The New York Times

SPECIAL SECTION: SECURITY NYT NOW

Hacked vs. Hackers: Game On

By **Nicole Perlroth**

December 2, 2014 9:31 pm

SAN FRANCISCO — Paul Kocher, one of the country's leading cryptographers, says he thinks the explanation for the world's dismal state of digital security may lie in two charts.

One shows the number of airplane deaths per miles flown, which decreased to one-thousandth of what it was in 1945 with the advent of the Federal Aviation Administration in 1958 and stricter security and maintenance protocols. The other, which details the number of new computer security threats, shows the opposite. There has been more than a 10,000-fold increase in the number of new digital threats over the last 12 years.

The problem, Mr. Kocher and security experts reason, is a lack of liability and urgency. The Internet is still largely held together with Band-Aid fixes. Computer security is not well regulated, even as enormous amounts of private, medical and financial data and the nation's computerized critical infrastructure — oil pipelines, railroad tracks, water treatment facilities and the power grid — move online.

SPECIAL SECTION: SECURITY
After a year of record-setting hacking incidents, companies and consumers are finally learning how to defend themselves and are altering how they approach computer security.

If a stunning number of airplanes in the United States crashed tomorrow, there would be investigations, lawsuits and a cutback in air travel, and the airlines' stock prices would most likely plummet. That has not been true for hacking attacks, which surged 62 percent last year, according to the security company Symantec. As for long-term consequences, Home Depot, which suffered the worst

security breach of any retailer in history this year, has seen its stock float to a high point.

In a speech two years ago, Leon E. Panetta, the former defense secretary, predicted it would take a "cyber-Pearl Harbor" — a crippling attack that would cause physical destruction and loss of life — to wake up the nation to the vulnerabilities in its computer systems.

No such attack has occurred. Nonetheless, at every level, there has been an awakening that the threats are real and growing worse, and that the prevailing "patch and pray" approach to computer security simply will not do.

So what happened?

The Wake-Up Call

A bleak recap: In the last two years, breaches have hit the White House, the State Department, the top federal intelligence agency, the largest American bank, the top hospital operator, energy companies, retailers and even the Postal Service. In nearly every case, by the time the victims noticed that hackers were inside their systems, their most sensitive government secrets, trade secrets and customer data had already left the building. And in just the last week Sony Pictures Entertainment had to take computer systems offline because of an aggressive attack on its network.

The impact on consumers has been vast. Last year, over 552 million people had their identities stolen, according to Symantec, and nearly 25,000 Americans had sensitive health information compromised — every day — according to the Department of Health and Human Services. Over half of Americans, including President Obama, had to have their credit cards replaced at least once because of a breach, according to the Ponemon Group, an independent research organization.

GRAPHIC
18 Months of Breaches, Flaws and Revelations

But the value of those stolen credit cards, which trade freely in underground criminal markets, is eclipsed by the value of the

intellectual property that has been siphoned out of United States corporations, universities and research groups by hackers in China — so much so that security experts now say there are only two types of companies left in the United States: those that have been hacked and those that do not yet know they have been hacked.

And this year, American companies learned it was not just Beijing they were up against. Thanks to revelations by the former intelligence agency contractor Edward J. Snowden, companies worry about protecting their networks from their own government. If the tech sector cannot persuade foreign customers that their data is safe from the National Security Agency, the tech industry analysis firm Forrester Research predicts that America's cloud computing industry stands to lose $180 billion — a quarter of its current revenue — over the next two years to competitors abroad.

"People are finally realizing that we have a problem that most had not thought about before," said Peter G. Neumann, a computer security pioneer at SRI International, the Silicon Valley engineering research laboratory. "We may have finally reached a crossroads."

Is There a Playbook?

Only certain kinds of companies, like hospitals and banks, are held up to scrutiny by government regulators when they are hacked. And legal liability hasn't been established in the courts, though Target faces dozens of lawsuits related to a hack of that company's computer network a little over a year ago.

But if there is a silver lining to the current predicament, Mr. Neumann and other security experts say, it is that computer security, long an afterthought, has been forced into the national consciousness.

Customers, particularly those abroad, are demanding greater privacy protections. Corporations are elevating security experts to senior roles and increasing their budgets. At Facebook, the former mantra "move fast and break things" has been replaced. It is now "move slowly and fix things." Companies in various sectors have started informal information-sharing groups for computer

security. And President Obama recently called on Congress to pass a national data breach law to provide "one clear national standard" rather than the current patchwork of state laws that dictate how companies should respond to data breaches.

There is growing recognition that there is no silver bullet. Firewalls and antivirus software alone cannot keep hackers out, so corporations are beginning to take a more layered approach to data protection. Major retailers have pledged to adopt more secure payment schemes by the end of next year. Banks are making it easier for customers to monitor their monthly statements for identity theft. And suddenly, pie-in-the-sky ideas that languished in research labs for years are being evaluated by American hardware makers for use in future products.

"People are recognizing that existing technologies aren't working," said Richard A. Clarke, the first cybersecurity czar at the White House. "It's almost impossible to think of a company that hasn't been hacked — the Pentagon's secret network, the White House, JPMorgan — it is pretty obvious that prevention and detection technologies are broken."

Companies that continue to rely on prevention and detection technologies like firewalls and antivirus products are considered sitting ducks.

"People are still dealing with this problem in a technical way, not a strategic way," said Scott Borg, the head of the United States Cyber Consequences Unit, a nonprofit organization. "People are not thinking about who would attack us, what their motives would be, what they would try to do. The focus on the technology is allowing these people to be blindsided.

"They are looking obsessively at new penetrations," Mr. Borg said. "But once someone is inside, they can carry on for months unnoticed."

The Keys to Preparation

The companies most prepared for online attacks, Mr. Borg and other experts say, are those that have identified their most valuable assets, like a university's groundbreaking research, a multinational's acquisition strategy, Boeing's

blueprints to the next generation of stealth bomber or Target's customer data. Those companies take additional steps to protect that data by isolating it from the rest of their networks and encrypting it.

That approach — what the N.S.A. has termed "defense in depth" — is slowly being adopted by the private sector. Now, in addition to firewalls and antivirus products, companies are incorporating breach detection plans, more secure authentication schemes, technologies that "white list" traffic and allow in only what is known to be good, encryption and the like.

"We're slowly getting combinations of new technologies that deal with this problem," Mr. Clarke said.

The most prominent examples are Google, Yahoo, Microsoft and Facebook. Mr. Snowden revealed that the N.S.A. might have been grabbing data from those companies in unencrypted form as it passed between their respective data centers. Now, they all encrypt their traffic as it flows internally between their own data centers.

Though intelligence analysts may disagree, security experts say all of this is a step in the right direction. But security experts acknowledge that even the most advanced security defenses can break down. A widely used technology sold by FireEye, one of the market leaders in breach detection, failed to detect malicious code in an independent lab test this year. The product successfully identified 93 percent of the threats, but as the testers pointed out, it is not the 99 percent of detected threats that matter. It is the 1 percent that are missed that allow hackers to pull off a heist.

Even when security technologies do as advertised, companies are still missing the alerts. Six months before Target was breached last year, it installed a $1.6 million FireEye intrusion detection system. When hackers tripped the system, FireEye sounded alarms to the company's security team in Bangalore, which flagged the alert for Target's team at its headquarters in Minneapolis. Then nobody reacted until 40 million credit card numbers and information on 70 million more

customers had been sent to computers in Russia, according to several investigators.

Part of the problem, security chiefs say, is “false positives,” the constant pinging of alerts anytime an employee enters a new database or downloads a risky app or email attachment. The result, they complain, is a depletion of resources and attention.

“We don’t need ‘big data.’ We need big information,” said Igor Baikalov, a former senior vice president for global information security at Bank of America, now chief scientist at Securonix, a private company that sells threat intelligence to businesses.

Securonix is part of a growing class of security start-ups, which includes Exabeam and Vectra Networks in Silicon Valley and several other companies that use the deluge of data from employee computers and personal devices to give security officers intelligence they can act on.

Many companies in the Fortune 500 are building their own systems that essentially do the same thing. These technologies correlate unusual activity across multiple locations, then raise an alarm if they start to look like a risk. For example, the technologies would increase the urgency of an alert if an employee suddenly downloaded large amounts of data from a database not regularly used, while simultaneously communicating with a computer in China.

The future of security, experts say, won’t be based on digital walls and moats but on these kinds of newer data-driven approaches.

“Most large organizations have come to the painful recognition that they are already in some state of break-in today,” said Asheem Chandna, a venture capital investor at Greylock Partners. “They are realizing they need to put new and advanced sensors in their network that continuously monitor what is going on.”

While much progress is being made, security experts bemoan that there is still little to prevent hackers from breaking in in the first place.

In May, the F.B.I. led a crackdown on digital crime that resulted in 90 arrests, and Robert Anderson, one of the F.B.I.'s top officers on such cases, said the agency planned to take a more aggressive stance. "There is a philosophy change. If you are going to attack Americans, we are going to hold you accountable," he said at a cybersecurity meeting in Washington.

Still, arrests of hackers are few and far between.

"If you look at an attacker's expected benefit and expected risk, the equation is pretty good for them," said Howard Shrobe, a computer scientist at the Massachusetts Institute of Technology. "Nothing is going to change until we can get their expected net gain close to zero or — God willing — in the negative."

Until last year, Dr. Shrobe was a manager at the Defense Advanced Research Projects Agency, known as Darpa, overseeing the agency's Clean Slate program, a multiproject "Do Over" for the computer security industry. The program included two separate but related projects. Their premise was to reconsider computing from the ground up and design new computer systems that are much harder to break into and that recover quickly when they have been breached.

" 'Patch and pray' is not a strategic answer," Dr. Shrobe said. "If that's all you do, you're going to drown."

A version of this article appears in print on 12/03/2014, on page F1 of the NewYork edition with the headline: Hacked vs. Hackers: Game On.