SM4 Safety
Planning • Prevention • Response • Recovery

# Hidden Cyber Security Threats

**By: William Hoffman**
Product Manager for Cyber Security Products, Satcom Direct

Cyber security is a hot topic in business aviation, but some of the most vulnerable targets are not taking the needed steps to protect themselves on the ground or in the air. Cyber espionage continues to grow at a rapid rate. Cyber criminals are stealing intellectual property, ransoming personal and sensitive information, impersonating businesses in the marketplace, and phishing for insider information for trading.

Corporations and high net worth individuals might have strong security practices, but hackers have learned to identify weak links. Cyber criminals are looking at the complete chain surrounding these highly valued targets. For example, they might not have the capability to break through a strong firewall of the desired target, but they might be able to hack into another source connected to the target. Law firms, accountants, publicists, hotels, aircraft, and even coffee shops are all connections or settings where hackers can discover backdoor access to highly valued targets.

Highly valued targets and those that support them often fly for business. Passengers expect connectivity, but not all passengers understand the lurking cyber security threats that are present when connected in the air. Passengers mistakenly believe that they do not have to worry about cyber threats while flying. But, an unsecured aircraft is one of the easiest places for a cyber criminal to attack.

**Take these real-world situations, for example:**

In 2016, a hacker impersonated a record label employee and sent an email to a management group asking for Lady Gaga's audio files. A few clicks later the files had made it to the hacker's hands.

In 2017, several studios were hacked in Hollywood. Some of the affected studios included Netflix, ABC, NBC, and CBS. Episodes of NCIS: Los Angeles, Portlandia, and Orange is the New Black were stolen. The studios had solid firewalls, but the hacker found a way to attack the studios through a postproduction company that was not as secure. The hacker demanded that

Netflix pay a ransom, or it would share the stolen episodes of Orange is the New Black. The media giant refused, and the hacker published 10 episodes of Netflix's hit show before the season premier.

Media is not the only intellectual property targeted. Cyber thieves are also looking for cutting edge technology. Intellectual property creates a unique advantage for a company, and cyber theft is hurting that unique advantage. Randolph A. Kahn stated in Business Law Today, "Economic espionage (sometimes called industrial espionage) is a major drain on competitive advantage, unique IP, and market share." Kahn asserts that cyber-attacks are most often used to steal intellectual property.

Three Chinese nationals were charged with coordinated and unauthorized cyber-attacks for stealing intellectual property from several companies, including Siemens. The intellectual property stolen included data from transportation, technology, and energy units of the company. Trimble, which was working on a new global navigation system. According to SecurityWeek, access to these companies was gained through spyware-laden security products for phones and computers.

Cyber criminals are also hacking into systems and ransoming personal information. World-renowned soccer player David Beckham had his emails hacked and held for ransom. Beckham did not pay the ransom, and the emails were released. The cyber thief obtained the emails by hacking Beckham's publicist. The emails contained information about his disappointment for not being knighted. Although Beckham's team asserted that the emails were doctored, his brand did take a negative hit from the incident.

Insider trading is another motive for hackers. A group of hackers attempted to access the systems of several companies. They were not successful, but they did discover a weak link in the companies' security -- their law firms. The hackers were identified as foreign nationals, and they used the stolen information to gain more than $4 million from insider trading.

It's happening in aviation, too. Between January 1 and March 31, 2018, Satcom Direct blocked hundreds of cyber-attacks on aircraft that were monitored by the company's cyber security solutions. These aircraft were protected, but there are still many aircraft that are flying with unprotected in-flight networks.

Cyber-crime is not going to abate anytime soon. Anyone or any business that conducts online activity needs to evaluate where hidden threats could be lurking. More importantly, this evaluation needs to extend beyond the four surrounding walls to encompass the complete chain of access. It only takes one weak link for cyber criminals to find their next victim.

Satcom Direct

Satcom Direct’s SD Data Center brings enterprise-level security audits to data transmissions on the ground and in the air. SD’s compliance experts use a consultative approach to provide aircraft cyber security audits focusing on both the cabin and the ground network. The audit addresses cyber security issues, best practices in network design, and policies and procedures, all to ensure passenger data is classified and properly protected.
http://www.satcomdirect.com