Security in the Digital Age: 4 Lessons from Recent Data Breaches

Posted by Dave Packer on 02.25.16 in

Recent data breaches, including 2015's infamous Ashley Madison hack, have shown the world two valuable lessons: in the age of big data, hackers can compromise almost any type of personal information, and that information needs to be protected at all costs. The reality is that nobody can be 100% safe from having their personal information stolen or exposed online. So how can enterprises navigate this troubling new world?

Hacking itself is not new; breaches date back as far as the 1970s. Today, though, enterprises around the world are increasingly dependent on technology and information services in order to transact everyday business. Because of the sheer volume of data available, and because most of it is stored enticingly behind firewalls, enterprises have become rich targets—and to a hacker's mind, the bigger, the better.

The motivations for attacks are varied. While cyber terrorism is certainly a reality, for many hackers it is the lure of financial gain; for others, their goal is to make a public statement regarding data privacy; and for yet others, it is simply 'because they can.'

The recent Sony Pictures breach serves as a perfect example. In 2014, hackers gained access to the company's internal network, containing employee health records (Sony was required to file for a HIPAA violation as a result), unreleased movies, emails, executive salary reports, etc. In a hacker's mind, how better to appear like a modern-day Robin Hood than by exposing nefarious activities and conversations between Sony executives and pirating out their library?

Although not every breach is financially motivated, for those that are, the goal is often to mine for personally-identifiable information (PII) and patient health records. Each record can fetch anywhere from $50USD to $500USD on the black market, and with a successful attack potentially netting millions of names, the monetary haul can be enormous. Health records are especially valuable because they enable a person to assume another individual's health insurance identity; with which they can receive benefits and medical treatments — all under an assumed identity.

My own personal example took place two years ago when my health insurance provider was breached and tens of millions of records containing PII (including mine) were stolen. The following April, someone opened a bank account and filed a U.S. tax return under my name in the hope that the $4000 refund would be deposited into their bank, then to be cashed out or transferred elsewhere. Fortunately, I discovered this when the bank rejected the deposit.

In some cases, attacks occur through a technical exploit, but more often entry is provided by social engineering techniques such as 'spear phishing.' Commonly, a target company is not doing enough to raise awareness across the organization and educate employees about the risks—specifically, how to be cautious in scrutinizing email requests. From there, a hacker is able to exploit a weakness in the system and get inside the firewall. The trouble is that many companies have based their networks on the assumption that their firewall will repel any marauders. They simply do not have the internal fortifications to thwart hackers attacking from the inside.

The impact of these hacks on an enterprise can be severe. In the short term, the reputation of the company is tarnished and ultimately damaged. But the long-term effects of a data breach should be much more troubling to a business: fines, lawsuits, firings, and (in the case of large-scale PII breaches) identity theft protection and restitution for parties affected. The total cost of a large-scale breach, such as the one targeting Anthem, Inc. in 2015, could easily reach into the hundreds of millions of dollars.

One silver lining to these numbers is that many of the affected companies are choosing to completely revamp, reinvest, and change their technology and processes to adhere to stringent compliance and regulation requirements—and to submit to regular audits to ensure their adherence. In these instances, although the wake-up call was painful, it often results in much more impactful results in the long term.

So, what lessons should an enterprise take away from these hacks?

1. If a breach has occurred, be proactive. Communicate to any clients impacted, and be sure to address the main concerns: Exactly what is the extent of the data breach? What is the company's incident response plan? How will the company remedy the breach? What will the company do to reduce the risk of future breaches?
2. Assume that you will be attacked. It is not a question of 'if' but 'when.' Ask yourself: "What safeguards would we need to have in place if a hacker had access to an internal machine?" A firewall alone is insufficient if, once inside, a hacker has unobstructed access to your entire network.
3. Invest in more stringent internal controls, including (but not limited to) two-factor authentication on systems holding sensitive PII-type data. Take all the necessary steps to guard and protect your data. The risks are too high not to.
4. Avoid becoming a target. While the misrepresentation of company data privacy policies is unique to the Ashley Madison hack, it provided the impetus for the attack and should serve as a warning to every enterprise.

The key to dealing with this new reality is to be proactive. Enterprises simply cannot afford the risk of being unprepared for a data breach or to suffer from one. Every organization with even the slightest digital footprint should have a strategy in place that addresses the issues that could arise and learn from the mistakes others have made. With this firmly in mind, companies can avoid having their hard-earned reputation tarnished and their business compromised.

To learn how to address the risks of dispersed data across your organization, download our latest report below.