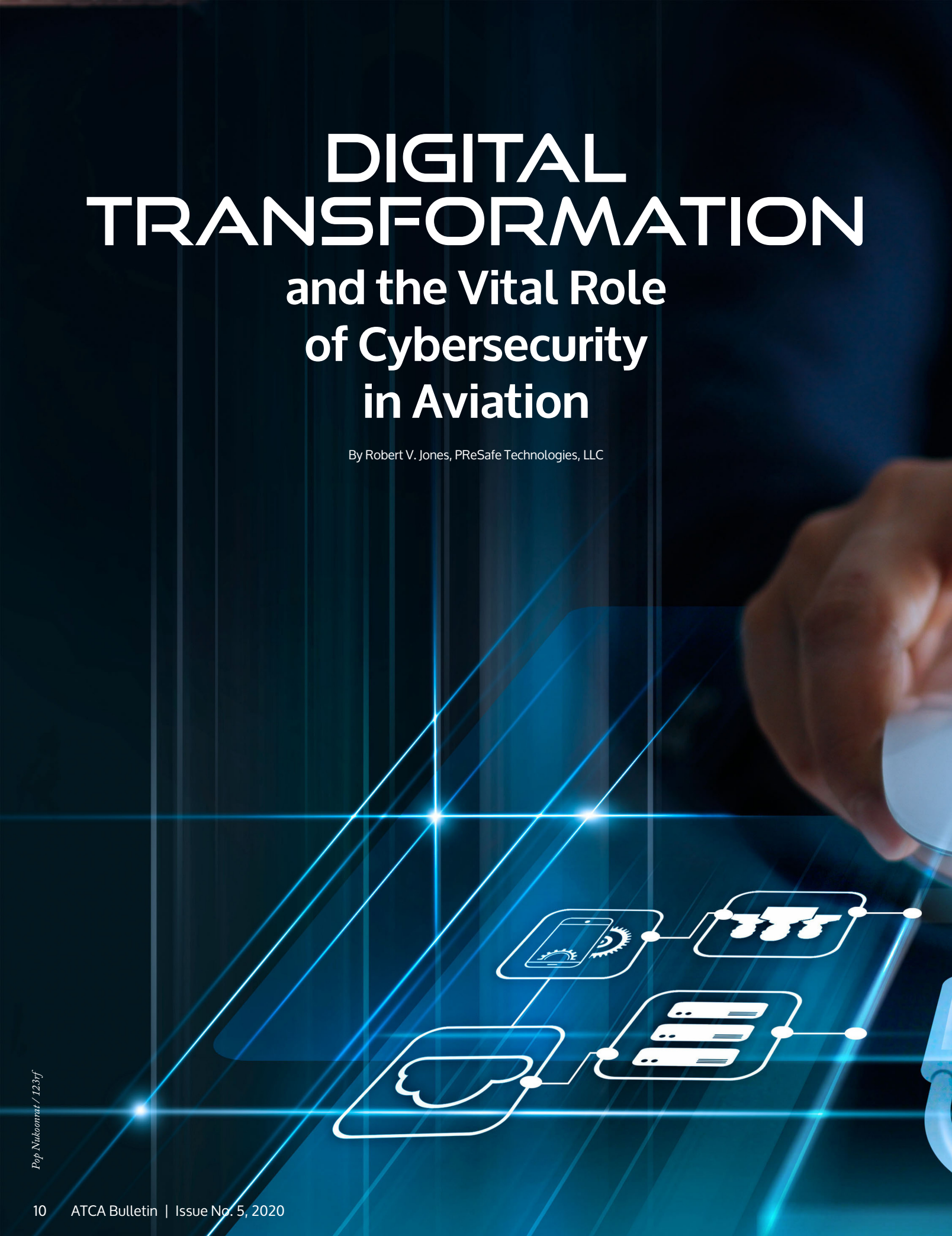
DIGITAL TRANSFORMATION

and the Vital Role of Cybersecurity in Aviation

By Robert V. Jones, PReSafe Technologies, LLC



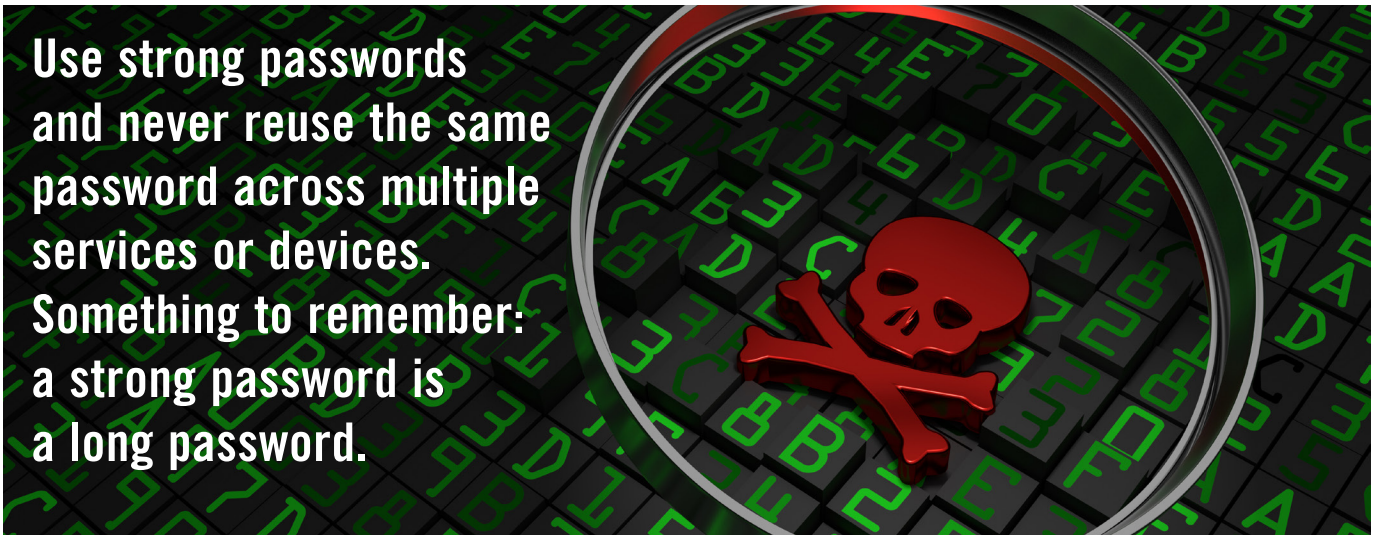
Pop Nukoonrat / 123rf

We are undergoing tremendous change at this moment. A considerable portion of this change is driven by an unprecedented global pandemic. Another major contributor is the extraordinary pace of technological innovation. So much of the change includes a digital transformation unlike we have ever experienced before. The "new normal," including remote work, telemedicine, online teaching and instruction, videoconferencing meetings (e.g. Zoom), and e-commerce, together with touchless delivery are now integral to our lives. Even the process to purchase an airline ticket, check baggage, generate a boarding pass, and board a flight can all be done from a handheld smart device. Last but not least, ATC tower capability delivered remotely is no longer a futuristic concept, it is a commercially available service.

We now rely on technology, innovation, and the digital world more than ever before. Intimately woven throughout the fabric of streamlined processes, innovative services and features, and increasingly more capable end user devices is the vital role of cybersecurity. Fundamentally, the role of cybersecurity is to establish and maintain the confidentiality, integrity, and availability of technology systems and related digital assets. Among other areas, cybersecurity encompasses applications, identity and access management, computing and networking infrastructure, all the way through to physical security of the same. Each area represents a comprehensive body of knowledge all its own that may take years to develop a master level proficiency. All along the way the foundation of technologies shifts and morphs into something new and more complex. Despite the continuous change, there are several practices and strategies that can improve resilience, drive down business risk, and increase confidence downing business in the digital marketplace.

Chief among these strategies and practices is to establish and maintain good cyber hygiene. Just as good personal hygiene (handwashing, avoiding touches to the face, social distancing, etc.) mitigates the spread of virus in the natural world, good cyber hygiene is equally effective at mitigating the infection and spread of malware and other computer viruses in the digital world.

Good cyber hygiene includes several measures such as: inventory of authorized/unauthorized devices and software; secure configurations for hardware and software; continuous vulnerability assessment and remediation (e.g. continuous monitoring – automate where possible); controlled use of administrative privileges; email and web browser protections; data recovery capability (e.g. data backups – especially important in the age of ransomware);



data protection (i.e. encryption); secure configurations for network devices; application security (secure development lifecycle); account monitoring and control (account activation and deactivation along with password management); and incident response and management, to name a few.

Each of the measures above and others are well defined and cross-referenced within comprehensive frameworks such as the National Institute of Standards and Technology 800 – 53/171, the Center for Internet Security Top 20 Controls, International Organization for Standardization 27001/2, and Control Objectives for Information and Related Technologies. Some of the frameworks are more detailed and extensive than others. Nonetheless, all are effective at presenting an approach that leads to greater digital resilience and reduced business risk. While no amount of cyber hygiene or use of a framework can guarantee 100 percent security, a respected segment of the expert community agrees "...that you can prevent 80 to 90 percent of all known attacks by implementing and staying current on basic cyber hygiene."[1]

For the individual working from home on a professional or personal level, the following are a few tips that reduce the risk of a cyber attack:

1. Use strong passwords and never reuse the same password across multiple services or devices. Something to remember: a strong password is a long password. Password length is perhaps the greatest contributing factor to password strength. Use a password phrase to help you remember (e.g. catschasedogs@nitefor$10&win). When necessary always adhere to the password requirements of the system or organization you are working within. Ideally, when possible, use two factor authentication. A number of leading financial institutions, government agencies, and social media services now offer this capability.
2. Be sure to change the default administrative password on WiFi routers and other devices that you rely on or use at home (e.g. smart TVs, digital assistants, video cameras/doorbells, etc.) and periodically change those passwords as well.
3. Keep software up to date (where possible, use auto update features) on all devices. Threat actors are always looking for the weakest point of entry. Small and medium-size businesses can present a path or threat vector into larger enterprises. More often than not, that point of entry is through an individual or group of hardworking professionals simply trying to work using technology resources that are readily available, but not commercially well-protected.

Most of the measures above are largely dependent upon technology and processes, and less on people. People, especially end users of applications and services that deliver efficiency, scalability, and reduced cost, are critical factors in establishing and maintaining improved resilience and reducing business risk from cyber threats. No matter how much is invested in the latest technology and associated processes, if a user is unaware of the implications of an errant action, or how to identify efforts to compromise a system through a phishing attempt – whereby malware is downloaded as a result of clicking on an infected link in a realistic looking email message, or credentials are mistakenly entered into a near identical looking, but fake, login page – the investment will be defeated. It is crucial that end user training and awareness are part of a good cyber hygiene program, otherwise the program is unlikely to succeed. Effective cybersecurity awareness training programs have support from the most senior levels of an organization regardless of size.

Embrace the digital transformation before us. The aviation industry is poised for an extraordinary digital transformation led by the proliferation of unmanned aerial vehicles, airport modernization, advanced aircraft, and more. A tremendous digital transformation is already underway throughout the industrial base of businesses that support the aviation industry ecosystem as a result of telework or work from home. Build vital cybersecurity and good cyber hygiene from the beginning to improve resilience and reduce business risks. Retrofitting cybersecurity after a cyber event is more costly and may be catastrophic. If unsure of what to do, get help from trusted organizations and professionals. Do business with confidence in the digital marketplace.

Interested in learning more about cyber hygiene? Join us for a panel at the upcoming ATCA Technical Symposium Sept. 14-18, and for ATCA presents Aviation Cybersecurity, a month-long webinar series taking place every Thursday in October. More information coming soon!

Reference

[1] SANS 2016 W. Witteker (Tripwire 2014).

Ton Snoei / 123rf