KEEPER | PRESS RELEASE

Keeper Security Advises Retailers to Safeguard Digital Storefronts For the Holidays

New report reveals retailers experienced a tremendous loss resulting from account takeovers and stolen or compromised devices over the past 12 months

CHICAGO, Nov. 10, 2020 – Keeper Security has examined new challenges for the retail industry as part of its **Cybersecurity in the Remote Work Era: A Global Risk Report**. With the holiday season quickly approaching, Keeper Security is issuing an advisory for retailers.

In the report, IT and IT security practitioners from around the world struggled to maintain their security posture as employees migrated to remote environments. When analyzing responses from the retail sector, the concerns are heightened:

- Since COVID-19 began, retailers have experienced a higher increase in account takeovers (62%) and compromised/stolen devices (56%) compared to global responses (49% and 48% respectively).
- Retail companies are most concerned about protecting financial information (56%) and customer records (45%).
- But they struggle with insufficient budget (43%) and no understanding of how to protect their organization from cyberattacks (40%), which prevents IT security posture from being fully effective during remote work environments.
- In the last 12 months, more than a quarter (27%) of retailers lost $5M to $10M or more from theft or damages to IT infrastructure and assets.
- Nearly a quarter (23%) of retail employees who are teleworking due to COVID-19 have access to their organization's critical, sensitive and proprietary information (e.g. privileged users). This explains why retailers are concerned about the lack of physical security in the employee's remote workspace (47%) and personal devices used to access company materials becoming infected with malware (29%).

Retailers looking to strengthen their security posture ahead of the busy holiday season - starting with Singles Day, which is one of the biggest ecommerce holidays before Black Friday/Cyber Monday, should take the following steps:

1. **Secure and Implement BYOD Policies:** Define clear procedures for reporting and responding to security incidents. This can include policies and parameters for employees' personal devices like requiring a PIN-based lock on phones, multi-factor authentication and auto-logout timer for work-related apps and materials. In the event their personal devices are stolen or misplaced , this helps add another layer of security.

2. **Educate and Train Employees on Cyberattacks:** Train your employees to never click on any unsolicited links or file attachments, even if it appears to have come from a legitimate source. Phishing and other scams have evolved in recent years and in addition to email, cybercriminals also frequently target victims through social media messages or SMS.

3. **Implement an enterprise password manager such as Keeper:** In addition to giving IT admins visibility into employee password practices and enabling them to enforce password security policies, such as strong, unique passwords and 2FA use, Keeper helps prevent employees from entering their credentials on phishing sites. Weak and compromised passwords are the biggest threats to a business's cybersecurity. A password manager like Keeper can not only help employees create, store and keep track of passwords, it also allows IT teams to add two-factor authentications and other parameters to these accounts.

For more information or to download the full report, visit: **keepersecurity.com/ponemon2020.html**

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the highly-rated and patented cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM). Learn more at **keepersecurity.com**.