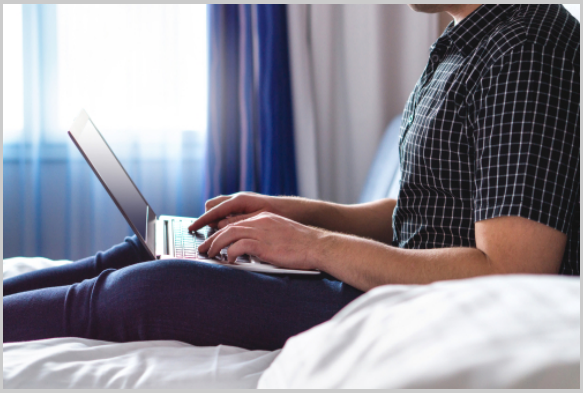
WINTER 2020 E-NEWSLETTER

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.

Security Risks Posed by Remote Working



A rapid cultural shift toward remote working, or telecommuting, has taken effect and it presents a major concern for companies focused on data security. A 2019 study by business consortium International Workplace Group reported that 50% of global employees said they worked outside their main office headquarters at least two and one-half days per week, with a majority of businesses responding that flexible work arrangements helped their companies manage and save on both capital expenditures and operating expenses (https://www.iwgplc.com/global-workspace-survey-2019). The shift away from traditional office environments to more distributed workplace options is made possible by advances in mobile technologies. However, being caught wearing pajama bottoms during a video conference call isn't the only risk to remote working! Remote working, if not approached judiciously, can threaten cybersecurity normally established in a traditional working environment by inviting attacks on not just devices used by a single remote worker, but potentially the entire company's data infrastructure.

Remote Creep isn't about Hackers

Mobile device technology is designed to increase computing mobility. We can easily check work and personal email from cell phones and tablets without repeatedly logging in. In addition, enabled notifications alert us to the arrival of new email upon receipt, often with a display that includes multiple facets of sensitive data contained therein. How many times have you checked your email while standing in line, riding public transportation, or sitting in a public venue? How many times have you done so without thinking about who might be watching your screen? While briefly displaying bits and pieces of random emails in public may not seem inherently risky, it is, and it is just the beginning of a cybersecurity threat.

Anecdotes about hackers hanging out in coffee shops are not only urban legends. Turns out, some legends are true. Public Wi-Fi networks are notoriously susceptible to attacks via network attack tools that reside on ordinary USB drives and “honeypot traps” that dupe unsuspecting Wi-Fi users into logging onto faked versions of the Wi-Fi service offered by the venue. Once others are logged onto the honeypot Wi-Fi, a black-hat hacker can steal passwords, launch ransomware attacks, and compromise email accounts.

Instead of accepting frequent data exposure in less secure environments as a fact of life, a company should consider how to exert control outside its company’s walls.

Safe as Houses?

Maintaining internet and data security in public places on unsecured networks is the first uphill challenge. The next is accepting a less intuitive awareness that allowing an employee to work remotely from his or her private residence also poses a major risk to cybersecurity. When working from home, workers often use laptops, either company-owned or within the scope of the employer’s Bring Your Own Device policy. The belief that laptops are self-contained units connected only intermittently to the internet and, therefore, more secure is a mistaken one. In the mistaken belief that they’re safe at home, in order to save time, users may not password-protect their laptops, much less employ a very worthwhile added layer of protection with multi-factor authentication.

Compounding the issue, many home internet routers are unsecured or protected by easily guessed passwords such as “password,” “admin,” or the house number and street name of the property. A Virtual Private Network (VPN) can enhance privacy by masking the user’s location while connected, and this is a recommended best practice for remote workers. Unfortunately, the use of VPNs is far from universal and users must be sure they are connected to a VPN before opening other applications to prevent undermining the VPN’s efficacy.

Using the same laptop for work and entertainment or allowing a third party to use a device on which company data is accessed or stored is also an invitation to cybercrime. Apps, especially those which install third-party keyboards or support keystroke logging functions as part of game apps and entertainment sites, don’t simply disappear when the user logs off. Those apps very often tap into data including usernames and passwords on other apps and sites. Apps with in-app purchasing options can be installed and purchases made without the owner’s knowledge, tying the device to a mobile banking system that may or may not be their own.

Interestingly, corporate IT security departments report that those most often responsible for lapses in remote working security are C-suite level executives with access to the company’s most sensitive data. iPass, now Parenteum, warned in its 2017 Mobile Security Report that IT directors at 500 companies around the world considered C-suite executives to be the most popular targets for cyber-attacks, as well as the most likely persons to not adhere carefully to IT security protocols (https://www.ipass.com/wp-content/uploads/2017/05/iPass-2017-Mobile-Security-Report.pdf). This double-edged sword is particularly dangerous in the healthcare and financial industries where a data breach subject to statutory privacy legislation can result in legal and financial trouble, as well as damage to the company’s reputation.

No Stopping This Trend

On March 7, 2019, the Pittsburgh Post-Gazette ran an article detailing how Bank of New York Mellon (BNY), which has a large presence in Pittsburgh, retracted a decision to end remote working options for employees, some 51,000 globally (https://www.post-gazette.com/business/career-workplace/2019/03/07/BNY-Mellon-work-home-Charlie-Scharf-layoffs-England-email/stories/201903070119). While citing "inconsistent implementation across the company," the decision to end remote work arrangements outraged employees around the world and BNY announced it would reconsider. Also in 2019, the United States Environmental Protection Agency (EPA) announced that as of August 4, 2019, employees of the EPA must report to their assigned office no less than four days per week, including those who worked remotely as an accommodation under the Americans with Disabilities Act. Once again, employees responded negatively, including staging a protest at the EPA's Boston offices (https://www.bostonglobe.com/business/2019/07/24/limits-telework-could-last-straw-embattled-epa-workers-say/eD4WGzT3XQ2NFV1198xcKL/story.html).

What these and similar incidents show is that despite security risks posed by remote work options, modern workforces are demanding remote work and telecommuting arrangements. Keeping ahead of cybersecurity issues will be key to guarding your organization's data.

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: