Client Update

Badger Breach: Good Housekeeping?

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

James Pastore
jjpastore@debevoise.com

Andrew Adair
amadair@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

The data breach just disclosed by the University of Wisconsin isn't the biggest you'll ever hear about. Only 1,213 individuals had their names and Social Security numbers exposed to a digital intruder. But it might be the best reminder in a while of a crucial cybersecurity maxim: Nobody can breach what you don't have.

WHAT HAPPENED?

Last month, an intruder gained access to a database that held information belonging to former applicants to the University of Wisconsin Law School. The breached information consisted of paired names and SSNs from 1,213 individuals who had applied in 2005-06.

Since discovery of the breach, the proverbial "series of unfortunate events" has unfolded, just as in a bigger breach. As required by state law, the university sent notice to the affected individuals – in this case, by both postal and electronic mail. The university notified law enforcement, which continues to pursue the hacker. The university reviewed its cybersecurity and announced improvements. It offered the individuals a year of free credit monitoring at the university's expense. And a slew of news stories publicized the breach, inflicting reputational harm on a great institution.

WHAT CAN BE LEARNED?

Though cybersecurity often presents complicated technical questions – Are we encrypting the data? Is file integrity being monitored? – the Badger Breach shows that simpler questions matter too:

- Do we need to collect that personal data in the first place? In its FAQ on the breach, Wisconsin stated that it must collect SSNs to match admission applications to applications for financial aid. Other organizations might take the episode as a prompt to ask: what forms are we using, what personal data do those forms request, and what business purposes if any do each of those data points really serve? A self-assessment along these lines can be as useful as an encryption upgrade in reducing an organization's attack surface.

- If we need to collect that personal data, how long do we need to keep it? Wisconsin's FAQ does not state why applicant data from 2005-06 were still being held. The incident can be taken as a prompt to ask whether your organization might be holding on to stale data. Consider a thorough exercise in data mapping – that is, a systematic survey of what you are holding onto, why, and where. The exercise may turn up old datasets that would only be interesting to a hacker.

We know of one large employer that conducted a systematic review of all instances where it was collecting SSNs across the organization. The employer determined that, in numerous instances, it actually had no compelling need to collect the SSNs. By ceasing to collect the data and purging what it had, the organization significantly reduced its exposure to a breach.

Good cyber housekeeping supports legal compliance and vice versa. U.S. and European authorities alike have underscored that "data minimization" is necessary to protect both data security and data privacy. In one enforcement case, the U.S. Federal Trade Commission ticked off a list of reasons why it believed a company's cybersecurity was so poor as to be unlawful. Besides a number of technical failings, the FTC noted, the company "never deleted any of the consumer data it had collected." (The case is now on appeal, on grounds largely unrelated to this conclusion.)

The technical side of cybersecurity is critical and cannot be minimized. But the Badger Breach highlights how important it also is to review those boring old document retention policies; to enforce them; and to periodically review what data you are collecting and why. Simply put: If you never collect it, or securely discard it, then no hacker could ever endanger it. On, Wisconsin!

* * *

We would be pleased to discuss these issues.