BARNES & THORNBURG LLP

CYBER SECURITY TERMS GLOSSARY

- **Encryption** - The process of converting information or data into a code, especially to prevent unauthorized access.
- **Hacking** – The process of using computers and the internet to access other's computers without permission.
- **Keylogger** – Persons who monitor keyboard use, including any information typed into a system such as email content, log-in information for local and remote systems and financial information such as credit card and social security numbers. Keyloggers may either require the cyber attacker to obtain data from the system or actively transfer the data to another system through email, file transfer or another method.
- **Malware** - Malware includes malicious software such as viruses, keyloggers and other spyware used to steal personal information or other sensitive data.
- **Phishing** – A scam through email or other electronic communication by which the user is tricked into revealing person information to a person who may use it illicitly.
- **Priority access management (a/k/a least privilege access)** - The principle of least privilege (POLP) is the practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs.
- **Ransomware** - A type of malicious software designed to block access to a computer or computer system until a sum of money is paid to the attacker.
- **Skimming** – A method used to steal credit card information, which can be done manually (by a corrupt employee or at a restaurant) or through a device (often placed at gas stations or ATM machines).
- **Spear-Phishing** – A form of phishing that targets by its content a specific type of person, e.g., HR, financial, legal.
- **Spoofing** – When a person or program successfully subterfuges as another by falsifying data.
- **Spyware** – Software that aims to gather information about a person or organization without their knowledge, that may send such information to another entity without the owner's consent, or that may take control over a device or system without the owner's knowledge.
- **Trojans** - Programs that, when installed on your computer, enable unauthorized access and spamming from such device.
- **Virus** – A program that comes onto your computer – often through email or website use – and replicates itself quickly using up all system memory available.
- **Vulnerability** – A flaw in a system or computer itself that can leave the system or computer open to attack.
- **Whaling** – A technique use to commit fraud by targeting a specific person in an organization. This type of attack is well planned, and requires knowledge of the individual and his/her travel and communication habits.

BARNES & THORNBURG LLP

Jason A. Bernstein
Phone: (404) 264-4040
jason.bernstein@btlaw.com

Barnes & Thornburg LLP
3340 Peachtree Road, N.E.
Suite 20900
Atlanta, Georgia 30326
www.btlaw.com

Partner

- Data Security & Privacy (Group Co-Chair)
- Technology Agreements
- Intellectual Property

Rev. 2/2024

Cyber Security Terms Glossary.docx