CASE STUDY

CYBER COMMON OPERATING PICTURE (CCOP)

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

PROJECT SNAPSHOT

Our researchers are developing a dashboard for gathering, analysing and visualising cyber security data, to help executive leaders make swift and efficient decisions to protect their organisations.

WHO'S INVOLVED

This project was funded by the Cyber Security Cooperative Research Centre (CSCRC), in collaboration with ACTewAGL, Jemena, TCS, the University of Adelaide and CSIRO's Data61.

WHAT'S THE ISSUE?

Cyber attacks are becoming more frequent, sophisticated and targeted. They are often widespread and can go undetected, with criminals 'preparing a network' for extended periods in the lead up to an attack. This means that cyber security decision makers need to make faster, critical decisions to contain and mitigate cyber attacks.

To keep their companies safe, boards and executives need to understand complex data about cyber security. This presents a challenge. Unfortunately, leaders often struggle to make swift, effective decisions because they are unable to easily assess risks and view the security status of the entire organisation.

Our researchers are developing ways to simplify this complex data so business leaders can easily comprehend, assess and respond to cyber threats. The CCOP platform will help improve executives and managers understanding of vulnerabilities and potential attacks, based on the level of security in their respective organisations.

This tool is expected to allow leaders to interpret information more easily with less technical metrics, which will help them allocate resources, and map out an operations plan in response.

WHAT WERE THE OBJECTIVES?

- Examine the challenges businesses face when dealing with cyber security
- Determine understandable metrics and visualisations that leaders can more easily interpret
- Create a platform that can analyse real and potential cyber security risks in organisations and facilitate swift decision making for protection.

TECHNOLOGY DESCRIPTION

Our team is developing a prototype dashboard that captures and presents the current security status of an organisation's systems, services and networks for its security staff and decision makers, including senior management, through a set of metrics and related visualisations.

The security status presented by CCOP emerges from multiple cyber security information feeds, such as IDS (Intrusion Detection System) and SIEM (Security Information and Event Management) alerts, patching coverage, new critical vulnerabilities, and external sources of threat intelligence.

The focus is on making sure executive decision makers have the correct information readily available, in a format that empowers them to make informed decisions.