THE TICKER

CYBER INSECURITY

The U.S. government spends billions of dollars each year on cybersecurity. But it still ranked 16 out of 18 when it comes to protecting computer systems and data from hackers, according to the *2017 U.S. State and Federal Government Cybersecurity Report*. Released by consulting firm SecurityScorecard in August, the survey found 80 percent of the federal organizations examined had an instance of malware communicating outside of the network in the last year, according to eWEEK.

Those vulnerabilities may become even more severe in light of eight members leaving U.S. President Donald Trump's National Infrastructure Advisory Council (NIAC) in August. Those resigning from the council—which advises the U.S. Department of Homeland Security on cybersecurity and infrastructure security—cited President Trump's "insufficient attention" to the nation's cyber vulnerabilities among their reasons.

The exodus came just days before the NIAC released the report *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. It examined how federal authorities and capabilities can best be applied to support cybersecurity of high-risk assets.

The report's conclusion was decidedly pessimistic: "We believe the U.S. government and private sector collectively have the tremendous cyber capabilities and resources needed to defend critical private systems from aggressive cyberattacks—provided they are properly organized, harnessed and focused. Today, we're falling short."

The council then offered an ominous call to action: "There is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyberattack to organize effectively and take bold action."

U.S. President Donald Trump listens during a meeting on cybersecurity at the White House in 2017.

PHOTO BY BRENDAN SMIALOWSKI/AFP/GETTY IMAGES

SECURITY STATUS

Cybersecurity threats are multiplying, with some industries better prepared to combat them than others. Here is how they ranked from best to worst.

1. Food
2. Entertainment
3. Retail
4. Information services
5. Financial services
6. Technology
7. Legal
8. Hospitality
9. Nonprofit
10. Manufacturing
11. Transportation
12. Construction
13. Health care
14. Energy
15. Pharmaceutical
16. Government
17. Telecommunications
18. Education

Source: *2017 U.S. State and Federal Government Cybersecurity Report*, SecurityScorecard

WHERE ARE THE WHISTLEBLOWERS?

U.K. companies have a corruption problem—or at least, a corruption perception problem. But employees do not seem to be willing to do much about it.

According to EY's *Europe, Middle East, India and Africa Fraud Survey 2017*, 25 percent of U.K. employees surveyed believe corruption to be widespread. On an individual level, 42 percent believe their senior management would act unethically to help the business survive. And while 37 percent of respondents are aware of a whistleblowing hotline within their company, 54 percent said they would not report such behavior due to concerns about career progression. One-third of respondents would refrain from reporting out of fear for their personal safety.

The results point to deep cultural problems within U.K. organizations that will not be solved with policy changes alone. "Rules and regulation are only part of the solution," says Jonathan Middup, partner, EY Fraud Investigation & Dispute Services, London. "It's critical that the tone is set from the top, with senior managers leading by example. Training and awareness programs also have a role to play, helping employees to understand the consequences of fraud and corruption, but to be effective these should include discussion of gray areas and ethical dilemmas."

42%

of U.K. employees surveyed believe their senior management would act unethically to help the business survive.

BYE-BYE BUDS

Not all press is good press. For San Francisco startup Kanoa, a single negative review proved fatal. One day the company was launching its crowdsourced wireless headphones and a mobile app. A few days later, it had shuttered operations.

It was a case of instant accountability that could only happen in the internet age.

It only took one stinging review from tech tester Cody Crouch, also known as iTwe4kz, on YouTube. In his review, Mr. Crouch says he had issues getting the $300 headphones to pair with the Kanoa app—a critical factor considering the app is what users were supposed to use to manipulate settings, including the level of ambient noise. Adding fuel to the fire, the earbud charging case failed to work, and the product's user manual was blank.

Mr. Crouch also said in his video review that after reaching out to Kanoa about his challenges, they offered him $500 for a good review, which he did not accept. Instead, he ended his video by advising: "You don't want to have these. This is not a company you want to deal with."

Investors started to back out, and a few days later the company ceased to exist. A lengthy statement outlining its decline was posted to Kanoa's now defunct website, which stated: "This is not the outcome we had foreseen, and with the quick turn of events, we are emotionally overwhelmed. We know you are disappointed, and can only ask that you understand that we genuinely tried."

One day the company was launching its crowdsourced wireless headphones and a mobile app. A few days later, it had shuttered operations.