SPRING/SUMMER 2020 $25

The NOW WHAT? Issue

A new remote-work reality will mean long-term changes for how M&E gets business done. Welcome to Hollywood's new normal. P. 15

M AND E JOURNAL
Media & Entertainment
Strategies. Solutions.

published by
MESA
Media & Entertainment Services Alliance

Securing and Supporting Your Remote Workforce During the COVID-19 Pandemic

Photo by Bongkarn Thanyakij from Pexels

By Michael Wylie,
Director, Cybersecurity Services,
Richey May Technology Solutions

Clear, written policies can help avoid micromanagement

Abstract: COVID-19 has caused businesses worldwide to activate business continuity plans (BCP) overnight, and work-from-home arrangements have become a critical necessity for most businesses, something that's been viewed with skepticism for years. Company leaders are having to make tough calls quickly and may not have the time to research their decisions like they once did. Now that the rush to get employees working from home is over, it's time to pause and take stock of your cybersecurity situation and your IT team's capacity.

For years many industries, including M&E, have been skeptical of remote workflows, with typical concerns covering lack of productivity and security controls over content. There are also practical concerns, like the speed of home internet connections and hardware accessibility.

Because working from home has been viewed as a "nice to have," or an incentive for certain employees, many organizations haven't developed the policies, resources or training to enable their people to work off-site securely and efficiently.

COVID-19 has quickly changed that mindset, and the need for an off-site working game plan.

In these unprecedented times, experts across the technology landscape need to lead the way with the resources at hand to successfully and rapidly transition teams into a new way of doing business. Here we offer a step-by-step strategic guide to securing a newly remote workforce, where air-gapped networks and face-to-face interaction are no longer viable in the creative community.

As **employees** get **adjusted to working from home,** reinforce **cybersecurity best practices** with security **awareness training** that covers **social engineering, strong passwords,** and **safe handling** of content.

Define and update policies

Clearly written and easily understood policies and procedures will act as a foundation and help govern employees while they are off-site. Organizational policies and procedures can help reduce the temptation to micromanage employees, as expectations are already written down and communicated. At a minimum, have comprehensive policies and procedures that address:

- **Acceptable use**
- **Asset and content classification**
- **Business continuity**
- **Disaster recovery**
- **Confidentiality**
- **Incident response**
- **Mobile device management**
- **Passwords**
- **Disciplinary actions/sanctions**
- **Internal anonymous reporting for piracy/mishandling of content**

Don't assume your policies and procedures are known and understood by your employees. It's unlikely your employees regularly access their onboarding materials. Develop a central location that's easy to access and remind employees of key points frequently. Use examples to add clarification and encourage users to ask questions about policies and procedures they don't understand.

Decentralized endpoint security

With a remote workforce, traditional perimeter security controls such as firewalls and network intrusion prevention systems (NIPS) no longer have the same level of effectiveness as they did with traditional on-premise workflows. Each device taken home by your workforce becomes an island with a perimeter that needs defending. With a remote workforce, the impact and time to quarantine incidents, such as ransomware, drastically increases. If you have not already considered endpoint detection and response (EDR) or managed endpoint detection and response (MDR), now is a good time to evaluate your options.

Physical security

Many organizations are allowing employees to take equipment home, which means computers are no longer protected by the office's physical security controls (e.g. alarm system, CCTV and door locks).

Now is the time to identify what data is being stored on endpoints and take appropriate action to protect company and content owner data. For some businesses, this may mean enforcing full disk encryption on all devices, while others may opt for a virtual desktop (VDI) deployment to keep data in a central location like Amazon Web Services or Microsoft Azure.

While working from home, it can be tempting for family and guests to use work computers left around the house. Remind employees that work systems are for their use only and ensure physical devices have strong password requirements. This may extend to mobile devices, which some employees may not realize, so ensure your communications clearly identify which items employees are responsible for.

Cybersecurity awareness

There can be a lot of distractions when working from home, especially with schools, day care centers and after-school programs suspended. A brief distraction, multitasking, or even just feeling rushed may result in momentary oversight in cybersecurity best practices. As employees get adjusted to working from home, reinforce cybersecurity best practices with security awareness training that covers social engineering, strong passwords, and safe handling of content.

Again, communication is key here. Ensure employees know who to contact if they receive suspicious communications and make sure they feel welcomed to do so. If employees feel like they are bothering your IT team or can't get a fast response, they may open attachments that contain malware or follow instructions from an impersonator. In a time when predators may take advantage of anxious, confused or distracted employees, erring on the side of more communication may save you from a costly breach.

Digital communication

What used to be an editing bay away can now feel like a hundred miles, while everyone works from home. Leaders need to implement catalyst technology that allows collaboration and breaks down the communication barriers while teams collaborate from different physical locations. Failure to provide a means to complete business objectives will result in employees solving problems themselves with potentially insecure/unencrypted channels of communications, such as SMS or third-party chat sites. The last thing you need during an already stressful time is for non-public information or content owner data to be leaked.

Managers, coworkers and HR departments all need to be easily accessible during these rapidly changing times. Tools like Zoom, Slack and Microsoft Teams can allow your team to securely message, screen share, voice call or video call anyone within the organization with a few clicks.

With an increase in email use and decrease in visibility into employees' usage, tools like Managed Methods, Cloud Access Security Brokers (CASB) and Proofpoint, a Secure Email Gateway (SEG), provide stronger shadow IT, data leakage and control over email use.

In these uncertain times with changes happening so rapidly, it's easy to feel like there are multiple competing priorities. Company leaders are having to make tough decisions quickly and may not have the time they once did to research their decisions. It's important that we stay connected throughout the industry and share our knowledge of best practices and daily developments. Many breaches are preventable and there are many tools at our disposal to help protect you. Now that the rush to get employees working from home is over, it's time to pause and take stock of your cybersecurity situation and your IT team's capacity. ■

Michael Wylie *is responsible for delivering information assurance by means of vulnerability assessments, risk management, project management, secure network design and training. He has developed and taught numerous courses for the Department of Defense, Moorpark College, California State Universities, and clients around the world. Michael is a qualified TPN assessor and has an industry focus on the media and entertainment industry. michael@richeymay.com @TheMikeWylie*

Protecting the Vision of Storytellers

Full-Service cybersecurity solutions for studios, vendors and distributors.

TPN Prep, Assessment & Remediation | Incident Response Prep & Management
Cloud Migration & Security | vCISO Services | Remote Work Security and More

richeymaytech.com
info@richeymaytech.com

RICHEY MAY Technology Solutions