How's Your Health?

Follow these tips to conduct a PCI DSS compliance health check.

A recent study by Verizon revealed that only 11.1 percent of companies subject to the Payment Card Industry Data Security Standard (PCI DSS) actually comply with all 12 requirements. Any business that accepts one of the major branded credit cards is subject to the scope of PCI DSS, but here are some common areas where companies fail to achieve compliance, and practical tips for getting them right.

1.

Perform penetration testing.

The latest iteration of PCI DSS, version 3.0, updates penetration testing requirements, providing more details on their scope and methodology. (The new requirements are effective June 2015.) Such testing must include network layer and application layer evaluations. Organizations subject to PCI DSS must perform this testing at least annually, and after any significant change to the environment. In all cases, testers must be professionally qualified.

2.

Follow through on vulnerability scanning.

Requirement 11.2 mandates quarterly scans following any significant network changes, performed from both an internal and an external perspective. The challenge here is twofold: follow-through and record keeping. It is not sufficient to simply perform scans. You must scan, fix vulnerabilities and rerun the scan until it shows clean results. Maintain records for each scan and provide four passing quarterly scans for the preceding year.

3.

Patch all systems.

Applying vendor updates to operating systems and applications is a time-consuming process that requires coordination and testing, but it provides a very high degree of security control by correcting known vulnerabilities with vendor-supplied patches. Requirement 6 specifies that critical security patches must be applied within a month of release. Automation is key here. Adopt system configuration management software to track patches and report noncompliance.

4.

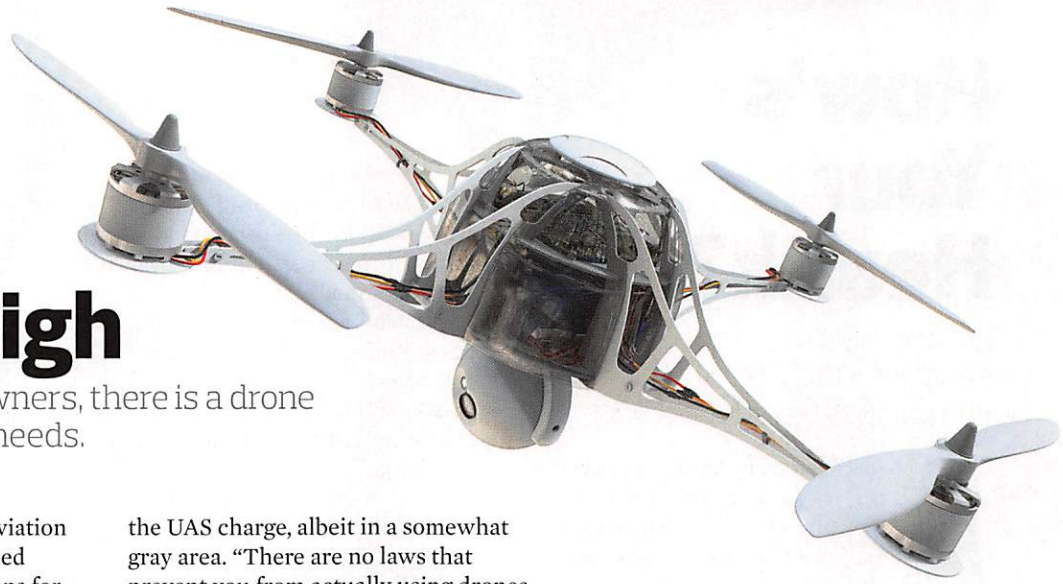
Keep it up.

The PCI DSS requirements in these three areas are long-standing, and it's hard to imagine that any organization simply is unaware of them. Why do so many companies fail these tests? Because each requires ongoing action. Remember, compliance is not a one-time or once-a-year activity but a continuous process that requires care and feeding throughout the year. ■

→ Learn more about the new requirements in the latest version of PCI DSS at **biztechmag.com/PCIDSS**.

MIKE CHAPPLE is senior director of IT service delivery at the University of Notre Dame.

Jupiterimages/Thinkstock



Flying High

Yes, small business owners, there is a drone to suit your business needs.

Last June, the Federal Aviation Administration grounded Amazon PrimeAir's plans for a drone delivery system. But two weeks *before* the Amazon decision, the FAA granted energy corporation BP permission to fly a drone over Alaska's North Slope to better survey roads and pipelines. That marked the first condoned use of a commercial unmanned aircraft system (UAS) over U.S. soil and, as U.S. Transportation Secretary Anthony Foxx noted, "another important step toward broader commercial use of unmanned aircraft."

Despite its reticence on UASs, the FAA is not blind to the demands and priorities of businesses. The agency's ban applies only to commercial use, except in instances where a waiver is granted. Six such waivers were given to movie and television production companies in September. Short of a waiver, however, the FAA Modernization and Reform Act of 2012 allows only for model aircraft, weighing 55 pounds or less, flown within line of sight for "hobby or recreation."

DRONES AT WORK

Does the FAA ban mean that drones remain verboten for small businesses? Well, yes and no.

Colin Snow, founder and CEO of Drone Analyst, says that while larger companies such as Amazon remain shackled, small businesses are leading the UAS charge, albeit in a somewhat gray area. "There are no laws that prevent you from actually using drones commercially," Snow says, "but there are FAA policies. Most people hold back without there being laws in place, but many small businesses, between 2,000 and 3,000 according to the research I've done, are operating in Class G uncontrolled airspace, which is the airspace right above us."

Snow says that those companies now engaging in commercial drone use — whether in a gray U.S. market or internationally, where UASs are more accepted — generally fall into six markets: precision agriculture; inspection and surveillance; mapping and surveying; film, photo and video production; public safety or emergency response; and environmental inspection and regulation.

From examining irrigation lines to staring down a refinery flare stack, drones offer a superior way to see what needs to be seen, in less time and at less expense.

Snow says drones are evolving to fill even more sophisticated business roles. Whereas today's uses focus on simple imaging, future applications will take a Big Data approach to analyzing footage.

"Photo and video are only part of the whole service offering," he says. "It's what you do with the data after you've captured it — the processing, storing and offering it up as useful, valuable information to somebody who's, say, doing precision agriculture and wants to know the crop vigor of their field. There's so much potential." ■

100,000

The number of jobs expected to be created within the UAS industry in the first decade after full integration for commercial use*

Fines Shot Down?

In March 2014, a judge dismissed a $10,000 fine against Raphael Pirker, ruling that the FAA's first fine against a drone operator was made in the absence of any FAA authority over model aircraft. Pirker had been shooting a promotional video in 2011. The FAA appealed the decision.

Discover more on the expected economic impact of drones on U.S. business at **biztechmag.com/Drones**.

coddy/Thinkstock

*SOURCE: Association for Unmanned Vehicle Systems International, "AUVSI statement on the Announcement of Google's Research into UAS Deliveries," Aug. 28, 2014