Have employees working from home? How to limit your cyber risk.

James Harrison, CEO INVISUS

Tuesday, April 21, 2020

With the spread of COVID-19, many firms are permitting or requiring attorneys and staff to work remotely. While there are many considerations in transitioning to a fully remote workplace including hardware, systems access, employee training and maintaining productivity, perhaps the most important issue is safeguarding your firm's sensitive information.

One of the main causes of data breaches has traditionally been employee error or negligence. Now, with people staying and working from home, law firms face an increase in potential attacks through weaknesses in home network environments that can lead to data breaches. Exposure of confidential business information can cause significant damage or losses. Exposure of personal information can trigger federal, state and even international data breach notification laws resulting in significant liabilities for a business and identity theft issues for individuals.

Now is a good time to evaluate your telecommuting plan as part of your firm's current COVID-19 response and beyond as the work-from-home trend accelerates and becomes the norm for many organizations and professionals. Here are some key issues to consider:

A Secure Home Environment

Home environments introduce a number of new security and privacy risks. Some IOT devices can be a risk. So can family members – especially smart teens. Be sure each employee's home network and Wi-Fi is secured. Enforce good passwords and restricted access to work computers.

Regular security checkups, perhaps quarterly, should be conducted on the employee's work computer (whether employee or company owned). Mobile devices used for work purposes should also be checked for proper security protocols.

Employees should know and follow the firm's telecommuting and work-from-home policies including the firm's internet use and social media policy that should still be in force at home.

Access and Authentication

Limit access to confidential and sensitive information including remote access to your firm's systems and databases. Also consider requiring the use of company provided VPNs, but understand that VPNs only create a safe tunnel from the employee's computer to your network.

If the employee's computer is compromised by a hacker from a phishing attack or through a home Wi-Fi router with weak security, the VPN (and the employee's computer) can essentially turn into a direct backdoor channel for cyber-criminals to access the firm's network – because the attack is coming via a known, trusted connection.

VPNs essentially create a network of new access points for malware that could remotely compromise a company's network. It's important to ensure every employee's computer, mobile device, and home network are all secured, patched and checked regularly.

Security Awareness Training

All staff should complete regular cybersecurity awareness training including proper handling of confidential data, and receive reminders to be vigilant and watch out for phishing emails, text or phone scams that try to convince them to grant server access or authorize transactions. Employees should have signed appropriate information security and non-disclosure agreements.

Information Security Compliance

It's important that you review and update your firm's telecommuting policies and procedures to ensure compliance with federal, state and industry requirements for preventing data breaches or violations of client privacy rights. This often-overlooked risk management activity is vital to keep the firm in a legally defensible position should the unthinkable happen and a breach incident occurs due to poor remote workforce planning.

Incident Response

While companies work hard to protect the health and safety of their employees, data breach incident response requirements remain in effect. Employees should be reminded to inform your firm's incident response coordinator should they become aware of a possible data breach while working from home. Your breach response team should discuss and prepare for the possibility of increased risk with staff working from home. Now might be a good time to also review any telecommuting or remote workforce terms and conditions of your firm's cyber insurance policy.

Identity theft monitoring

Consider providing an identity theft monitoring benefit to your employees. An employee whose identity has been stolen can be a security risk to your firm. Cyber criminals targeting your firm often target employees first. To use an old adage, catching employee identity theft could be the canary in the coalmine that prevents a full-scale cyber-attack on your business. As an employee benefit, this is a great way to help protect your firm and your employees at the same time.

Remote Technical Support

For employees working from home, problems connecting to the network, or a printer, or dealing with a slow, problem ridden computer can be frustrating and is a real productivity drain. Tech support problems can also be a sign of a security issue that needs to be addressed immediately.

While providing remote technical support assistance can be a challenge across a remote workforce for many organizations, there are solutions available that can work together with your current IT infrastructure to save your firm time and money – as well as help keep your workforce productive and secure.

***

Every organization is dealing with significant human resource, health and operational issues associated with COVID-19. With a little extra attention and care towards securing and supporting your remote employees, you can avoid having to deal with the painful consequences associated with data breaches and the loss of valuable business and client information. Working from home can be converted from a liability to an asset for your firm, if managed properly.

About the Author

James Harrison, CEO INVISUS

James is the founder and CEO of the cyber defense solutions company INVISUS. As chief strategist and product visionary for INVISUS, he led the development of the company's cybersecurity, identity theft, and InfoSafe® data breach compliance and breach response lineup that protects businesses and organizations throughout the U.S. and internationally. James frequently writes for, speaks and trains in a wide variety of industry and trade groups including financial services, legal, insurance, IT services, home security, and more.