MFM bcca

INFORMATION AND INSIGHT FOR MEDIA FINANCE PROFESSIONALS

JULY/AUGUST 2021

TFM

THE FINANCIAL MANAGER

ALSO INSIDE

MISSION CRITICAL

Cyberattacks are on the rise, inflamed by remote-work environments. Hybrid home-office environments may extend the trend.

TFM
The Financial Manager

The Official Publication of the Media Financial Management Association is published six times annually under the supervision of:

MARY M. COLLINS, President & CEO
Mary.Collins@MediaFinance.org

JANET STILSON, Editor
TFMeditor@MediaFinance.org

BILL KNIGHT, Art Director
wknight5@nyc.rr.com

Limited commercial messages of interest to our membership and readers will be accepted. Rates and specifications on request to:

MEDIA FINANCIAL MANAGEMENT ASSOCIATION
550 W. Frontage Road, Ste. 3600
Northfield, IL 60093
telephone (847) 716-7000
facsimile (847) 716-7004
and at www.mediafinance.org.

Subscription $69.00 per year.

What is MFM?

The Media Financial Management Association is a not-for-profit corporation organized in 1961. The MFM membership includes more than 1,200 of media's top financial, IT and human resource personnel, station general managers and other media management personnel as well as associate members in the allied fields of auditing, tax, software, sales and the law.

MFM sponsors telephone seminars and conferences, publishes special studies and surveys, files position papers with federal agencies on behalf of its members and its industry, cooperates with other media industry groups and helps its members grow and learn both personally and professionally.

MFM also is involved in media industry credit matters through its wholly-owned subsidiary, BCCA, which provides members with a Credit Inquiry Service, an annual Conference, directory of Credit Personnel, credit reports accessed via bccacredit.com online credit search, Commercial Credit Reports and a credit and collections handbook.

FEATURES

DEPARTMENTS

RISING CRIME, RISING RESPONSE?

Hackers had a field day when companies went into remote-worker mode. Mission-critical information must be better protected.

BY MARY J. HILDEBRAND

COVID-19 has changed the way we interact with technology and focused renewed attention on data privacy and security. U.S. companies are grappling with the enhanced business and legal risks associated with remote working, especially their vulnerability to cyberattacks.

Currently, cyberattacks rank as the fastest growing crime in the U.S., according to the Information Systems Audit and Control Association (ISACA). Globally, cybercrime damages were estimated by ISACA to reach $6 trillion by 2021.

That alarming vulnerability of mission-critical information could continue. Rather than disappear as a relic of pandemic, the remote-work trend may become permanent, or at least morph into a hybrid model. It's imperative that businesses intending to retain (or introduce) remote-work infrastructures take steps to minimize exposure from these increasing cybersecurity risks.

HOW DID WE GET HERE?

Before delving into best practices to mitigate the risks, let's backtrack slightly to understand the extent of the current quandary. When COVID-19 rampaged through America, the disruption stressed not only the millions of individuals involved, but also the complex technology infrastructures that were suddenly required to accommodate massive traffic volumes.

While this stimulated innovation to meet rapidly changing needs, well-organized hackers and other bad actors moved to exploit security weaknesses in the technology infrastructure supporting the newly decentralized workforce. Their goal: obtain control of data assets for future monetization or extort payments from companies desperate to access their highly sensitive data after a ransomware attack.

When a business sustains a cyberattack, direct financial losses are only part of the story. Businesses must comply with the applicable data-breach laws of every state and country where the affected individuals reside. U.S. companies may have obligations to notify individuals, law enforcement and governmental authorities around the world.

For businesses in highly respected industries that process valuable personal information (often financial or medical data) the reputational impact may be the most challenging. Once shaken, the confidence of consumers and business partners is hard to regain. Ironically, companies that moved most rapidly to ensure business continuity during COVID-19 may be among the most vulnerable to cyberattacks.

For every well-known company hit by cyber criminals that make national headlines such as Twitter, Marriott, Zoom, Magellan Health, Colony Pipeline and Cox Media Group, there are many others managing the fallout of cyberattacks within their own industries.

The top cyber fraud incidents are social engineering, phishing, data security lapses, ransomware and patch management, according to analysts at the ISACA. Preventing

such intrusions by increasingly organized and tech-savvy criminals is a massive challenge.

BEST PRACTICES

While the risks to mission-critical data associated with remote work environments involve many complex factors, successful risk mitigation is often a matter of common sense and strict monitoring of compliance. Our team recommends:

Involve Strategic Leaders – Ensure that key stakeholders are involved and accountable from the outset of the planning and risk-mitigation process. They should include top executives from IT (operations, security, data analytics); legal and compliance; marketing and business operations; human resources; finance; and representatives from the C-suite and the company board.

Vet the Vendors – Revisit and evaluate third-party vendor dependencies that support remote working, including an appropriately scaled security diligence process. Companies are responsible under applicable data breach laws (and frequently in commercial contracts) for the consequences of security incidents sustained by third-party vendors engaged in processing their data.

Employee Engagement – Alert staff members regarding the enhanced cybersecurity risk and conduct appropriate training in connection with the remote-work environment. Then do it again. There is no substitute for a well-trained workforce, but humans will continue to fall for social engineering, phishing and similar incidents.

Alert staff members regarding the enhanced cybersecurity risk and conduct appropriate training in connection with the remote-work environment.

The best programs keep these issues constantly in front of employees by providing frequent training, and reminders in the form of emails, updates and internal tests using "fake" intrusions.

Update Company Policies – Internal security practices and policies – including provisions for remote-work environments – should be monitored and updated as new threats arise. They should address the use of personal devices remotely, including, as applicable, devices that were previously approved. The security measures should include information regarding the installation of applications to either protect or wipe business data from a device.

Revise Emergency Strategies – Update plans for incident response, disaster recovery and other data security issues. Be sure to include your remote workforce and conduct remote-work tabletop exercises with your cybersecurity teams. When employees are remote they are alone, and it is critical that they know exactly what to do – and what not to do – in the event of a security incident.

Revisit Insurance Coverage – Analyze current cyber insurance policies to ensure coverage extends to your remote workforce and the third-party vendors that enable and support remote work environments.

In conclusion, I probably don't need to remind you that during the worst months of the pandemic, the immediate goal was to ensure continuity of business while maintaining the health and well-being of employees. As we move toward, releasing restrictions on business and other activities, the vulnerabilities associated with remote work infrastructures still remain.

In 2021, it's more important than ever for companies to prioritize protection of their data assets.

Mary J. Hildebrand is a partner, founder and chair of the privacy and cybersecurity practice at Lowenstein Sandler LLP. She can be reached at mhildebrand@lowenstein.com.

THE WEAKEST CONDITIONS

THERE ARE DOZENS OF FACTORS THAT contributed to enhanced cyber risk at companies operating a remote work environment, but some stand out:

IT Resources Stretched — IT staff members may have been deployed for extended periods to address system-bandwidth issues and server capacity for the remote workforce at the expense of cybersecurity.

Acquisition Issues — Shelter-in-place orders left many businesses scrambling to purchase (and provide workers with access to) company-issued laptops and/or security software at a time when there was soaring demand and supply disruptions.

Lack of Proper Vetting — Organizations were frequently compelled to quickly expand or even establish new relationships with third-party vendors and platforms to support the remote workforce. They often had insufficient time to conduct privacy and security diligence or provide current training suitable for the new model.

Inadequate screening of third-party vendors is a perennial issue for many companies, but the sheer volume of new and expanded relationships undertaken during COVID-19 escalated the risk substantially. These deficiencies remain in place as companies contemplate making remote work a permanent feature of their workplace environments.

Personal Devices — As businesses struggled to adapt, employees often resorted to using their personal devices and accounts to communicate (internally and externally) by email, especially in the context of communicating about COVID-19. These personal devices and accounts frequently do not have security measures in place that are comparable to those in many companies' primary IT system.

Additionally, many employees had little or no experience with remote work and communications. Because they had always worked within a secure system at their place of employment, they were not sensitized to the potential repercussions of sharing personal, confidential or business information through unsecure networks.

Thus, the incredibly rapid implementation of remote working, while socially responsible, has made individual employees – and therefore the organizations that employ them – more susceptible to targeted phishing, fraud and malware attacks.