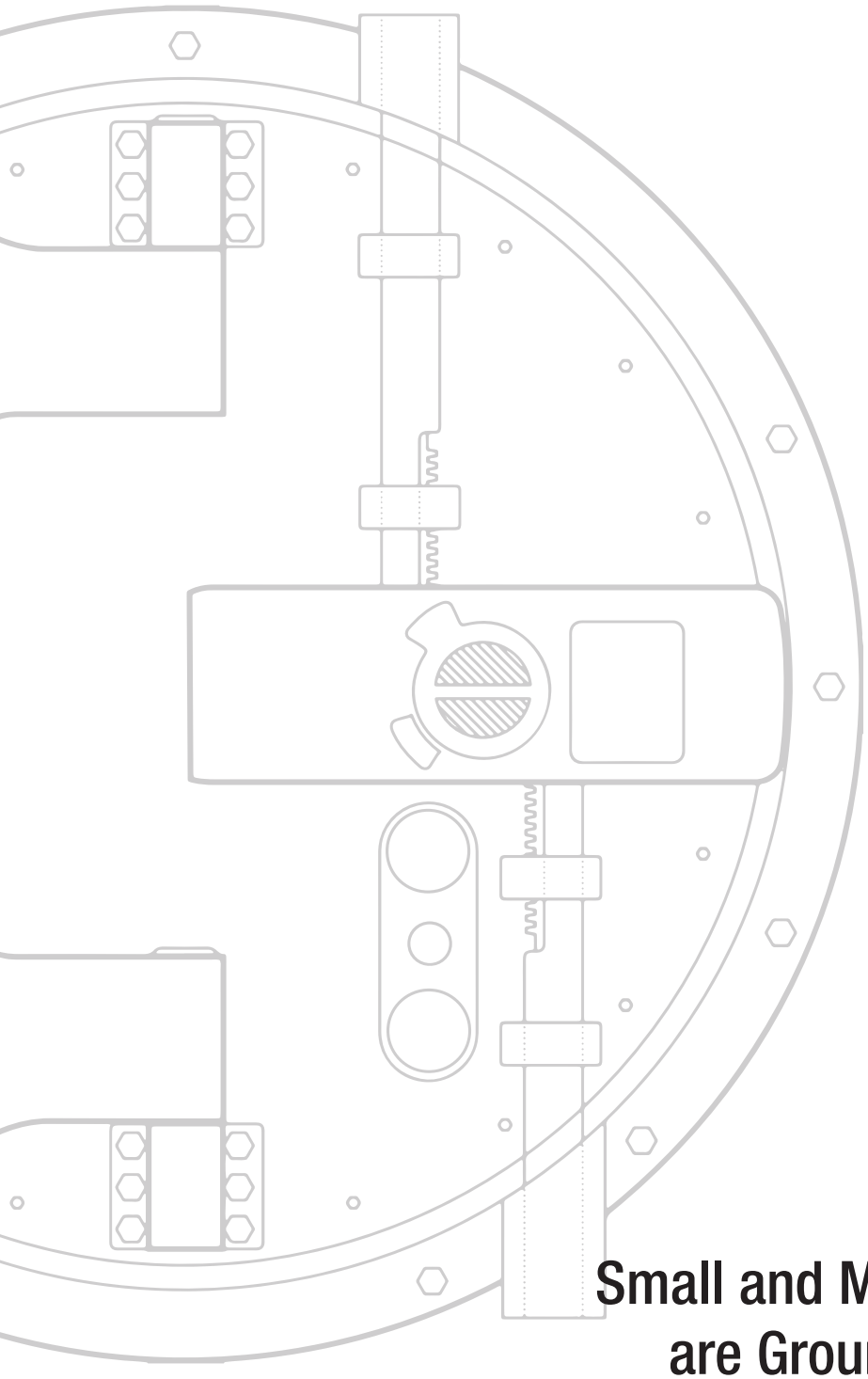
keeper



Survey Says

Small and Medium-Sized Businesses are Ground Zero for Cyber Attacks

Breaches Rampant, Confidence to Mitigate Risks Low

Would you park your car in a place where the odds are one in two it will be broken into? Would you stay at a hotel knowing that there's a 50% chance your credit card data and other personal information would be stolen? The answers are obvious.

Yet half of small and mid-sized businesses (SMBs) today will suffer data breaches involving customer and employee information this year. What's more, hackers simply step around conventional anti-virus solutions – the front line of data protection for most SMBs – in three quarters of known data breaches at SMBs.

These are sobering, if not startling findings in the recent State of Cybersecurity in SMBs survey conducted by the Ponemon Institute and sponsored by Keeper Security. Ponemon surveyed 600 IT leaders in this groundbreaking research. As noted by Larry Ponemon, the Institute's founder, "We've conducted many surveys on enterprise security in the past, but this unique report on SMBs sheds light on the specific challenges this group faces."

Security Challenges are Plentiful

The most notable of these challenges is that SMBs often lack the budget or in-house security expertise to protect systems and networks against the aggressive and persistent threats that target them. In fact, just 14% of the 600 companies polled rated their ability to mitigate cyber risks and attacks as highly effective (see Figure 1).

Figure 1

And the results in figure 1 above are probably even worse than they look. Ponemon says researchers have to account for the 'halo effect,' wherein respondents often rate their performance or that of their organizations higher than it really is.

In addition, the mission-critical task of prioritizing IT security initiatives and defenses is seldom centralized to one specific function in SMBs. The result: there is vastly reduced accountability for security, which has led to less informed decision making compared with the SMBs' enterprise counterparts.

An Ultra Dangerous Threat Environment

The bottom line? “Attacks are becoming more targeted, more sophisticated and more severe,” says Ponemon. “Meanwhile, for the SMB there is not enough money or enough people to fight back effectively.”

The research further shows that attacks are coming fast and furious at virtually all entry points into the SMB (see Figure 2). Therefore, any security strategy must be comprehensive by definition.

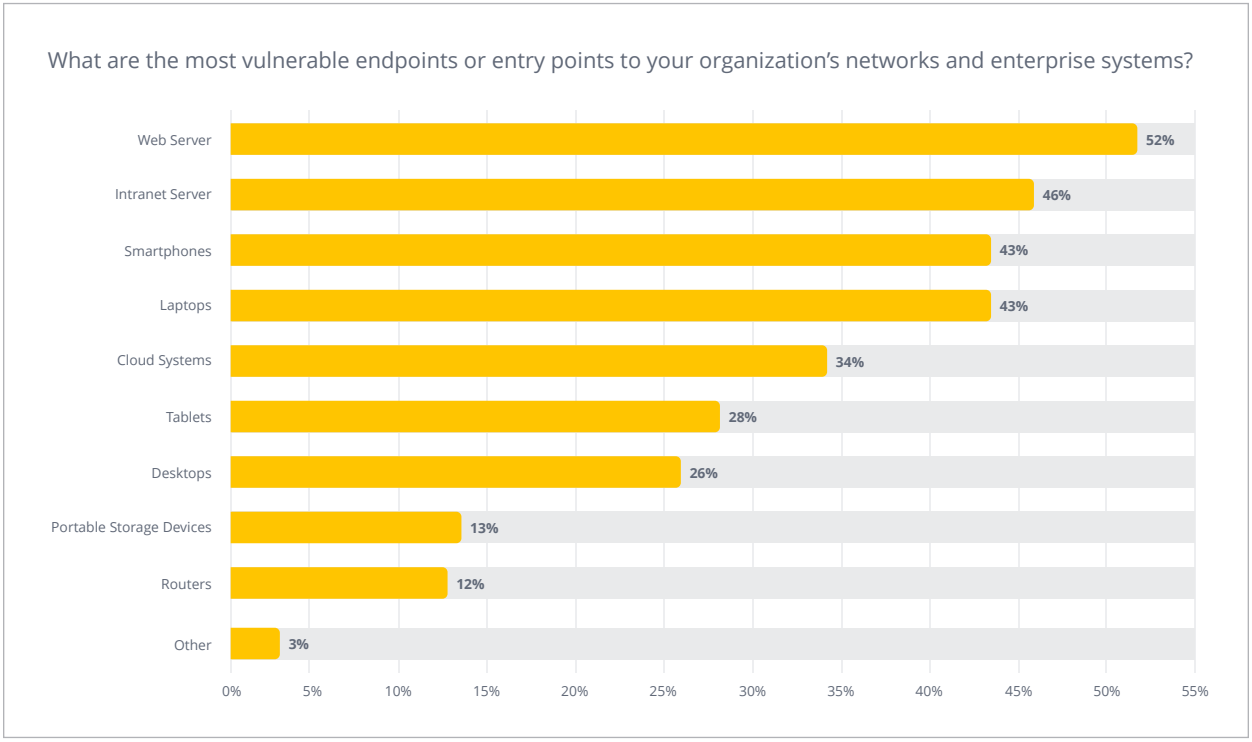


Figure 2

Things wouldn’t be nearly as bleak as they are if SMBs used more common sense about passwords. For example, strong passwords are widely held to be an essential piece of the security puzzle. But nearly six in 10 of companies surveyed by Ponemon have no visibility into employees’ password practices. These include use of unique or strong passwords and secure sharing of passwords with co-workers.

Not only that, but Ponemon found that even if an organization has password policies, 65% do not strictly enforce them. So it’s no wonder that 60% of employees use the same password for everything. By contrast, what is really needed in today’s hyper-threat environment is military-grade password encryption for smartphones, tablets and laptops.

Seeing the Light with Password Protection

The CIO of one company took matters into his own hands when he arrived at the Quest Federal Credit Union in Ohio two years ago. He quickly realized that the credit union had significant data assets in need of very high-grade security. These assets included member and employee data, business intelligence, proprietary handbooks and operating manuals, to name a few. And like the bigger financial companies, Quest has to comply with numerous regulations and data security requirements.

“I felt it was essential to extend a password protection solution to all employees,’ recalled Brian Sprang, Quest’s CIO.

Working with senior executives, Sprang listed requirements for such a solution. They included:

- Secure, encrypted password management
- An easy-to-use platform available to all OS’s and devices
- Visibility into password behavior and full audit capabilities
- Fast user deployment

Sprang and his team selected the password management solution from Keeper Security. “With Keeper we got a robust zero-knowledge security architecture, great password policy enforcement and visibility and protection for all devices regardless of platform or operating system,” he said.

The results were just what Sprang wanted. Full deployment to all employees took less than three days. He has what he termed “great visibility” into password use and compliance. Sprang also praised Keeper’s ease of use and zero-knowledge architecture which enables Sprang to monitor password behavior and effectiveness without having access to the employees actual password.”

“And we noticed a sharp reduction in password-related helpdesk calls,” Sprang says. “As I am the helpdesk, this was very important to me!”