WINTER 2020 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we provide an overview of the security implications of remote working, or telecommuting, in the modern workspace and risk mitigation.

Preventing Security Risks of Remote Work

Remote workers are at inherently greater risk of unintentionally jeopardizing data security than those in-office workers connected to a highly controlled network. While there is a trend toward allowing remote work, attention must be paid toward security issues potentially caused by remote employees. “Do what you can to minimize the damage” has become a mantra of IT security. Securing a digital workforce is no easy matter, and there’s no limit to risk that must be considered. Organizations that seek to counter risk by pulling remote workers back into the office is not only unrealistic given unsuccessful attempts by large firms and government agencies which have resulted in reduced employee morale, protests, and even knowledge-loss from employees leaving, but it also doesn’t solve the problem of securing organizational data for employees who access data remotely as part of their job functions. How, then, does the organization address security risks that grow as remote workers log on in increasing numbers?

Start with a Plan

Not unlike implementing a Bring Your Own Device (“BYOD”) policy which also heightens the risk of exposing sensitive data, working securely while working remotely requires a well-thought-out policy that applies to all employees, including C-suite executives. Digital Mountain recommends examining your current attack surfaces – both local and distributed – to find existing weaknesses and shut those down immediately. Concentrating on the theoretical threat is tempting, but not as effective as plugging the holes in your existing security.

Next, look at the job functions, equipment configurations, and data access requirements subject to remote working arrangements. Is a BYOD arrangement allowing employees to log into organization apps and data on unsecured equipment or via unmaintained software?

Organizations may wish to update BYOD policies to require regular inspection and maintenance of employee-owned devices. Compensating employees accordingly for security software subscriptions mandated by the organization but purchased by employees is a good way to encourage best practices with a BYOD policy. When employees create their own shadow IT functions by servicing devices on their own, they can undermine the security goals of the organization.

The goal of keeping your organization functioning optimally with remote workers needs to balance necessary access with security restrictions. Defining the data and apps required to successfully perform tasks and job functions can go a long way toward preventing malicious data capture, whether accidental or by a cybercriminal. Organizations can increase security by turning on logging features for web-based apps and reviewing event logs for unusual activity. When addressing the remote work habits of those managers and executives with access to wide swaths of the organization's data, having an experienced digital forensics team, such as Digital Mountain, on hand to demonstrate how unsecured devices with access to confidential information can create a potentially dangerous situation for the company can be very valuable.

Intelligent Data Storage

Data storage and retention create numerous security hazards when employees work remotely. Employees who work remotely may find it attractive to download information to their mobile devices. Additionally, temporary, contract, and freelance workers who download and store data on their devices may retain the information long after the expiration of their contracts and any oversight by the organization. Addressing these issues can help prevent security breaches without compromising employee efficiency, however, be wary of the simple fix: moving data to cloud storage may provide a false sense of security if employees can download or print from the cloud. Some organizations have found that disabling functions such as downloading, printing, and saving to external storage devices has helped to secure cloud-based data. Yet even these measures aren't flawless – capturing data with a camera, video recording device or screen capture is one way that information can be duplicated without having to circumvent cloud-based security settings. Here watermarks can be considered. It's also common for people to take handwritten notes that include sensitive data while working. So many loopholes to digital security highlight a vital need for comprehensive workforce training on data security.

Encrypting data, especially email to prevent packet snooping by hackers, is another way to help deter cybercrime when employees are working remotely. The Advanced Encryption Standard (AES) used by governments and other security-conscious organizations is the current standard for data encryption. There are AES encryption applications that include multi-language translation, decoy passwords to thwart hackers, as well as ones that claim brute force attack immunity. New "Honeypot Encryption" methods respond to hacking attempts with fake data to confuse and frustrate hackers. While no method is undefeatable, this next level of encryption may provide additional security. Also, ensuring the latest software updates are implemented, as well as installing Antivirus and Endpoint protection software will help protect your organization. Encrypting mobile devices and having Mobile Device Management (MDM) software deployed will help safeguard lost or stolen devices, so your organization's data doesn't end up in the wrong hands.

Practice Safe Computing

The importance of training employees to work smartly when working remotely is essential to securing a distributed network. The belief that the internet is becoming more secure often leads to a relaxed approach – but the reality is hackers need only the smallest opportunity to launch an attack. While it's difficult to ensure policy compliance by remote workers, regular reminders are necessary and part of a consistent plan. Remind employees to:

- Keep separate work and personal accounts;
- Prohibit non-employee use of organization-owned devices;
- Avoid using public Wi-Fi;
- Install new software only after checking for compatibility with organization approved security applications; and,
- Stay on top of regular password maintenance.

Digital Mountain's expertise in setting up systems to keep the personal and work data of remote workers separate, clearing corporate data off non-company owned devices at the end of employment or contract term, and closing network security holes can prevent a serious data crisis. Your efforts to train employees on mobile technology safety will go a long way toward maintaining a strong security focus in the minds of out-of-sight workers. Whether your organization is developing a secure data security system in order to provide employees with attractive remote work options or educating the C-suite executive team on how vital it is to carefully protect organizational, client, and customer information, Digital Mountain can help.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

LEGALWEEK NEW YORK
New York, NY: February 3-6, 2020

THE SEDONA CONFERENCE WORKING GROUP 6 ANNUAL MEETING 2020
New York, NY: February 10-11, 2020

THE SEDONA CONFERENCE 2020 EDISCOVERY NEGOTIATION TRAINING
New York, NY: February 12-13, 2020

NETDILIGENCE CYBER RISK SUMMIT, TORONTO
Toronto, Canada: February 20-21, 2020

RSA CONFERENCE 2020
San Francisco, CA: February 24-28, 2020

Click here to see more upcoming events and links.

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: