Aerospace and the threat of a cyberattack

The world of cyber security is never ending, and forever connected. The cyber world is growing by the millisecond and with it, the threats of cyber security breaches in aerospace are growing as well. From sophisticated simulations and 3D printing to robotics and automation, and computer-aided manufacturing (CAM), all sectors of aerospace—aviation, space and unmanned aerial systems—are vulnerable to the potential disruptive and debilitating risks of cyberattacks.

Most people think of a shadowy figure crouching over a bright screen in a dark room when conjuring up images of a computer hacker, but cyber threats can look like something as simple and innocent as an email asking you to reset an account password. This is called phishing, and is one of the most prolific ways cyberattacks are introduced into a business' network and spread near and far.

In the cyber security world, the bad guys are manipulative and insightful. They are adept at using the weakness of human nature to gain access to the information they wish to exploit. Tom Captain, retired vice chairman, Deloitte LLP Aerospace and Defense, warns that "it is important for aerospace companies and their suppliers and vendors to invest in addressing this strategic vulnerability."

While it is imperative every industry add measures to prevent cyberattacks, it is critical for aerospace. Think of an airline or maintenance repair operator doing heavy maintenance, or a machine shop using a software-guided design to manufacture the parts or components of an aircraft. These are at risk of potentially dangerous cyberattacks. "As the design and manufacturing of commercial aircraft have become more reliant on the

internet and computer modeling, the risk and exposure to cyber threats has increased. The Stuxnet virus that infected the centrifuges at the Iranian nuclear facilities has demonstrated that our CAD and CAM computerized systems are targets for strategic and tactical cyber threats," said Captain.

By starting with a secure network, a company can prevent many of the obvious and very simple cyber security attacks. Implementation of comprehensive endpoint protection solutions such as antivirus tooling, behavioral tracking and firewall protection are standard approaches today, and should be maintained and monitored at all times. These types of programs will look for codes that are not recognized by the systems, and help to block and notify the user of abnormal activity within their system.

According to the FBI"s cyber security division, monitoring company systems and acting as quickly as possible when and if an attack does occur is crucial to the protection of a company's intellectual property and/or to preventing disruption and manipulation of a company's work activity. The FBI further recommends dividing the company network with separate routers and additional firewalls. Implementing separate secure networks, called "air gapping," stops a would-be hacker from creating havoc on an entire network.

Being proactive by setting up preventive security measures will only get you so far if your employees are not properly trained. Every single employee in a company must be aware of the types of attacks used to gain access to company or personal information. Phishing attacks are very common, and can be disguised to look exactly like a legitimate concern to the employee. Phising is a simple concept, and employees can easily fall victim if they are not trained to look for telltale signs of an attack.

Hackers are getting more and more mature, and are shifting to a new, more targeted form of phishing. "Spear phishing" is a targeted attack on an individual at a company that would have access to the exact information that the hacker is seeking. They do this by researching and finding as much information as they can about the employee's position at the company, as well as their interests, family members and their interests, and even their possessions. This information is easily gained by looking at an employee's profile on the company website and personal and professional social media accounts. Employees should be encouraged to guard their personal information and not to post or share information that could be used to a hacker's advantage.

All of these factors contribute to a healthy cyber security environment. Companies of all shapes and sizes, in all industries—and especially in aerospace—cannot afford to hesitate when it comes to taking every precaution necessary when protecting their employees, their information, and their customers.

The objective is for companies and system vendors to do an "extraordinarily effective job of protecting these systems from cyberattacks, with firewalls, isolation from the public internet, virus detection and procedural protocols," said Captain.

by Megan Anderson, AFA