Sony breach fuels email security fears at other companies

December 31 2014, by Paresh Dave And Sarah Parvini, Los Angeles Times

You're welcome to dance like there's nobody watching. But you'd better write emails like your email provider is going to be hacked.

The Internet-era twist on the old maxim is the lesson that technology entrepreneur Greg Isenberg learned from the cyberattack that ravaged Sony Pictures Entertainment's computer network last month, sending thousands of sensitive email exchanges into the public domain as the studio, under threat, fretted over whether to release "The Interview."

Isenberg, who runs a popular video-watching app called 5by, lost control of his email account in June after a fraudulent message lured him to a malicious website resembling YouTube. The hacker reset Isenberg's PayPal password, drained his account and found his Social Security number in another email. Immediately after, Isenberg changed his passwords and turned on two-step authentication so someone would need to know his password and have his smartphone to log into his accounts.

The Sony breach spooked him again, though. He toughened up each of his key passwords to a Ft. Knox standard this time around, said Isenberg, a self-described "double-neurotic."

"I felt so burned in June and then sad with what happened to Sony," he said. "We take for granted that our data is all secure. It reminded us all that we're all subject to this."

The public airing of Sony's dirty email laundry - along with nearly 50,000 Social Security numbers, salary information and movies still under wraps - lifted paranoia about security across the business world.

Frank Mong, general manager of enterprise security solutions at Hewlett-Packard Co., called the breach a watershed moment: Sensitive Sony files being held hostage by hackers represent a new threat.

"That is concerning not just for the movie industry but for all industries within the U.S. economy or world economy," he said.

Cybersecurity experts say most companies will wait a couple of months for the post-breach chaos at Sony to settle before deciding whether their computer policies need modifying. But some executives see no reason to tarry.

David Angelo, founder and chairman of El Segundo advertising agency David & Goliath, has shifted his routines to let his lips do as much talking as possible instead of e-mailing. His simmering frustration with complicated email threads was bad enough; security concerns pushed him over the edge. Recently, he called together six people for a meeting rather than let one of those confusing electronic conversations weave on.

"The power of a company will always come down to the day-to-day interaction between people," Angelo said.

He'd been considering an "email etiquette forum" for his 200 employees early next year; the situation at Sony pushed him to follow through. Change will start at the top. Important company announcements won't be delivered via a medium Angelo sees as devoid of flavor, feeling and body language.

"Let's do it in person because when it's sent out in a companywide email

you're not feeling the intent and passion of the top people in the company," he said.

The cyberattack is leading Hewlett-Packard to bulk up its training, using Sony as a case study, Mong said. The latest teachable moment for employees will push the old adage of "If you don't have something nice to say, don't say it" in corporate correspondence.

"Now you have to operate under the mind-set that my email is not confidential," Mong said.

"We should all live with a little more paranoia when we do these things - ask, 'Is this really legitimate?' Should I really be clicking that?" he said.

To be sure, some vigilant companies said the Sony saga hasn't given them a reason to tighten the hatches any more than they already are.

Nadel Architects, the Los Angeles firm behind projects such as the lighted pylons that greet visitors to LAX, employs an encrypted system called Newforma to transfer renderings and blueprints to clients.

Outside cybersecurity services see an opportunity to sell new services in the Sony hacking's aftermath, but such upgrades can be "very costly," said Alex Gonzalez, the firm's information technology director. What happened to Sony, he said, isn't enough to change the math yet.

Still, the Sony headlines have helped boost cybersecurity stocks as analysts predict that worried corporations will seek the vendors' expertise. LifeLock, which monitors an individual's credit and identity information, has been among those outperforming the market, up about 4.7 percent on the New York Stock Exchange in the last month.

Employers often purchase LifeLock for employees or customers whose

personal information is exposed in a leak. (Sony went with a competitor called AllClear ID.) But costs rise almost 50 percent if an employer waits until after a breach to sign up, said Eric Warbasse, LifeLock's senior director of financial services and breach response.

Unpreparedness could lead to additional liabilities. Last month, some U.S. Postal Service workers' unions filed a labor complaint alleging that the agency should have collectively bargained breach response, including the purchase of credit monitoring services.

Warbasse expects many companies to come calling once results of employees' lawsuits against Sony emerge and more details are revealed about the supposed culprits.

The allegation by federal authorities that North Korea spearheaded the Sony attack has drummed up discussions at some companies about whether retaliation tactics should be built into cyberattack response plans, according to security analysts.

It is illegal for the private companies battling attackers in the digital Wild West to "hack back." But many companies see the eye-for-an-eye approach as a means to stymie criminals, particularly if they sit abroad, where the legality of a retaliatory response is unclear and the chance of hackers being prosecuted is low.

Shawn Henry, whose cybersecurity company CrowdStrike Services has defended clients from about 70 hacker groups originating from at least seven countries, said someone could run their "fingers down the phone book and you would find a company running into this problem."

5by's Isenberg - and the almost three dozen companies contacted by The Times - declined to say what's included in the breach response plan of his small New York City operation or what alterations the Sony situation

might spur.

But personally, he began using an app called LastPass to securely store his passwords. According to leaked internal files, several Sony employees had listed personal and corporate passwords in unencrypted documents on work computers.