# Business Aviation Confronts the Cyber Threat

Information assurance and cyberdefense have been vital areas for aerospace companies for some time – but the business aviation industry has perhaps not yet seen much reason to prioritize cybersecurity. All that is beginning to change, though, as the sector is increasingly coming to the attention of cybercriminals and hackers.

Member organizations are seeing increasingly frequent attempts to breach digital defenses, according to Richard Mumford, chairman of BACA, the UK's trade association for the business aviation industry. At present attacks vary greatly in their sophistication and methodologies but have one thing in common: They are motivated by money.

"All of the reports we have seen have been entirely focused on financial gain," Mumford tells *ShowNews*. "I have seen no evidence of hacks taking place for any other purpose. It may be that some attacks in other areas of the market, and in other areas of aviation, have been designed to steal classified, proprietary or operationally sensitive data, so far the business aviation community is faced primarily with lower-tech attempts at stealing money. Perhaps as a result, Mumford says no BACA member has as of yet reported a successful attack.

BACA chairman Richard Mumford

**If our members can provide us with coherent evidence to support a crime, we will refer that on to the police, border force, the CAA or such other authority as might be relevant.**

***—Richard Mumford, BACA Chairman***

"It seems to be opportunistic in nature. The kind of attacks that are designed to secure one-off payments rather than anything more organized and concerted," he says.

"A typical example has been where the criminal has managed to clone an email account and has sent emails from that cloned account to operators or brokers asking that future payments be redirected to a new bank account. Of course, this should set alarm bells ringing with any professional business, and indeed that is what has happened here. Most of our members will have specific policies in place to prevent this type of mistake from being made."

The defenses against attacks of this nature are, as a consequence, procedural rather than technological in nature, and straightforward for organizations to implement. Training staff to be on the lookout for tell-tale signs of a fraud attempt sent via email will go a long way to ensuring the resilience of the company. Just as important – and perhaps a little more difficult to implement in an industry where competitive advantages are hard-won and zealously guarded – is a willingness to share information and intelligence on attacks across the sector.

"I have been recently approached by the police over an initiative to gather data about fraud," Mumford says. "If our members can provide us with coherent evidence to support a crime, we will refer that on to the police, border force, the CAA [Civil Aviation Authority – the UK's aviation regulator] or such other authority as might be relevant. We are very lucky that our professional members care sufficiently about the integrity of the market that they are prepared to share their experiences to help their competitors ensure that they stay one step ahead of the criminals."

**—Angus Batey**

## Maybe *Don't* Call the Police

Data-sharing is not just an issue in a cross-industry sense. Calling in police may not be the best option for a company that has suffered an attack, and this is another area where BACA chairman Richard Mumford feels organizations such as his can help the sector develop a coherent response to fraudsters, whether they use the internet or not.

"There is often a low degree of confidence about the police and their ability to deal with fraud," he says. "This is not a criticism of the police: It is a highly specialist area and requires significant investment of time, money and specialist resources that the police struggle to provide. Recovering assets removed by fraud is a very expensive exercise, and accordingly clients will only generally pursue it either on a point of principle, or where there are large sums of money at stake.

"Involving the police can make civil recovery slower and more difficult," he adds. "It can also effectively prevent or harm the chances of swift civil remedies, such as freezing bank accounts. Generally, therefore, clients will refer matters to the police when they are too small to justify handling themselves, or where a matter has been conducted and civil remedies have failed or concluded." **—AB**

Money makes the crooks come 'round.