From: **Eric Rabe** e.rabe@hackingteam.com
Subject: Information from Hacking Team - 22 July 2015
Date: July 22, 2015 at 6:29 AM
To: Eric Rabe e.rabe@hackingteam.com

ER

We are providing this information at www.hackingteam.com in response to various questions and commentary since the attack on Hacking Team was revealed on July 6. It is for your immediate use.

You are receiving this because of your previous interest in Hacking Team, but if you do not wish to receive future emails such as this one, just let me know.

Best,

Eric

Eric Rabe
Chief Marketing & Communications Officer

mobile: +39 337 1143876
Skype: ericrabe1
e.rabe@hackingteam.com

News Release

July 22, 2015

Statement from Hacking Team

The single fact not generally covered by news media is this: there is only one violation of law in this entire episode, and that one is the criminal attack on Hacking Team. The truth is that the company itself has operated within the law and all regulation at all times.
However, commentators dislike the fact that strong tools are needed to fight crime and terrorism, and Hacking Team provides them. So the company is being treated as the offender, and the criminals who attacked the company are not. Had a media company been attacked as Hacking Team has been, the press would be outraged.

Here are the facts:

- Hacking Team was the victim of a criminal act or acts sometime before July 6. The attackers stole and then exposed via the Internet company proprietary information as well as personal information of our employees and even some information about our clients.
- Data from investigations conducted by Hacking Team clients was not exposed during the attack. Such information is only maintained on the systems of clients, and cannot be accessed by Hacking Team.
- The criminals exposed some of our source code to Internet users, but by now the exposed system code is obsolete because of universal ability to detect it. However, important elements of our source code were not compromised in this attack, and remain undisclosed and protected.

- The company has always sold strictly within the law and regulation as it applied at the time any sale was made. That is true of reported sales to Ethiopia, Sudan, Russia, South Korea and all other countries.
- There have been reports that our software contained some sort of "backdoor" that permitted Hacking Team insight into the operations of our clients or the ability to disable their software. This is not true. No such backdoors were ever present, and clients have been permitted to examine the source code to reassure themselves of this fact.
- Hacking Team has not been involved in any program to use airborne drones as has been reported.

100% Compliance with laws and regulations

Hacking Team has been accused of selling technology to various countries at a time that such sales were banned. This is not true. In the case of every sale, Hacking Team has complied with regulations in effect at the time of the sales. Today the company complies with new regulation developed in 2014 and enacted in January 2015. Under this new regulation, Italy reviews all sales of Hacking Team technology in accordance with European Union and Wassenaar Arrangement requirements.

The sale of "weapons" have been banned to certain countries. Hacking Team technology has never been categorized as a weapon. At the time of the company's only sale to Sudan in 2012, the HT technology was not classified as a weapon, arms or even dual use.

In fact, it is only recently that has Hacking Team technology been categorized under the Wassenaar Arrangement as a "dual use technology" that could be used for both civil and military purposes. Dual use technologies are regulated separately from weapon technologies.

# # #

For further information:

Eric Rabe, Chief Marketing and Communications Officer, +39 337 1143876

info@hackingteam.com