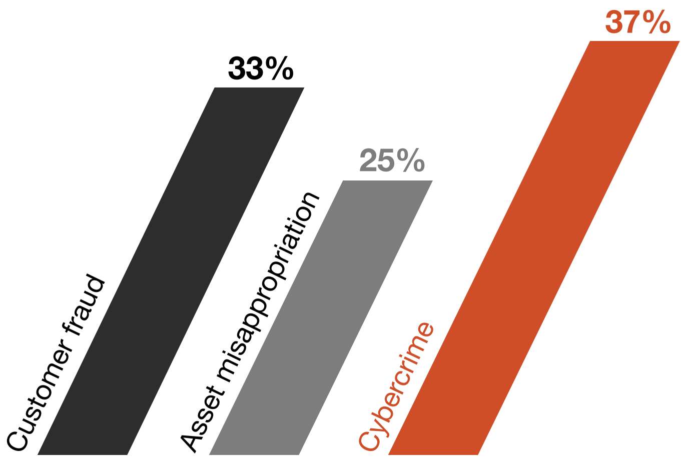
# The new controls playbook against cyber-enabled vendor fraud

# The new controls playbook against cyber-enabled vendor fraud

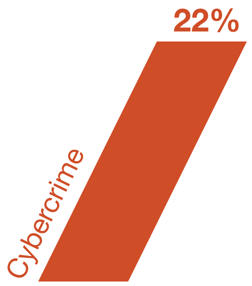
- Vendor fraud is rising with widespread digitization, increased reliance on third-party vendors and a shift to remote and hybrid work arrangements.
- Organizations may need a new controls playbook — one that combines finance and cyber controls — to help counter cyber-enabled vendor fraud at the speed and scale of these attacks.
- There are considerable payoffs from enhancing fraud risk management, from decreasing losses and business disruption to improving compliance efficiency and enabling business growth.

Vendor fraud isn’t new, but it’s becoming more sophisticated and successful. In recent incidents, fraudsters combined cyber and financial crime techniques to hijack, impersonate or manipulate their victims for personal gain. Data from PwC’s 2022 Global Economic Crime Survey shows that cybercrime was the most common and the most disruptive crime experienced by organizations over the past two years regardless of industry or revenue.

## Type of fraud experienced



## Most disruptive fraud experienced



B2. What types of fraud, corruption or other economic/financial crime has your organization experienced in (country/territory of responsibility) within the last 24 months? Base: All those who have experienced fraud, corruption or economic/financial crime within their territory (602)
B3. Of the fraud, corruption or other economic/financial crimes experienced by your organization in the last 24 months, which was the most disruptive/serious in terms of the impact on your organization (monetary or otherwise)? Base: All those who have experienced fraud, corruption or economic/financial crime within their territory (602)
Source: PwC, 2022 Global Economic Crime and Fraud Survey, April 2022.

As technology demands continue to accelerate and access to data becomes more widespread, we expect further growth in these types of incidents. Many companies are opting for faster, digital payment methods to transact business, and that compresses the timeline needed to mitigate frauds and require faster detection methods. Then there's the added risk generated by having multiple payment platforms. With employees and vendors shifting to remote or hybrid work arrangements, the risk has heightened. Without accountability or supervision, and with distractions that may come with remote work, employees are not only more likely to be targeted by fraudulent scams, they're also more likely to perpetrate and facilitate them.

Going digital-first can empower organizations and their vendors, but it also enables new types of fraud. Today, cyber-enabled vendor fraud schemes are becoming easier to execute — with higher success rates.

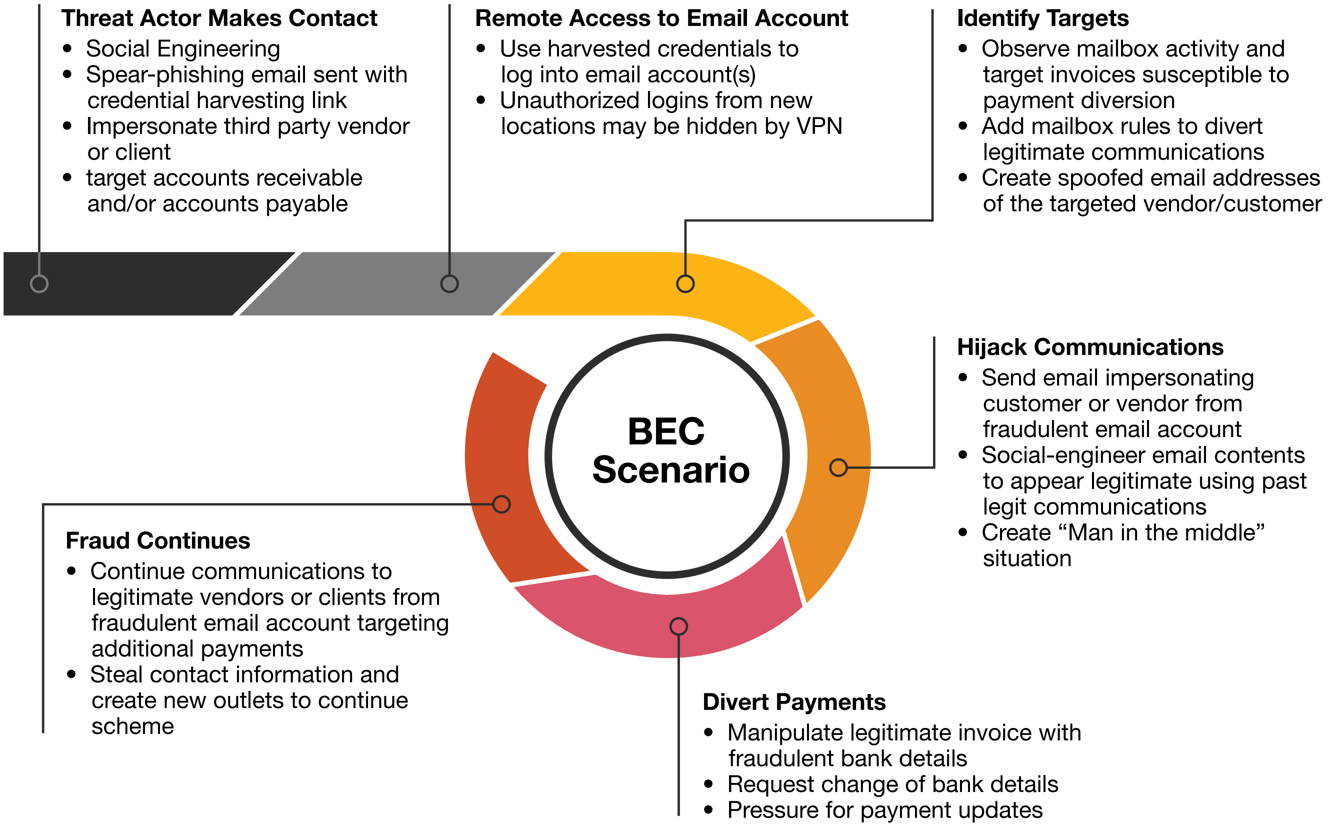
The antidote to cyber-enabled vendor fraud? A panoramic view of risk management that integrates cyber and financial controls.

# Discover: How cybercrime drives vendor fraud

Vendor fraud is a method of payment fraud. Here the scammer gains access or knowledge of the victim's accounts payable or accounts receivable and impersonates a trusted source or otherwise hijacks communications between the payee and payor. What differentiates cyber-enabled vendor fraud from similar crimes is the perpetrator's use of technology to expedite and simplify these acts. Today, one of the most common techniques used by cyber criminals to execute cyber-enabled vendor fraud schemes is business email compromise (BEC).

**Business email compromise** doesn't always lead to vendor fraud, but cyber-enabled vendor fraud frequently starts with business email compromise. BEC schemes typically involve the use of social engineering techniques to trick targets into divulging sensitive information such as login credentials that can be used to execute any number of fraudulent activities, including payment diversion and account takeovers, or into initiating a fraudulent transaction themselves. At stake for the victims of these attacks are financial losses, increased legal liability and significant reputational damage with customers, clients and business partners.

## Typical BEC Scheme



**Threat Actor Makes Contact**
- Social Engineering
- Spear-phishing email sent with credential harvesting link
- Impersonate third party vendor or client
- target accounts receivable and/or accounts payable

**Remote Access to Email Account**
- Use harvested credentials to log into email account(s)
- Unauthorized logins from new locations may be hidden by VPN

**Identify Targets**
- Observe mailbox activity and target invoices susceptible to payment diversion
- Add mailbox rules to divert legitimate communications
- Create spoofed email addresses of the targeted vendor/customer

**Hijack Communications**
- Send email impersonating customer or vendor from fraudulent email account
- Social-engineer email contents to appear legitimate using past legit communications
- Create "Man in the middle" situation

**Divert Payments**
- Manipulate legitimate invoice with fraudulent bank details
- Request change of bank details
- Pressure for payment updates

**Fraud Continues**
- Continue communications to legitimate vendors or clients from fraudulent email account targeting additional payments
- Steal contact information and create new outlets to continue scheme

# Do now: Address increasing risk in these four areas

To help prevent cyber-enabled vendor fraud schemes, we recommend focusing your risk management efforts on four key areas.

## The procurement process

A closer examination of your procurement process and all of its steps can help your organization identify the risks, threats and vulnerabilities embedded in each. Pay particular attention to steps where the potential for vendor fraud is particularly high and how both internal and external threat actors might take advantage of any weak points.

From purchase requisition to requisition review, the solicitation process to evaluation and contract, to order management, invoice approvals and disputes, and record keeping — each step could have vulnerabilities where vendor fraud is most likely to occur. Conduct comprehensive cyber and fraud risk assessment to identify, analyze, evaluate and compare the resulting risks so they can be prioritized for mitigation. And don't neglect to document the results so that they can be used to inform decision-making as well as any future risk assessments.

## The vendor master

The vendor master is a repository containing sensitive data such as payment details, bank account information, authorized payee details and the like. The dynamic nature of this repository — and the failure of many organizations to build adequate controls around it — makes it possible for criminals to circumvent outgoing payment controls. Any time a new vendor is onboarded, an existing vendor's bank information changes, a business rebrands or relocates, or a merger or acquisition occurs, the vendor master must be updated and those changes validated by trusted sources.

Even with adequate outgoing payment controls in place, if the controls around the vendor master are weak it significantly reduces the effectiveness of those preventative measures. We suggest you conduct a fraud risk assessment that includes processes and controls around the vendor master, the data it holds and how it's being managed with the following questions in mind: Who has access to the vendor master? Who can make changes and what changes can they make? How are we verifying the legitimacy of changes? What other controls are in place to reduce error or deter the manipulation of data?

## Payment points

During the vendor master assessment, you should also evaluate your payment processing methods within the vendor master to make sure that they're compliant with your internal policies and procedures. Even the most well-managed vendor master can be rendered defenseless if it allows for manual payments or information overrides. To avoid these types of scenarios, we recommend that all payments be initiated through the systematic process for payments, which includes linking to the vendor master. Processes allowing for initiation of payments to payees outside of the vendor master and with overrides of the vendor master file should be eliminated.

That said, many organizations simply aren't aware of all the ways in which their employees can initiate payments to vendors during the procurement process. By identifying payment initiation points, your company can reduce payment complexity, gain visibility into the vendor risk landscape and better understand the current status of its internal controls. Pinpointing where and how payments are taking place can help you evaluate the efficacy of your policies, procedures, controls and technical safeguards against the reality of the process itself, and then make the necessary adjustments. Corporates should maintain an inventory of all outbound payment processes. Too often legacy payment processes, exceptions processes, system access rights and processes associated with acquisitions are not adequately documented or controlled, and that can lead to fraud.

## Employees

While no organization wants to admit that its employees are capable of fraud, they're often involved in corporate payments fraud — intentionally or not. Many remote workers are vulnerable targets for schemes involving BEC, but in some cases they may be the ones responsible for perpetrating fraud. Remote work increases risks of ghost vendors or malicious diversion of payments. In fact, over the last two years, many organizations have seen an increase in financial crimes — some by as much as 26 percent — resulting from collusion between internal and external actors.

To monitor, detect and prevent these types of schemes, businesses should modernize their controls while also providing training to employees. Employees are much more likely to comply if they understand not only the *how* behind a particular control but also the *why*. Incorporating fraud training into security awareness programs can help your organization build technological literacy, enforce compliance and reduce employee negligence and ignorance.

In addition to training on modern fraud schemes and their techniques such as BEC, social engineering and phishing, organizations should adopt a multi-competency approach that successfully fuses finance and cybersecurity controls. A few simple cybersecurity controls such as implementing multi-factor authentication (MFA) on cloud email platforms; enabling anti-phishing, domain spoofing and malicious email identification capabilities; and regular review of access rights and permissions to financial platforms can be a great place to start.

# Do next: Update your controls playbook to better detect and prevent vendor fraud

Successfully preventing and responding to cyber-enabled vendor fraud requires an approach to risk management that fuses cybersecurity and finance controls that enhance data analytics and facilitate more open communication across departments.

## Modernize controls and conduct periodic assessments to evaluate them

As your company examines its anti-fraud controls and evaluates their effectiveness, you should prioritize areas where those controls are regularly touched by employees, vendors or other stakeholders. These are usually the areas where controls are the weakest and new solutions are needed the most. Regularly testing whether controls are successfully preventing or at least detecting vendor fraud can also help your company gain valuable insight into its overall risk management.

### Use tools and technology

Preventing cyber-enabled vendor fraud is an excellent objective, but it isn't always possible. When an incident does occur, your organization will need to make sure that it has the right tools and technology in place to respond. Sophisticated modern attacks call for sophisticated modern solutions, and cyber-enabled vendor fraud is no exception.

To automate the operation and testing of controls, consider moving to a technology platform such as Enterprise Control that can continuously monitor and help detect trending fraud schemes and sharpen fraud investigations to identify root causes as well as financial risk and exposure. Using Enterprise Control, companies can also conduct periodic fraud control assessments, freeing internal teams from the tedious processes of fraud risk management.

### Implement verification and validation processes

For additional protection, consider implementing controls around verification and validation. These processes generally require an employee to check the legitimacy of any requests for changes to existing data directly with the vendor — typically via a phone call. To reduce the burden of manual verification, consider automated validation processes. These can include comparing vendor information against publicly available databases and resources such as the IRS TIN Matching program and the European Commission's VIES VAT number validation, as well as paid external services that verify bank account details and validate and identify phone numbers, email addresses and other contact information.

Risk Detect from PwC is one automated solution used to match vendor information to these sources and manage the exception handling workflow. Securely automating verification and validation processes not only helps save time but also reduces the likelihood of cyber-enabled vendor fraud due to human error.

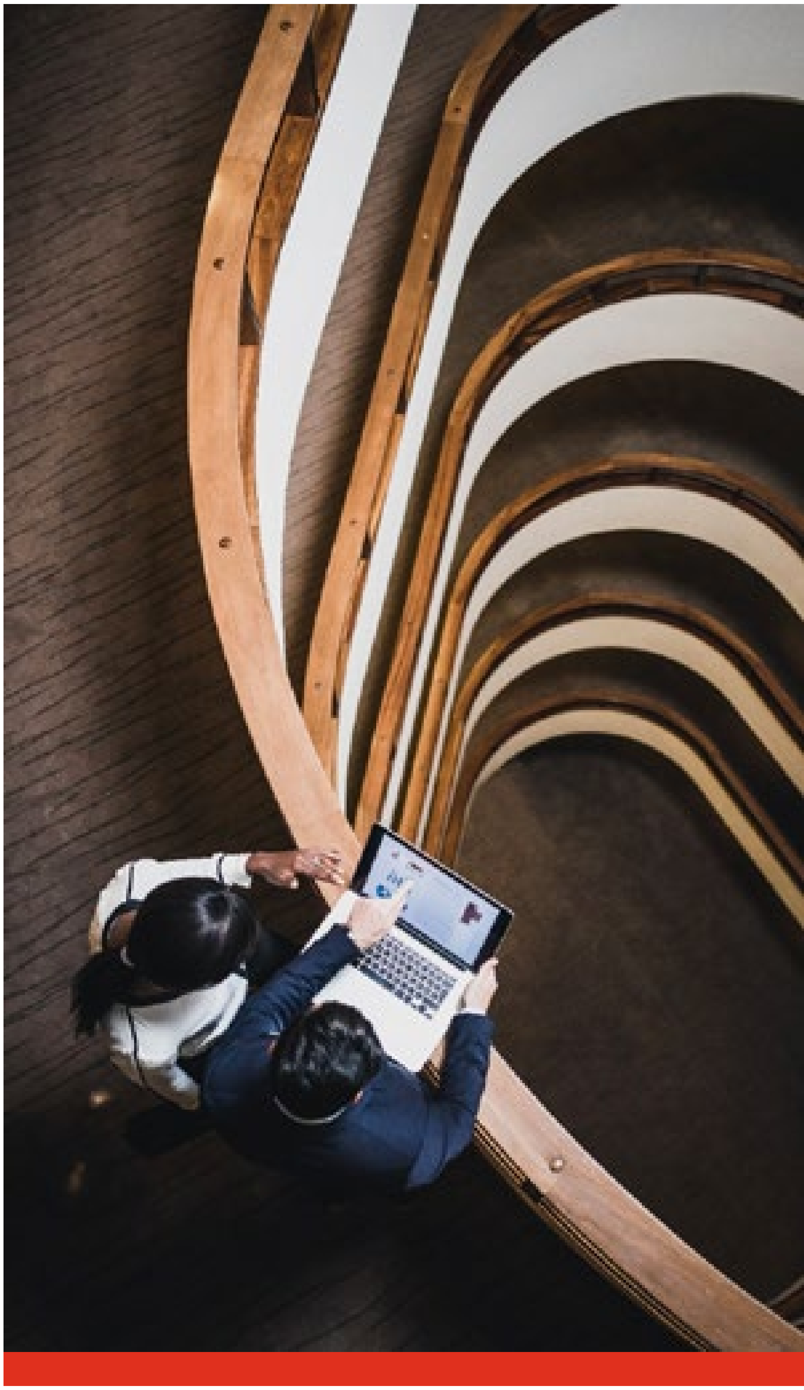
## Make use of data analytics for a more comprehensive view

Fraud risk management processes can generate huge amounts of data, and it can get overwhelming in no time. That's a challenge for risk professionals who must explain their priorities and decisions to management and other internal stakeholders.

Automated tools designed to help mitigate risk and compliance can help here. Risk Detect, for example, uncovers hidden patterns that can help your organization detect fraud, misuse, errors and noncompliant transactions, providing a 360-degree view of risks. Using such solutions can help businesses spot errors and patterns across channels and pinpoint the employees, vendors and transactions that pose financial, cybersecurity and compliance risk.

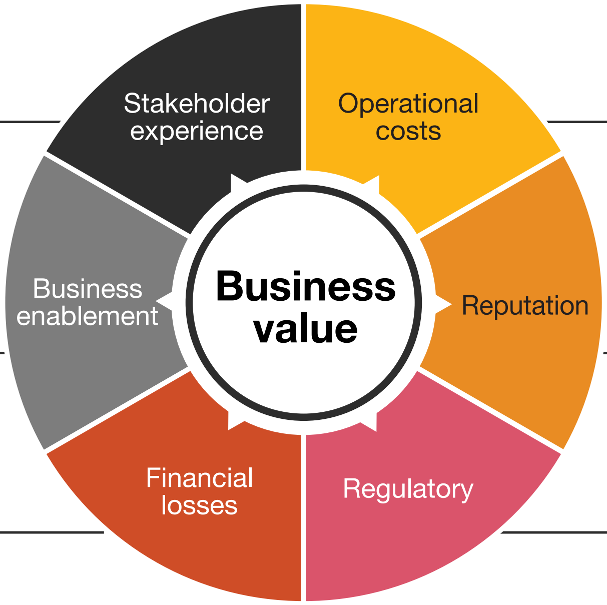
## Update fraud management with a panoramic approach

Cyber threats and fraud are often handled by separate departments that don't always work together or communicate about risk — and today's criminals know it. As cyber-enabled vendor fraud becomes more sophisticated, organizations should adopt a unified approach that successfully fuses cyber and finance controls. They should simultaneously facilitate open communication between cybersecurity and finance teams so they have a clear understanding of how these controls will impact each other. Taking this panoramic view, your company might find that it needs to refresh its fraud management program framework to organize teams differently, align roles and develop better playbooks and technology strategies.



## Bottom-line: The ROI from better fraud risk management

Companies can pursue digitization with confidence by updating their controls playbook and improving overall fraud risk management. The payoffs can be measurable, both for the organization and its stakeholders. Growth-minded fraud risk management can accomplish several goals, including minimizing losses and business disruption as well as improving compliance efficiency and enabling business growth.



Minimize inconvenience to stakeholders such as vendors, employees, business partners and customers (e.g., reduce customer abandonment and churn rate)

Enable the business to achieve growth goals by finding solutions to risk problems; have scalable controls; minimize business disruptions

Minimize real hard-dollar fraud losses

Maximize efficiency of anti-fraud controls and operations; minimize total operational cost of fraud controls

Maximize reliability and trust with direct and indirect stakeholders; minimize mistrust, which will hurt the brand

Increase effectiveness of regulatory compliance program; minimize regulatory penalty

# Contact us

**Ryan Murphy**
Partner, US Investigations & Forensics Leader
PwC United States
ryan.d.murphy@pwc.com

**Claudia Nestler**
Partner, Forensic Services Leader
PwC Germany
claudia.nestler@pwc.com

**Grant Waterfall**
Partner, Cyber Security & Privacy Leader
PwC Germany
grant.waterfall@pwc.com

pwc.com