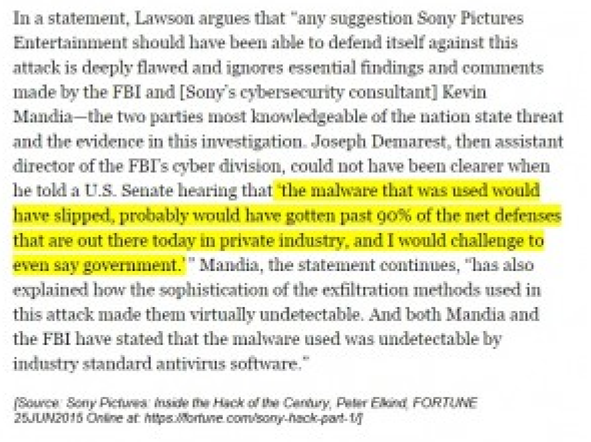
SONY PICTURES POSTMORTEM REVEALS DEATH BY STUPID



In a statement, Lawson argues that "any suggestion Sony Pictures Entertainment should have been able to defend itself against this attack is deeply flawed and ignores essential findings and comments made by the FBI and [Sony's cybersecurity consultant] Kevin Mandia—the two parties most knowledgeable of the nation state threat and the evidence in this investigation. Joseph Demarest, then assistant director of the FBI's cyber division, could not have been clearer when he told a U.S. Senate hearing that 'the malware that was used would have slipped, probably would have gotten past 90% of the net defenses that are out there today in private industry, and I would challenge to even say government.'" Mandia, the statement continues, "has also explained how the sophistication of the exfiltration methods used in this attack made them virtually undetectable. And both Mandia and the FBI have stated that the malware used was undetectable by industry standard antivirus software."

[Source: Sony Pictures: Inside the Hack of the Century, Peter Elkind, FORTUNE 25JUN2015 Online at: https://fortune.com/sony-hack-part-1/]

We already knew Sony Pictures Entertainment's (SPE) hack was bad. We knew that the parent, Sony Group, had been exposed to cyber attacks of all kinds for years across its subsidiaries, and slow to effect real changes to prevent future attacks.

And we knew both Sony Group and SPE shot themselves in the feet, literally asking for trouble by way of bad decisions. Sony Electronics' 2005 copy protection rootkit scandal and SPE's utter lack of disregard for geopolitics opened the businesses to risk.

But FORTUNE magazine's expose about the hacking of SPE – of which only two of three parts have yet been published – reveals a floundering conglomerate unable to do anything but flail ineffectively.

It's impossible to imagine any Fortune 500 corporation willing to tolerate working with 1990s technology for any length of time, let alone one which had no fail-over redundancies or backup strategies, no emergency business continuity plan to which they could revert in the event of a catastrophe. But FORTUNE reports SPE had been reduced to using fax machines to distribute information, in large part because many of its computers had been completely wiped by malware used in the attack.

Pause here and imagine what you would do (or perhaps, have done) if your computer was completely wiped, taking even the BIOS. What would you do to get back in business? You've given more thought about this continuity challenge than it appears most of SPE's management invested prior to last November's hack, based on reporting to date.

A mind-boggling part of FORTUNE's expose is the U.S. government's reaction to SPE's hack. The graphic above offers the biggest guffaw, a quote by the FBI's then-assistant director of its cyber division. Knowing what we know now about the Office of Personnel Management hack, the U.S. government is a less-than-credible expert on hacking prevention. While the U.S. government maintains North Korea was responsible, it's hard to take them seriously when they've failed so egregiously to protect their own turf.

A fast read of Part 1 of the expose validates previous concerns about SPE's and Sony Group's approach to security. At a minimum, each of the following issues would have been addressed by a savvy business, substantially reducing risk:

- Adequate physical site security
- Secured hardware, cordoned off by its function, by way of physical location, firewalls, other services
- Adequate security software from mobile devices to servers
- Monitoring of all content transmissions for size, frequency, pattern, authorization
- 2-step authentication across organization, with frequent mandatory resets
- Catastrophic business continuity planning (especially important in an earthquake-prone area)
- Security screening of all new hire personnel and contractors
- Personnel trained on IP security practices, appropriate to job level, refreshed regularly
- Appropriate response time to security threats and breaches

- Geopolitical risk assessment on all content production
- Ethics reporting mechanism allowing employees to notify management of suspect behavior
- Process improvement mechanism through which employees can suggest improvements and receive rewards for same
- Accountability throughout management chain
- Management aware of risks inherent to digitized intellectual property

The FORTUNE expose, nor any previous reporting by any other outlet, indicates that these issues were addressed before the November hack as part of corporate policy and practices.

It’s clear there is a serious problem at SPE from FORTUNE’s opening grafs. It’s hard to imagine any Fortune 100 business allowing un-vetted visitors to sit unattended with ready access to unsecured. computers and network. The rest of the article is equally disturbing, casting the U.S. State Department and the FBI in equally unflattering light.

Why didn’t the State Department and the FBI come right out and tell SPE it was at serious risk of cyber attack, given what they already knew about North Korea’s alleged attacks on other U.S. systems and businesses?

Why didn’t the State Department spell out just how big a risk Seth Rogen’s ego-inflating boy flick The Interview was, even if it meant giving SPE executives and Rogen a basic history lesson in Japanese-North Korean/U.S.-Korean history?

We know there’s a relationship between the Department of Defense and Hollywood — why wasn’t the DOD likewise involved to provide assistance with shaping message and providing cyber defense?

Given the tepid efforts offered by the U.S. government, one can only wonder if SPE and Sony Group weren’t a sacrificial offering in cyber warfare.

Bait, as it were. Or a propaganda opportunity.