Bloomberg Technology

Twitter's Security Woes Included Broad Access to User Accounts

By Jordan Robertson Kartikay Mehrotra and Kurt Wagner
July 27, 2020, 6:00 AM EDT

- Dorsey, Twitter's board warned repeatedly, ex-employees say
- Company says 1,500 staff and contractors can access user data

Twitter Inc. has struggled for years to police the growing number of employees and contractors who have the ability to reset users' accounts and override their security settings, a problem that Chief Executive Officer Jack Dorsey and the board were warned about multiple times since 2015, according to former employees with knowledge of the company's security operations.

Twitter's oversight over the 1,500 workers who reset accounts, review user breaches and respond to potential content violations for the service's 186 million daily users have been a source of recurring concern, the employees said. The breadth of personal data most of those workers could access is relatively limited -- including such things as Internet Protocol addresses, email addresses and phone numbers -- but it's a starting point to snoop on or even hack an account, they said.

The controls were so porous that at one point in 2017 and 2018 some contractors made a kind of game out of creating bogus help-desk inquiries that allowed them to peek into celebrity accounts, including Beyonce's, to track the stars' personal data including their approximate locations gleaned from their devices' IP addresses, two of the former employees said.

Concerns about Twitter's ability to protect user data deepened this month after hackers hijacked the accounts of some of its most famous users, including political leaders, business titans and celebrities, as part of an apparent cryptocurrency scam. The pressure on Twitter to protect its users isn't limited to the personal data it collects on them -- which is minimal compared to some other social media sites -- but extends to the influence its users wield, especially world leaders or the political dissidents who oppose them.

While federal and internal investigations are ongoing, Twitter has said that hackers somehow duped employees to gain access to the hacked accounts.

The attackers contacted at least one Twitter employee over the phone in an effort to obtain security information that would help them access Twitter's internal user-support tools, according to people familiar with the investigation. Twitter required employees to take an online security training course last week, which covered a number of phishing techniques including phone calls, the people added. A Twitter spokeswoman said the company conducts regular security training "in line with our commitment to protecting the privacy and security of the people we serve."

The spokeswoman disputed the former employees' characterization of the company's oversight of user accounts, while claiming the company has tools to "stay ahead of threats as they evolve."

Twitter is consistently improving its security apparatus with new tools, she said, and cited recent privacy-related programs that have bolstered user protections, including new employee training.

She confirmed that Twitter's oversight of user accounts includes 1,500 full-time employees and contractors, but said "we have no indication that the partners we work with on customer service and account management played a part here," referring to Twitter's recent account breach.

Employees and contractors have access only to the tools they need to do their jobs, which includes permissions to execute password resets to accounts, the spokeswoman said. Access also comes with "extensive security training and managerial oversight," she said.

Dorsey, addressing the recent hack, told investors this week that the company "fell behind, both in our protections against social engineering of our employees and restrictions on our internal tools."

This account is based on interviews with four former Twitter security employees, in addition to more than a half dozen other people close to Twitter.

According to the former security employees, Twitter management has often dragged its heels on upgrades to information security controls while prioritizing consumer products and features, a source of tension for many businesses.

Efforts to better govern Twitter's user-support staff and contractors have also gotten short shrift, resulting in a workplace where too many people have access to too many powerful tools, the former employees said. Even with some basic tracking systems in place, contractors have found workarounds to explore details about former lovers, politicians, favorite brands and celebrities, they added.

In the July 15 attack, 130 accounts were compromised -- including those belonging to Barack Obama, Joe Biden, Jeff Bezos and Elon Musk -- and account data was stolen from eight of those, Twitter said without identifying the accounts. Tweets were sent from the hijacked accounts promising followers who sent Bitcoin to a specific address would be paid back double -- or their support would contribute to pandemic relief efforts. Twitter acknowledged that several of its employees were the targets of a malicious campaign to acquire credentials for its internal system, "only available to our internal supports team," according to a July 17 statement.

An obscure hacking collective that is devoted to buying and selling short and clever Twitter and Instagram usernames has claimed to have been involved in the attack, which is being investigated by the FBI.

Concerns over insider access to Twitter accounts were brought to Twitter's board of directors almost annually during a period from 2015 to 2019, only to be deferred for other priorities including other cybersecurity programs, according to two of the former security officials. Those presentations weren't always presented as an urgent threat to Twitter security or its users' privacy, according to four people familiar with the board's presentations.

Security programs, like shoring up the system that houses Twitter's backup files or enhancing oversight of the system used to monitor contractor activity were, at times, shelved for engineering products designed to enhance revenue, according to two of the former employees. Some of Twitter's contractors that became proficient in snooping on Beyonce's and other celebrity accounts were employed by Cognizant Technology Solutions Corp. in as many as a half-dozen locations, the two former employees said.

Cognizant, which continues to work with Twitter, declined to comment. A representative for Beyonce didn't respond to a request for comment. Twitter declined to answer questions about access to Beyonce's account. Through a company spokeswoman, Twitter's board declined to comment.

Snooping on accounts wasn't considered a major security concern among Twitter executives, even as the company's dependence on contractors to handle back-office support functions has grown in the last half decade, according to two of the former members of Twitter's security team.

Spying on accounts happened so often that members of Twitter's full-time security team in the U.S. struggled to keep track of the intrusions, according to the two former employees. While some of the contractors were caught and fired, others started beating the formal logging system by creating fraudulent tickets that claimed something was wrong with a user account, only to grab that complaint themselves to resume their escapade, according to the employees.

"Very few companies understand how vulnerable their operations are to compromise as they expand outside of their headquarters," said Paul Ortiz, a supply chain security consultant. "This risk exponentially increases if third-party contract workers are introduced into the equation."

Last week's attack was the latest in a string of embarrassing security breaches at Twitter in recent years, some of them involving internal access to accounts. In November 2017, President Donald Trump's account was temporarily deleted as an act of rebellion by a customer support employee on his last day at the company. In August 2019, Dorsey's account was hacked and used to post anti-Semitic messaging. Twitter blamed Dorsey's mobile carrier. Last year, the Justice Department charged a pair of former Twitter employees for allegedly spying for Saudi Arabia and abusing their access to collect the private data of prominent Saudi critics.

Twitter's intrusion highlights a security failing common among high-flying startups and younger tech companies, according to Patrick Westerhaus, a former FBI cyber and cryptocurrency investigator.

"The problem we see over and over again with technology companies that are hyper-focused on growth and revenue is an immature framework and general lack of concern for security, third-party risk and anti-fraud controls," said Westerhaus, chief executive officer of Cyber Team Six, a security company.