Security Matters

A BUSINESS CYBERSECURITY GUIDE

Fall 2020

The Top Business Threat Is Cybercrime. Are You Fully Protected?

Small and midsized businesses are prime targets for cybercrime. The 2020 AFP Payments Fraud and Control Survey reports that payments fraud activity continues at a near-record levels.

> "THE STUDY SIGNALS THAT ORGANIZATIONS CANNOT BE COMPLACENT ABOUT THE THREATS OF PAYMENTS FRAUD AND THEY SHOULD MAKE IT AS DIFFICULT AS POSSIBLE FOR CYBERCRIMINALS TO SUCCEED IN THEIR ATTACKS."
>
> *2020 AFP Payments Fraud and Control Survey*

Strategic Treasurer found that most corporations still view cyberfraud as a significant threat. Three points were clear:

- Focus is on security controls and policies
- Fraudulent activity continues; losses are steady
- Security controls are better; more work is needed

The key is adopting a different viewpoint about cybersecurity. Traditionally, many executives viewed cyber-risks as a technology issue, but they are more than that. Cybersecurity is a significant business problem to be addressed. Your focus should not be solely tech related; the real question is, how will you protect your entire organization from cybercrime?

CYBERCRIME METRICS	
$1.7B	In losses to business email compromise in 2019
81%	of organizations were targets for payments fraud in 2019
Top Targets	74% had check fraud; 40% were subject to wire fraud
33%	of organizations had ACH debit fraud
61%	experienced CEO fraud on business email compromise attacks

Sources:
FBI: Internet Crime Report 2019
AFP 2020 Payments Fraud and Control Survey Report

Fraud Defense: How to Reduce Risk

So how do you prevent your businesses from becoming a cybercrime statistic? You need a comprehensive approach, because cybercriminals are threatening your businesses from several different angles. Organizations need fraud protection that balances people and process with strong internal controls.

To do that, you need a multipart approach to become more cyber-resistant.

1. Defend your business
2. Secure your process
3. Educate your staff
4. Protect your banking assets

Tips for making your process more secure	Why you need protection
Control access points. Use separate, dedicated computers for banking functions.	
• One computer for online banking access • One computer for ACH payments or wire transfers	*Fewer people using these machines cuts down on the risk of bad links and attachments compromising them.*
Two heads are better than one. Institute dual authorization for payments.	
• Wire transfers • ACH transactions • Checks over a specific amount • Company card purchases over a specific amount	*Dual authorization encourages companies to scrutinize requests. This way, businesses aren't vulnerable because of a single mistake.*
Verify everything. All requests for information changes and/or unusual payments must be verified before acting.	
• Never rely on email instructions alone to authorize a wire or ACH transfer, even if the email comes from company leadership	*Criminals can hack or spoof executives' email addresses and instruct you to send money to the cybercriminal's bank account.*
• Ensure that all payment requests from out-of-office executives require approval from other executives. Do not allow "rush" or confidential requests to override the company procedures.	*By sending a message from someone who's away, criminals are betting you won't verify the request's legitimacy.*
• Ensure that all vendor payment address changes (including internal changes) must be verified independently with the vendor	*All it takes is one compromised email account to figure out who your company's vendors are. Criminals can then send fake invoices, hoping victims pay them.*
• Verify all email requests from employees for a change to their direct deposit of payroll instructions	*If an HR person is duped into sending the funds to the fraudster's account, then the crook ends up with the paycheck.*

Defend Your Business

Improved security starts with the executive/owner's commitment to protecting the company. Rick Mills, the CFO of Headsets.com, warns, "Until your company has been hit by an attack, you probably think you're more protected than you are." Reviewing your payment procedures is an effective way to address cyberfraud protection. Studies have found that weak internal controls were responsible for half of all fraud losses.

Secure Your Process

Companies' payment processes are favorite targets of cyberthieves because they allow criminals to steal funds before victims even know the money is gone. The weakness cybercriminals are exploiting is the emphasis on speed in today's corporate environments. To combat this, it's helpful to rethink the acronym ASAP. Rather than focusing on doing things "as soon as possible," make sure any staff members who handle payments are working "as securely as possible."

Let employees know that it's OK to ask questions or double-check information before releasing payments. In short: **Verify, review, release.**

Educate Your Staff

While antivirus software, spam filters and firewalls are getting better, the best tools any company has in fighting cybercrime are its own employees. The human element in cybersecurity cannot be overstated. Empower your employees to identify and report possible cybersecurity threats.

> "IT IS CRITICAL TO RECOGNIZE THAT THE MOST COMMON TARGET AND MOST VULNERABLE PART OF YOUR BUSINESS IS YOUR EMPLOYEES, CUSTOMERS AND PARTNERS—THE HUMANS THAT MAKE DECISIONS EVERY DAY."
>
> *Agari Data, Inc.*

An Employee Firewall Means That Employees:

- Secure their workspaces
  - Know where their devices (mobile phones, laptops, computers, etc.) are so they can secure them against unauthorized access
- Protect company data
  - Keep company and client data secure so it's not accessible by the wrong people
- Have a cybersmart mindset
  - Avoid phishing and social media scams to protect data, payments and accounts
  - Delete emails of unknown origination
  - Know the signs of a hijacked online banking session, such as a sudden loss of connection immediately after entering login credentials
  - Don't share user IDs/passwords/online credentials
  - **Know that banks (including Hancock Whitney) won't solicit confidential client information by email, telephone or text**
- Use complex passwords
  - Strong passwords use 8-10 characters with letters, numbers and symbols
  - Don't use the same password for multiple sites
  - Never save user IDs or passwords to the system
  - Don't use the same password for personal and business login credentials

What makes cybercrime such a threat is this: Almost every method cybercriminals use to target your company requires someone taking an action most people don't think twice about. Opening emails, visiting websites, clicking on email attachments and responding to payment requests—these normally routine tasks can open the door to fraud and loss if prompted by clever cybercriminals. Your employees are your first and often best line of defense against cybercrime.

Because your company's systems likely require usernames and passwords, credential theft (stealing those usernames and passwords) is one type of cybercrime that should be top of mind for your staff. With key employees' credentials, criminals can log in and open the door for serious and costly cybercrimes. In fact, Microsoft found that 63% of all network intrusions and data breaches were due to compromised user credentials.

Protect Your Banking Assets

After committing to defending your business, securing your process and educating employees, it's time to work with your bank to protect your assets. Hancock Whitney offers various ways to add control as well as additional layers of security so you can identify and prevent fraudulent transactions.

HOW YOUR BANK CAN HELP KEEP YOUR BUSINESS SAFE

Commercial Online Banking

Conveniently keep a watchful eye on your business's finances, even when you're on the go.

- View current-day ACH, wire and teller transactions
- Review prior-day transactions, balances and deposits
- Manage accounts with daily reports, alerts and statements
- Mobile and tablet banking for wire and ACH approvals
- Dual administration adds transparency and control because a second administrator approves any changes

Paper-Based Transactions

Good recordkeeping helps ensure that nothing slips by you.

- Positive Pay provides daily monitoring of check activity and the ability to return a fraudulent item

ACH and Wire Transactions

Your business can be smarter now that money changes hands faster than ever.

- ACH Positive Pay offers a daily review of all ACH debits that are scheduled to post to an account; you decide to pay or return each one
- ACH Block lets you block all ACH transactions on an account
- Unique account identifiers use a special code to replace your bank account number for security. This feature works with ACH credits (ACH UPIC) or incoming wires (SafeWire).
- All ACH originations and outgoing wire transfers require security tokens and dual authorization to initiate and approve a transaction

IBM® Trusteer Rapport Security Software

This online security tool is free for Treasury Services clients. It protects you in ways firewalls and antivirus software can't— it blocks malware, key-logging and man-in-the-middle attacks. Trusteer Rapport also identifies potential phishing sites and notifies you about online threats. The connection between your computer and the website you're visiting is locked, and you are protected.

The Best Cyberdefense Layers Security Controls

Strategic Treasurer says the best method of defense is to employ multiple layers of security and internal controls, not just focus on one or two areas. Consider these principles for your defense:

1: Segregate duties
2: Protect/encrypt sensitive data
3: Use multifactor authentication
4: Use principle of least privilege
5: Reconcile bank accounts daily

Conclusion

THE BEST CYBERDEFENSE IS A GOOD OFFENSE

By adopting a strong stance on cybersecurity now, you can stay a step ahead of cybercriminals. Building up your cybersecurity helps protect your business and maintain the trust of those you count on most: your employees, partners and customers. In our increasingly digital world, this trust may just be one of your company's most valuable assets.

For more information on how to protect your business from cybercrime, please contact a Treasury Services representative.

FRAUD DEFENSE
COVER ALL YOUR BASES

- Defend Your Business
- Secure Your Process
- Educate Your Staff
- Protect Your Banking Assets

Sources:
AFP: 2020 Payments Fraud and Control Survey Report
Strategic Treasurer, 2019 Treasury Fraud & Controls Survey
The Human Factor Study – ProofPoint
Krebs on Security, Issue #20 Cyber-Hackers: Waging War Against An Invisible Enemy
Harvard Business Review Podcast – Why Cybersecurity Isn't Only a Tech Problem
CFO Magazine Turning the Tables on Attackers Whitepaper, Agari

10/20