Is your mobile workforce a security threat?

Boost business mobility, without risking security

Small and medium-sized businesses (SMBs) may have a smaller footprint than larger enterprises, but that doesn't mean SMBs are immune to threats. In fact, almost two-thirds of local SMBs have experienced a cyberattack in 20181.

56% of local SMBs have experienced a cyberattack.

Even the smallest breach can have a large impact. And with agility being a key advantage of smaller-sized businesses, on-the-go security should be a top-of-mind issue for all SMBs. Here's why, and how you can go about improving your security for devices, data and identity, while giving employees the edge of mobility:

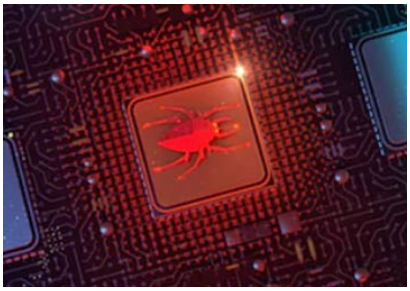
The workforce is increasingly mobile.

66%
of SMB employees perform work-tasks outside their typical workspace daily.

53%
of SMB employees view and edit work-related documents on work devices when working remotely.

65%
of SMB employees view work-related documents on a personal device.

How does that affect your security?



MALWARE AND OTHER THREATS
Your employee could pick up malware and other threats from unsecured external networks. When an infected device accesses the company network, your SMB is compromised.

DATA LEAKS
Increasing mobility may lead to data leaks. Documents and other information can be compromised when left unsecured in places like a printer queue or on network servers.

IDENTITY THEFT
Even if you set up your employees' work devices to secure them against threats, security breaches and identity theft may occur through their personal devices.

What can I do?

PREPARE FOR THE WORST

Look for start-up and access control to minimize damage from malicious virus and malware attacks.

Use PCs with a self-healing basic input/output system (BIOS), which automatically restores a system's BIOS to its previously safe state if attacked or corrupted.

KEEP YOUR DEFENSES UP

Protect data and simplify access with device access management and credentialed permissions to use removable storage when needed.

Look for integrated security features that enhance software tools and support, such as built-in privacy, self-encrypting hard drives, security kits and sensors.

SAFEGUARD USERS' IDENTITIES

Restrict access when needed with multi-factor authentication and protected passwords, even when they need to be reset.

Stop threats before they start with BIOS security, port control and boot options. For next-level security, use biometric solutions such as facial recognition, and iris and fingerprint scanning.

Want to improve your business mobility securely?
Start today.

In the Future of Work, business leaders will tap into talent across cities, region and countries, regardless of their location. But to make it work, it's important growing businesses have a strong security infrastructure in place.

With the right mobility devices and reliable tech partners, security is simple. Check out how HP business laptops and devices can help you equip your people with the freedom to work everywhere, with no extra security risks.

Find out more at www.hp.com/sg/business.

[1]Straits Times, "Report flags lack of cyber preparedness among SMEs in Singapore", https://www.straitstimes.com/business/companies-markets/report-flags-lack-of-cyber-preparedness-among-smes-in-singapore