How A Data Breach Led To A 'Billboard Bomb'

by William T. Kellermann

On Saturday, May 9, 2015 a bomb went off at a busy intersection of the affluent Atlanta suburb of Buckhead. Nobody was killed or physically injured, so you probably didn't read or hear about it with your Sunday morning coffee. But both the FBI and Homeland Security are investigating the incident. The "bomb" has come to be known as the "Buckhead Billboard Bomb." The incident reflects the ever-growing need for businesses large and small to pay attention to data security.

The Buckhead Billboard Bomb resulted when a hactivist group calling itself Assange Shuffle Collective accessed a web-connected digital billboard to display an obscene pornographic image to passers-by at the intersection of Peachtree and East Paces Ferry roads. The software running the billboard had no system security in place and, worse yet, a cyber-security expert had warned the company it was vulnerable. The billboard company responded "not interested…" to the expert's offer to assist.

Based on documents made public around the same time the billboard bomb occurred, a much more ominous data security breach was reported. On April 17, 2015, the FBI applied for a search warrant to search computer equipment belonging to cybersecurity consultant Chris Roberts. Roberts allegedly hacked into computer systems aboard airliners up to 20 times while in flight. He allegedly caused one of the airplane engines to climb, resulting in a lateral or sideways movement of the plane during one of these flights. He purportedly did so by hacking into the plane's in-seat entertainment system using known default passwords, and then accessing the control computer, overwriting code and issuing a 'climb' command to one engine.

While experts dispute Roberts' ability to do so, United Airlines has banned him from flights on their aircraft and the FBI determined an entertainment system box under Roberts' seat on one of the flights was tampered with consistent with Roberts statements to investigators.

While public sentiment for news of data breaches may be wearing thin in the aftermath of chronic, recurring breaches such as the Target, Home Depot, Anthem Health, Sony, Citibank, CareFirst Blue Cross, etc., the threat is not going away. On the

contrary, incidents of security breaches are both on the rise and evolving into many different kinds of persistent threats.

While the dangers of hacking an airliner are obvious, hacking a billboard at first blush may not appear to be any more than a humorous or aggravating incident, depending on one's point-of-view. But the effects of this hack can have serious legal and economic consequences. The Buckhead billboard was already controversial with respect to local sign ordinances written in a pasteboard era ill equipped to handle modern technology. Multiple businesses are involved including the building owner, billboard owner and software technology company. Each may find themselves the target of nuisance lawsuits or worse, including criminal charges for disseminating obscene pornographic material.

So what is a business to do? First, a company should take stock of its systems for creating, receiving, using, managing and storing its information. Identify each information sub-system in use at the company and the kind of information addressed by the system. Attention should be given to confidential or private information, how that information is created or received and most importantly who can access it and how they do so.

Next, a security vulnerability assessment, as part of a broader incident preparedness and response plan is essential. The assessment should identify both technical issues as well as human-factor based threats. Employee inattention or negligence is the largest root cause of many incidents, whether media reported or not. The preparedness plan identifies how a company can prevent incidents, identify potential or actual incidents as they occur, insure timely reporting and remediation, and allow the company to properly manage the legal, technical and public relations aspects of the incident when it occurs. These steps are essential to limit or eliminate liability in the event a breach occurs.

In concert with the incident preparedness and response plan the company should develop a data classification policy. Information identified as confidential for business reasons or identified as private based on statutory or regulatory schemes should be addressed immediately. Attention should also be given to systems holding information, the loss of which might prove embarrassing or aggravating, but which may not represent an obvious target or threat.

Following the identification, planning and classification efforts, a retention and disposition program is essential. In addition to the high cost of managed storage, holding information unnecessarily has indirect economic effect on productivity and leads to extensive risk with no counterbalancing benefit to the organization.

Last, but not least, the company should conduct an insurance policy review to make sure it has the appropriate coverage for an event consistent with the risks identified above. As the pace of breaches quickens, the parameters of loss and risk are better understood. This results in both changes in coverage or exclusions, as well as premium adjustments.

Criminal hackers, identity thieves and hactivists will continue to lead us into uncharted waters as the pace of technology quickens. Businesses of all sizes must mature and adapt to these threats to prevent them where possible and recover quickly when a vulnerability is exploited.

For more information, please contact:

William T. Kellermann, Counsel
415-995-5829
wkellermann@hansonbridgett.com