SONY, HACKED: IT'S NOT ONE MASSIVE BREACH – IT'S MORE THAN 50 BREACHES IN 15 YEARS

Ever try to follow an evolving story in which the cascade of trouble grew so big and moved so fast it was like trying to stay ahead of a pyroclastic flow?

That's what it's like keeping up with emerging reports about the massive cyber attack on Sony. (Granted, it's nothing like the torture report, but Hollywood has a way of making the story spin harder when it's about them.)

The *second* most ridiculous part of the Sony hack story is the way in which the entertainment industry has studiously avoided criticizing those most responsible for data security.

In late November, when the hacker(s) self-identified as "Guardians of Peace" made threats across Sony Pictures' computer network before releasing digital film content, members of the entertainment industry were quick to revile pirates they believed were intent on stealing and distributing digital film content.

When reports emerged implicating North Korea as the alleged source of the hack, the industry backpedaled away from their outrage over piracy, mumbling instead about hackers.

The industry's insiders shifted gears once again it was revealed that Sony's passwords were in a password-protected file, and the password to this file was 'password.'

At this juncture you'd think Sony's employees and contractors – whose Social Security numbers, addresses, emails, and other sensitive information had been exposed – would demand a corporate-wide purge of IT department and Sony executives.

You'd think that anyone affiliated with Sony, whose past and future business dealings might also be exposed would similarly demand expulsion of the incompetents who couldn't find OPSEC if it was tattooed on their asses. Or perhaps investors and analysts would descend upon the corporation with pitchforks and torches, demanding heads on pikes because of teh stoopid.

Nope.

Instead the industry has been tsk-tsking about the massive breach, all the while rummaging through the equivalent of Sony Pictures' wide-open lingerie drawer, looking for industry intelligence. Reporting by entertainment industry news outlets has focused almost solely on the content of emails between executives.

But the *first* most ridiculous part of this massive assault on Sony is that Sony has been hacked more than 50 times in the last 15 years.

Yes. That's More Than Fifty.

Inside Fifteen Years.

Granted, this is not just Sony's film studio business, but Sony Corporation, the Japanese conglomerate which includes Sony Pictures Entertainment, and Sony Computer Entertainment (the parent of PlayStation products). The cyber attacks have focused on these two entities, more so than Sony's manufacturing and finance subsidiaries. But one would think that management at the top of the holding company structure would eventually demand ALL subsidiaries institute a baseline cyber security overhaul.

The first hack was in 1999, when a Sony website was defaced. This was a recurring theme for

several years – 52 times websites across the Sony Group were defaced, between 1999 and early 2011.

Two times during the same period, Sony Computer Entertainment's PlayStation PS3 games or accounts were hacked; customer credit card numbers were compromised, and SonyRewards program was breached – that's a total of 56 attacks inside twelve years.

The attacks exploded after the first quarter of 2011, amounting to a total of 21 in that banner year alone. The worst attack in terms of scale affected 77 million PlayStation Network (PSN) users' accounts. It was only the first multi-million account breach in 2011, however, and PSN was offline for 24 days due to another attack.

Though far fewer in number, cyber attacks since 2011 have been costly to Sony subsidiaries. The entire catalog of Michael Jackson's songs was stolen sometime in 2011, but acknowledged in March 2012. In November 2013, Sony PSN notices unusual activity and resets passwords for an unspecified number of PSN user accounts.

The massive cyber attack in November was not the only one this year. In August, a group calling themselves the "Lizard Squad" spawned a distributed denial of service focused on PSN; at the same time, a bomb threat had been called in, causing diversion of the plane on which Sony's president of its online entertainment subsidiary was traveling.

In February 2014, credentials for one or more Sony Pictures Entertainment servers were obtained by hackers and used to upload malware. Sony did not disclose the attack to the public as the breach appears to have occurred in Brazil, where no law requires such a disclosure. This may have been the initial vector of infection and attack by the Guardians of Peace, culminating in the November data breach, though it is not clear based on the information available to date.

What is clear from Sony subsidiaries' cyber

security history is that Sony has a massive, holding company-wide problem with operations security, and the problem is deeply embedded in its culture if attacks have not been stemmed over the last 15 years.

It is also clear that the entertainment industry – beyond the disturbing attributes like racism and sexism revealed by materials exposed in Sony's breached records – shares an equally troubled attitude toward operations security.

This seems particularly odd for an industry that relies on intellectual property and digital distribution. The industry may complain heartily about piracy, but they are not prepared to lock the doors against incursions, preferring instead to buy influence – through its trade association MPAA – with politicians and law enforcement rather than actually protect their creative works and their employees.

Reaction among the other major film studios has been tepid to altogether mute. One report said Twenty-First Century Fox was considering a request for employees to change their passwords.

(Oh, such bold leadership with aggressive implementation of heightened security efforts…)

But the proof is in the pudding. Hackmageddon's aggregate reports of cyber attacks on major firms over the last handful of years reveals that of the major studios, only Warner Brothers and FOX were attacked a couple of times each, and the breaches were relatively small compared to the scale of 2011 aand 2014 attacks on Sony.

Putting aside the issue of lousy OPSEC, one might well ask why Sony? The theory that North Korea is behind this latest massive breach is split among the cyber security community. NK's complaint filed with the United Nations about Sony's scheduled release of the comedy, The Interview, poking fun at Kim Jong-un supplies a motive. But the complaint letter was filed in June, and the two known breaches from February and November this year don't align well with that time frame. NK was cryptic in response to

early questions about its responsibility; it later denied responsibility.

Some speculate the attack was cyber crime, intended to extort money out of the corporation based on the threat sent to executives on November 21st, before the hackers released Sony's data. The demand read, "We've got great damage by Sony Pictures. The compensation for it, monetary compensation we want. Pay the damage, or Sony Pictures will be bombarded as a whole."

A payout was not and is not feasible, as any sizable cash payout would necessarily require the sign-off of board of directors, and they in turn would be held accountable by shareholders. It's simply not a logical, workable scenario.

It's not impossible the breach was the work of hacktivists. Motives for such an attack are not clear, however. The messy clues to the hack's origins fit more closely with reasons of vengeance, though any rationale beyond NK's anger about The Interview is murky.

No matter the origins of the hack, the beneficiaries of the attack are the competing major studios. Sony Pictures' ~11% share of the movie industry may fall if confidence in the studio does not improve. Investors shorting Sony may also benefit from a recent downturn in Sony's ADR price.

The losers are the employees and larger creative community dependent upon Sony's business. They deserved better protection that even simple changes to security would have afforded them.

And of course the public deserved better than the questionable testimony the president of Sony Network Entertainment International Tim Schaaf gave before Congress back in June 2011, after the enormous breaches of PSN's users' data that spring:

> "Sony Network Entertainment and Sony Online Entertainment have always made concerted and substantial efforts to

> maintain and improve their data security systems.”

Ri-ight.

[graphic: Merrill College of Journalism via Flickr]