THE
NATIONAL LAW REVIEW

Business Email Compromises Bilking U.S. Companies Out of $301M Per Month

Robinson+Cole
Article By
Linn F. Freedman
Robinson & Cole LLP
Data Privacy + Security Insider

- Communications, Media & Internet
- Criminal Law / Business Crimes
- Consumer Protection

- All Federal

Thursday, July 25, 2019

The United States Treasury Department came out with a report last week that concludes that business email compromises (BEC) are costing U.S. companies more than $301 million **per month**. The report confirms that the two industries hit the hardest by these scams are manufacturing and construction.

The report, issued by the Treasury Department's Financial Crimes Enforcement Network, reports that 1,100 BEC scams occurred each month against U.S. companies in 2018, which is an increase from 500 per month in 2016. The BECs cost U.S. companies $301 million per month, which is an increase from $110 million per month in 2016.

The scams outlined in the report are the same ones that we see every day. They start with phishing schemes to an executive in the company, then the intruder either impersonates the executive to request other members of the company to send information or money, or they follow the executive's email, forward it to a Gmail account without the knowledge of the executive, and start to follow the email trails to determine who the executive and business are doing business with, who the vendors and third parties are, and to whom the company owes money. They are patient, and at just the right time, the intruder copies the signature line of the executive, and requests that Accounts Payable wire a known vendor tens or hundreds of thousands of dollars to a bank account that the fraudster drains after the money is

wired.

According to the report, the manufacturing and construction industries are getting hit the hardest, and the losses in those two industries account for 25 percent of the total amount lost. Commercial services have been hit hard and have seen increases in BEC.

There are several steps businesses can take to combat BECs. These include: frequent employee education sessions on phishing, malware and ransomware, implementing security tools to block suspicious emails from breaking through the perimeter, having employees on high alert for phishing scams and providing resources on common scams so they can identify them, encouraging employees to report phishing emails, having processes in place to authenticate all requests for transfer of money, encourage the use of the telephone and avoid reliance on email communication, having processes in place regarding large transfers of funds, and having appropriate insurance to cover any losses.

BEC continues to be a huge problem for U.S. businesses, as outlined by the Treasury Department, and the schemes are getting trickier. Staying vigilant and understanding the risk, including your employees in the solutions, and prioritizing measures to respond to the risk are key to managing the risk.

Source URL: https://www.natlawreview.com/article/business-email-compromises-bilking-us-companies-out-301m-month