision-making models.



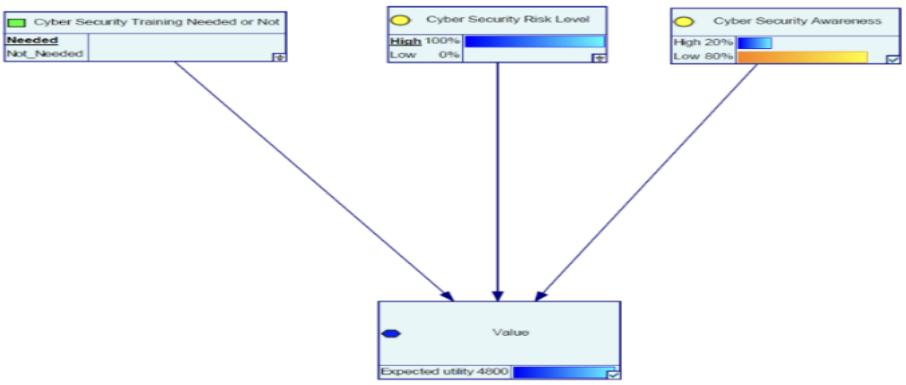
Workflow of a typical Decision Support System

[1] Bayesian Networks (BNs) refer to probabilistic graphical models used for reasoning uncertainties and probabilities in a wide range of applications. BNs are particularly useful for analysing complex systems with interrelated variables.
[2] Decision Trees are widely used machine-learning algorithms to visually represent decision-making processes. Decision trees are particularly useful for tasks involving classification and regression.
[3] A neural network is a type of machine-learning model inspired by the structure and functioning of the human brain's interconnected neurons.

- Among the DSS models, Influence Diagrams (IDs) provide simple visualisation systems to enhance decision-making process in complex and fluid situations, and circumvent the “black-box” problem of AI systems. While IDs were first created manually to map out decision-making scenarios, these IDs can be built into computer software to support the visualisation and analysis of the diagrams especially when the scenarios grow more complex.

- IDs have been used in decision-making in sectors such as agriculture, medical and military. In agriculture, IDs are used to optimise crop management decisions by considering factors such as weather conditions, soil quality, and market prices. In the military, IDs can be used for strategic planning and resource allocation in consideration of factors such as troop movements, equipment availability, and players’ capabilities in a broad spectrum of combat and non-combat operations. Qualitative influences such as geo-political tensions can be modelled by representing relationships between variables, factors and decisions without assigning specific quantitative values or probabilities.

- IDs, known for their adaptability and capacity to handle uncertainties, can also be applied to decision-making in cybersecurity crises. Firstly, IDs make it easier for cyber security professionals to understand and communicate complex concepts. Secondly, IDs allow for probabilistic modelling, enabling decision-makers to incorporate uncertainty into their assessments. Thirdly, cyber security-specific IDs can model various cyberattack scenarios and their potential consequences. This enables exploring of multiple "what-if" scenarios, helping organisations to be prepared for different types of cyberattacks.



Potential application of ID in cyber security training

- At the 22nd European Conference on Cyber Warfare and Security in June 2023, a research study shared on the potential application of IDs to cyber security. The above diagram was used to illustrate the application of ID in assessing the need for cybersecurity training in an organisation. The uncertainty nodes are *"Cyber Security Risk Level"*, and *"Cyber Security Awareness",* decision node is *"Cyber Security Training Needed or Not"* and the utility node is *"Value"*. The researchers provided example values to the Conditional Probabilities Tables (CPTs) of the uncertainty nodes and example utilities for different policies in the utility node. This ID can be used by managers to determine an expected utility when they decide whether or not to provide cyber security training. In this example, the expected utility value when they make a decision to provide cyber security training is 4800, whereas the expected utility when they make a decision to not provide cyber security training is 300. In this case, they can choose to provide cyber security training, which provides higher expected utility compared to the other choice.

- The application of IDs in decision-making can enhance cyber security resilience within organisations and nations. Effective modelling of cyber threats and vulnerabilities allows different players to collectively contribute towards a safer digital environment within a cyber security ecosystem. Moreover, governments and organisations can become more capable of countering cyber security threats when they train their workforce with the expertise to use IDs for accurate, relevant and timely decision-making in times of cyber security crises. Governments and organisations should look to enhancing decision-making in their cyber security strategies, so as to stay ahead of the fast-evolving cyber threat landscape.

Terrorism

Bomb Threat Hoaxes

- From 22 to 25 August 2023, there were alleged bomb threats at 18 locations around Singapore, including government buildings, embassies and other places of interest. These email bomb threats were sent under the name of "Takahiro Karasawa", stating that these bombs would be detonated.

- The bomb threats were eventually assessed by Singapore authorities to be hoaxes that had originated from an online movement aimed to harass Takahiro Karasawa, a Japanese lawyer, who rose to internet infamy in Japan in 2012.[4]

- Bomb threats emanating from this movement had previously targeted entities in Japan, the Republic of Korea (ROK) and Taiwan. Similarly, no explosives linked to the threats were found. The recent incident in Singapore marked the first of this series' threat messages in Southeast Asia.

- Subsequently, a similar threat message circulated in the Philippines from the same alias on 8 September 2023, of alleged bombs targeting the Metro-Rail Transit in Manila, which also turned out to be a hoax.

[4] In 2012, Takahiro Karasawa fought a court case in defence of Hasegawa Ryota, who was much hated by online users for slandering and abusing many behind his handle name of Yagama Taichi.

Annex

References

Cognitive Operations

1. Applying Influence Diagrams to Support Collective C2 in Multinational Civil-Military Operations
http://www.dodccrp.org/events/16th_iccrts_2011/papers/063.pdf

2. Towards Data-Driven Solutions to Interactive Dynamic Influence Diagrams
https://link.springer.com/article/10.1007/s10115-021-01600-5

3. Modelling Security of Power Communication Systems Using Defence Graphs and Influence Diagrams
http://www.sommestad.com/teodor/Filer/Sommestad,%20Ekstedt,%20Nordstrom%20-%202009%20-%20Modeling%20Security%20of%20Power%20Communication%20Systems%20Using%20Defense%20Graphs%20and%20Influence%20Diagrams.pdf

4. Probabilistic Risk Analysis and Terrorism Risk
https://www.dhs.gov/xlibrary/assets/rma-risk-assessment-technical-publication.pdf

5. Modelling Adversaries and Related Cognitive Biases
https://www.rand.org/content/dam/rand/pubs/reprints/2010/RAND_RP1084.pdf

6. Developing a Decision-Making Model for Security Sector Development in Uncertain Situations
https://ciaotest.cc.columbia.edu/journals/jssm/v6i2/f_0022147_18215.pdf

7. Probabilistic Warnings in National Security Crises: Pearl Harbor Revisited
https://www.semanticscholar.org/paper/Probabilistic-Warnings-in-National-Security-Crises%3A-Blum-Pat%C3%A9-Cornell/327cae768e030c08a87d219f89d4da8e5322a26d

8. Military Information Operations Analysis using Influence Diagrams and Coloured Petri Nets
https://catalogue.nla.gov.au/catalog/288444

9. Operations Research for Deterrence and Strategic Influence Analysis
https://irp.fas.org/agency/dod/dtra/or-deterrence.pdf

10. A Spatial Fuzzy Influence Diagram for Modelling Spatial Objects Dependencies: A Case Study on Tree-related Electricity Outages
https://core.ac.uk/download/pdf/161931997.pdf

11. Influence Diagrams in Cyber Security: Conceptualisation and Potential Applications
https://papers.academic-conferences.org/index.php/eccws/article/view/1303/1156

12. Artificial Intelligence in Cyber Security: Research Advances, Challenges and Opportunities
https://link.springer.com/article/10.1007/s10462-021-09976-0

Terrorism

1. Bomb threats at 18 locations including government buildings; police found no items of security concern
https://www.channelnewsasia.com/singapore/police-bomb-threats-18-locations-government-building-mse-environment-lockdown-scotts-road-3718856

2. No suspicious activities after hoax bomb threat hits MRT-3, says DOTr
http://www.cnnphilippines.com/news/2023/9/8/Alleged-bomb-threat-in-MRT-3-prompts-stricter-security-check-.html

3. South Korean embassy in Tokyo reports bomb threat
https://www.japantimes.co.jp/news/2023/08/14/japan/crime-legal/south-korea-embassy-threat/

4. Police probing bomb threat email for Seoul City Hall
https://www.koreatimes.co.kr/www/nation/2023/09/113_356970.html

5. Karasawa Takahiro
https://krsw-wiki.org/wiki/Karasawa_Takahiro

Contact Details

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence