EINPRESSWIRE

Consumer Cybersecurity expectations that the aviation industry should embrace

Hensley Elam CEO releases cybersecurity awareness call to action for charter operators and fixed base operators.

Russ Hensley CEO CISSP

LEXINGTON, KENTUCKY, USA, November 24, 2021 / EINPresswire.com/ -- As a Certified Information Systems Security Professional (CISSP) I am asked by both business associates and friends for advice on how to keep data and records secure. Data security is much different today than it was even 5 or 10 years ago. Data breaches are a daily occurrence by both small and large business as well as personally. There are many industry standards in place but those standards have not been adopted across the board, leaving glaring holes that put businesses and individuals at risk. Let me explain.

Cybersecurity’s meaning in this article will be inclusive of what may be considered good data housekeeping and not exclusive of defending off hackers. For example, is data being backed up off-site; is software being kept up to date; and is staff being trained on how to see a phishing email? Not all companies are doing this, but yet people every day entrust companies with their personal and financial data.

In the past 18 months the United States has experienced much turmoil because of repeated cyber breaches that either steal data to gain access to a banking account or credit card number or ransom essential company data for a hefty price. This has brought many people and companies to a screeching halt while they scramble to recover their data and business. This has been brought to the attention of many via the world media.   For example, in the past few months the news has reported about ransomware affecting national gas pipelines as well as daily reporting about how thousands of American businesses have been exploited. As a result of this, the presidential administration is proposing $2 billion for cyber defense grants to

> "These actions should help their members and clients understand the responsibility of the data they hold, where it is held and how to protect it using best practices."
>
> *Russ Hensley CEO CISSP*

government agencies. This topic is squarely now on the minds of the American consumer so you can be assured that it is on the minds of travelers who are passing through FBO and Charter operator doors.

In my review of audit and program management documents from industry leaders, like the NBAA, Wyvern and FAA, they currently do not address data security in ways that other industries like retail, banking, or healthcare do. For example, retail organizations that process credit card transactions have to abide by PCI compliance, which is audited on a regular basis additionally. However, businesses that do smaller volumes are not audited by an outside company. They are expected to self-audit, potentially leaving many gaps in the system. Furthermore, because no one is auditing the actual security posture of places like FBOs or charter operators, their security may be lacking leaving the business and their client's data vulnerable as well as their own data.

Implementation of the NIST Cyber Security Frameworks and other standards are a requirement for day-to-day operational integrity coupled with training programs specific to cyber security in many industries. Yet, there is a glaring absence of discussions about this outside of the airline industry in air travel even at a basic level. In my anecdotal review of multiple sources, only one article was published by NBAA in the last year addressing the issue in aviation. Outside of that the rest of the information is typically geared toward security of aircraft avionics systems with no mention of actual good cyber security hygiene to protect consumer information or the back-office data.

FBO and Charter operators also fall under federal, state and local cybersecurity laws in the areas where they are based or operate in some cases. If operating in the European Union, they may have obligations to GDPR data requirements.

Industry leaders and auditors must rapidly adjust their business practices to incorporate a specific and direct approach to information security management programs. These actions should help their members and clients understand the responsibility of the data they hold, where it is held and how to protect it using best practices.

While we wait for the changes to take place, what can businesses do to protect themselves and protect their consumers? My recommendations come from two standpoints, tactical and strategic.

A tactical short-list of places to start.

- First – backup, backup and then backup off-site. Hurricanes, tornadoes, fire, ransomware all have this in common. Have MULTIPLE entire system backups of data and systems, one of which is off-site.

- Apply multi-factor authentication to all cloud services and remote access passwords.
- Patch everything and patch often.
- Endpoint Detection and Response – In the past this would be called anti-virus. Now, it’s more computer artificial intelligence protection to see the EDR anticipate malware is working on your machine and about to move to another platform.
- Train your staff – Security awareness training about what things like hackers and malware want you to do and the steps to report when they see something suspicious are critical.

Strategically:

- Implement the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). This framework of policies is based on best practices to get staff, IT service providers or any other person involved in a business on the same page.   This is a very well-organized set of checks on 5 areas: Identify, Protect, Detect, Respond and Recover your businesses data.   The framework is not something that only a technical person should review. This is a core business document that should at least be reviewed and familiar to the owner or CEO.
- Partner with a managed cybersecurity firm with tools in place where they have experience with these areas and can help implement them.

About the author - Russ Hensley is a Cyber Security professional with over a decade of direct security experience consulting banks, healthcare entities, flight departments and a lengthy list of other industries, with over 26 years of general IT experience running one of Kentucky’s largest IT service companies.   He is also a multi-engine commercial instrument airplane pilot, AOPA Life Member, NBAA member, Civil Air Patrol member and avid aviation supporter having served on several airport boards and sub-committees. Hensley / Elam is an NBAA corporate member.
www.hea.biz

Camille Clemons
Hensley Elam
+1 859-389-8182
cclemons@hea.biz
Visit us on social media:
Facebook
Twitter
LinkedIn