# Cybersecurity Risk Update: Hackers Take Over Bank via DNS

A recent cyber-attack on the domain name system (DNS) registrations of a Brazilian financial institution has reinforced the need for businesses not only to have a robust cybersecurity infrastructure in place but to be cognizant of the emerging threats they face.

The DNS is a core part of the internet, providing a mechanism whereby internet domain names (e.g., thsh.com) are located and translated into internet protocol (IP) alphanumeric addresses enabling users to be directed to the appropriate sites.

In the aforementioned instance, by accessing and altering the Brazilian bank's DNS registration at its domain registration service, hackers were able to change the bank's DNS registrations, control the bank's website domains and, for several hours, redirect clients to an identical fake site constructed and operated by the cyber criminals. In conducting their normal banking activities, such as inputting access codes and typing in account numbers, clients inadvertently exposed their personal account information, giving unfettered access to the individuals who infiltrated the financial institution's DNS. The fake sites had valid https certificates issued in the bank's name, further masking the illegitimacy of the site, and infected users with a malware download when they visited the copycat sites. Furthermore, because the attack was so sophisticated and thorough, the bank could not use its email to notify customers of the attack.

While DNS attacks are just one form of cyber-attack, the difficulty in detecting DNS attacks, resulting in significant periods of time during which customers/users are re-routed to fake addresses, renders these attacks particularly dangerous. The attack on the Brazilian bank is not the only DNS attack to gain public attention; most recently an attack on DNS services at Dyn (an internet infrastructure company) rendered websites such as Amazon, Twitter, Netflix, Etsy and Spotify inaccessible to users.

As with all cyber threats, it is important to be aware that cyber criminals are continuing to develop innovative ways to exploit vulnerabilities to access sensitive information. Cyber-attacks cannot always be avoided. To place your company in the best possible position, however, it is crucial to periodically conduct security checks of your company's systems, including your company's DNS, and monitor emerging threats to your cybersecurity infrastructure. As part of the DNS security checks, companies should consider implementing security measures before any changes to their IP addresses can be made, such as requiring a two-factor authentication. At the same time, businesses should have plans in place enabling them to be prepared to identify, contain and mitigate the effects of a successful attack, as well as to comply with legal obligations imposed on companies whose systems are breached.

For more information on the topic discussed or if you have any questions or concerns with respect to your organization's cybersecurity practices, please contact any member of Tannenbaum Helpern's Cybersecurity & Data Privacy practice:

Andre R. Jaglom
212.508.6740 | jaglom@thsh.com

David R. Lallouz
212.702.3142 | lallouz@thsh.com

Michael J. Riela
212.508.6773 | riela@thsh.com

Beth Smigel
212.702.3176 | smigel@thsh.com

Maryann C. Stallone
212.508.6741 | stallone@thsh.com

Vincent J. Syracuse
212.508.6722 | syracuse@thsh.com

*Special thank you to Daniel Altabef for his contribution to this article.*

About Tannenbaum Helpern Syracuse & Hirschtritt LLP

Since 1978, Tannenbaum Helpern Syracuse & Hirschtritt LLP has combined a powerful mix of insight, creativity, industry knowledge, senior talent and transaction expertise to successfully guide clients through periods of challenge and opportunity. Our mission is to deliver the highest quality legal services in a practical and efficient manner, bringing to bear the judgment, common sense and expertise of well trained, business minded lawyers. Through our commitment to service and successful results, Tannenbaum Helpern continues to earn the loyalty of our clients and a reputation for excellence. For more information, visit www.thsh.com. Follow us on LinkedIn and Twitter: @THSHLAW.