MAINTAINING CYBERSECURITY VIGILANCE WITH REMOTE WORKFORCE

March 20, 2020 | Alert

Companies have had to respond quickly to the social distancing required to reduce the rate of COVID-19 infections. To the extent possible, most of the workforce has now transitioned to working from home and we are all adapting to new environments and technologies. We are relying more on e-mail and cloud-based communication services. Our new working environments are ideal opportunities for bad actors to exploit and increased vigilance is necessary. These cyber threat concerns are not new, but bear repeating as we navigate our new work environments.

Vigilance with protecting information systems. In our efforts to facilitate working from home solutions, we cannot lower our guard in defending against cyber threats. Our new work environment means many more employees are connecting to their employer's systems from home computers and personal devices. These connections expose organizations and employees to increased security risks from opportunistic bad actors. There are steps we can continue to take to minimize those risks.

- **Utilize a Virtual Private Network (VPN).** Accessing systems through unsecured Wi-Fi connections can create an easy gateway for bad actors to access information and data. A VPN will establish a secure connection and encrypt online activity. Ensure that your key systems which contain sensitive personal and business information are only accessible through your VPN. Configure access to web-based systems and applications to only allow access once connected to your VPN.
- **Implement two-factor authentication.** Increased remote access to systems creates a greater risk of unauthorized access to systems. Two-factor authentication is a more secure way to access work applications. Two-factor identification requires the user to verify his or her identity with a single device that only the user has access to – such as a mobile phone – to confirm that the specific user is requesting access. In practice, two-

RELATED PROFESSIONALS

Victoria R. Collado

Susan Miller Overbey

RELATED PRACTICE & INDUSTRIES

Banking and Financial Services

Litigation

factor identification requires an extra step. After the user supplies the standard user name and password, the system sends a request for verification to the user's phone, requesting a click or supplying a code for continued access to the system. Yes, the extra step for two-factor authentication will mean that it takes a few seconds longer to access a system, but requiring a second step of user identity verification greatly limits the ability of hackers to access those systems.

- **Use strong, unique passwords.** We have all heard this before, but it bears repeating. Do not use combinations of your name or your birthday, length trumps complexity, and use at least 16 characters whenever possible. Do not use the same credentials across different platforms. In the event a hacker gains your password to one account, the hacker will not have access to others.

Vigilance with unexpected or suspicious e-mail communications. With many of us relying on emails to work remotely, we must be extra vigilant with cyber threats that can reach and disrupt our information systems through a single email. We need to stay aware of signs that indicate a threat and report those threats as we all share responsibility to maintain safe and secure systems.

- **Check the sender email address/domain name:** You get an email, it looks like it is from your bank, your vendor, your client. If any communication appears new or out of the ordinary, check the sender's email address and domain name, which is different than the display name. If you are working from your phone, this will take a second step to uncover the account details of the sender. Checking may reveal that the communication is not from the entity you thought but is instead a phishing attempt. For example, the email is not from "Acme Sales" as displayed as the sender name, the email is actually from 'clietjtllbbl@eztheft.com.'
- **Determine authenticity without clicking.** You get an email, saying someone has sent you documents to download, or documents need your signature, or attaching a receipt for your $1,000 purchase. If you are not expecting documents or a receipt, do not click. If the communication is plausible, follow up outside of the email communication to determine its authenticity. Clicking on links in an email exposes you to malware and ransomware.
- **Protect passwords and personal information.** You get an email, asking you to confirm your account name and password or other personal information, or informing you that your account name or password have changed. Check the domain. Be wary of phishing attempts to obtain your personal information and passwords.
- **Alert others in your organization to suspicious communications.** If you received a suspicious email, others in your organization likely received it too. Alert your IT folks or your colleagues of suspicious emails so that others are aware of the threat. These are distracting times and we are all human, so what is obviously fraudulent to one person may not be so obvious to another. Assistance in identifying cyber threats and regular intra-company communications regarding cyber threats can eliminate unwitting exposure and raise awareness of the need for vigilance to stay ahead of hackers.

As we all do our best to stay safe in these challenging times, with vigilance we can also ensure that our systems and information stay safe.