February 11, 2015

PRESS RELEASE
FOR IMMEDIATE RELEASE

VIR-SEC® Introduces Cyber Security Standards, Sets Example for Best Practices in Data Security

WASHINGTON, D.C. — Vir-Sec, Inc., a cybersecurity company based out of Clearwater, FL, is introducing a set of cyber standards to accompany the commercial rollout of its SecureAxcess™ cybersecurity technology. The current cybersecurity strategy deployed by companies is to identify, chase, close, and mitigate damage after a cyber breach happens. Vir-Sec's cybersecurity standards and strategy are aimed at prevention of cyber-breaches and protection of internal data networks.

Vir-Sec says its standards and practices set precedent for best practices regarding U.S. companies in protecting their secure internal networks and for the U.S. government in protecting critical infrastructure, and can provide policymakers with a framework for federal standards for protecting internal data.

VIR-SEC® Data Security Standards:

- **Secure data can only be accessed through a non-browser method**. By eliminating browser access to secure data and using a non-browser method to access secure data, most major vulnerabilities and methods of attack are eliminated.
- **Promotional websites and secure data websites must be maintained at unique IP addresses**. Hackers were able to exploit vulnerabilities of public-facing websites and data portals in recent retail and financial data breaches. By maintaining them in this manner, hackers will only have access to public content and secure data can be isolated and only accessed by those who need to access it.
- **True two-factor authentication is mandatory when accessing secure data**. When an individual is accessing secure data there should be no such thing as anonymity. As a provider of security, there should always be a record of what individual accessed the data, what data they accessed, when they accessed it and where they accessed it from. This provides forensic data in case of a breach and also ensures authentication without data mining.
- **Secure data that has been accessed cannot be written to any permanent storage device, including temporary data**. Any data written can be found and exploited by hackers. Deleting the data only removed the location of the data, not the actual data itself and therefore can still be exploited.

- **Access to secure data cannot be granted through any installed applications**. Hackers can compromise browsers and other installed software easily. The best way to secure data and access to data is to require a token that allows authentication to happen at a secure, off-site location.
- **No data mining can be performed by the application providing the access to the internet application or secure data**. Data mining is a backdoor and can allow hackers to exploit users by exploiting their security provider. Vir-Sec doesn't view the communications of users to the secure server, Vir-Sec only time stamps who, when, and where the individual authenticated to the application server, never any communications between the user and server.

Vir-Sec believes its standards will help U.S. companies and the government better secure their data without disrupting the technologies they already use. Protecting internal data from external threats, they explained, is the first step to a successful cybersecurity strategy that prevents cyber-attacks as opposed to just mitigating damage and chasing the problem afterwards.

"Our standards are common-sense prevention methods by which to secure internal data and remove major vulnerabilities," said John Foti, Director of Government Affairs for Vir-Sec. "Our standards now set precedent for best practices in data security and in protecting critical infrastructure from cyber-attacks."

Vir-Sec's announcement comes as the House Subcommittee on Commerce, Manufacturing, and Trade convened a hearing on data security with industry stakeholders at the end of January. The hearing was designed to gauge an understanding of where industry stakeholders were on a national law regulating data security.

The Subcommittee and parties involved displayed a clear interest during the hearing in setting a national standard for data security that will preempt state laws that create obscurity in an interstate activity.

"A single requirement across the states would give companies some confidence that their methods are sound in handling electronic data, an inherently interstate activity," said Subcommittee Chairman Rep. Michael C. Burgess, M.D. (R-TX). "Moreover, it would put all companies on notice that if you fail to keep up with other companies and if you aren't learning from other breaches, you will be subject to federal enforcement."

Vir-Sec agrees with Chairman Burgess and is offering to present its standards and be a resource to the Subcommittee to showcase best practices for protecting internal networks and securing data. By introducing the standards that accompany Vir-Sec's SecureAxcess™ technology, the U.S. government can now make a definitive determination whether or not companies that have been breached have deployed best practices in protecting their internal networks.

"Vir-Sec has eliminated all major vulnerabilities and typical methods of cyber-attacks," said Foti. "If other companies don't have the same standards and can't equally protect their internal networks, then they should have to answer to federal law enforcement officials."

CONTACT:

Chris Murphy
Founder, Chairman & CEO
Vir-Sec, Inc.
chris.murphy@vir-sec.com

John Foti
Director
Government Affairs
Vir-Sec, Inc.
Email: JFoti@Vir-Sec.com

###