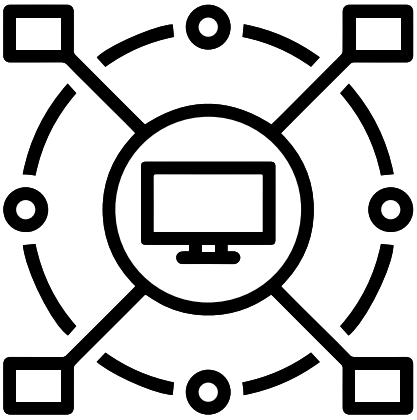
LORCA NEEDS ACCELERATOR: MEDIA

LORCA

LIKE MANY INDUSTRIES, MEDIA ORGANISATIONS NEED TO PROTECT THEIR INTELLECTUAL PROPERTY.



The media industry is particularly vulnerable to malicious activity on their network”

Like many industries, media organisations need to protect their intellectual property, comply with an increasingly complex regulatory environment and retain their readers’ trust. But, unlike other industries, they can be the target of state-sponsored attacks with geopolitical objectives.

At the same time, remote teams using unsecured devices, the use of legacy hardware and complex supply chains are making the media vulnerable to leaks and attacks through a range of entry points.

To understand the nature of the most pressing challenges facing the sector, LORCA brought together cybersecurity experts, members of our accelerator programme and some of the most influential decision makers in the media.

HELD UNDER THE CHATHAM HOUSE RULE, OUR DISCUSSION UNVEILED A RANGE OF INSIGHTS, CHALLENGES AND OPPORTUNITIES.

01

Organisations are vulnerable to malicious activity on their network, but many haven't got the tools and resources they need to stay secure

02

Media organisations find supply chain security a challenge

03

The media is a target for geopolitical threat actors, making it vulnerable to disinformation campaigns or supply chain attacks

04

Legacy hardware is widespread and isn't being replaced any time soon

05

Intellectual property protection is a top priority

06

Remote teams and shadow IT poses a security threat

ORGANISATIONS ARE VULNERABLE TO MALICIOUS ACTIVITY ON THEIR NETWORK, BUT MANY HAVEN'T GOT THE TOOLS AND RESOURCES THEY NEED TO STAY SECURE.

Some of the largest media organisations use a large and complex network of computers. But the tools and resources they use to monitor network traffic have not advanced at the same pace as their other capabilities.

At the same time, the media industry is particularly vulnerable to malicious activity on their network. For some organisations, their entire revenue is dependent on an asset that's secured through IP protections. If that IP is circumvented – for example a copy of a movie is stolen before its official release date – then their revenue is directly affected.

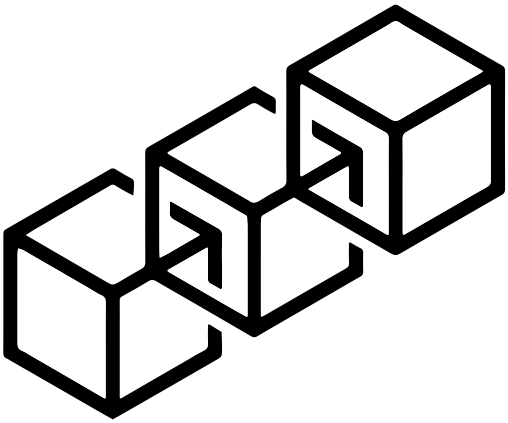
To secure their IP, media organisations require tools that can analyse a large volume of network traffic in real time as well as quickly and correctly identify threats that require action. The media sector has a unique network activity profile and the parameters of what good and bad activity looks like in other sectors can't be applied. This means there's a need for solutions that can learn and adapt to unique network activity profiles.

There are some solutions like this already, but they have their limitations. For instance, existing machine learning solutions learn the unique network activity profile of an organisation and immediately block irregular activity. But they require separate devices for each segment of the network and produce many false positives. If media organisations used a solution like this, data would have to be integrated across a geographically dispersed network and operations would be frequently interrupted by false positives.

Participants spoke of a need for solutions that can monitor network activity and traffic data on an enterprise scale while providing qualitative analysis of what good and bad activity looks like in a unique network activity profile. For example, if there's a surge in traffic it's important to know whether it's likely to be benign or indicative of a threat that requires action.

> *"While media organisations are investing in their own cybersecurity practices to protect this information, being confident in the security practices of third parties is more challenging."*

MEDIA ORGANISATIONS FIND SUPPLY CHAIN SECURITY A CHALLENGE.



Valuable data, including intellectual property and commercially sensitive data, moves through a media organisation's supply chain, which can include printers, sound studios and production companies. While media organisations are investing in their own cybersecurity practices to protect this information, being confident in the security practices of third parties is more challenging. These supply chain security challenges make media organisations vulnerable to attacks or leaks.

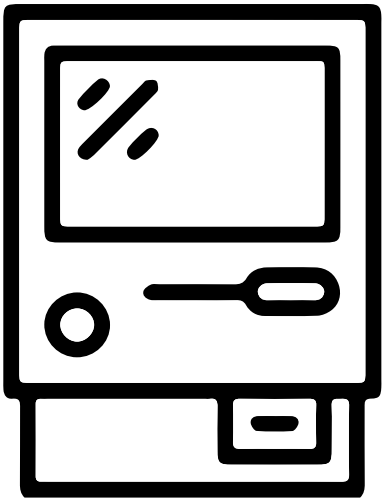
Cyber attacks on sound studios are an example of this, where malicious actors have leaked a television series to the public before the release date. The use of enterprise-grade cloud solutions by the media (which are favoured because they're scalable, flexible and cost-effective) also adds risk and complexity when cloud providers use third-party vendors.

THE MEDIA IS A TARGET FOR GEOPOLITICAL THREAT ACTORS, MAKING IT VULNERABLE TO DISINFORMATION CAMPAIGNS OR SUPPLY CHAIN ATTACKS.

News organisations are a target for geopolitical threat actors who want to disseminate disinformation or degrade trust in the media, which is often a source of soft power for nation states.

Participants discussed common tactics, including targeting third parties (such as printing services), SMS phishing attempts, creating imitation websites or skewing the conversation in a comments section using bots. They spoke of the importance of protecting the integrity of the data they hold and the online conversations taking place.

LEGACY HARDWARE IS WIDESPREAD AND ISN'T BEING REPLACED ANY TIME SOON.

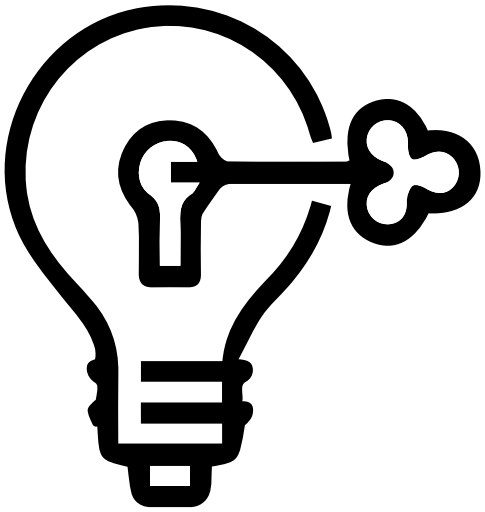


Using legacy hardware makes it more likely that a cyber attack will be successful, often because the hardware isn't compatible with new features like multi-factor authentication or its security flaws are publicly known. One participant spoke about the hiring of broadcasting hardware for an election night programme, which "frightened the life" out of him because of the sheer volume of equipment and the lack of understanding of its security features or vulnerabilities.

Legacy operational technology (OT) presents a particular challenge for the media industry. This is because legacy OT is either the industry standard for certain media functions or its preferred by industry professionals who aren't aware of the security risks.

This means that replacing, deprecating or restricting legacy hardware isn't always practical for the media and the sector requires an innovative solution that can mitigate the risks of its OT assets.

INTELLECTUAL PROPERTY PROTECTION IS A TOP PRIORITY.



Protecting IP is a priority for media organisations and there's demand for solutions that directly protect sensitive data and IP.

Participants expressed an interest in new technologies that allow the user to attach protections directly to their IP using technologies like blockchain. For instance, new smart contract solutions enforce licence agreements, and solutions such as GoChain can register IP rights in a decentralised ledger.

With threats to IP becoming increasingly sophisticated, the development of innovative and specialised solutions will be critical to the cybersecurity of media organisations.

REMOTE TEAMS AND SHADOW I.T POSES A SECURITY THREAT.

Journalists are a law unto themselves and it's not for us to mandate what they use"

News organisations often have teams spread in multiple locations, many of whom work on a freelance and autonomous basis for more than one media company at a time as newsroom budgets shrink. Protecting these remote teams from hostile actors seeking to steal data or threaten a journalist's personal safety is a particular challenge.

Meanwhile, the use of shadow IT by journalists is widespread (for example, journalists often use local mobiles and multiple SIM cards in foreign territories). Shadow IT transmits data outside of the centralised IT infrastructure, meaning that attackers targeting the main infrastructure can't access it.

However, shadow IT doesn't always meet an organisation's security standards or adequately protect the data (in the case of unsecured mobile devices). In fact, one participant said it was "impossible to vet all tools being used" and they didn't actually think it was the role of the CISO to dictate which tools a journalist could or should use when dealing with sensitive sources such as whistle-blowers. "Journalists are a law unto themselves and it's not for us to mandate what they use," the participant said.

This presents a challenge for CISOs in this industry: employees favour shadow IT because it protects them in the field, but it also makes it harder to manage a sprawling IT infrastructure. Journalists also want to be visible online and contactable – something CISOs have to accommodate.

Corporate-grade security tools provide some security, but remote teams don't always find them easy or practical to use in the field. There's a distinct need security tools created with the end user in mind to help them practice good cyber hygiene.

CONCLUSION: THE OPPORTUNITIES FOR INNOVATORS.

They're calling out for security solutions that can empower the end user"

In many ways, the media faces many of the same challenges as any industry: BYOD policies make the CISO's life harder, complex and digital supply chains add risk, and they find it hard to gather actionable insights about network activity to prevent teams from chasing false positives or missing significant threats. But there are also many unique security challenges.

Remote teams are operating in high-risk situations and acquiring sensitive information – a media organisation's prized intellectual property. CISOs accept that these remote teams will inevitably use tools that aren't on an approved list, and they're calling out for security solutions that can empower the end user – the freelance journalist – to practice good cyber hygiene.

The media is also being caught up in geopolitically motivated attacks that threaten online debate and intellectual property. At a time when many organisations are competing for paid subscribers, it's essential from a reputational point of view that they retain people's trust and protect the valuable intel their journalists gather.

And cyber innovators should also note the challenges faced by the media when it comes to securing legacy hardware. While digital technology has changed the way the news is produced and consumed in many ways, media organisations are also reliant on a huge amount of legacy hardware that's keeping CISOs awake at night.

CONNECT WITH US

lorca.co.uk
info@lorca.co.uk

Twitter: @LORCACyber
LinkedIn: LORCA Cyber

FIND US

Plexal, The Press Centre
Here East, 14 East Bay Lane
Queen Elizabeth Olympic Park
London, E20 3BS

LORCA