KEEPER | PRESS RELEASE

Ponemon: Cyberattacks on SMBs Rising Globally, Becoming More Targeted and Sophisticated

66% of SMBs globally reported a cyberattack within the past 12 months, 76% in the U.S

CHICAGO, Oct. 8, 2019 – For the third consecutive year, small and medium-sized businesses (SMBs) have reported a significant increase in targeted cybersecurity breaches. A newly released global survey conducted by the Ponemon Institute, a world-renowned independent research organization, found that attacks against U.S., U.K. and European businesses are growing in both frequency and sophistication. Further, nearly half (45%) of the 2,000 respondents described their organization's IT posture as ineffective, with 39% reporting they have no incident response plan in place.

The 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses report underscores growing cybersecurity concerns best illustrated through the year-over-year trends dating back to 2016. The survey, commissioned by Keeper Security, measured responses from 2,391 IT and IT security practitioners in the U.S., U.K., DACH, Benelux, and Scandinavian.

"Cybercriminals are continuing to evolve their attacks with more sophisticated tactics, and companies of all sizes are in their crosshairs," said Dr. Larry Ponemon, chairman and founder, The Ponemon Institute. "The 2019 Global State of Cybersecurity in SMBs" report demonstrates cyberattacks are a global phenomenon- and so is the lack of awareness and preparedness by businesses globally. Every organization, no matter where they are, no matter their size, must make cybersecurity a top priority."

Significant 2019 Findings:

- **Overall, attacks are increasing dramatically** – 76% of U.S. companies were attacked within the last 12 months, up from 55% in 2016. Globally, 66% of respondents reported attacks in the same timeframe.
- **Attacks that rely on deception are rising** – Overall, attacks are becoming more sophisticated, with phishing (57%), compromised or stolen devices (33%) and credential theft (30%) among the most common attacks waged against SMBs globally.
- **Data loss among the most common impact** – Globally, 63% of businesses reported an incident involving the loss of sensitive information about customers and employees in the past year. That number is 69% in the U.S.– an increase from 50% in 2016.

"More businesses are experiencing highly-targeted, sophisticated and severe cyberattacks than ever before, yet the results of our study show they aren't doing enough to close the gap," said Darren Guccione, CEO, and co-founder of Keeper Security. "We sponsor this annual research with Ponemon because we want SMBs to understand that no target is too small for cybercriminals and it's not enough to simply be aware of the cyberthreats that exist. It's absolutely critical that these businesses take the next step toward cybersecurity preparedness and get a strong prevention strategy in place."

New Technologies, New Cybersecurity Risks

SMBs globally are adopting emerging technologies like mobile devices, IoT and biometrics despite a lack of confidence in their ability to protect their sensitive information. Nearly half (48%) of respondents access more than 50% of their business-critical applications from mobile devices, yet virtually the same portion of respondents (49%) said the use of mobile devices to access business-critical applications diminishes their organization's security posture.

In addition, a large majority of respondents (80%) think it's likely that a security incident related to unsecured IoT devices could be catastrophic, yet only 21% monitor the risk of IoT devices in the workplace. The study also suggests biometrics may be becoming mainstream; three-quarters of SMBs currently use biometrics to identify and authenticate or have plans to do so soon.

Regional Highlights:

United States

- 82% of U.S. respondents reported experiencing a cyberattack in their organization's lifetime, which is higher than any other region
- U.S. businesses are more confident in their in-house security expertise than any other region
- Nearly 9 in 10 (88%) of U.S. respondents indicated they spend less than 20% of their overall IT budget on security
- U.S. businesses are nearly twice as likely to be the victim of a cyberattack due to a company insider (77%) versus an external hacker (40%)

United Kingdom

- 65% of SMEs in the U.K. experienced a cyberattack in the last year, but the number of attacks in this region grew at half the pace they grew in the U.S.
- Web-based attacks (49%), phishing (48%) and general malware (42%) were the most common types of cyberattacks experienced in the U.K.
- U.K. respondents are losing confidence in their organizations' IT security posture, with 4% fewer rating it as very effective compared with 2018.

DACH (Austria, Germany, and Switzerland)

- SMEs in DACH are less concerned about employee passwords being stolen or compromised compared to the rest of the world, with only 58% expressing concern.
- In DACH, two-thirds of SMEs (66%) said laptops are one of the most vulnerable endpoints or entry points to their organizations' networks and enterprise systems, more than the global average of 56%.
- DACH businesses are more likely to inform and educate employees and third parties about the risks created by IoT devices than any other region, with more than a quarter (27%) currently doing so. Similarly, they are most likely to monitor the risk of IoT devices used in the workplace, with 25% actively monitoring.

Benelux (Belgium, Netherlands, and Luxembourg)

- While more than half (56%) of SMEs in Benelux experienced a cyberattack in the past 12 months, this region experienced 20% fewer than the U.S. for the same period (76%).
- Most respondents said mobile devices (60%), laptops (55%) and cloud systems (49%) are the most vulnerable endpoints or entry points to their organizations' networks and enterprise systems.
- More than two-thirds of businesses in Benelux (68%) agree or strongly agree that passwords are an essential part of a security defense strategy.
- Benelux respondents use biometrics to identify and authenticate more than any other region, with 51% saying they currently use them.

Scandinavia (Denmark, Norway, and Sweden)

- Almost two-thirds (64%) of SMBs in Scandinavia have experienced a cyberattack. Still, that's below the global average of 72%, which may point to better cybersecurity practices in this region.
- Respondents in Scandinavia are most concerned about protecting their intellectual property from cybercriminals (58%), while U.S., U.K. and DACH businesses are most concerned about customer records.
- The number of SMEs in Scandinavia who experienced situations when exploits and malware have evaded their intrusion detection systems (71%) surpassed the global average of 69%.
- Most respondents (56%) think the use of mobile devices, such as tablets and smartphones, to access business-critical applications and IT infrastructure diminishes security posture. This is above the global average of 49%, suggesting SMEs in Scandinavia may be less trusting of mobile devices compared to other regions.

Learn More During Upcoming Webinars

Keeper and Ponemon will discuss the findings of the Ponemon 2019 Global State of Cybersecurity in SMBs study in more depth during live webinars for the **U.S.** on Oct. 30 at 10:30 a.m. EST and for the **U.K. and Europe** on Oct. 31 at 3:30 p.m. GMT.

About the Ponemon 2019 Global State of SMB Cybersecurity Study

Ponemon Institute interviewed approximately 2,391 IT and IT security practitioners from companies in the U.S., U.K., DACH, Benelux, and Scandinavia between August 7 and September 30, 2019, using a web-based collection method. Respondents represented companies with headcounts ranging from 100 to 1,000.

About Keeper Security, Inc.

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-knowledge security and encryption software covering password management, dark web monitoring, digital file storage and messaging. Named PC Magazine's Best Password Manager (2018) & Editors' Choice (2018, 2019) and awarded the Publisher's Choice Cybersecurity Password Management InfoSec Award (2019), 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. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the Federal government through the System for Award Management (SAM). Keeper protects businesses of all sizes across every major industry sector. Learn more at **https://keepersecurity.com**.