12/29/2014

By: Mark Pribish, Special for The Arizona Republic, December 19, 2014, used by permission of the author

Is Sony's data-breach event about to change how hackers go after our personally identifiable information in 2015?

When the news broke that the information of more than 6,800 Sony employees including Social Security numbers, birth dates, and salaries – most consumers, including me, thought "Here we go again" with another typical major data breach event.

However, this is anything but typical. Unlike Target or Home Depot hacks, the Sony breach exposes a new threat realm that includes stealing and exposing health-care information, employee e-mails and project e-mails involving clients, partners and other employees.

Can you imagine private e-mails from your employer, health provider, banker, social media or child's school about your salary, medical records, credit score, child's grades, personal or business relationships going public for everyone to read and see?

In Sony's case, files that were hacked included unreleased movies (even forcing the cancellation of one), thousands of employees' Social Security numbers, executive pay packages and internal e-mails that were uploaded to the Internet. Sony has described this breach as an "unparalleled crime" that is unprecedented in nature.

Sony Pictures now has legal, financial and public relations liabilities in protecting its image, responding to the needs of individuals affected by the breach and complying with state and federal data- breach laws.

I believe we will see more of the Sony-type hacks — targeted attacks specific to both our personal and business information.

I encourage you to check out Experian's just released second annual data breach industry forecast report. Here are some of Experian's 2015 data breach predictions:

- **Internet of things.** Cyberattacks likely will increase via data accessed from third-party vendors

- **Employees will be companies' biggest threat.** A majority of companies will miss the mark on the largest data breach threat: employees. Between human error and malicious insiders, time has shown us the majority of data breaches originate inside company walls.

- **Data-breach fatigue will grow among consumers.** A growing number of consumers are becoming more apathetic and are taking less action to personally protect themselves.

- **Business leaders will face increased scrutiny.** Where previously IT departments were responsible for explaining security incidents, cyberattacks have expanded from a tech problem to a corporate-wide issue. With this shift, business leaders are being held directly accountable.

- **More hackers will target cloud data.** Cloud services have been a productivity boon for consumers and businesses. However, as more information gets stored in the cloud and consumers rely on online services for everything, the cloud becomes a more attractive target for attackers.

Mark's most important: Set goals in 2015 to focus on risk management and cybersecurity. Be proactive and prepared for a broader range of hacking threats.

Mark Pribish is vice president and ID-theft practice leader at Merchants Information Solutions

Inc., a national ID-theft and background-screening provider based in Phoenix.