Sony hacking fallout puts all companies on alert

December 18 2014, byMae Anderson

A poster for the movie "The Interview" is taken down by a worker after being pulled from a display case at a Carmike Cinemas movie theater, Wednesday, Dec. 17, 2014, in Atlanta. Georgia-based Carmike Cinemas has decided to cancel its planned showings of "The Interview" in the wake of threats against theatergoers by the Sony hackers. (AP Photo/David Goldman)

Companies across the globe are on high alert to tighten up network security to avoid being the next company brought to its knees by hackers like those that executed the dramatic cyberattack against Sony Pictures Entertainment.

The hack, which a U.S. official has said investigators believe is linked to North Korea, culminated in the cancellation of a Sony film and ultimately could cost the movie studio hundreds of millions of dollars. That the hack included terrorist threats and was focused on causing major corporate damage, rather than on stealing customer information for fraud like in the breaches at Home Depot and Target, indicates a whole new frontier has emerged in cybersecurity. Suddenly every major company could be the target of cyberextortion.

"The Sony breach is a real wake-up call even after the year of mega-breaches we've seen," says Lee Weiner, Boston security firm Rapid7's senior vice president of products and engineering. "This is a completely different type of data stolen with the aim to harm the company."

This should signal to all U.S. businesses that they need to "take cybersecurity as serious as physical security of their employees or security of their physical facilities," says Cynthia Larose, chair of the privacy and security practice at the law firm Mintz Levin in Boston.

The breach is particularly troubling in Hollywood, where secrecy is supposed to be paramount to insure that movie secrets worth millions don't get leaked.

"Movie studios have, by and large, behaved as high-security intellectual property purveyors; prints have been tightly controlled, screeners are watermarked, and bootleggers are prosecuted wherever possible," says Seth Shapiro, a professor at the University of Southern California's School of Cinematic Arts. He said that's what makes it so surprising that email leaks showed that Sony executives apparently gave out passwords in unencrypted emails and made other security blunders.

"The apparently laxity of Sony IT security—given the history of prior hacks—is unprecedented in the history of media technology," he says.

Sony Corp.'s PlayStation network was hacked in 2011.

Studios are trying to tighten up procedures in the wake of the Sony attack. Warner Bros. executives earlier this week ordered a company-wide password reset and sent a five-point security checklist to employees advising them to purge their computers of any unnecessary data, in an email seen by The Associated Press. "Keep only what you need for business purposes," the message said.

Even so, some say there is little that corporations can do to prevent such a sophisticated cyberattack. The key may lie more in detection and limiting damage.

"There are very few companies that can withstand that kind of large assault," says Rich Mogull, an analyst with security firm Securosis in Phoenix. "But a lot of companies do need to improve what they're doing on security, I see it every day with companies I work with."

Companies also need to invest in identifying vulnerabilities on their networks and work quickly to address them. Jonathan Sander, strategy and research officer at data security firm Stealthbits in Hawthorne, N.J., recommends undertaking a comprehensive review to ensure outdated files, such as digital copies of old contracts and electronic conversations that occurred years ago, are no longer being stored on the corporate networks.

"There is a lot of stuff just sitting there waiting to be taken and used for the kind of thing that has happened at Sony right now," Sander says.

He says the Sony breach has been coming up in every customer meeting that Stealthbits Technologies had held since the stolen information began leaking out and making international headlines earlier this month.

"We used to have to lead people to the idea that you need to protect this kind of data," he said. "Now we walk in and they're asking, 'How can I keep my data from ending up on the Internet like Sony's did?"

Some customers have been wondering if they should reduce their reliance on email and switch over to other digital forms of communication, such as messaging systems that don't store the data. Sander doesn't believe that provides as much protection as making a telephone call to share passwords and other sensitive information.

Most importantly, companies need to focus on the ability to detect hacks quickly and limit them as fast as possible. Currently, the average amount of time it takes a company to detect a breach is 200 to 230 days, Rapid7's Weiner said. "That allows the attacker time to gain a lot of knowledge and do a lot of damage," he said.

While none of Weiner's clients have made large-scale changes to their security in reaction to the Sony attack specifically, cybersecurity is becoming a bigger focus in general. "There has been increased investment in information security and increased awareness of the risk and threats of these kind of attacks," he says. "We're starting to see information security as a boardroom issue, it's getting much more attention."

One example companies could follow is in the technology sector, where most firms have been tightening their security measures during the past 18 months in response to revelations about the digital spying tactics of the U.S. government.

Documents leaked by former National Security Agency contractor Edward Snowden revealed that the U.S. government had been tapping into the computer networks of Google, Yahoo, Facebook and other technology companies in search of emails and other electronic

communications that might uncover terrorist plots and other illegal activity. The U.S. government has maintained that it has never collected the kind of highly personal details stolen in the Sony Pictures breach. But tech companies being targeted by the NSA have since tried to thwart the surveillance by encrypting their internal email systems as well as the free accounts available to the general public. Both Google and Apple, the makers of the world's leading software for mobile devices, also are automatically encrypting the data stored on smartphones so the information is indecipherable to unauthorized users, including government authorities.

General Motors says it has bolstered cybersecurity in the past two years by bringing information technology in-house from outside vendors. The auto giant has a cybersecurity chief on staff to prevent hackers from getting into GM vehicle computers and has consolidated electronic data storage from 23 centers worldwide into two located near Detroit.

"I would say we have a higher level (of security) than some other companies do," says spokeswoman Jennie Ecclestone.

A key to thwarting attacks is knowing your enemy and figuring out exactly who might want to hurt your company, adds Tom Chapman, head of cyber-operations at EdgeWave Security in San Diego.

"In the past people were looking for a firewall or an individual product," for protection, says Chapman, a retired Navy intelligence officer who specialized in hunting down hackers. "Now, they're realizing there is a human element. They need to understand who might be after them. By better understanding your likely adversaries, you can better craft your defense."