Security Headlines

Changing behavior or causing fatigue?

Breaches are commonplace in today's world. In fact, the number of U.S. data breaches tracked in 2015 totaled 781, according to a recent report released by the Identity Theft Resource Center (ITRC). This represents the second highest year on record since the ITRC began tracking breaches in 2005. The headlines have followed in droves.

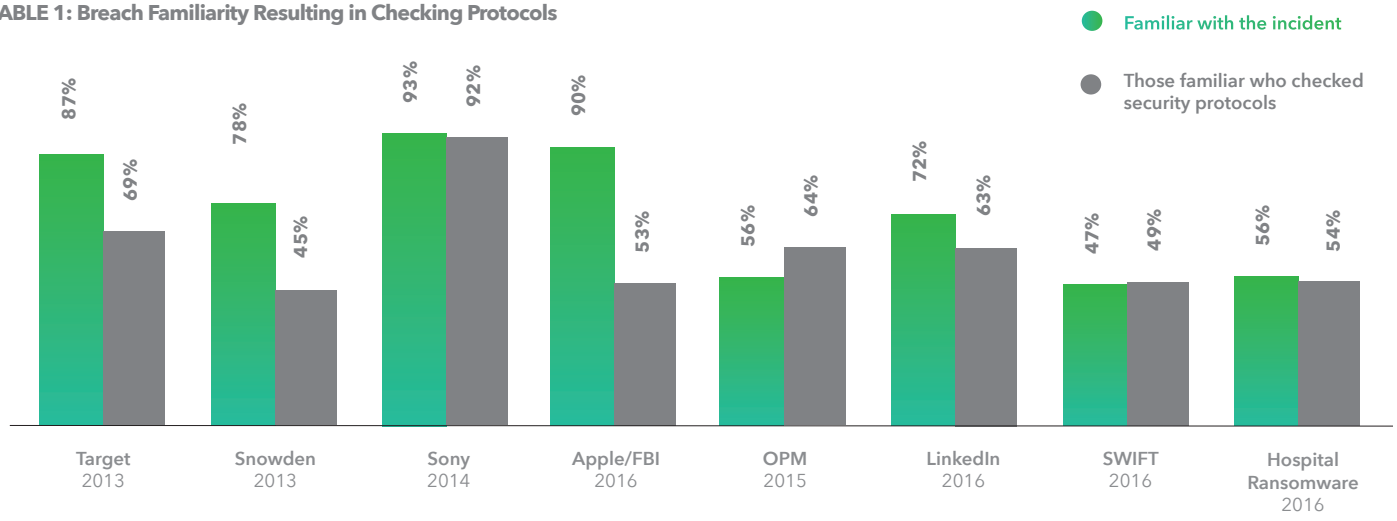
It isn't just breaches making security news. The Snowden revelations in 2013 and the iPhone unlocking dispute between Apple and the FBI in 2016 took over news cycles, making cybersecurity a dinner table conversation. With this new, constant drumbeat of security headlines Lookout, the leader in securing mobility, asked the question, "Is security news urgent enough to capture enterprise leaders' attention, or have they become numb to the noise?"

IT/Security Professionals are tuning out the breach headlines

As incidents continue to surface, IT/security professionals seem to be experiencing "breach fatigue." They are tuning out the news instead of acting, making necessary changes so their organization doesn't become the next headline. 93.4% of security professionals had heard about the Sony hack that happened in 2014, but only 72.1% were familiar with the equally significant LinkedIn hack that exposed hundreds of millions of user credentials that happened in 2016. That's a full 20% decrease.

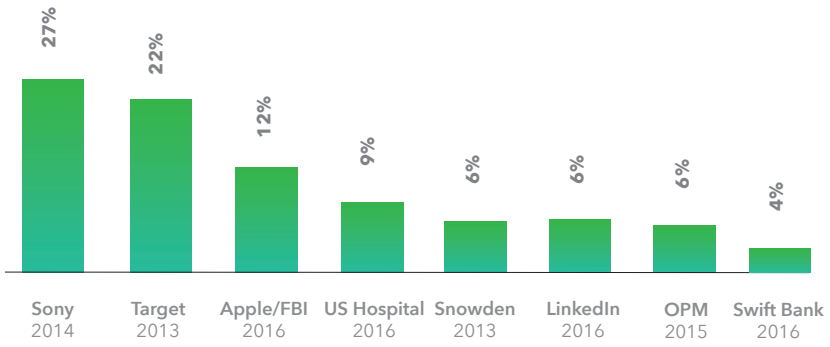
While knowledge of security incidents in general has declined over the years, those who have been following the news have made tangible changes to their organization's security infrastructure. On average, if an IT/security professional reads about a high-profile breach, two-thirds of the time they will react by checking their own security protocols. IT/security professionals check security protocols after a major incident like the Apple/FBI case or Snowden revelations about half of the time.

TABLE 1: Breach Familiarity Resulting in Checking Protocols



However, not all incidents are treated equally. The Sony and Target hacks, for example, had twice the impact on security protocol changes compared to the Apple and FBI tussle. The two were four-times as likely to impact security protocol changes as the LinkedIn hack. This might have been because the Sony attack was one of the first big breaches to be paraded in the public eye. The news about the Target attack focused on its revenue losses and eventual departure of its then-CEO. Headlines like these are enough to spur any IT/security team into action.

TABLE 2 : Which Incident had the Biggest Impact?



Where is the weakest link?

Based on our survey findings, organizations seem to think employees are the biggest vulnerability. Companies believe their employees' mobile use and weak password decisions are the surfaces most susceptible to attack. In fact, after checking their protocols, companies feel most inadequate on mobile and employee-password protection – consistently in the top three categories of insecurities across all kinds of security incidents.

TABLE 3: Top Areas Where IT/Security Felt Less Secure

Companies most commonly increase their overall security spend and invest resources into training staff on security after seeing a security event in the news. They then increase their spend on mobile security and overall employee education on new protocols.

TABLE 4: Top Areas of Increased Spend

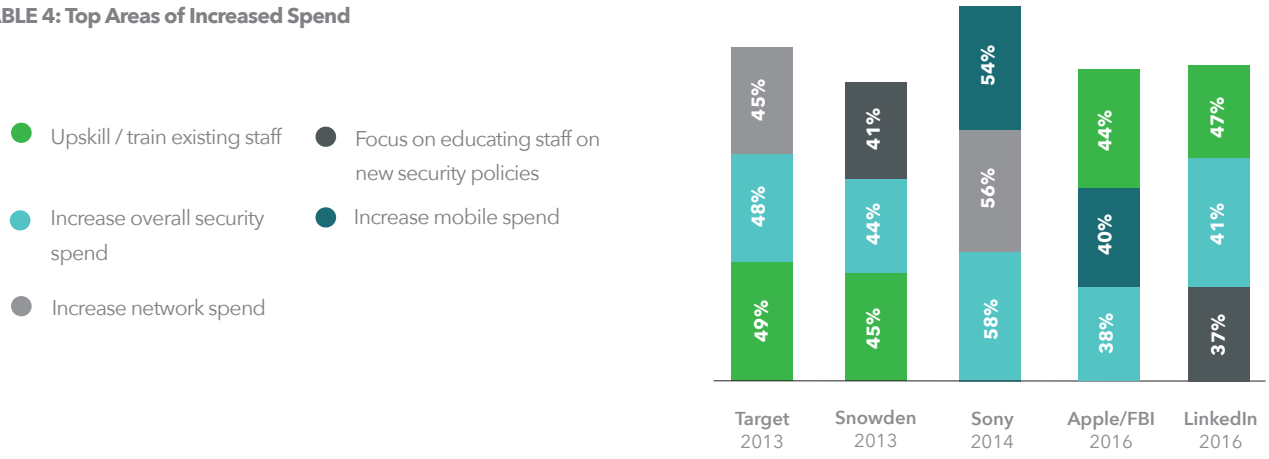
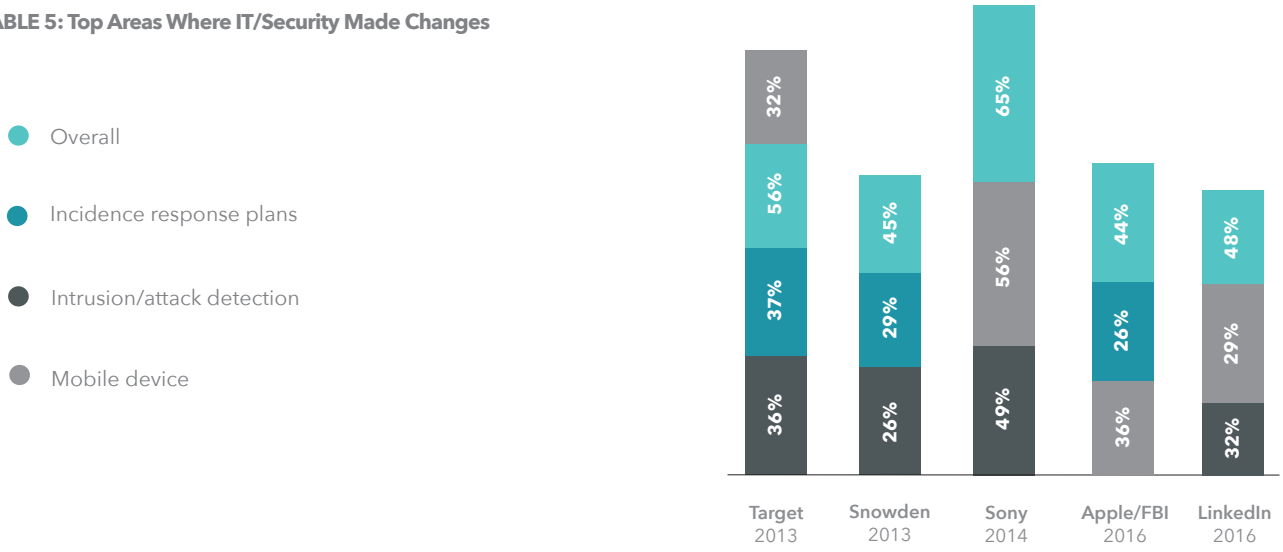


TABLE 5: Top Areas Where IT/Security Made Changes

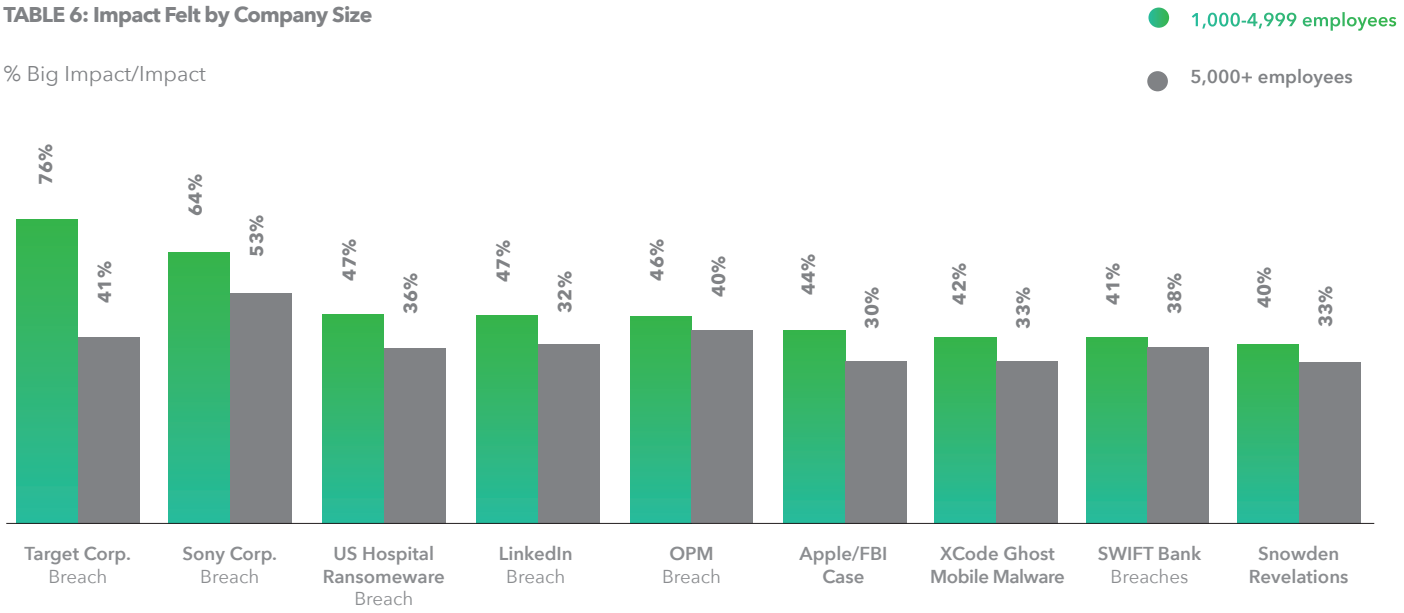


Who is paying attention?

Smaller enterprises (between 1,000 and 5,000 employees) are not only more likely to report that breaches have had a big impact on their security protocols, but they are also more likely to take action to improve their security, despite the fact that large enterprises have many more points of vulnerability as they have many more employees.

TABLE 6: Impact Felt by Company Size

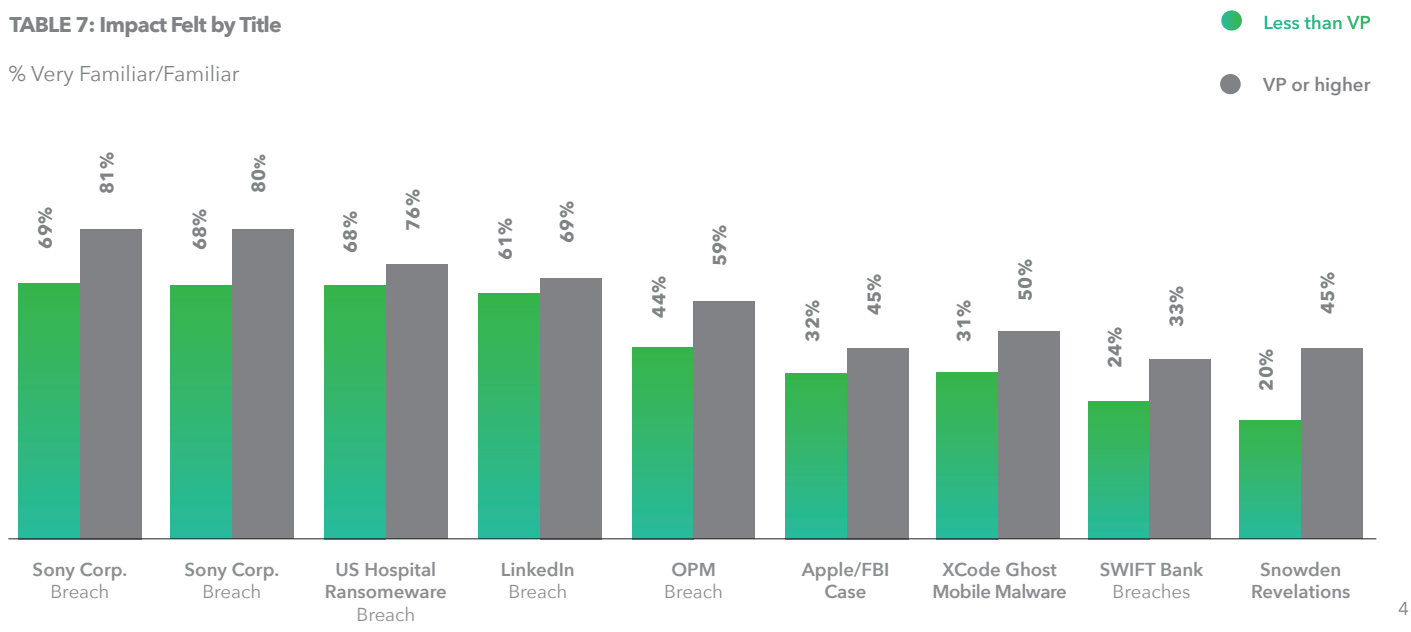
% Big Impact/Impact



When analyzing how breach headlines impact different IT/security professionals across levels of seniority, it became clear that headlines impact VP's and other executives more than they do IT managers and directors. Not only were VP's and other executives more aware of the security incidents generally, they were also more likely to take action to improve their security following the media headlines.

TABLE 7: Impact Felt by Title

% Very Familiar/Familiar



Survey Methodology

An online survey was conducted to a panel of potential U.S. respondents. The recruitment period was July 7, 2016 to July 22, 2016. A total of 500 respondents completed the survey (excluding terminates and abandonments). All respondents were 18 years of age or older, employed at a company with 1,000 employees or more, a decision maker or involved in decision making process as related to IT security, and had a title level above intern, entry level, analyst/associate. The sample was provided by Market Cube, a research panel company. All were invited to take the survey via an email invitation. Panel respondents were incented to participate via the panel's established points program. The margin of error is 4.4%.