4 Critical Steps SMBs Must Take to Boost Cyber Security

February 20, 2019 **Kayla Elliott**

Cyber security is a growing topic, whether it is at home with friends or family, or at work with the boss or colleagues. Online threats have continued to advance year-over-year with cyber crime costs consistently increasing. With the growing risks, it is important small and medium businesses (SMBs) understand the key steps they need to take to boost their cyber security, keeping their data and devices secure.

Update, Update, Update

Ensuring third-party applications and operating systems are updated in a timely fashion is critical. It is during these updates that any known vulnerabilities are patched, closing security gaps from hacker exploitation. By putting off these updates, SMBs are giving hackers an open invitation to infect their devices and steal company and consumer data.

Cyber Security Training

Employees can be a strong asset or the weakest link. Unfortunately, when it comes to cyber security, they're often the latter. Employees are typically uneducated on current cyber threats, or do not comprehend the risks associated with cyber crime. By taking the time to educate them on modern online threats including how to spot red flags associated with cyber crime, can help the SMB develop a stronger line of defense.

Deploying a Proactive Antivirus

Most of today's cyber security solutions are reactive. They place a heavy emphasis on endpoint detection and response (EDR). In addition, they use an outdated malware detection methodology, known as a blacklist. This list will allow for all unknown files to run, only blocking known threats. Unfortunately, with new threats evolving every day, keeping the blacklist updated is impossible. Instead, SMBs must focus on being proactive. The best proactive malware detection approach is the deployment of application whitelisting. This detection methodology only allows for known, trusted programs to run. All others will be blocked until proven secure.

Data Backups

Technology is great and has come a long way in the last 20 years. However, that doesn't mean all of the "hair pulling moments" have been resolved. Whether it is inopportune timing for an update, a program fails, or the hard drive crashes — there will be times backups are critical. SMBs should update their backups at least daily, possibly every hour, depending on business needs. Additionally, these backups should be stored on an external device or cloud-based service. If opting for an external device, it is important the backup device is only connected to the PC during the backup process.