

# GUARDING AGAINST CYBERCRIME

If Willie Sutton were alive, he'd be looting corporate IT systems, not banks.



**F**ROM LOCKHEED MARTIN, Google, and Sony to Citigroup and MasterCard, no company is immune to cybercrime, whether perpetrated by criminal gangs, hostile governments, or tech-savvy “hacktivists.” “Willie Sutton once said he robbed banks because ‘that’s where the money is,’” says Joseph Petro, executive vice president and managing director of Citigroup Security and Investigative Services, and former president of the International Security Management Association (ISMA). “Robbing a bank with a gun no longer makes sense because that’s not where the money is. It’s online now, and the risks of getting caught are much, much lower.”

In bygone years, cybercriminals trolled bank and credit card databases, looking to steal personal data for resale on the black market. Now, notes Ray Mislock, DuPont’s director of

corporate security, the focus has shifted to intellectual property, the crown jewel of virtually any business. How big is the market? A recent study by McAfee Inc. and Science Applications International Corp. estimates that companies are losing in excess of \$1 trillion a year to data leaks. The study also notes that trade secrets—from R&D and customer lists to marketing plans and source code—are far more valuable and vulnerable than financial assets.

ISMA’s Petro suggests that companies need to employ a three-pronged defense consisting of security tools, such as state-of-the-art firewalls and encryption technologies; internal policies and procedures that detail how and where employees use and access IT; and ongoing security education for employees, customers, and suppliers.

Another security specialist points to a different risk—so-called shoulder surfing. With mobile computing on the up-

swing, staffers working in public spaces like coffee shops, trains, and airplanes are vulnerable to snooping, says Hugh Thompson, chief security strategist at People Security and a consultant to 3M.

A savvy corporate spy, explains Thompson, might position himself in a Starbucks near a target company “just to see what he can see” on the laptop, tablet, or smartphone screens of coffee-sippers. Shoulder surfing can also be a casual affair: Someone standing in line at an airplane lavatory can casually observe the screens of nearby passengers absorbed in editing documents and presentations. The powerful, five-to-eight megapixel cameras that are standard in new smartphones magnify the threat.

Unlike other cyber-risks, shoulder surfing has a simple solution: Require employees who work in public places to attach privacy filters to their laptop, tablet, and smartphone screens. 3M Company invented privacy filters in the early 1990s, using its expertise in light management and optical clarity, and the company’s Privacy Filters remain a category leader. The newest addition to the 3M line, the 3M Gold Privacy Filter, shows only a vibrant golden hue to anyone viewing a protected screen from an angle, says 3M marketing manager Beth Edgar, yet it maintains a sharp and bright onscreen image from a user’s vantage point.

With businesses storing increasing amounts of precious information in the cloud and trusting the staff to work remotely, companies are making enormous investments in their IT systems. The savvy ones recognize that investments in the right security tools, policies, and behaviors are equally important. ●



## Because George is curious.

Stay private when needed. Share info when wanted. Upgrade to 3M clarity and privacy that leave others in the dark.



**\$1 trillion**  
The amount of money companies are losing in data leaks.

SOURCE: McAfee Inc. and Science Applications International Corp.