

Three ways treasurers can up their cybersecurity game

published on 29.10.2018 by Jan Dirk van Beusekom

Treasury departments are now a prime target for cybercriminals

The costs of cybersecurity incidents are expected to reach USD\$6tr. per year by 2021^[1]. Corporations are increasingly being attacked by cybercriminals and treasury departments are now prime targets.

As outlined in our [Journeys to Treasury Report 2018-19](#), treasurers have a growing, frontline role to play in protecting the organisation, given the large financial value of transactions that the department processes and the sensitivity of the data it holds.

Here's how treasurers can get involved:

1. Embrace co-ordinated defence. Cybercrime has become structured and organised, so the defence needs to be similarly structured. As such, IT, Finance and the technology partners that support treasury need to work together closely and proactively to identify threats and weaknesses, and resolve them collaboratively.

2. Look beyond payments. While treasurers have traditionally tended to focus their efforts on protecting payments, equal attention needs to be given to protecting data and information. Bank account details, financial and commercial counterparty settlement instructions, employee details and financial data about the company are all valuable assets to hackers. These need to be protected with the same degree of care as payments.

3. Instil the right controls and culture. People and processes are just as important, if not more so, than specialist technology in the fight against cybercrime. Good training is crucial in order to ensure treasury staff are equipped to fend off evolving cyber threats, including increasingly sophisticated phishing emails and CEO fraud, which involves the impersonation of senior executives.

Banks also have an important role to play in helping treasurers to safeguard their operations and assets. BNP Paribas invests heavily in its channels to ensure they remain robust and offers cybersecurity awareness training for corporate clients. We are also happy to work hand in hand with treasurers to increase the cyber resilience of their function.

[Download Journeys to Treasury report](#)

^[1] 1 - Top cybersecurity facts, figures and statistics for 2017, Cybersecurity Observatory <https://www.cybersecobservatory.com/2017/06/15/top-5-cybersecurity-facts...>

Related Articles

Inside Cash - Episode 1: SWIFT gpi, Journeys to Treasury & World Payments Report

Trends & Vision 19/10/2018

Discover how the evolution of SWIFT GPI is impacting the future of x-border payments.

Virtual accounts: a 60-second guide

Managing Collections 15/10/2018

Instant payments: what treasurers REALLY need to know

Paying Here & Abroad 02/07/2018

For many treasurers, building the business case around real-time payments (RTPs) may seem like a tough call. After all, what treasurer wants to pay money away more swiftly? Delve a little deeper into the topic, however, and the potential use cases become clear.

PSD 2: What are the Concrete Benefits for Treasurers?

Trends & Vision 30/08/2018

The European Commission's Payment Services Directive 2 (PSD2) went live on 13 January 2018. Although hailed as the start of a new era for financial services, corporate treasurers seem to be largely underwhelmed by the changes that PSD 2 has brought about.

Real-time Collections: The Rise of Request to Pay

Managing Collections 17/08/2018

Much has been written in the trade press about real-time payments, but real-time collections are yet to hit the headlines in the same way. The good news, however, is that these are now becoming a reality ? thanks to the growth of so-called ?Request to Pay? (RTP) schemes.

Netherlands Antilles

Newsletter

Email *

I want to receive Cash Management related content, articles and information from BNP Paribas Cash Management. *

* Mandatory fields

Source URL: <https://cashmanagement.bnpparibas.com/our-solutions/trends-and-vision/three-ways-treasurers-can-their-cybersecurity-game>