AGMA GLOBAL
Advancing Intellectual Property Protection

FOR IMMEDIATE RELEASE

Media Contact:
Stephanie Olsen
Lages & Associates
(949) 453-8080
stephanie@lages.com

AGMA to Tech Industry: Don't Lose Focus When It Comes to Protecting Digital IP

Non-Profit Technology Consortium Advocates a Proactive, Back-to-Basics Approach to Keeping Digital Assets Safe

WASHINGTON, April 27, 2020 – In the complex world of digital intellectual property (IP) protection, it's time to refresh on security fundamentals – before it's too late. According to AGMA, a non-profit organization solely focused on intellectual property protection for the high-tech industry, a simple, forward-thinking approach utilizing basic information security best practices will go a long way toward securing a business's digital assets.

More than just a cornerstone of innovation and technological advancements, digital IP represents the most rapidly growing portion of the global economy – making it an especially attractive target for criminals. By 2021, Cybersecurity Ventures estimates that cybercrimes will impact businesses across the globe to the tune of $6 trillion annually – the University of Maryland calculates that's one malicious attack every 39 seconds. Every company with digital assets – from software to music to firmware, and everything in between, is at risk. Due to digital IP's intangible nature, protecting it is an especially difficult task that comes with its own unique challenges.

Set a Clear Focus

On a mission to hinder threats to IP and render these activities more difficult, undesirable and unprofitable, AGMA has identified six key areas of focus as 'must-haves' to protect digital IP on a basic level:

1. **Access Control Policies and Procedures** – Typically the very first requirement in information security, access control is a must-have when it comes to protecting digital assets. Uncontrolled or poorly controlled access to data and business systems can leave organizations exposed. Ensuring a comprehensive access review of all applicable systems is imperative to identifying access risks. This should include appropriately restricting access and ongoing reviews of access levels. A robust access control policy should outline the controls placed on both direct and remote access to computer systems to protect networks and data.

2. **Event Logging** – Event logging is essential to maintaining a healthy system, as the ability to see what is happening in the environment is crucial. Log and retain records of what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. To monitor and report on "bad actors," logging should be comprehensive.

3. **Monitoring and Reporting** – Appropriate data analytics should be used to monitor and identify trends or transactions outside of norms or expectations on an ongoing basis. Any unauthorized use should be reported to the appropriate parties, and enforcement actions should start immediately.

4. **User Awareness and Training** – Information security awareness training is an effective tool against IP theft – when specifically targeted to the appropriate users. Ensuring that users are made aware of the ways in which they might unintentionally expose IP is of extreme importance.

5. **Security by Design** – Security should be at the core of design. From conception through market release, security should be a top priority throughout the entire lifecycle of a digital asset. Planning and policies for building security up front (vs. after the fact) should be implemented and adhered to, as it is much more expensive to add security later than it is to design it in right from the start. Security capabilities should be proactively included within applications, programs and infrastructures.

6. **Continuous Improvement** – Securing digital IP is not a "one and done" activity. Monitoring information security best practices, performing risk reviews, and scaling security policies and controls continuously is needed to keep ahead of emerging threats. Companies should drive a culture and implement processes that prioritize security improvements on an ongoing basis.

Urgent situations – including product deadlines, customer crises or fast-approaching sales goals – often cause protection protocols to break down. According to AGMA president Sally Nguyen, "Don't put yourself in a position where you lose focus on security. It's an easy mistake to make in the hyper-competitive business world of today – and the bad guys know it. Cyber criminals are looking for businesses to drop their guard. Ensuring you have protocols in place to proactively address threats puts you in a better position to protect your business."

Additionally, as a best practice, AGMA strongly encourages companies to ensure they comply with the key information security standards and requirements applicable to their areas of business. These may include guidelines from International Standards Organization (ISO), and government standards such as HIPAA and NIST, in the United States and GDPR in the European Union.

Knowledge Is Power

"AGMA exists to educate the industry and the public – by sharing and developing best practices in the fight against IP theft," continued Nguyen. "We do this through worldwide events, educational initiatives, industry guidelines, and more."

To learn more about AGMA, or to become a member, please visit www.agmaglobal.org.

About AGMA

AGMA is a non-profit organization comprised of influential companies in the technology sector. Incorporated in 2001, AGMA's mission is to address gray market fraud, parallel imports, counterfeiting, software piracy, and service abuse of technology products around the globe. The organization's goals are to protect intellectual property and authorized distribution channels, improve customer satisfaction and preserve brand integrity.

AGMA welcomes technology manufacturers, as well as persons or entities that own or hold intellectual property rights to finished goods outside the technology industry; government and law enforcement officials; product and service providers who provide goods and/or services to combat gray market fraud, counterfeiting and warranty and service abuse threats. AGMA uses a variety of avenues to cultivate change in the marketplace, including event speaking, educational initiatives, benchmark studies, industry guidelines, and, where appropriate, public policy advocacy. To learn more about AGMA’s initiatives or to become a member, please visit www.agmaglobal.org or follow them on LinkedIn and Twitter.

# # #