CYBER EXTORTION: The Golden Age for Zero Trust in the Media & Entertainment Industry

White Paper: Cyber Extortion: The Golden Age for Zero Trust in M&E
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>05</td>
</tr>
<tr>
<td>Cyberthreats in the Media &amp; Entertainment Industry</td>
<td>01</td>
</tr>
<tr>
<td>Why Cybercriminals target the M&amp;E Industry</td>
<td>02</td>
</tr>
<tr>
<td>Conventional Cybersecurity Models are Flawed</td>
<td>03</td>
</tr>
<tr>
<td>Upping the Ante: Compliance Guidelines</td>
<td>04</td>
</tr>
<tr>
<td>Zero Trust: A New Way Forward</td>
<td>05</td>
</tr>
<tr>
<td>Isolation-Based Security</td>
<td>06</td>
</tr>
<tr>
<td>Conclusion</td>
<td>07</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Members of the media and entertainment ecosystem face increasing pressure to produce extraordinary results while accelerating their businesses and protecting their organizations from relentless cyber attackers. As innovative use of digital technologies and third-party vendors to create and distribute digital assets accelerates, increased risk from cyberthreats comes with the territory. 22.14% of all cyberattacks target the M&E industry, making it the second-highest attacked industry.1

Like every industry, M&E has to protect personal information such as Social Security numbers and credit card numbers, as well as emails and sensitive company information. What’s different is hackers see a more attractive target in M&E: content. Content produced and distributed across a sprawling supply chain that is difficult to protect. Complexity, the enemy of security, increases because collaboration with third parties, regardless of size, function, and security capabilities, is required to get the job done. And innovative attackers develop more ways to extort organizations, both encrypting internal content for ransom and exfiltrating content to use spoilers about the buzziest new show or film for extortion.

Cybersecurity that works for M&E needs to address issues of speed, simplicity, and scalability to protect fully against the growing number and sophistication of threats. Zero Trust security does just this by operating under a policy of "never trust, always verify," ensuring no unauthorized access is ever granted to the endpoint or network. By implementing a solution based on the principles of Zero Trust, through browser isolation, all members of M&E, from production to distribution to vendors, can secure their largest source of risk without changing user behavior or requiring additional resources for its administration. In 2020, it’s time to rethink our security architectures using Zero Trust.
Cyberthreats in the Media & Entertainment Industry

From content creators complying with MPA Security Guidelines to prohibit production networks from directly accessing the internet, to post-production facilities adhering to strict Netflix NP3 benchmarks, to IT and Security staff implementing innovative technology to improve productivity and lower costs, it’s hard to balance productivity needs against those of security. Yet, data breaches continue to embarrass and inflict damage to the industry. Hackers have built successful business models around repeatable attack workflows.

In a notorious plot, an anonymous hacker contacts a VFX house and claims to have stolen terabytes of intellectual property and unreleased content entrusted to them, then demands a multimillion-dollar ransom payment to prevent its release. Regardless of whether the victim brings in law enforcement, negotiates, refuses to pay the ransom, or tries to buy time to ascertain if the claim is real, we know it won’t end well. How do M&E leaders protect their organizations against ransomware and cyber extortion as cyber attackers continue to innovate?

Public data breaches in M&E go beyond account numbers and PII to terabytes of intellectual property and pre-release content. Cyber extortion—using a combination of phishing, ransomware, and other cyberattacks—has a proven track record of success. In M&E, reimaging a compromised machine is petty theft compared to paying ransom to recover control of a pre-release blockbuster.

The attack surface in M&E has never been larger as creating content on smartphones using web apps, managing brands on social media, and expecting instant access to web research everywhere become the norm. The conventional security methods of the M&E industry are failing to keep organizations safe from breaches. Detecting threats and stopping them before they can do damage is no longer realistic and assumes that the number of alerts created is manageable. In reality, it is not. There are too few security staff and too many security alerts. The detection-based security model means getting hacked is a question of “when”, not “if.”

To address the security crisis facing M&E, we need to assess new security architectures and rethink how the industry approaches cybersecurity.

Cyber Extortion in M&E raises the bar

Cyber Extortion has become the leading motivation for attacks on the M&E ecosystem. Hackers increasingly threaten to expose sensitive material—embarrassing emails or intellectual property like unreleased movies and scripts—instead of simply stealing passwords or credit card data, or locking access to victims’ systems as with ransomware. Hackers are also attracted to M&E because the attack surface is vast. Collaboration and distribution across a broad range of organizations of all sizes and security capabilities leave content vulnerable at the weakest link in the supply chain. M&E needs a new approach to handle the latest business threats.

Cybersecurity has become a thorn in the side of the M&E Industry. The trend is an alarming one. Organizations spend more on cybersecurity each year yet experience more pain from cyberattacks. Cybersecurity is increasingly becoming more complex as M&E organizations add tools to address the latest threats. How much security is enough to protect our organization without impacting productivity? Where can I find trained security staff to implement and operate our security tools? How do I find the tools that provide the best value when there are so many cybersecurity vendors? Do I need to buy insurance coverage for cyberextortion? Painful questions indeed!
Why Cybercriminals target the M&E Industry

Two conditions make M&E a lucrative target for cybercriminals: high-value assets and complex production processes.

Lucrative Assets

The $703 billion US M&E Industry produces some of the most valuable assets consumers love—movies, series, music, video games, and more. The latest of these typically come out at a premium price, and consumers worldwide have shown willingness to get access to these at a discounted price by buying on the black market. Cyber attackers have found it lucrative to either steal and sell the product on the black market, or hold it for ransom.

Structural Vulnerability

The highly collaborative and interconnected nature of the M&E industry, while it has enabled the industry to produce high-value creative content at a reasonable cost, has, in the Internet era, exposed some “weak links” in the chain.

If we look at the M&E industry’s process in terms of pre-production, production, post-production, and broadcasting or streaming, we can broadly classify the various entities involved as Production, Distribution, and Vendors (third parties offering a range of services to the industry).

Production Companies

The larger studios produce some of the most culturally relevant, era-defining projects. Perpetrators try to conduct cyberattacks against these highest-profile projects because they are most rewarding. Projects rely on lots of work outsourced to vendors, often smaller companies, that specialize around specific expertise. While these smaller specialty content creators are critical to the overall content creation project, they are likely to lack the technical resources needed to safeguard the asset and are therefore a weak link in the network that can be exploited by cybercriminals.
Distribution Companies

In the past, those that distributed content were not themselves content creators. That has dramatically changed over the past decade where broadcasting/streaming companies now create original content—typically through outsourced content creation. Cybercriminals do not need to target Netflix, Hulu, or NBC—they can target any of their numerous smaller partners with the same devastating effect.

Broadcast companies are also vulnerable through many points: through social media, especially Facebook, and the Content Delivery Networks they rely on to push current news.

Vendors (Third Party Providers)

As post-production begins, several specialists enter the scene—editing, special effects, overlaying musical score, subtitles, dubbing, and so on, mostly provided by outside agencies, all of whom require some access to the content.

The success of the project depends on collaboration, which requires a great deal of trust. “Our business relies heavily on third parties,” says Stephen Fridakis, former VP of Media and Tech Operations at HBO. “You cannot make a series; you cannot develop a documentary on your own. You require heavy collaboration.”

The MPA makes it clear that it only provides guidelines and assessments to analyze and score how well vendors adhere to best practices. It does not certify, accredit or endorse vendors. Now vendors have to incur costs to complete audits knowing compliance doesn’t guarantee security.

Opportunities for Cybertheft Abound

As a project moves through each phase (pre, production, post-production, and distribution), various entities have to access the content where their expertise is needed. This sharing or transferring of content with one entity or another—primarily through digital means—introduces a security gap and opportunity for a cyberattack. And while the MPA’s exhaustive guideline addresses many of the physical gaps, closing the digital gaps continue to be a challenge as cybercriminals vary their method and point of attack.

M&E is no exception to the sheer magnitude and variety of cyberattacks. As the second most targeted industry, M&E companies must find effective ways to ward off this digital onslaught.

Visual Effects (VFX) and Cyber Security

Henric Larsson, the CEO of Chimney, says that to protect against cyberattacks and data breaches, they set up a separate department in their office that has no internet access, no phones or cameras, or alarms.

Employees at Chimney work with encrypted files, hardware locks on workstations, and constant monitoring of operations. However, he says that larger projects need more layered and costly solutions. The company also trains all staff on security threats and how they should operate within the studios. Larsson states that his studio's flexibility is hindered by beefed up security, as they need to plan out projects through a long-term lens as opposed to implementing new ideas quickly.

One of the main struggles of setting up a separate department with no internet access is that they have to buy music from iTunes and use CDs, as opposed to stream music from external sources. Larsson goes on to say that he believes 90% of the shops do not have MPA and studio approval when it comes to best practices.

Larson Studios/Netflix

Larson Studios does post-production sound for several Hollywood projects. In the winter of 2016, Larson Studios was hacked by an anonymous group called the Dark Overlord, who hacked into a Larson Studio computer that was using an old version of Windows. Cyberattackers blackmailed Larson Studios into paying more than $50,000. However, some of their most prolific work, including ten unreleased episodes of Netflix original, “Orange Is the New Black,” was still leaked on the internet. This leak left a permanent dent in Larson Studio's reputation.

This incident was an ecosystem challenger, as it highlighted the security pitfalls of having a third-party work on projects post-production. It also highlights that smaller companies without enough resources are often targets for hackers.
Despite all the hard work by IT & security teams and the money spent by Media & Entertainment companies, traditional security architectures are still failing to meet the most pressing needs of the industry. Conventional security models, such as those suggested by the MPA and NP3 compliance, rely on policies for access via a secure web gateway or depend on detection to stop a threat before it can harm.

These approaches come with their own sets of flaws. While a base level of policy can help, policies that are too strict can limit the organization's capabilities, productivity, and become a significant undertaking for administrators to manage. Furthermore, utilizing detection to stop attacks before damage occurs creates a tremendous workload for administrators to handle. Most Security Operations Center (SOC) analysts can effectively handle 7-8 incident investigations per day. Not only are far more alerts coming in than can be managed, but roughly 55% of the alerts cybersecurity teams face are also false positives. Faced with more alerts than they can handle and the knowledge that many of them are false alarms, many administrators experience "alert fatigue syndrome." And that's for the organizations that have dedicated security staff.

Experience has shown that overwhelmed workers can become desensitized to alerts, potentially neglecting to follow up and allowing threats to thrive inside the system. Coupled with a severe shortage of skilled individuals trained to handle the threats, this creates a highly challenging timeline from the first detection to response and remediation. Hackers exploit this weak link to infiltrate the entire network.
Industry organizations and thought-leading companies are helping to increase the security standards for the M&E industry’s production and distribution supply chain through standards and guidelines. The Motion Picture Association (MPA) has partnered with the Content Delivery & Security Association (CDSA) to launch the Trusted Partner Network (TPN). And rather than work on two security standards and ask organizations to comply with both, CDSA is throwing its weight behind MPA’s Content Security Guideline. The Netflix Post Partner Program (NP3) requires partners to meet their security standards, amongst others, before they are badged NP3. Compliance doesn’t guarantee security, but it does motivate organizations to implement valuable guidelines to reduce the risk of cyberthreats, and avoid fines or lost business opportunities.

The MPA provides a comprehensive guideline designed to prevent or lower the risk of cyberattacks. However, cybercriminals have significantly evolved from simple thefts of credentials or finding vulnerable ports to significantly more sophisticated attacks using combinations of phishing, malvertising, and other social engineering techniques designed to steal legitimate credentials.

Limitations in Implementing the MPA’s Guidelines

As we saw with Chimney, the recommendations by the MPA to separate digital systems connected to the Internet from those used for content production is neither easy nor inexpensive to implement. Our calculations show that it can cost up to $10,000 a year per employee or more. While larger M&E companies may be able to absorb this cost, smaller ones will likely not. Furthermore, it is cumbersome and disrupts creativity and productivity, adding additional soft costs.

The result is that many of the smaller—yet vital—players within a media production project will forgo implementing this recommendation, creating a gap in cybersecurity.

Virtual isolation provides better ROI than physical isolation. No new infrastructure is needed. There’s also a productivity win as employees do not have to move between two machines to complete their work, no more googling on one machine to create on another.

Visual Effects (VFX) and Compliance

Henric Larsson: [Compliance] is a major pain... and it’s more expensive than ever. Studios used to pay their guy to come audit you and give recommendations to get clearance. The industry is now moving to something called “Trusted Partner Network” where you have to pay a 3rd party to audit you. Costs about 3K US$ (Edit: That’s the cost of the audit. Not the cost of implementing all the crazy stuff. Critical ones are: Airgapped internet (i.e. no internet on any machine that touches plates). How do you google issues and references then?

Henric Larsson: The artists bring in separate laptops connected to a Wi-Fi that doesn’t have access to the production network and do their reference lookups on those. It’s inconvenient. If they need to download something, someone from IT or a production coordinator gets it for them. Not defending it - just describing how I’ve seen it done at client sites.
As we examine the breaches affecting the industry, it becomes evident that the security model we have come to rely on is not sustainable, especially as we accelerate digitization and interconnectivity. Working with solutions that were built without consideration for the scope, delivery, size, volume, and magnitude that attacks hurts us and makes us vulnerable to a breach. To strengthen the industry and address their needs, M&E organizations must reassess their fundamental approach to cybersecurity.

The key requirements that any solution needs to focus on include:

**SPEED**
Attackers are getting smarter and the business & regulatory impact breaches are getting more expensive

**SIMPPLICITY**
Cybersecurity should be simple enough to be within reach of every business & individual

**SCALE**
Help business scale cybersecurity as more processes get digitized without being handicapped by limited pool of professionals
Zero trust security is based on the principle that everything has the potential to do harm and handles everything like a potential threat. Zero trust focuses on reducing the attack surface and impact through the use of various technological approaches such as identity validation, privilege management, and endpoint isolation. The framework was first introduced by Forrester analyst, John Kindervag, in 2010 and is a model that kicks to the curb the old castle-and-moat mentality that organizations had in defending their perimeter and assuming everything inside didn’t pose a threat.

The zero trust philosophy also addresses the need to reduce the number of false alarms administrators encounter, because zero trust security takes place before the point of detection using a truly proactive model that stops all threats before contamination is possible.

Zero trust security is performed through the implementation of solutions aimed at securing specific points of access or entry to the endpoint. For instance, a zero trust model assumes that all interactions with the internet are unsafe – whether a reputable site or an unknown site – thereby limiting attacks that use reputable sites as a point of infection. Zero trust model also segments the network to ensure that even if one endpoint is compromised, it doesn’t automatically result in free lateral movement to other systems.

A complete zero trust model secures against all attacks both external and internal treating every interaction with the endpoint or server as a threat. By incorporating the right zero trust solutions into an organization’s security strategy, it becomes possible to secure entire portions of your attack surface by closing the entry point to threats.

The largest exposed attack surface in most organizations is comprised of attacks coming from the internet, an estimated 98% of all endpoint compromises start with the web. These could be prevented by adopting a zero trust approach to security known as isolation.
Isolation-Based Security

Isolation-based security is founded on the principles of zero trust, working to secure a portion of your attack surface by denying access to outside sources that have the potential to harm your endpoint and network. By transforming all Internet-content – code, media, scripts, files, etc. into harmless pixel streams delivered to the endpoint, isolation removes the (exploited) trust away from the endpoint and creates a clean computing environment that nearly eliminates infections and compromises.

Operating under the principles of zero trust security, isolation-based security does not look to detect or classify content as good or bad. Instead, it assumes all content has the potential to be malicious and transforms everything into pixel streams. This simplicity creates a solution that immediately reduces the number of alerts administrators need to address, decreasing the burden on IT teams and giving time back to administrators so they can work on other priorities.

In an industry where the demand for adopting new technologies to enable business functions is so essential, building a strategy that enables IT productivity is essential to success. When M&E organizations adopt isolation technology, they are also contributing to creating a stronger network for the entire industry by closing holes that can be created by “weak links in the chain.” An organization that enables browser isolation can send and receive information from third-party vendors and remain confident that all content they are exposed to has been safely transformed. Additionally, if writers, editors, producers, or performers access a compromised application or website, the “air gap” created by isolation prevents hackers from using that application to gain access to the network.

Isolation: The most Practical Way to Meet MPA and NP3 Compliance Requirements

There are different ways to implement the Isolation-based security model. Governments pioneered the use of physical air gaps for multilevel secure networks. Creating duplicate physical networks and computing resources isolates every security level from each other.

Physical isolation has two main downsides compared to browser isolation: cost and usability. Browser isolation does not require new infrastructure, so the incremental cost is a subscription in the range of hundreds of dollars per user per year. Physical networks require a doubling of resources -- PC hardware and software, internet service provider, IT and Security staff to patch and manage, implementation of a central monitoring system for distributed endpoints, and more ($10,000 initial cost of infrastructure plus thousands of dollars per user per year to maintain.

The other downside to physical isolation is users who need to access the internet to do their jobs and have to continually switch between production and non-production machines. Browser isolation provides the best dollar value and fastest time to value.

<table>
<thead>
<tr>
<th>Security based on Physical Separation</th>
<th>Security based on Virtual Isolation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial cost</strong></td>
<td>No duplication. Users use the same hardware/software and the same network for production and non-production use.</td>
</tr>
<tr>
<td><strong>Ongoing cost</strong></td>
<td>Typically in the low hundreds of dollars per user per year</td>
</tr>
<tr>
<td><strong>Productivity cost</strong></td>
<td>No productivity loss as users use the same machine and system for research and production.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initial cost</th>
<th>Ongoing cost</th>
<th>Productivity cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchase separate machines for production and non-production use, software costs for each machine, separate networks Typically around $10K per user</td>
<td>Can range from $3,000 to $10,000 per user per year to maintain the separate systems</td>
<td>Productivity hits of as much as 20% as very expensive talents have to switch between systems to research and then apply findings on projects</td>
</tr>
</tbody>
</table>
CONCLUSION

Why Change?

The current approach to cybersecurity isn’t working for M&E. Compliance with MPA and NP3 requirements increases costs, yet data breaches continue and risk from extortion increases. Security vendors provide more tools to detect new threats but they come with an unintended consequence – they create more work for understaffed security and IT teams to triage alerts and mitigate incidents. Without dedicated security staff, smaller organizations in the M&E ecosystem struggle to keep up. Brute force approaches creating duplicate networks of physical systems to isolate production from non-production work impacts staff productivity – googling internet resources on one machine to create assets on another is like player Twister® to get your job done. Stop spending more to get less.

Why Now?

It is time to reevaluate the way we think about cybersecurity. By implementing a zero trust framework through isolation, M&E organizations can once again utilize technology to meet the challenge of scale facing their industry. Browser isolation provides a simple, streamlined approach to cybersecurity, built to withstand increasing attack volumes without hurting productivity or changing the user experience. By doing this, your attack surface is reduced by up to 98%.

Why Cyberinc?

Cyberinc’s approach provides the best value, and the fastest time to value. Simply put-if you could stop breaches before they happen, why would you choose not to?
References

ABOUT CYBERINC

Cyberinc helps you experience a safer Internet by proactively stopping web, email, and document-based threats. Cyberinc’s Isla platform uses cutting-edge isolation technology to neutralize threats and prevent them before they have a chance to act, simplifying the security strategy and delivering immediate protection. Cyberinc is trusted by businesses of all sizes and governments around the world.

Contact us
www.cyberinc.com +1-925-242-0777 info@cyberinc.com