Could the Sony breach have been prevented?

By now, most security experts have weighed in on the recent Sony Pictures breach, and most agree on a couple things. The first is that Sony was careless with its security measures. The second is that many organizations follow the same flimsy practices. Sony has been justly excoriated for the plain-text passwords and Social Security numbers zipping through unencrypted emails that allowed the Guardians of Peace (GOP) hack to grow so large. But the truth is that most security experts believe the company is far from alone in these practices and that Sony's won't be the last hemorrhage we hear about.
While most agree that corporate security needs to improve, one question still remains: Even with best practices in place, could the Sony debacle have been prevented?

Modern era of "WarGames"
The debate still continues over whether North Korea was behind this particular attack, but we do know that intimidation tactics like these will only continue. Hackers will always look for ways to take advantage of organizations and countries, but Sony's surrender in the face of threats, both of violence and more data leaks, will only increase the likelihood of breaches.
It's doubtful that we'll ever get to the point where young kids are hacking into the U.S. nuclear program and accidentally attacking Russia, but fiction isn't as far from reality as we might hope. We've already seen Stuxnet effectively set back Iran's nuclear capabilities by exploiting the Windows AutoRun feature, hackers steal the personal data of more than 100,000 people from the U.S. Department of Energy, and North Korea initiate cyberattacks on South Korea's banking systems.
Espionage, both corporate and governmental, will continue to increase in frequency. We now know that an entire nation-state likely spearheaded the Sony attack, and no amount of preparedness would have stopped the breach. But while the Sony hack might not have been preventable, it didn't have to escalate to such heights.

Security best practices can save businesses

For Sony — and companies that want to avoid a similar fate — security needs to be an integral part of company culture, from the top all the way down.

Email, for instance, doesn't have to be abandoned, but all corporate communication should be encrypted as a matter of practice. After all, it's not just passwords and Social Security numbers that can cause damage to a company.

Companies need to teach employees how to live and breathe best security practices. Employees need to understand the context of not only their surroundings (don't leave computers alone in public places, and think twice about joining public Wi-Fi hotspots), but also of their data. Information is valuable, and realizing this can go a long way in fixing people's cavalier attitude toward it.

Meanwhile, IT departments need to step up their game. Minimal compliance may as well be no compliance. They need to practice constant vigilance and consistently scan for viruses if they want to take these threats seriously.

The security game changes from week to week and company policies need to follow suit. Third-party audits should become commonplace so companies can have a critical set of eyes scrutinizing their security measures. Technology should be updated regularly, as well. What you were using in 2007 is no longer relevant today. More advanced measures like network intrusion detection and penetration testing can help prevent and detect security breaches. One of Sony's biggest problems wasn't being hacked; it was failing to detect the hack until it became public. By then, it was too late.

The last, but arguably most important, aspect of security is the contingency plan. Even with the best security measures in place, no organization is completely protected. Companies need to wake up to this fact if they hope to survive a data breach.

Sony could have done better. Most companies could do better. But the moral of the story is to consider the implications of your actions. Are there competitors or individuals you could be upsetting? Are you using secure agile practices when building software or leaving holes that could render you vulnerable to an attack? While the government might take steps to protect the U.S. from global hacking attempts, this protection is no guarantee of safety (especially given the NSA's less-than-stellar track record on security). Companies and individuals need to take matters into their own hands and realize that the challenge isn't simply prevention; it's mitigation. Cyberattacks aren't going away, but the damage that ensues doesn't have to be so disastrous.