FIGHTING CYBER-RISK IN TREASURY AND FINANCE

Q&A with Treasury and Cyber-Risk Subject Matter Expert Jeff Diorio

The number of cyber and fraud attacks have been increasing, as have their level of sophistication. As the owners of remittance and payments processes, treasury and finance are right in the center of this issue. In March of 2020, APQC interviewed Jeff Diorio (Director, Treasury Strategies) on the topics of cyber-risk and fraud mitigation in treasury and finance. Diorio has more than 30 years of experience working with financial technology, global treasury operations, disaster recovery and redundancy planning, and cyber-risk and fraud mitigation. Diorio co-heads the Treasury Advisory practice at Treasury Strategies, working with corporate treasury departments, treasury technology vendors, and financial institutions. In the interview, Diorio described some of the most common forms of cyber-attack on treasury and Accounts Payable (AP), techniques bad players are incorporating, examples of the tools and technologies that organizations are using to mitigate cyber-risks, and practices/recommendations organizations can utilize to help minimize risk in treasury and finance.

Cyber Risk Trends

APQC: What are some of the most common cyber-attacks you see in your work with clients? How do these attacks work?

Diorio: One common type of cyber-attack is known as Business E-mail Compromise (BEC). An example of this is an instance where somebody purporting to be the CEO or another internal senior executive reaches out to someone authorized to make payments on behalf of an organization via email and requests a large wire transfer for an urgent business purpose. It's reasonable to believe that a company could be in the middle of an acquisition and need a large transfer, but typically this is done through a more formal process with appropriate approvals. These kinds of attacks often seem credible and are sophisticated in their construction. The e-mails appear to be coming from the executive's account and are written in a style that effectively mimics them. Attackers might even use recordings of the executive's voice to give the requests more credibility.

A second kind of attack is an attempt to redirect valid vendor payments. Attackers, pretending to be a vendor, reach out to tell an organization that accounts payable needs to change the delivery instructions for payment. For example, "We just changed our lockbox and here are the new instructions." The attackers are often able to send very sophisticated messages that include the name of the actual vendor and a proper PO number. These attacks are often much more successful than BEC attacks.

APQC: What are some of the pitfalls or mistakes that make organizations more vulnerable to these kinds of attacks?

Diorio: BEC attacks succeed typically when someone in the organization sends the requested money without following proper payment workflows and obtaining proper approvals, often in violation of their own payment policy. Most treasuries have a formal payment request channel, workflow, and process for executing these kinds of payments. These kinds of attacks tend to be less successful in general because most treasury departments are used to dealing with higher value and high risk payments, follow their policies, and are staffed with more senior and experienced finance people.

Not having dual-factor authentication in place also makes organizations more vulnerable to this kind of attack. For example, hackers targeted the CEO of one startup company through his personal e-mail account, which served as the backup for his corporate email account. The attackers gained access to his corporate account by resetting the password, and used his administrative privileges to gain access to other employee e-mail accounts. They were ultimately able to alter and transmit this firm's receivables deposit directions for invoicing that went to their clients, resulting in a $5 million loss for this company. Dual-factor authentication on their e-mail accounts alone could have prevented that loss.

Dual Factor Authentication

A method of confirming users' claimed identities by using a combination of two different factors. For example, a banking Web site might send an access code to a user's phone as an extra step in the login process to verify the user's identity.

Organizations make themselves vulnerable to payment fraud when they don't properly validate requested changes for vendor payment instructions. I've had people tell me things like, "We received something on bank letterhead," and I chuckle and say, "You know, my kids can do that." Just because it's on bank letterhead doesn't mean anything.

Mitigating Cyber Risk

APQC: What role do strong processes play in helping to prevent cyber-risks?

Diorio: One important step to prevent cyber-attacks is putting a really good workflow in place that routes a payment request, gets it authorized properly, and doesn't transmit payment to the bank until it's gone through all the proper steps. Companies are putting a lot of these workflow systems in place (a majority are incorporated into their ERP systems) and they work very well. They require dual authentication to get into the system so you can be certain the requests and approvals are coming from the right people.

Another important step is making your processes as efficient as possible so you don't have an army of people processing requests. Make sure that you minimize the number of people that have

> *"By reducing the number of people, the number of accounts, and the number of banks you use, you will shrink the footprint of what you have to control and the risk will become exponentially smaller as a result."*
>
> *—Jeff Diorio, Treasury Strategies*

access to bank accounts and have rights to open bank accounts. By reducing the number of people, the number of accounts, and the number of banks you use, you will shrink the footprint of what you have to control and the risk will become exponentially smaller as a result.

APQC: What are some of the tools and technologies that are available to help with treasury and finance's fraud mitigation efforts?

Diorio: Organizations are focusing on putting systems and tools in place to help them validate vendors and payment instructions. One account validation tool, Early Warning, is a database with a massive number of bank accounts in it. You can query the tool to confirm that an account is truly owned by the vendor or payment recipient using details like the organization's name, tax ID, and street address. One challenge with this tool is that you may need to have four or five different ways to verify (e.g. name, street address, tax ID) because sometimes some of the details don't match a legitimate account. There may be things like a missing comma in the organization's name, or the street address is actually a PO Box.

There are many other really good vendor account validation tools to help ensure your payment account details are correct like SAP's Ariba. Ariba is a vendor management system with a self-service feature that lets vendors enter their settlement instructions. The system has a feature that says things like "15 other organizations pay that company to that account, so we can tell you it really is their account." The validation it provides is wonderful—I'm always a little surprised by how many organizations are not using it as a core feature of Ariba.

Anomalous detection tools are another very valuable type of tool to help organizations identify fraudulent transactions. These are the same tools the credit card companies have been using for years to flag transactions that seem irregular given a customer's purchase history or location. Vendors like Splunk have made applications specific to finance where you can drop your payment files into a directory and the tool will analyze them. After a period of time and with enough data to work with, the tool will start to flag payments that look irregular for further review. For example, maybe 90 percent of your payments look fine, but 10 percent are going to a bank account that hasn't been used before. The tool will discover and present that for you to review, hopefully before they have been sent to the bank for processing.

APQC: What advice do you have for smaller organizations that might not be able to put large fraud detection systems in place?

Diorio: Organizations that don't have the wherewithal to put a big system in place can still have a good process in place for account validation. Many vendors are proactively having conversations with customers to say, "If you receive a note from us saying we've changed our bank account, you have to call us. Do not accept an e-mail, letter, or anything else unless you talk to us first." Have a preset contact list for validating requests to change a vendor's account information and have those conversations in advance and call to verify any payment requests from the vendor that don't come through the usual channels.

Another effective validation approach, especially before executing larger transfers, is doing a "penny test." If you have no other way of validating the vendor, you can send a very small amount to the specified account, call the vendor to ask whether they received it, and ask them to confirm the amount you sent. It's a pain to do that in some ways because it's a very manual approach, but it's an effective way to validate.

One of the easiest things a treasurer or controller can do is talk to their banks and ask what tools they have in place to protect against payment fraud. The banks are the entities that are sending the money and processing the payment, and they have very good tools that act as another layer on top of the organization's preventative measures.

"One of the easiest things a treasurer or controller can do is talk to their banks and ask what tools they have in place to protect against payment fraud."

—Jeff Diorio, Treasury Strategies

APQC: Beyond securing processes and technology, what other steps should organizations take?

Diorio: Fraud insurance is very important because fraud is going to happen—it's not question of if but when you will be impacted. Everybody has some kind of insurance, but you have to go through the insurance rider carefully to make sure you know what the policy covers. Even if you are insured for financial fraud, the policy may not cover cyber-attacks or have mitigating clauses that stop you from being covered. You can buy cyber-risk insurance, but many policies only cover the release of Payment Card Industry (PCI) information and not financial fraud. You also won't be covered if your employees execute a payment in violation of your internal policy. You have to make sure you have the right coverage and understand where the holes are in that coverage. Another positive to financial cyber fraud insurance is your provider will probably have a list of best practices and requirements you have to incorporate before you qualify for coverage. These by themselves are very informative.

Another best practice we recommend is reconciling your bank accounts daily. You'll only catch something after the fact with daily cash reconciliations, but it's much better to catch something the first time it happens than the tenth time. Unfortunately, a lot of organizations don't reconcile their cash daily—they'll do it weekly, monthly, or in some cases, not at all. They'll just go to the end of the year and say "well, it kind of matches up." If you're trying to avoid fraud, daily reconciliation will at least tell you that it happened and help you catch it early.

Lastly, I would emphasize that fraud prevention and cyber risk protections are a "C"-level issue. You have to build a culture that takes these things seriously from the top down. Having to raise compliance issues to senior management can be very challenging and even expose you to personal job-risk if that culture is not in place. For example, one corporate treasurer identified a potential area where there was a problem in his organization—Money was going somewhere it shouldn't. When he brought it to the attention of the relevant group, they immediately got defensive. Instead of wanting to understand what was happening, they simply denied that anyone would have made that kind of mistake and stuck their heads in the sand. That was kind of a shock—he was the organization's treasurer and chief risk officer with a C-level title, and he was getting pushback.

Every organization has to embrace the idea that this is going to happen and the role that all internal and external partners might potentially play in it. People need to feel confident that if they do report an issue, they won't be treated like the boy who cried wolf and castigated when they report it.

Practices to help minimize cyber risk and payment fraud:

Organizations should consider the following practices that can help prevent cyber-risk and payment fraud in the finance function:

- Segregation of duties
- Workflow with physical and electronic forms
- Multiple approval layers for large payments
- Dual-factor authentication on critical payments
- Payment authorization limits
- Payment technology enforcing thresholds and workflow (ERP, TMS, banking systems, etc.)
- Bank controls (authorized payer, mobile authorization, payment limits, etc.)
- E-mail flagging on all external e-mails
- Written policies that are widely communicated
- Employee education (certified and updated at least annually)
- Fraud action plans
- Internal and external controls
- Understanding and support from senior management
- Quarterly refresh and update for controls
- Penetration testing from white hat type organizations
- External audits
- Fraud insurance
- Penny tests

ABOUT APQC

APQC helps organizations work smarter, faster, and with greater confidence. It is the world's foremost authority in benchmarking, best practices, process and performance improvement, and knowledge management. APQC's unique structure as a member-based nonprofit makes it a differentiator in the marketplace. APQC partners with more than 500 member organizations worldwide in all industries. With more than 40 years of experience, APQC remains the world's leader in transforming organizations. Visit us at https://www.apqc.org/, and learn how you can make best practices your practices.