Data Breaches

Three actions dealers should take to mitigate risks

by: Greg Goldberg, BTA General Counsel

This month's Legal Perspective takes a look at an ominous and increasing threat that hangs over every member of the dealer channel: data breaches. Generally speaking, a data breach consists of any security incident where an unauthorized party gains access to sensitive, confidential or proprietary information. Although the terms "data breach" and "cyberattack" are often used interchangeably, a cyberattack is only a data breach if it involves unauthorized access to data. For instance, a cyberattack that seeks to disable a website by hitting it with an overwhelming amount of traffic is not a data breach. A ransomware attack, on the other hand, where the attacker restricts access to data in exchange for a monetary payoff, is considered a data breach.

According to researchers at IBM, the global average cost of a data breach to an enterprise is $4.88 million. For data breaches in the United States, that average cost jumps to $9.36 million. In fact, some of the most notable data breaches in history have resulted from cyberattacks leveled against U.S. companies.

In perhaps the most famous example, from 2013 through 2016, a group of hackers based in Russia used a series of backdoors, stolen backups and access cookies to compromise 3 billion user accounts at Yahoo, gaining access to sensitive information including users' names, email addresses, telephone numbers, birth dates, passwords and even answers to security questions. In the aftermath, Yahoo faced fines of tens of millions of dollars and 41 separate class-action lawsuits. In 2019, another group of hackers exploited an unprotected server at Facebook and posted the private personal profile information of 530 million users on a free online forum.

The cost of a data breach can actually be even greater in highly regulated industries such as health care, finance and public service. In those sectors, state and federal laws and regulations may include fines and penalties that accrue, in addition to the downstream costs of a data breach, such as lost business, decreased revenue and customer dissatisfaction. Earlier this month, a not-for-profit health insurance plan servicing the New York metro area learned this lesson the hard way, paying more than $1.2 million to settle claims brought by the U.S. Department of Health and Human Services (HHS).

The case, HHS v. Affinity Health Plan Inc., should serve as a cautionary tale to the dealer channel, particularly those offering multifunction equipment. The fact pattern, which came to light as part of an investigative report by the CBS Evening News, is all too common. As part of its reporting, CBS purchased a copier/MFP that came off lease from Affinity. An examination found that the machine's hard drive contained confidential health information belonging to nearly 350,000 individuals. CBS informed Affinity of the data breach and, in turn, Affinity self-reported to HHS. The HHS investigation revealed that Affinity had failed to erase sensitive data from multiple devices returned to leasing agents, thereby disclosing the protected health information of potentially millions of individuals without authorization. HHS found that Affinity had failed to consider information stored on hard drives as part of its required risk assessments and lacked adequate policies and procedures for managing data on leased equipment.

Had Affinity merely undertaken the same steps that most people walk through when trading in a used mobile phone (i.e., erasing the onboard memory and restoring it to factory settings), Affinity potentially could have avoided paying out a seven-figure settlement to HHS — to say nothing of the likely hundreds of thousands of dollars spent on attorneys' fees. Dealers seeking to mitigate against the risk of landing in a situation like Affinity's should consider taking a few actions.

First, conduct a risk assessment to evaluate vulnerabilities, particularly for customers in highly regulated industries. Second, consider adding stronger indemnity language to service agreements that clearly outlines which parties are responsible in the event of a data breach. Third — and, really, this should be first — invest in a comprehensive cyberinsurance policy that covers both losses and defense costs.

The following resources may be helpful on your path toward achieving cybersecurity:

- FTC page on copier data security: https://www.ftc.gov/business-guidance/resources/digital-copier-data-security-guide-businesses
- NIST's draft publication regarding media sanitation guidance: https://csrc.nist.gov/files/pubs/sp/800/88/r1/final/docs/sp800_88_r1_draft.pdf
- HHS's Medscape resources from the Office of Civil Rights: https://www.medscape.org/sites/advances/patients-rights ■

Greg Goldberg, partner at Barta | Goldberg, is general counsel for the Business Technology Association. He can be reached at ggoldberg@bartagoldberg.com or (847) 922-0945.