CYBERSECURITY: A RISING CONCERN WITHIN BROADCAST AND MEDIA ORGANISATIONS

Cybersecurity is a widely known and well understood concept within most industries with many companies having huge investments to safeguard their infrastructure and data from prying eyes and unauthorised access. These kinds of systems and approaches used to be normally associated with organisations which manage sensitive information and high security environments like banks and national security agencies. But with more and more organisations getting connected and providing online services this has now become a norm regardless of the industry and size of the organisation. Many broadcasters and media organisations are also providing content online and streaming services to its audiences now, and with the approach towards IP-based infrastructures and connected systems within broadcast facilities the need to safeguard these systems from cyber-attacks have risen.

In the past few years there have been many reported cases of cyberattacks to media centric entities with these organisations incurring huge losses financially as well as credibility. Some of these attacks are directed at hindering running operations, disrupting services, some completely hijacking on-air channels and asking for ransom or propagating unauthorised messages, while others just steal valuable content and data. Although most of reported cases of major attacks have been within Europe and Americas, recent studies suggests that the Asia-Pacific region is now becoming a target. A recent study published by IBM noted that Asia is now the #1 target for cyberattacks representing 26% of attacks analysed in 2021. This data showed a significant regional shift compared to the past decade and signals the growing need for security investments within organizations in the region.

It is paramount that organisations understand that cyber threats are real, it is not a hoax or thinking that it would not affect your network, or your devices is to be very naive. Understanding the accepting that this is a real threat is the first step to move forward. There is a huge need to educate broadcasters and media organisations about cybersecurity and its dangers. Noting this, the ABU Technical Committee has setup a study group that has taken up the task of following developments in this area and to educate and update the members on these developments. In addition to these reports the ABU has supported and issued three recommendations related to Cybersecurity and Media. These are the result of collaboration with the World Broadcasting Union's Technical Committee (WBU-TC) where the studies and work conducted by our sister unions NABA (the North American Broadcasters Association) and the EBU (European Broadcasting Union) has been very beneficial.

These recommendations are part of the ongoing efforts to inform and educate member broadcasters and to help them with the steps that needs to be taken in order to strengthen and safeguard their systems from potential cyberattacks. All these recommendations are widely available to all our members from the WBU and the ABU websites.

In addition to these recommendations ABU Technology have addressed the topic of cybersecurity within its workshops, conferences and symposia in recent years. These have seen growing interest from members and the recently organised Virtual Forum on Cybersecurity and Media was one of the most attended webinar series early this year. This shows the importance broadcasters and media organisations are giving to learn about this growing threat. Following is a quick look and the topics and discussions from the aforementioned forum.

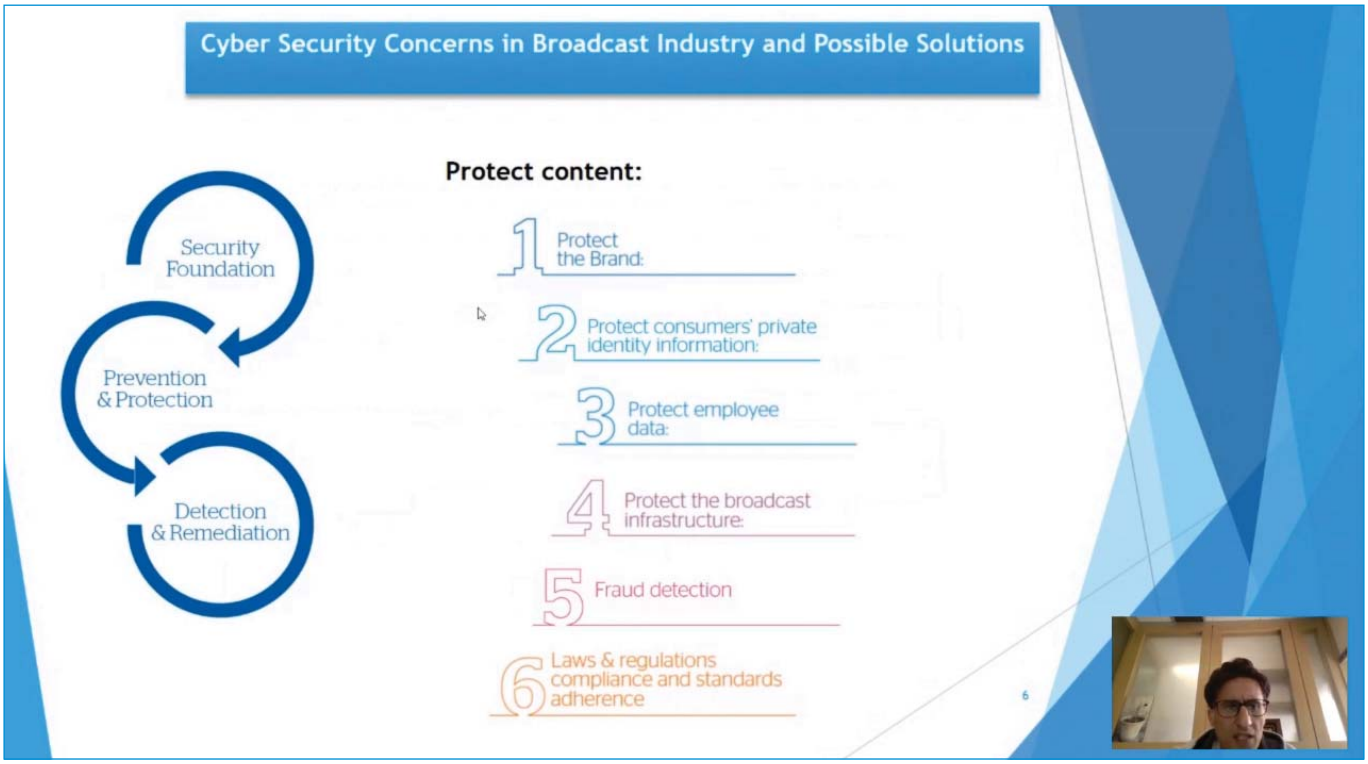
ABU VIRTUAL FORUM ON CYBERSECURITY AND MEDIA – 24-25 MAY 2022

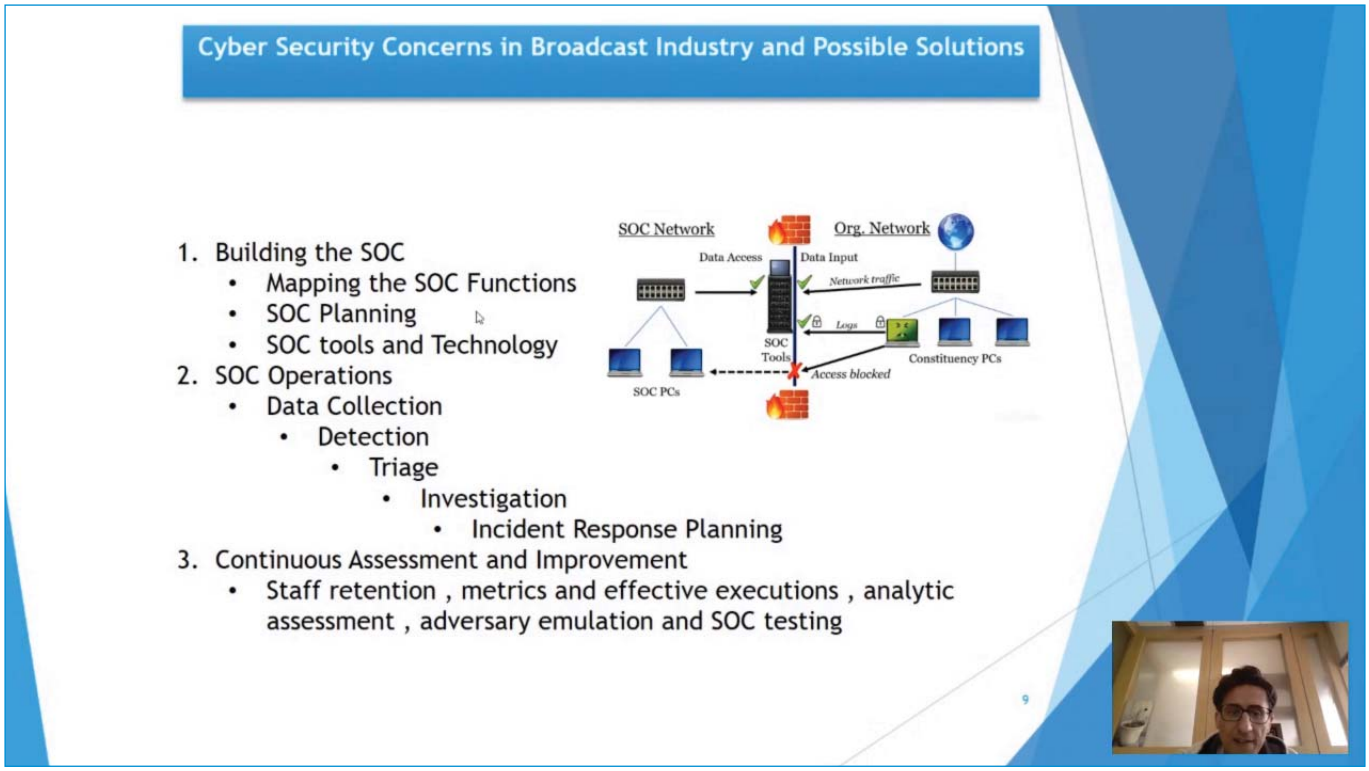
ABU Technology hosted a Virtual Forum on Cybersecurity and Media from 24 to 25 May 2022. The Forum discussed the latest tools, technologies, and best practices to mitigate cyber related risks in the media industry. Experts from IRIB in Iran and Skyline Communications in Germany and a Senior Broadcast Engineer in Australia shared their recommendations and experiences to further strengthen and safeguard broadcasters' networks from potential attacks. More than 600 registrations were received to join the multi-topic sessions and close to 250 participants, representing 40 countries from Asia, Europe, and Africa, attended the Forum over the 2 days.

CYBER SECURITY CONCERNS IN THE BROADCAST INDUSTRY AND POSSIBLE SOLUTIONS – EMAD NASEREDDIN, IRIB-IRAN

The traditional media value chain has been disrupted, enabled by the Internet and mobile connectivity. Content is now expected to be delivered anytime, anywhere and on any platform. Likewise, broadcasters are switching from SDI to IP and broadcasting and IT domains are converging. This sounds simple but, in fact, may be deceptive security-wise. As the content flows through the broadcast chain, it is essential to overcome the challenges for broadcast media in terms of security concerns. For this, the standard IT processes and architectures must be properly adapted. Furthermore, these should be deployed to meet the specific requirements of broadcast applications and operations in terms of service levels, reliability, business continuity and security.

To start with, where and how to secure the broadcast





media sector, the first and foremost step is to set up a solid security foundation covering the end-to-end broadcast media production chain. There is no need to reinvent the wheel, but just to follow best practices coming from the IT world. Examples of such practices are CIS TOP20, NIST, COBIT, ISO-27000, DPP, CDSA, MPAA, EBU Cyber security policies etc.

Three levels of protection envisaged are, security foundation, prevention and protection, detection and remediation. Security foundation ensures protecting content, brands, consumer information, and infrastructure along with fraud detection by keeping compliance with, and adherence to, laws and regulations. Prevention and protection is meant to build a cybersecurity culture and develop end to end cybersecurity strategy. Likewise, digital surveillance, proactive detection, 24/7 monitoring etc. are the measures taken for detection and remediation.

To help with such protection issues, building the security operation centre (SOC) will be another important step. It takes account of mapping the required functions, planning, and using proper tools and technology. SOC operations include works for data collection, triage and incident response planning with continuous assessment and improvement. SOC operates in different tiers for security analysis, incident response, support and threat intelligence.

Attackers will use different tactics to get what they want, such as phishing, supply chain attacks, site cloning, ransomware, wiper malware, rootkits, worms, DDOS, scripting, credential theft etc. SOC identifies, minimises and remediates incidents with the use of detection, triage and incident response tools based on the threat level and environment data from network and endpoint events. Network and endpoint collection and detection technologies are available that may be event or alert focused.

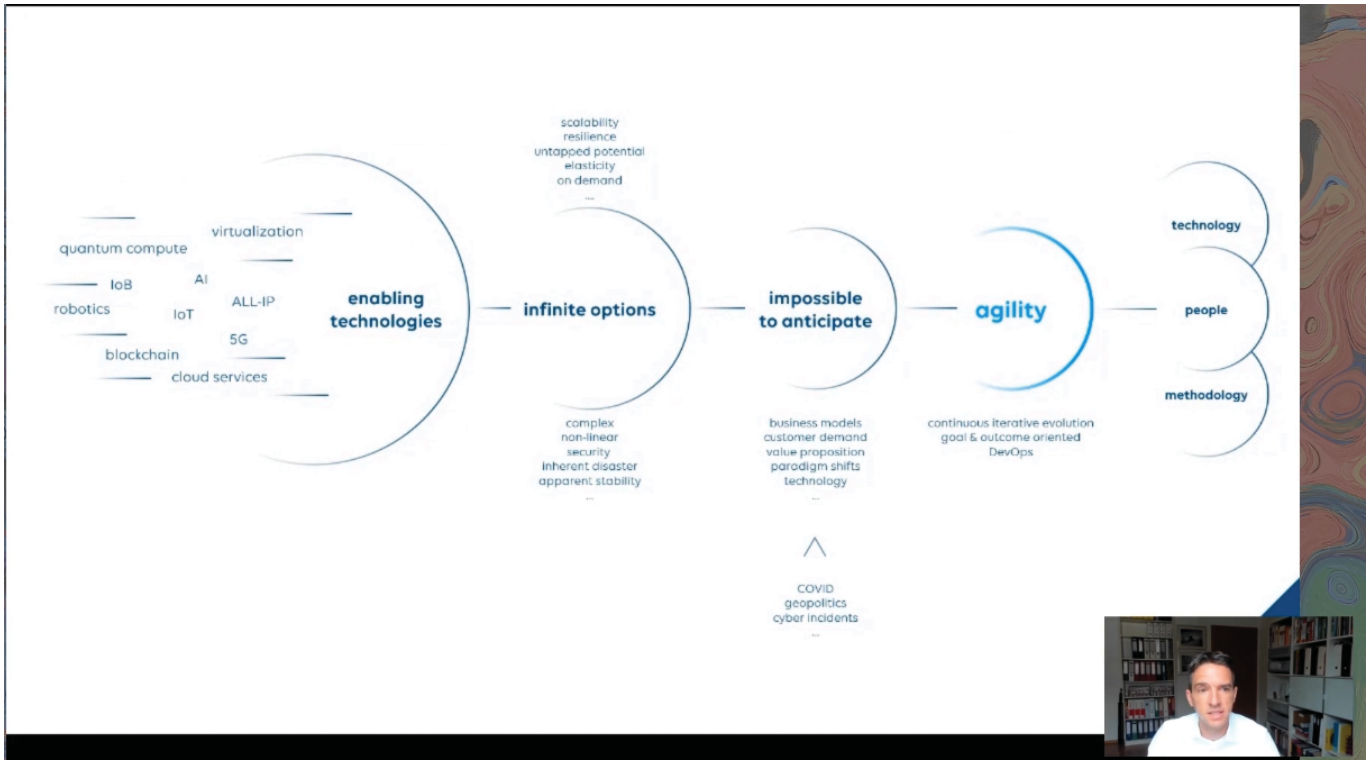
Security information and event management (SIEM) is another most important SOC tool for centralised log search, data correlation and alerting, visualisation and reporting for any cyber security incidents. Open source host and network data collection tools are available in the market. Network data monitoring takes place at different OSI layers using diverse service logs or tools. Host data monitors who is logged in, what is running, what tasks are presented etc. using security tools.

A 'blue team' in the SOC work to protect the organization's critical assets against any kind of threat with standardization of attack descriptions. Common tools and standard for attack techniques and protection practices are MITRE ATTandCK, Yara, Sigma, Jupyter etc.

DIGITAL TRANSFORMATION IN THE MEDIA BUSINESS-EVOLVING TOWARDS AN AGILE-DRIVEN OPERATION – THOMAS GUNKEL, SKYLINE COMMUNICATIONS

For transforming a company into digital, cybersecurity component has to be embedded upfront. Technologies are evolving, industry is moving to all-IP and adopting other enabling technologies. DevOps help to run such digital transformations and allow to operate diverse workflows and agile operation. Scalability, resilience, elasticity and on-demand operations are the benefits on one hand; non-linearity of behaviour, apparent instability, security issues etc. are to be looked into on the other hand. Becoming agile and continuing business with security is a must.

DevOps is the combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity. It enhances evolving and improving products at a faster pace than organizations using traditional software development and infrastructure management processes.



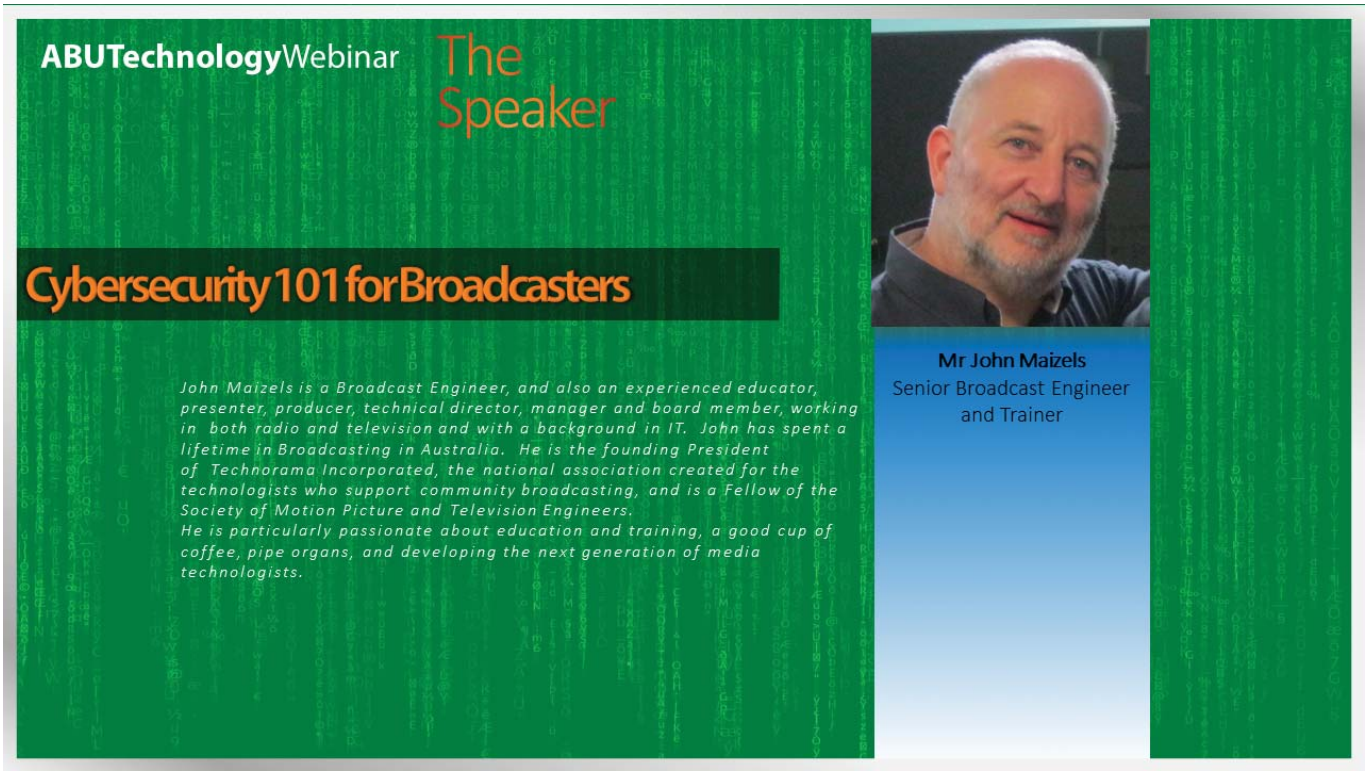
This is the key to success in a data-driven future.

DevOps is an absolute must in the new emerging ICT media and broadband segment. It enables you to continuously deliver incremental value to your business in the most efficient manner. It multiplies your return on the existing infrastructure investments. Requirements for agile transition are transformational technology, flexible architecture and agile culture/mindset. In concise, you need people with right technology and agile mindset. Broadcasters need to position them to evolve easily, safely securely and continuously.

An instance of DevOps solution, DataMiner, has three components. Data collection and control plane at the foundation layer collects files and data from anywhere agnostic to any technology. The digital twin function supports reading and controls. On top is the data consumption in the form of visualization, monitoring, automation, or orchestration. Third party tools as well may be employed here. Its stack functions incorporate multiple components including security and cloud service functions. This solution represents powerful out of the box utilisation of data and unified secured interfacing with Third party consumers or controllers. With open architecture, it allows customising connectors, automation and orchestration for interfacing customer dashboards with visual overview.

Skyline delivers the technology, people and methodology, in a consolidated and highly integrated ecosystem. The ultimate goal is to make digital transformation a success, and to establish an agile operation ready for a data-driven future, enabling a company to evolve continuously. DataMiner Dojo Community is a community for ICT media and broadband transformation for sharing knowledge and expertise.

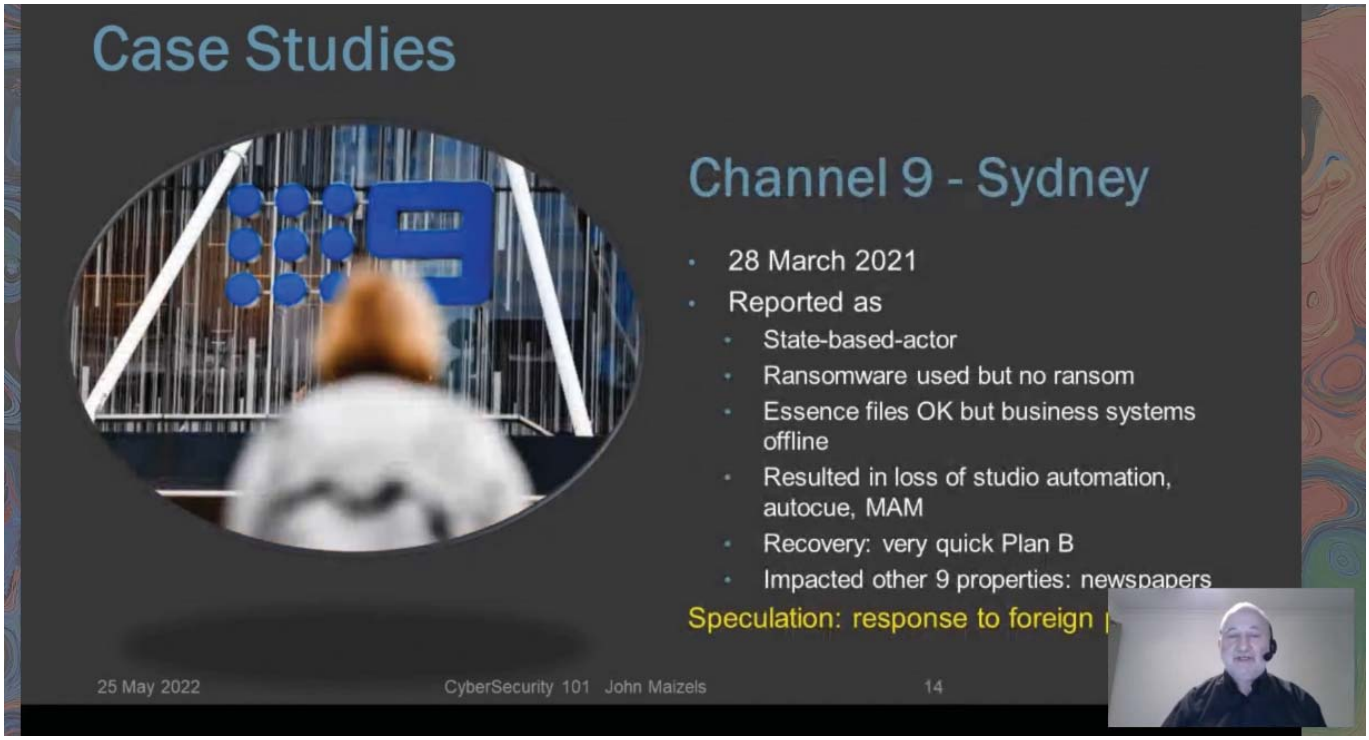
CYBERSECURITY 101 FOR BROADCASTERS – JOHN MAIZELS, SENIOR BROADCAST ENGINEER AND TRAINER



Cyber Security has recently become a fact of today's life in the connected world. It is not going away, and can't be disregarded, at least by broadcasters, media industry and regulatory agencies. So, we have to learn to live with it.

Getting caught in a cybersecurity storm or being attacked can have extensive consequences. For public organisations like broadcasters, losses in business and credibility, or warrants for proactive and reactive behaviours if one is not prepared in advance. And it may happen that these lessons are not learned, and mistakes are repeated. Cybersecurity shouldn't be seen as a business cost, but as a business investment with top priority. There are different reasons for attacks, not always obvious, be they for ransomware, opportunism or just for recreational mischief. Some hackers have criminal motives, for profit and theft and other unseen reasons.

A few case studies are worth mention. The attacks on TV5 Monde, Channel 9, for example. TV5 Monde in



France was attacked in 2015 and service disrupted across 21 channels for 18 hours. The goal apparently seemed to be sabotage and resulted in significant business impact for months, with huge cost over the four years it took to fully recover. Likewise, a recent attack occurred in March 2021 on Channel 9 in Sydney.

This resulted in the loss of its studio automation and MAM system, and also impacted its other 9 properties, including newspapers. The station recovered with a quick 'Plan B' resuming service from a station in another state on a different IT network. Other instances of cyber-attacks occurred to KQED station and an FM station in the US, and to Marketron, an advertising provider.

Attack vectors will take different forms, like steganography, i.e., hiding messages inside other objects, fake emails with social manipulation, and products of false trust.

Suggested approaches for recovery from such attacks may include having a solid 'Plan B', assembling a CIRT team, having mitigation strategies, building a security operations centre (SOC) with different colour coded teams etc. Keeping corporate and broadcast networks segregated, separating IoT devices from business/broadcast LANs, using proxy connections will indeed augment broadcaster's network. Revisiting and reviewing these approaches often and testing or triaging will keep stations less exposed to attack. ■