www.pipelinepub.com
Volume 17, Issue 2

Cybersecurity for a Remote Working World

By: Paul Caiazzo, Corey McReynolds

For most of 2020, shelter-in-place and COVID-19 public health and safety guidelines have kept many US workers remote. This reality has strained organizations that were unprepared for this rapid shift. For instance, existing virtual private network (VPN) infrastructure was designed to support less than 30 percent of the workforce at any given time, rather than the 90 to 100 percent using it during the outbreak.

The new threats associated with a mostly or fully remote workforce increase the probability that an organization will experience a data breach or other cybersecurity incident. At the same time, an organization's incident response plan is operating in a very different environment than is currently covered. If your organization moved most or all employees home during the crisis, creating cybersecurity policies and procedures to reflect this *new normal* is essential to protect your business.

In this article, we provide the top areas to consider when adapting your procedures—for now and in the future.

Cover your assets

Remote workers should use corporately owned devices such as laptops, smartphones, and tablets to provide the most sustainable security. However, even if an organization has such a policy in place—and many don't—additional security considerations must be addressed.

With a remote workforce, employees may be working from personal devices, and not all business traffic may be visible to the security operations center (SOC). This means that identification of a potential incident may be delayed, and root cause analysis may be difficult or impossible. Because most organizations do not have technical architectures that support logging

and monitoring for remote devices, log information critical to the mission of digital forensics and incident response may be inaccessible or non-existent.

Updates and patches

Organizations should consider how remote devices will receive necessary updates and patches. Many on-site devices pull directly from the corporate intranet upon connecting to the network. On average, 48 percent of on-site systems receive patches within three days, but only 42 percent of remote devices are patched within the same window. While this difference may seem small, it raises the average patch time for vulnerabilities from around seven days if everything were on-site to around 38 days to include off-site assets.

This means an organization is likely to have six accessible attack vectors for every 100 systems that can grant access to their network and data for 38 days, on average. This delay exposes these devices to exploitation and significantly increases an organization's cyber risk.

Another potential issue is how to retrieve devices from laid-off employees. During COVID-19, many companies have reduced their workforces yet may not be able to physically retrieve company-owned devices due to quarantine restrictions. If an employee refuses to voluntarily surrender a corporate device, an organization must have measures in place to ensure this lapse cannot cause a data breach or other security incident.

Ensure understanding on security policies

It is challenging to manage company assets outside the organization's network, but it is also difficult to manage the remote working environment. It is easy to become lax with security practices that are routine in the workplace when working away from the office, especially at home. Adhering to clean desk policies and making sure to lock, log off or shut down computers are just a few tasks that employees do while in the office that they may not do at home. It's important to make sure documented policies and procedures lay out the specific requirements for working in the home environment. These should then be reinforced with technical controls like Active Directory Group Policies to ensure compliance.

Your new remote workforce policies and procedures should also cover home network security. This is an excellent opportunity to enhance employee knowledge, increase security awareness, get employee buy-in by helping them protect their home network and add further protection for remote work.

Make sure that employees can:

- Change default ISP router passwords
- Ensure ISP/home router firewalls are active
- Get company-offered free or low-cost home network monitoring solutions
- Recognize signs of home network attack
- Understand and agree to employee privacy and consent stipulations for personal device use

During this period of remote work, most organizations have required employees to use virtual private networks (VPNs) for network security. A full-tunnel VPN routes all traffic from the employee's computer through the corporate network for security scanning before sending it on to its destination.

Because of the sudden need to transition to remote work, many companies lack sufficient numbers of company-managed laptops to support a fully remote workforce. As a result, many employees are working from personal devices instead.

This dual use of devices creates significant privacy concerns if all traffic from an employee-owned laptop is routed through the corporate VPN. A telework policy must contain an explicit "consent to monitor" clause explaining that traffic resulting from personal use of a laptop connected to a corporate VPN flows through the organization's network and may be monitored. Failure to receive explicit consent from employees may put an organization in breach of data privacy laws.

How to spot a phish!

It's more important than ever to stay vigilant and watch for nefarious activity. To protect your employees and your organization from the increased phishing scams during COVID-19 and beyond, organizations should be train and communicate with remote workers. For example, train your employees to spot the warning signs, notify IT of any suspicious emails or messages and delete the correspondence. Guide employees to access information by going directly to a trusted website to find the data. Build a safe security culture, so employees feel comfortable notifying IT immediately without fear of recourse if they do click on a link. Test your workforce regularly, analyze the results and educate employees accordingly.

Have a plan

Most organizations' incident response plans are based on the assumption that incident response team (IRT) members will be able to respond in person to a potential incident. With a remote workforce, especially when COVID-19 shelter-in-place requirements in place, this may not be possible.

When responding to a cybersecurity incident involving a remote worker, an IRT may have to rely upon the remote worker—who may have limited technical knowledge—to respond to and recover from the incident. This will likely delay response times, potentially increasing the impact of the incident, and may make recovery activities, such as reimagining the machine, much more difficult to complete. To prepare for this situation, organizations may wish to create "IR kits" containing automated scripts for common data collection and recovery activities.

Rules to live by: contract and comply

Many organizations are governed by data protection regulations that apply to certain jurisdictions. Depending on the location where sensitive data is being processed and potentially breached, different regulations may apply.

Most organizations have strategies in place for ensuring compliance with data protection and contractual regulations. However, these strategies likely rely upon the assumption that all employees and data processing occur on-site. With a remote workforce, this may no longer be valid, potentially impacting an organization's ability to secure sensitive data and maintain regulatory and contractual compliance.

Organizations with remote workforces must establish policies and security controls to ensure that sensitive data is protected in accordance with contractual and regulatory requirements. Additionally, organizations should investigate how remote work expands and impacts their regulatory obligations and put in place any additional security controls required to achieve compliance with these new requirements.

Security policy and protocol

Remote work introduces a number of new security threats and considerations that must be incorporated into an organization's security policies and procedures. If a business contemplates a permanent or extended shift to remote work, implementing the security controls necessary to minimize the associated cyber risks will help maintain a more secure workplace.

COVID-19 and remote work are certainly still a part of our present and will be for some time to come. Organizations should embrace a robust approach to cybersecurity in this new reality.