# Cybersecurity News

NEWS AND INFORMATION TO HELP PROTECT COMPANIES AND EMPLOYEES

**OCTOBER/NOVEMBER 2019**

## Business email compromise scams increasing and becoming more sophisticated

In July, 2019, the U.S. Treasury Financial Crimes Enforcement Network (FinCEN) released a strategic analysis of Bank Secrecy Act (BSA) reporting. The findings include a report that the number of suspicious activity reports (SARs) describing business email compromise (BEC) incidents reported monthly grew significantly.

- Nearly 500 BEC incidents were reported per month in 2016. In 2018, this number grew to 1,100 per month.
- The SARs total value of attempted BEC thefts rose significantly from $110 million per month in 2016 to an average of $301 million per month in 2018.

To assess BEC trends and methods, FinCEN analyzed randomly selected, statistically representative samples of SARs narratives on BEC incidents filed in 2017 and 2018. Findings include:

- Impersonating a CEO or other business officer accounted for 33% of sampled incidents in 2017, declining to 12 percent in 2018. Meanwhile, 20% of impersonations were from an outside entity in 2018 reports (up considerably from an unmeasured amount in 2017).
- In sampled 2017 incidents, 30% used fraudulent vendor or client invoices. This number rose to 39% in 2018.
- In 2017 incidents, 73% of scams directed funds to domestic accounts, which the report asserts are likely controlled by money mules that are considered to be a stop in the money laundering process (based on the FinCEN analysis of BEC networks and law enforcement insights on use of money mules for other scams).

### What is Business Email Compromise (BEC)?

BEC is a scam that targets businesses as well as educational, government, and non-profit institutions for fund transfers. The victim is typically tricked into thinking a legitimate email from a trusted person or entity is directing them to make a payment for a normal business activity.

Organizations that normally conduct large wire transfers and rely on communication via email for these wires are generally targeted. Convertible virtual currency, ACH transfers, and gift cards can also be used in BEC schemes.

Perpetrators frequently compromise a key email account by using computer intrusions or social engineering and then send and fraudulent email directing funds to criminal-controlled accounts. BEC criminals also use spear phishing, specialized malware, and spoofed emails.

***Money Mules**: Individuals who knowingly or unwittingly transfer money on behalf of the BEC perpetrators to launder BEC proceeds. Money mules are often recruited online through other scams.*

*(continued)*

- In 2017 and 2018, the Manufacturing and Construction sector was the most targeted sector, representing 20 percent of all analyzed transactions in 2017 and 25 percent in 2018.

*Source*: Financial Crimes Enforcement Network, FinCEN. *Financial Trend Analysis, Manufacturing and Construction Top Targets for Business Email Compromise,* 2019. https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf.

## October is National Cybersecurity Awareness Month: Own IT. Secure IT. Protect IT.

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) and National Cyber Security Alliance (NCSA) lead observance of National Cybersecurity Awareness Month (NCAM) every October.

This year, the strategic focus is to promote personal accountability and proactive digital privacy, security best practices, common threats, and cybersecurity careers through the theme: Own IT. Secure IT. Protect IT.

**Own IT.** Understand personal digital profiles. Includes staying safe on social media and managing privacy settings and devices.

**Secure IT.** Secure digital profiles. Includes managing passphrases and multi-factor authentication as well as securely shopping online and identifying phishing.

**Protect IT.** Maintain the digital profile. Includes understanding the need to update systems, Wi-Fi safety, and protection of customer data.

For more information about how to promote Cybersecurity Awareness month, visit the National Cybersecurity Alliance Stay Safe Online site: https://staysafeonline.org/.

*Source*: National Cyber Security Alliance. *Stay Safe Online.* https://staysafeonline.org/.



## The M&A dealbreaker: cybersecurity issues

Increased connectivity opens the door to cyber attacks. When it comes to M&A deals, a cybersecurity review is an essential part of the due diligence process. Earlier this year, Forescout Technologies, Inc. conducted a survey of 2,779 IT decision makers and business decision makers in the U.S., France, United Kingdom, Germany, Australia, Singapore, and India to understand cyber risk within the M&A lifecycle.

**Key Findings:**
**More than half of respondents (53%) indicate their organizations found a cybersecurity issue or incident that jeopardized a deal.**

**Cyber is a top priority** 81% of IT and business decisionmakers are putting more focus on a target's cybersecurity posture, more so than in the past.

**Surprise data breaches = no deal** In keeping with their companies M&A strategies, 73% of respondents noted that an undisclosed data breach equates to an instant deal breaker.

**More time for M&A cyber review** The majority of decisionmakers feel they need more time to evaluate cybersecurity as part of an acquisition with only 36% of respondents agreeing that IT teams are given time to review cybersecurity standards, processes, and protocols before an acquisition.

**M&A regrets due to cyber risks** 65% of respondents indicated that their companies experienced regrets due to cybersecurity concerns.

**Cyber risk assessment skills** Only 37% of IT decisionmakers responded that IT teams have the necessary skills to conduct cybersecurity assessments for acquisitions. Nearly all respondents—97%—responded that their organizations allocate funding to contractors for IT audits and cybersecurity risk assessments.

**Risk areas** 51% of respondents indicated human error and 50% noted configuration weakness and connected devices put organizations at risk.

**Overlooked risks** 53% of IT decisionmakers find unaccounted for devices after completing integration of new acquisitions.

*Source*: Forescout Technologies, Inc. *The Role of Cybersecurity in Mergers and Acquisitions Diligence,* 2019. https://www.forescout.com/company/resources/cybersecurity-in-merger-and-acquisition-report/.