The New York Times https://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html

Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say

By Nicole Perlroth and Vindu Goel
Sept. 28, 2016

SAN FRANCISCO — Six years ago, Yahoo's computer systems and customer email accounts were penetrated by Chinese military hackers. Google and a number of other technology companies were also hit.

The Google co-founder Sergey Brin regarded the attack on his company's systems as a personal affront and responded by making security a top corporate priority. Google hired hundreds of security engineers with six-figure signing bonuses, invested hundreds of millions of dollars in security infrastructure and adopted a new internal motto, "Never again," to signal that it would never again allow anyone — be they spies or criminals — to hack into Google customers' accounts.

Yahoo, on the other hand, was slower to invest in the kinds of defenses necessary to thwart sophisticated hackers that are now considered standard in Silicon Valley, according to half a dozen current and former company employees who participated in security discussions but agreed to describe them only on the condition of anonymity.

When Marissa Mayer took over as chief executive of the flailing company in mid-2012, security was one of many problems she inherited. With so many competing priorities, she emphasized creating a cleaner look for services like Yahoo Mail and developing new products over making security improvements, the Yahoo employees said.

The "Paranoids," the internal name for Yahoo's security team, often clashed with other parts of the business over security costs. And their requests were often overridden because of concerns that the inconvenience of added protection would make people stop using the company's products.

But Yahoo's choices had consequences, resulting in a series of embarrassing security failures over the last four years. Last week, the company disclosed that hackers backed by what it believed was an unnamed foreign government stole the credentials of 500 million users in a breach that went undetected for two years. It was the biggest known intrusion into one company's network, and the episode is now under investigation by both Yahoo and the Federal Bureau of Investigation.

Certainly, many big companies have struggled with cyberattacks in recent years. But Yahoo's security efforts appear to have fallen short, in particular, when compared with those of banks and other big tech companies.

To make computer systems more secure, a company often has to make its products slower and more difficult to use. It was a trade-off Yahoo's leadership was often unwilling to make.

In defense of Yahoo's security, a company spokeswoman, Suzanne Philion, said the company spent $10 million on encryption technology in early 2014, and that its investment in security initiatives will have increased by 60 percent from 2015 to 2016.

"At Yahoo, we have a deep understanding of the threats facing our users and continuously strive to stay ahead of these threats to keep our users and our platforms secure," she said.

The breach disclosed last week is the latest black eye for Ms. Mayer, whose failed turnaround effort resulted in Yahoo's agreement in July to sell its core operations to Verizon for $4.8 billion. It is unclear whether the episode will affect the sale. Although Yahoo's email users are its most loyal and frequent customers, the company has been losing market share in email for years.

"Yahoo is already suffering. I don't think they'll suffer more because of this," said Avivah Litan, a security analyst with the research firm Gartner.

Ms. Mayer arrived at Yahoo about two years after the company was hit by the Chinese military hackers. While Google's response was public, Yahoo never publicly admitted that it had also been attacked.

A former Google executive credited with creating the search company's simple, colorful aesthetic, Ms. Mayer turned her attention at Yahoo to beating Google at search, creating new mobile apps, and turning Yahoo into a video powerhouse with television-style broadcasts featuring big-name talent like Katie Couric.

But in matters of security, Ms. Mayer, current and former employees said, was far more reactive. In 2010, Google announced it would start paying hackers "bug bounties" if they turned over security holes and problems in its systems. Yahoo did not do the same until three years later, after it lost countless security engineers to competitors and experienced a breach of more than 450,000 Yahoo accounts in 2012 and a series of humiliating spam attacks in 2013. Yahoo said it had paid out $1.8 million to bug hunters.

In 2013, disclosures by Edward J. Snowden, the former National Security Agency contractor, showed that Yahoo was a frequent target for nation-state spies. Yet it took a full year after Mr. Snowden's initial disclosures for Yahoo to hire a new chief information security officer, Alex Stamos.

Jeff Bonforte, the Yahoo senior vice president who oversees its email and messaging services, said in an interview last December that Mr. Stamos and his team had pressed for Yahoo to adopt end-to-end encryption for everything. Such encryption would mean that only the parties in a conversation could see what was being said, with even Yahoo unable to read it.

Mr. Bonforte said he resisted the request because it would have hurt Yahoo's ability to index and search message data to provide new user services. "I'm not particularly thrilled with building an apartment building which has the biggest bars on every window," he said.

The 2014 hiring of Mr. Stamos — who had a reputation for pushing for privacy and antisurveillance measures — was widely hailed by the security community as a sign that Yahoo was prioritizing its users' privacy and security.

The current and former employees say he inspired a small team of young engineers to develop more secure code, improve the company's defenses — including encrypting traffic between Yahoo's data centers — hunt down criminal activity and successfully collaborate with other companies in sharing threat data.

He also dispatched "red teams" of employees to break into Yahoo's systems and report back what they found. At competitors like Apple and Google, the Yahoo Paranoids developed a reputation for their passion and contributions to collaborative security projects, like Threat Exchange, a platform created by Yahoo, Dropbox, Facebook, Pinterest and others to share information on cyberthreats.

But when it came time to commit meaningful dollars to improve Yahoo's security infrastructure, Ms. Mayer repeatedly clashed with Mr. Stamos, according to the current and former employees. She denied Yahoo's security team financial resources and put off proactive security defenses, including intrusion-detection mechanisms for Yahoo's production systems. Over the last few years, employees say, the Paranoids have been routinely hired away by competitors like Apple, Facebook and Google.

Mr. Stamos, who departed Yahoo for Facebook last year, declined to comment. But during his tenure, Ms. Mayer also rejected the most basic security measure of all: an automatic reset of all user passwords, a step security experts consider standard after a breach. Employees say the move was rejected by Ms. Mayer's team for fear that even something as simple as a password change would drive Yahoo's shrinking email users to other services.

"Yahoo's policy is that if we believe a user's password has been compromised, we lock the account until the user resets the password," Ms. Philion said.

With the 500 million accounts involved in the breach disclosed last week, the stolen passwords were encrypted. Yahoo concluded the risk of misuse was low so it notified users and encouraged them to reset their passwords themselves.

On Tuesday, six Democratic senators, led by Patrick Leahy of Vermont, sent a letter to Ms. Mayer demanding more details about the 2014 breach and what Yahoo was doing to prevent a recurrence. Another senator, Mark Warner, Democrat of Virginia, has asked the Securities and Exchange Commission to investigate Yahoo's disclosures to investors regarding the incident. And the company is already the subject of several class-action lawsuits from users over the intrusion.

A version of this article appears in print on , Section B, Page 1 of the New York edition with the headline: Hacker Threat Took Back Seat at Yahoo, Insiders Say