The study revealed that SMBs increasingly face the same cybersecurity risks as larger companies, but only 28 percent rate their ability to mitigate threats, vulnerabilities and attacks as “highly effective.”

Root Cause of Data Breaches
The risk of negligent employees and contractors causing data breaches is getting worse.

 Attacks against SMBs have severe financial consequences
Among the SMBs that have been attacked in the past 12 months:

- $1.43M on average were spent because of the damage or theft of IT assets in 2018, vs. $1.03M in 2017
- $1.56M on average were spent because of disruption to normal operations, vs. $1.21M in 2017

Cybersecurity posture and governance in SMBs isn’t highly effective
- 47% of SMBs have no understanding of how to protect their companies against cyberattacks
- 35% of SMBs have no one function that determines IT security priorities

Passwords are the Keys to the Kingdom
40% of SMBs experienced attacks due to compromised employee passwords, costing $383,165 on average

Top 2 password-related pain points for SMBs:
1. Passwords being stolen or compromised
2. Employees using weak passwords

A lack of visibility into employees’ password practices is exacerbating the likelihood of attacks involving passwords

Human memory and spreadsheets are mostly used to remember passwords

How SMBs Can Protect Against Cyberthreats
- Enforce strong passwords and biometrics
- Implement password policies for employees
- Prepare an incident response plan
- Reinforce security across all devices that employees use
- Allocate adequate budgets and in-house expertise for cybersecurity

Keeper Security is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cyber theft. Keeper is trusted by millions of people and thousands of businesses to protect their digital assets and help mitigate the risk of a data breach.