WPP license no. MR/TECH/WPP-82/North/2018 License to post without prepayment Postal Registration No. MCN/99/2018-2020
Published on 3rd of every month. Posting date: 5th & 6th of every months Posted at Patrika Channel Sorting Office, Mumbai-400001
Registered with Registrar of Newspapers under RNI No. MAHENG/2009/33418

Total number of pages 56
Vol. 10 | Issue 03 | MARCH 2018 | ₹ 50

digitalstudio

BROADCASTING AND PRODUCTION IN INDIA

SAFE & SECURE

Being prepared with layered security systems and detailed protocols is one of the best ways to protect valuable content

BY BINDU GOPAL RAO

Broadcasters and media companies are delivering content across various platforms and are increasingly transitioning towards IP-based delivery services. This has made them vulnerable to cyber breaches, attacks and theft. So how are they safeguarding their networks, protecting their precious systems, data, IPR and customer information from these attacks?

As evidenced by an increasing number of high profile attacks that have wreaked havoc on the segment, it is clear that the media and entertainment industry has become a prime target for cybercrime. Security concerns facing the industry as a whole include valuable client assets being compromised and held ransom such as the 2016 attack on Larson Studios, where hackers demanded $50,000 in return for stolen content.

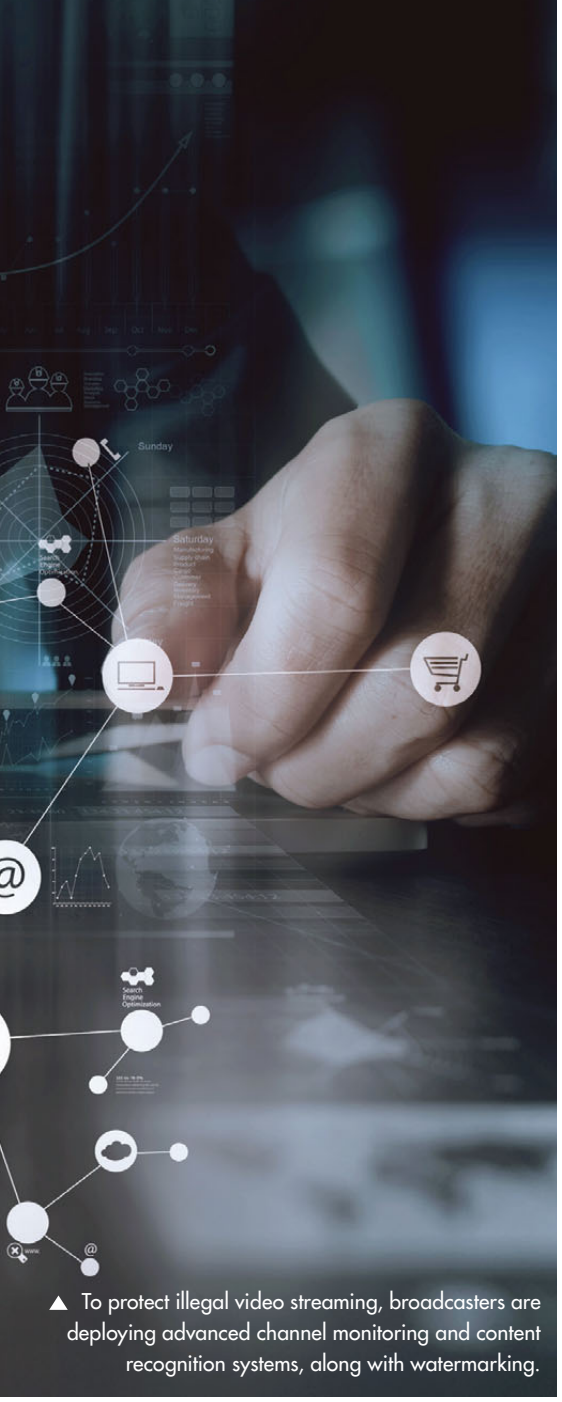
Also of threat is a company's internal confidential documents being leaked, as witnessed by the 2014 hacking incident at Sony Pictures. Hackers stole an estimated 10TB of data and assets from Sony Pictures and leaked three unreleased movies, a script for James Bond Spectre and personal information and emails from countless Sony employees.

"The damages included Sony co-chairperson Amy Pascal's career, a heavily-damaged IT infrastructure and millions of dollars in civil damages," recalled Peter Lambert, sales director, EditShare. Illegal redistribution of broadcast content continues to grow rapidly around the world. It is a very serious threat to the revenues of broadcasters and rights owners, especially with respect to premium live sports and entertainment content.

SAFETY MEASURES

Compliance with evolving security best practices is expected to ultimately become become big stakes for doing business in the media and entertainment space. Even today, audits against these best practices are becoming more common as part of the selection process for service provider partners.

The globally governing Motion Picture Association of America (MPAA) and the Content Delivery and Security Association



▲ To protect illegal video streaming, broadcasters are deploying advanced channel monitoring and content recognition systems, along with watermarking.

Globally, the TV industry loses an estimated $28 billion in revenues due to piracy. Of that, $7 billion could be recaptured if effective anti-piracy actions and legitimate offerings were put in in place.

Source: 2017 global Pay-TV Innovation Forum research

(CDSA) advocate for a multi-layer approach spanning management, personnel asset management, physical access, IT security, training, incident management, workflow and script handling. To protect their content from illegal video streaming, broadcasters are deploying advanced channel monitoring and content recognition systems, along with watermarking for advanced subscriber level identification.

"The latest watermarking technologies are completely invisible to viewers, and comply with the security requirements of premium sports rights holders and movie studios. Importantly, the watermarking can identify any subscribers leaking content in seconds to allow rapid termination of content theft," said Neil Sharpe, product marketing director, Friend MTS.

Key elements of the network access layer include WAN security (firewalls, etc), Internet security (antivirus, etc), network access, authentication and account management and I/O management. "The management layer focuses on the organisation and management of the facility. It could span management policy, risk management and incident response, business continuity and disaster recovery, workflow, segregation of duties, employee hiring practices and how to engage with third parties. The physical layer focuses on the mechanisms and practices that prevent unauthorised entry to your facility. A comprehensive network access layer will focus on the mechanisms and practices that manage who has access to your video production infrastructure and the assets it provides access to," added Lambert.

PRIVACY MATTERS

Unlawful distribution of premium content is a growing concern for content owners and platforms and companies are using various tools to deal with this threat. K Yegneshwara Iyer, VP and head of technology, Times Network explained, "We take care to continuously educate our users on best practices to handle all content and on the legal, financial, goodwill and operational consequences of mishandling content. We also put reasonable restrictions on access to content in a shape and form that could be exploited to our company's detriment. This could be as simple as denying access to people who don't need the access to allowing only low-resolution access to premium content or allowing delayed access to content – once it has passed its use-by date."

Broadcasting companies, typically, work

"IN THE PAST, SECURITY EFFORTS WERE FOCUSED ON CREATING BARRIERS PREVENTING ACCESS TO MEDIA ASSETS. HOWEVER, AS CYBER CRIMINALS HAVE FOUND WAYS AROUND THESE, THE FOCUS HAS SHIFTED TO FILE AUDITING TO PREVENT INTERNAL AND EXTERNAL THEFT." **– PETER LAMBERT, SALES DIRECTOR, EDITSHARE.**

in an open internal environment that is not immediately conducive to tight security measures. In an industry that is constantly working under time pressures, imposing security workflows is seen as affecting business deliverables. Consequently, internal risks are higher than external.

Broadcasters are generally able to secure their external perimeter but are less successful when it comes to creating internal fences. This leaves them open to potential insider attacks. However, this is not unique to the broadcasting business alone, but is applicable to other industries as well.

"In broadcasting, however, the ease of transporting data and media in the modern world means that the risk of breaches and leakages is higher. In broadcasting, as in other industries, ample solutions exist to protect and safeguard media and other data assets. The biggest challenge in broadcast is the workflow and the perceived efficiency reduction brought on by lockdowns of access on a need-to-have basis," Iyer pointed out.

TECH TALK

In the security industry, it is well understood that some security events can be more easily detected through correlation of separate events occurring on different systems throughout the facility. For example, it may be possible to detect unauthorised media asset access via file moves in a storage server combined with file copies to removable storage device such as a USB. Solutions supporting this approach are called Security Information and Events Management (SIEM) systems.

"To harness the power of SIEM in your video production facility, it is important to choose media production elements that are capable of forwarding file audit logs to third-party systems. These systems provide centralised collection of file audit log data as well as log data from switches, routers, firewalls and other elements of the IT infrastructure. They also normalise the data so that it can be stored efficiently," explained Lambert.

SIEM systems also provide the capability to look across individual files and correlate events to more precisely identify specific events and threats. Once detected, SIEM systems are capable of notifying responsible parties so that an immediate response can be mounted. The broadcasting sector is challenged in the application of many standard IT technologies due to the kind of workflow and processes that have evolved.

Identification of content is extremely difficult. Unlike a PDF or any other office document, media - both audio and video can be cut up and bits and pieces used making tracking much more difficult. While it is easy to restrict access to media, once access is provided, tracking usage is a tedious, expensive and impractical solution.

"Restrictions are imposed on users' ability to copy material on non-authorised media like external hard disks. The ability to upload or FTP is also restricted from end-points where media is accessible. Ideally, broadcasters would like fingerprinting every distinct frame of media, which could, then, be tracked throughout its lifecycle. But, that will require all systems to come on a common platform to share tracking information," said Iyer.

CLOUD CONTROL

That modern, collaborative production workflows owe a great deal to the use of file-based content shared on enterprise-wide and cloud-wide networks for their efficiency is undeniable. But equally indisputable is the fact that as workflows transitioned from tightly-guarded tapes to enterprise-wide and worldwide cloud-based networks, the exposure to exploitation; the 'threat surface' in security speak, has grown exponentially.

With new broadcast workflows and the growth in OTT platforms, there is a greater potential for content redistribution because many of the OTT apps have an insufficient level of security to prevent content redistribution. "To provide end-to-end security, it is essential for broadcasters and platform operators to address content protection across set-top boxes and OTT apps, using a unified, watermarking based approach to security," averred Sharpe.

Motivated by the value of the content being produced, pirates seek to exploit vulnerabilities in lax studio operations as well as the closely associated and often interconnected ecosystem of post-production service providers. "Preparedness with layered security systems and protocols is one of the best ways to protect valuable content in the era of cybercrime. In the past, security efforts were focused on creating barriers preventing access to media assets. However, as cyber criminals have found

▲ Through IOT you can automate many of these mundane tasks remotely. With this attractive global exchange comes the risk of hacks.

ways around these, the focus has shifted to file auditing to prevent internal and external theft," said Lambert.

NET FIX

Cloud workflows for broadcast are still maturing. Many processes like second copies, multiple-GPU based tasks among many others are good candidates for cloud workflows and are being adopted at pace. However, security of data in transit, security of data at rest in a third party data centre and the chances of data loss and the potential for recovery after a loss are all variables today.

Controlling security of cloud-based workflows needs to be approached much the same way as one would approach internal

"IN BROADCASTING, AMPLE SOLUTIONS EXIST TO PROTECT AND SAFEGUARD MEDIA AND OTHER DATA ASSETS. THE BIGGEST CHALLENGE IS THE WORKFLOW AND THE PERCEIVED EFFICIENCY REDUCTION BROUGHT ON BY LOCKDOWNS OF ACCESS ON A NEED-TO-HAVE BASIS."

K YEGNESHWARA IYER, VP AND HEAD OF TECHNOLOGY, TIMES NETWORK

workflows. It is important to consider cloud resources as an extension of internal processes and apply appropriate controls of access and data protection at every step of all workflows.

MAKING THE CONNECTION

Broadcasters should be aware of risks of liability of data loss that cloud vendors are willing to undertake and factor that into their management processes for data and its security. Managing security of cloud workflows and cloud storage of large media assets becomes complicated due to the addition of latency in data transfers.

"While media was streaming locally within a facility as SDI signals, everything was hard wired and secured. With increasing transmission of media data over IP, media has become as vulnerable as other data that is transmitted over IP links. Consequently, it is important to apply the same measures of securing connections, end-points, monitoring data flows and using methods like checksums to minimise data corruption in transmission," Iyer emphasised.

As IoT becomes a reality in the broadcasting industry, security solutions are changing too. Connectivity is a huge advantage to clients who are working on global productions. Previously you would need to send the tape or hard drives back to the facility, which could be 5,000 miles away.

Through IOT, one can automate a huge amount of tasks, such as ingest, transcode and file based delivery. Being connected to the post-production house from any location worldwide helps improve efficiency, reduces wasted time on shipping and helps with the bottom line of a production.

"Furthermore through IOT you can automate many of these mundane tasks remotely. With this attractive global exchange comes the risk of hacks," Lambert cautioned.

FUTURE PERFECT

Almost any production/post production leveraging the IoT for content exchange will require cloud based security as part of the workflow. Clients want to make sure that there content is secure at all times and how can they do that if their files are on a third party server somewhere around the globe.

"We are seeing media and entertainment companies turn towards more integrated security services. There's a demand for managed content protection services that deliver demonstrable success against video piracy, as opposed to just deploying security software and hardware devices," said Sharpe.

He added that increasing use of cloud based workflows will help standardise and homogenise many of these processes and as this happens, security will become easier to configure and maintain. However, the efficacy and practicality of security of cloud based broadcasting workflows and the usability of cloud based security solutions for broadcasting remains to be proved. Iyer is confident, though, that both will improve to a point that they will become the standard rather than the experimental alternative that they now are. Here is hoping that his confidence that piracy and other threats will be unsuccessful in disrupting the industry is not misplaced.