



CYBERSECURITY

[NSA Issues List of Vulnerabilities Used by Chinese Backed Hackers](#)

The National Security Agency (NSA) issued a Cybersecurity Advisory on October 20, 2020, entitled “Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities,” alerting IT professionals to 25 vulnerabilities that Chinese state-sponsored hackers are using against U.S. businesses that “can be exploited to gain initial access to victim networks using products that are directly accessible from the internet and act as gateways to internal networks.” The Advisory is designed to share information with security professionals to urge them to update systems to protect against the attacks. [Read more](#)

HIPAA

[OCR Settles with NY Spine for Failure to Provide Access to Records](#)

Continuing its enforcement priority of assisting patients with obtaining access to their health records, the Office for Civil Rights (OCR) recently settled its ninth case with a covered entity that it alleged failed to provide proper access of health records to a patient. [Read more](#)

ENFORCEMENT + LITIGATION

[New York Department of Financial Services Issues Report on Recent Twitter Hack](#)

You probably heard about the recent hack of Twitter accounts that took place on July 15, 2020. The hackers took over several prominent Twitter accounts, which resulted in a scam that netted over \$118,000 in bitcoin for the hackers. One of the most startling things about the cyberattack was that it was led by a 17-year-old along with his accomplices. The hackers took over the accounts of well-known individuals including Barack Obama, Kim Kardashian West, Kanye West, Bill Gates, Elon Musk and many others, and tweeted a “double your bitcoin scam” from these Twitter accounts directing people to send bitcoin to fraudulent accounts. [Read more](#)

NEW + NOW

[Secureworks 2020 Incident Response Report Confirms Increased Vulnerabilities with At Home Workers During Pandemic](#)

Secureworks issues an annual Incident Response Report that is very helpful in obtaining information on what types of incidents are occurring

October 22, 2020

FEATURED AUTHORS:

[Linn Foster Freedman](#)

[Deborah A. George](#)

FEATURED TOPICS:

[Coronavirus](#)

[Cybersecurity](#)

[Enforcement + Litigation](#)

[HIPPA](#)

[New + Now](#)

[Privacy Tip](#)

VISIT + SHARE:

[Insider Blog](#)

[R+C website](#)

[Twitter](#)

[Facebook](#)

[LinkedIn](#)

in order to become more resistant to threats. The 2020 IR Report was recently issued, and it contained some conclusions that made sense, while others were surprising. [Read more](#)

PRIVACY TIP #256

[COVID-19 Scams Continue to Plague U.S. Public](#)

Cyber criminals know that people are concerned about the coronavirus and looking for more information to protect themselves and their family members. They are also preying on the distraction of working from home. This week's privacy tip covers phishing emails and scams using the COVID-19 pandemic to lure people in. [Read more](#)



Boston | Hartford | New York | Providence | Miami | Stamford | Los Angeles | Wilmington | Philadelphia | Albany | New London



© 2020 Robinson & Cole LLP. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission. This document should not be considered legal advice and does not create an attorney-client relationship between Robinson+Cole and you. Consult your attorney before acting on anything contained herein. The views expressed herein are those of the authors and not necessarily those of Robinson+Cole or any other individual attorney of Robinson+Cole. The contents of this communication may contain ATTORNEY ADVERTISING under the laws of various states. Prior results do not guarantee a similar outcome.