



BLACK BOTTLE IT™



A Cybersecurity Webinar

When the Old Way of Keeping your Employee Data
Secure Doesn't Work Any Longer



Agenda

- Part 1 -- Who is Black Bottle IT: A Breach Story
- Part 2 -- Current Cyber Attack Trends
- Part 3 -- Assessing Cyber Risk
- Part 4 -- Mitigating Risk



- It's ALL ABOUT Analyzing & RESPONDING to Risk!
- We secure endpoints for our clients, **BUT more importantly, we are working to educate business owners/leaders on cyber risk.**
- We lead with Cybersecurity Consulting -- as every environment is different.
- Cybersecurity is what we are all trained and experienced to do.

Tech Talk:

- We offer a Breach Hotline.
- Our solution delivers 24x7 security monitoring with a LIVE person
- We help clients implement and test incident response plans



Bridget Escobar
CTR
President



Doug Emmereth
CTR
Director of Technology



John Hensberger
Black Bottle IT
President

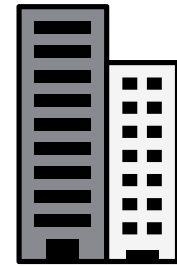


Marc Malloy
Black Bottle IT
Cybersecurity Advisor

Presenting

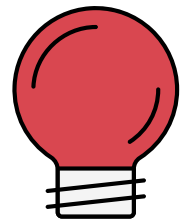
A Breach Story

Scenerio



- Traditional Security Tools
 - Anti Virus/Malware
 - Updated Firewall
 - Annual Security Training
 - Backups
- Outsourced IT Third-Party Managed Service Provider
- Cyber Insurance policy in place
- Experienced a data breach

Key Takeaways



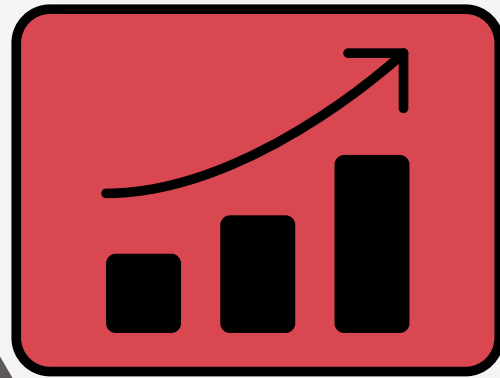
- Traditional security tools were insufficient
- No good plan to respond to an incident
- Managed Service Provider was little help in preventing or responding
- Many third parties wanted to assist in recovery and response, challenging to decide which services were needed.
- No internal process for filing a claim with cyber insurance

Part 2

Current Cyber Attack Trends



Data Doesn't Lie



Phishing Attacks

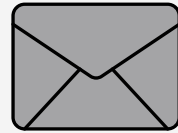
More than 255 million **phishing** attacks occurred over six months in 2022, a 61% increase in the rate of **phishing** attacks compared to 2021

Largest 2022 Data Breach

Acorn Financial Services (August 2022)

An Acorn **employee was likely targeted via phishing**, and their email credentials were stolen. Once attackers had access to the employee's email account, they accessed internal information contained in the email account. Attackers stole names, addresses, dates of birth, driver's license numbers, financial account numbers, Social Security numbers, and other client account-related information. Acorn launched a full investigation and sent a breach notification to their impacted customers. Acorn could have further mitigated exposure should they have implemented a phishing detection and takedown service before their employee fell victim to the phishing attack.

More Data Points



A ransomware attack occurs every 2 seconds

Data breaches, ransomware attacks, phishing scams, are showing NO SIGN OF SLOWING DOWN

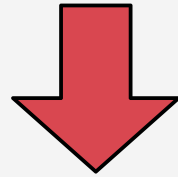


Ransomware accounts for 10% of all breaches

Phishing, remote desk protocol (RDP) exploitation and software vulnerabilities are the principal root causes of ransomware infections

More Data Points

Just 17% of small businesses have cyber insurance.



46% of all cyber breaches impact businesses with fewer than 1,000 employees



75% of SMBs could not continue operating if they were hit with ransomware

Part 3

Assessing Cyber Risk



Remote Work

42% of small businesses have revised their cybersecurity plan since the COVID-19 pandemic.

How COVID-19 dramatically increased remote work cybersecurity risks

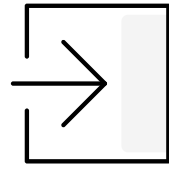
Has Your Business?

Source: strongdm.com

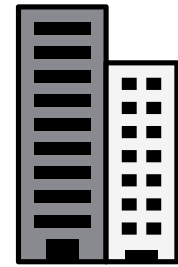
The infographic consists of four vertical panels, each representing a cybersecurity risk. Each panel features a stylized illustration of a person's head and shoulders within a window frame, accompanied by icons of speech bubbles, gears, and a virus. The text below each illustration describes the risk.

- Expanded attack surface due to added devices and connections, many not optimized for security**
- Massive increase in targets and target locations due to company data in employee homes**
- Reduced or diverted cybersecurity budget and resources due to negative impacts on the business**
- Criminogenic climate of fear, uncertainty and doubt due to threatened livelihoods, health risks, rapidly changing regulations**

Analyzing Risk:



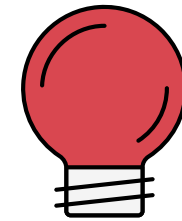
What are cyber risks?



- Sensitive Data
- Employee Risk
- Vendors Risk
- Computer Infrastructure Risk



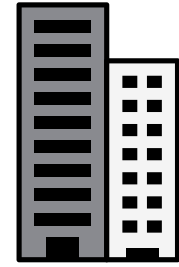
Defining what needs protected:



- Determine what sensitive data resides in your IT Systems
- Determine where sensitive data is stored and who has access
- Analyze critical third-party vendors that have access to client data
- Evaluate employee cyber security awareness

Examples of risky data

Types of Data



- **Employee Data**
 - Social Security Numbers
 - Bank Account
 - Health Care information
- **Client Data**
 - Account numbers
 - Sensitive information owned by Client
 - Credit Card/Bank Account
- **Protected Information**
 - Industry specific proprietary information
 - Controlled Unclassified Information

How to calculate my risk

Methods:

- Impact Rating Scale
- IT Assessment
- Assessment against a compliance standard
- Phishing Simulation
- Vulnerability Scans
- Penetration Tests
- Assess cyber security maturing of third-party vendors
- Incident response fire drill

Examples

Impact Rating Scale

IMPACT RATING SCALE					
Area	Rank				
	1 - Insignificant	2 - Low	3 - Moderate	4 - High	5 - Critical
Confidentiality: Disclosure of sensitive information to unauthorized individuals or systems	Loss of confidentiality would NOT expose Sensitive or Non-Sensitive customer information	Loss of confidentiality could potentially expose limited <u>Non-Sensitive</u> customer information	Loss of confidentiality could potentially expose very limited Sensitive Company, <u>customer</u> or team member information	Loss of confidentiality could potentially expose some Sensitive Company, <u>customer</u> or team member information	Loss of confidentiality could potentially expose significant Sensitive customer, <u>Company</u> or team member information
	No customers impacted	Small number of customers impacted ' 100 to 1,000	Moderate number of customers impacted ' 1,000 to 10,000	Large volume ' 10,000 to 100,000 customers	High volume ' over 100,000 customers
	No customer or regulatory notification required	Some notification to impacted customers and/or regulators; no regulatory fines/penalties imposed	Notification to impacted customers and regulators required; remediation of customer accounts; minimal regulatory fines/penalties imposed	Notification or disclosure required to Board or agencies; Some regulatory fines/penalties imposed	Notification to regulators, customers, Board and/or agencies (SEC)); Significant regulatory fines imposed (up to \$7,500/record)
	No litigation	Litigation is unlikely	Litigation is likely	Protracted litigation is likely	Severe or protracted litigation is highly likely

Vendor Questionnaire



Cyber Questionnaire

Company Name

Date Completed

1. Is cyber security discussed at a management / board level?

Yes
 No

2. Do you currently have cyber insurance? If yes, please provide proof of coverage.

Yes
 No

3. Do you have a process to audit 3rd parties for their cybersecurity resilience before sharing confidential information?

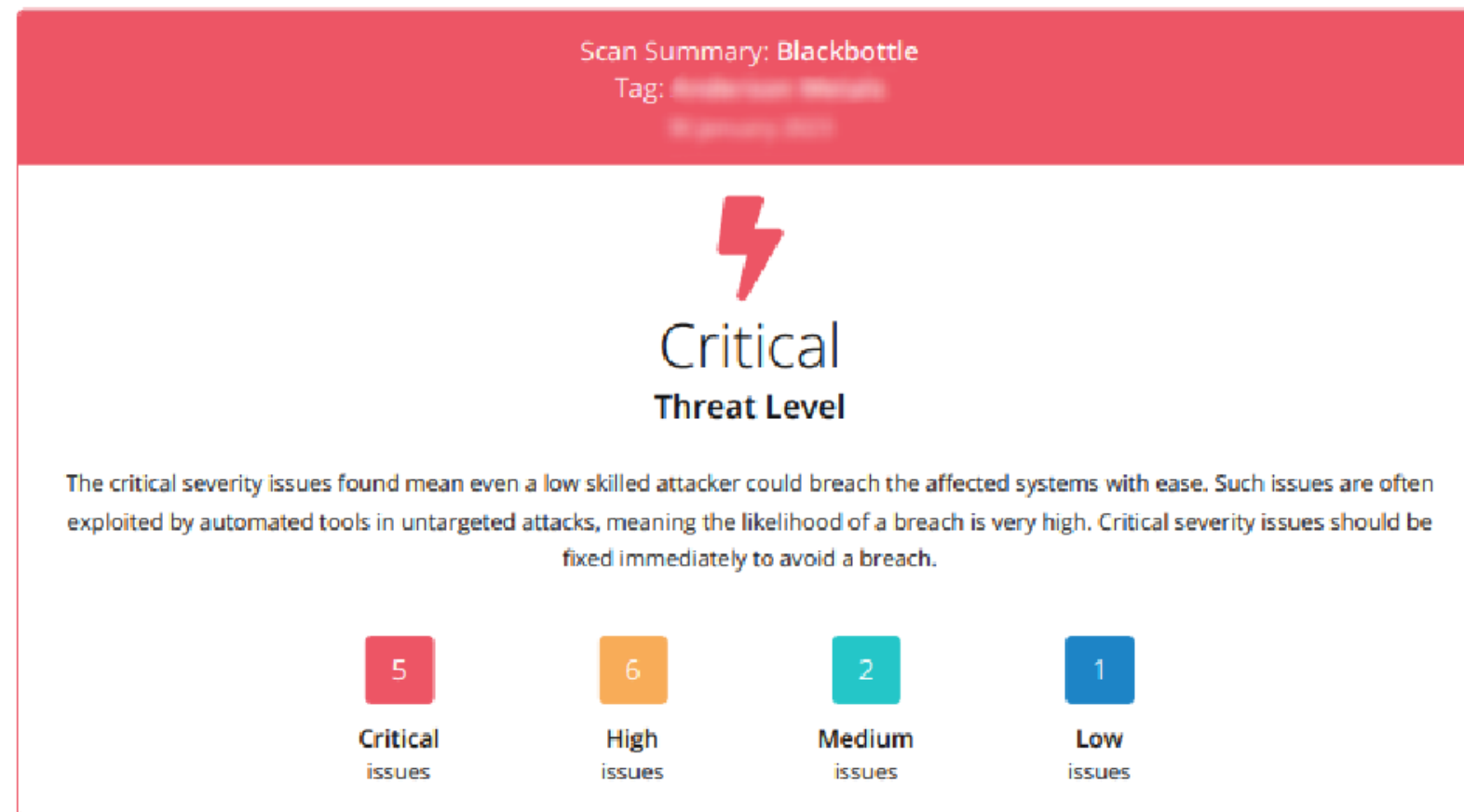
Yes
 No

4. Do you have encryption enabled on all devices and a policy to ensure that all new devices have encryption enabled by default?

Yes
 No

More Examples

External Vulnerability Scan Findings



Compliance Framework (NIST)

NIST 800-171 Check List		
	3.1	Access Control
<input type="checkbox"/>	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
<input type="checkbox"/>	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.
<input type="checkbox"/>	3.1.3	Control the flow of CUI in accordance with approved authorizations.
<input type="checkbox"/>	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
<input type="checkbox"/>	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
<input type="checkbox"/>	3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.
<input type="checkbox"/>	3.1.7:	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
<input type="checkbox"/>	3.1.8:	Limit unsuccessful logon attempts.
<input type="checkbox"/>	3.1.9:	Provide privacy and security notices consistent with applicable CUI rules.
<input type="checkbox"/>	3.1.10:	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
<input type="checkbox"/>	3.1.11:	Terminate (automatically) a user session after a defined condition.
<input type="checkbox"/>	3.1.12:	Monitor and control remote access sessions.
<input type="checkbox"/>	3.1.13:	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
<input type="checkbox"/>	3.1.14:	Route remote access via managed access control points.
<input type="checkbox"/>	3.1.15:	Authorize remote execution of privileged commands and remote access to security-relevant information.
<input type="checkbox"/>	3.1.16:	Authorize wireless access prior to allowing such connections.
<input type="checkbox"/>	3.1.17:	Protect wireless access using authentication and encryption.
<input type="checkbox"/>	3.1.18:	Control connection of mobile devices.
<input type="checkbox"/>	3.1.19:	Encrypt CUI on mobile devices and mobile computing platforms.
<input type="checkbox"/>	3.1.20:	Verify and control/limit connections to and use of external systems.
<input type="checkbox"/>	3.1.21:	Limit use of portable storage devices on external systems.
<input type="checkbox"/>	3.1.22:	Control CUI posted or processed on publicly accessible systems.

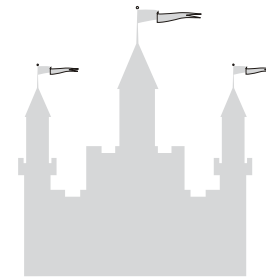
Part 4

Risk Mitigation

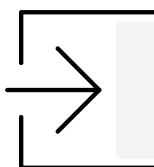
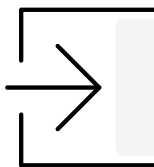
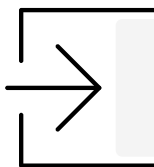
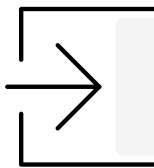


Out with the Old in with the New

Traditional Security Tools



- Anti virus/malware to prevent all known threats
- Firewall - used for blocking traffic going in/out against all known threats
- Annual Security Awareness Training
- Quarterly external vulnerability scanners



Modern Security Tools



- Endpoint Detection & Response - with real-time monitoring of alerts
- Multi-factor Authentication + Password Policy & Procedures
- Next-Generation Firewall - that is tied to real-time threat intelligence to guard against latest attacks
- Monthly Vulnerability Scans

It's more than just tools...

Expertise

- Acting on alerts from security tools
- Understanding the latest attack trends
- In-house vs. third-party outsource

Preparedness

- Incident Response Plan
- Employee Training

Strategy

- Backups
- Cloud vs. On-Premise Assets
- Choosing the Right Vendor



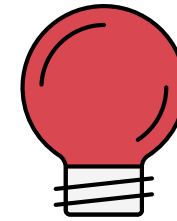
Reduce Third-party Risk

Top 3 Things to Know BEFORE Partnering with Vendors

1. Does YOUR BUSINESS have a PROCESS to audit third-party vendors for their cybersecurity resilience before sharing confidential information?
2. VERIFY that your third parties have implemented strong third-party risk cybersecurity monitoring and plans.
3. DEFINE cybersecurity risk expectations and requirements with your vendors.

By understanding third-party security policies and procedures, you can take corrective steps to address the risks to your data. Without the proper controls, your vendors and contractors can become the weakest link to your organization and customers' privacy.

CTR Security



- Annual SOC Compliance Audit
- Hosted on Microsoft Azure
- Daily redundancy and backups
- Dual Factor Authentication
- Vendor Oversight Process
- Intrusion and End Point Detection
- Employee Education and Training

Proof of Annual SOC 1, Type 2 Compliance

Houdyshell & Associates, Inc.
100 North Sunset Lane • Raytown, Missouri 64133
CERTIFIED PUBLIC ACCOUNTANTS
Integrity • Objectivity • Personal Service

Independent Service Auditor's Report on CTR's Description of its Solved Payroll Processing System and the Suitability of the Design and Operating Effectiveness Management of CTR Employment Management Services, Inc.

We have examined CTR Employment Management Services, Inc. (CTR) CTR's description of its payroll processing system entitled "CTR's Description of its Solved Payroll Processing System" for processing user entities' transactions throughout the period July 1, 2021 to June 30, 2022 (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "CTR's Assertion" (assertion). The controls and control objectives included in the description are those that management of CTR believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the payroll processing system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of CTR's controls are suitably designed and operating effectively, along with related controls of the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

CTR uses a subservice organization to provide its payroll processing application and hosting service. The description includes only the control objectives and related controls of CTR and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by CTR can be achieved only if complementary subservice organization controls assumed in the design of CTR's controls are suitably designed and operating effectively, along with the related controls of CTR. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization's controls.

In section 4, CTR has provided an opinion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. CTR is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion,

The description fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period July 1, 2021 to June 30, 2022. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls of a service organization may not present, or detect, or correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls of a service organization may become ineffective.

The specific controls tested and the nature, timing, and results of those tests are listed in section 5c.

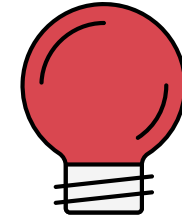
In our opinion, in all material respects, based on the criteria described in CTR's assertion—

- a. the description fairly presents the payroll processing system that was designed and implemented throughout the period July 1, 2021 to June 30, 2022.
- b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2021 to June 30, 2022 and subservice organizations and user entities applied the complementary controls assumed in the design of CTR's controls throughout the period July 1, 2021 to June 30, 2022.
- c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2021 to June 30, 2022 if complementary subservice organization and user entity controls assumed in the design of CTR's controls operated effectively throughout the period July 1, 2021 to June 30, 2022.

This report, including the description of tests of controls and results thereof in section 5c, is intended solely for the information and use of management of CTR, user entities of CTR's payroll processing system during some or all of the period July 1, 2021 to June 30, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to conduct it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Houdyshell & Associates, Inc.
Kansas City, Missouri
August 28, 2022

Cyber Fraud



Email spoofing

Bad Actor impersonates employee's email account

Bad Actor gains access to employee's email account

Then request changes to direct deposit account information.

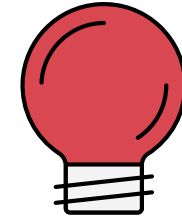
Unemployment Fraud

Fraudsters gain information on employee and file a claim on their behalf

User account is compromised

Sending unsecured Personal Identifiable Information

Fighting the Bad Guys



Your first line of defense:

- Use strong passwords
- Use Two-Factor Authentication (2FA)
- Change passwords frequently
- Do not share user logins
- Do not reuse passwords
- Make passwords unique to each web site or application
- Secure username and passwords
- No public wifi
- Restricting online access by location (IP address)

We are trying to deter unwanted access by making it harder for the bad guys to get in.....

Two-Factor Authentication (2FA) Example

We don't recognize the computer you're using

We'll need to confirm your identity before you can log in.

Click the link below and a temporary Authorization Code will be sent to the email address on file, or texted to the cell phone number on file, for this user.

Email: ####@ctrhcm.com

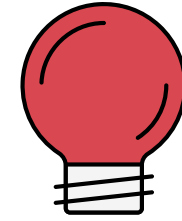
Text: ###-###-8245

[Get Authorization Code](#)

Why has this happened?

- You're using a new computer or one you haven't used before.
- The IP address is not recognized as one used by you in the past 30 days.

Fighting the Bad Guys




Google Docs - Access Request

SE support@office-email.com.au
To [redacted]

[If there are problems with how this message is displayed, click here to view it in a web browser.](#)
[Click here to download pictures.](#) To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Caution: This is an external email. Please take care when clicking links or opening attachments. When in doubt, contact BlackBottle.


 Google Docs would like to:

 Read, send, delete, and manage email 

 Manage your contacts 

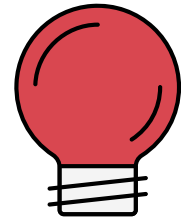
By clicking Allow, you allow this app Google to use your information in accordance with their respective [terms of service](#) and [privacy policies](#). You can change this and other [Account Permissions](#) at any time.

Deny 



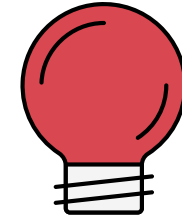
- Employee Training
- Test Phishing Campaigns
- Evaluate your performance

Fighting the Bad Guys



- Securely store all payroll reports and shred when not needed any longer.
- Provide a way for employees to send secure emails when including PII (Personal Identifiable Information) data.
- Recommend your employees use your payroll system's employee portal to make changes, especially direct deposit changes.
- If payroll department is making direct deposit changes, confirm changes over the phone not by email.
- Make it easy for your employees to report a cyber incident.
- If a cyber incident occurs notify your IT staff or IT Provider immediately.
- Notify CTR. We can assist you in determining the scope and assist you with resolving the issue.
- CTR begins the process of sending funds to our banks for ACH processing at 3:30 pm. CTR has a small window to get these funds back for you.

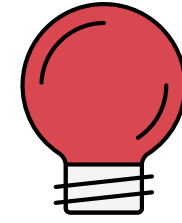
Fighting the Bad Guys



CTR has developed an internal process that looks at all ACH files for potential fraud.

- **Duplicate Employee Payments** - Reports employees that have the same direct deposit accounts.
- **Customer ACH Threshold** – Reports per pay amounts that are over the established CTR customer threshold.
- **Individual Threshold** – Reports employees that have been paid more than the configurable CTR Threshold.
- **Duplicate Direct Deposit Accounts** – Reports employees that have been paid to the same direct deposit account multiple times.
- **Suspect Routing Numbers** – Reports when an account is used that is on CTR Suspect Routing Number List and has surpassed our pre-defined threshold amount.

Bad Guys can come from Within



Payroll Fraud by Payroll / Supervisor Staff

- Ghost Employees
- Payment Redirection
- Pay Rate Alteration
- Misclassification of Workers

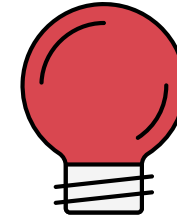
Look out for:

- Unusual bank activity
- Changes in employee's behavior
- Employee living beyond means
- Employee unwilling to take time off
- Employee unwilling to share or delegate duties

Deterring:

- Consider reference and background checks
- Split up processes so job task and responsibilities are handled by more than one employee
- Establish checks and balances
- Establish thresholds and approval processes
- Scrutinize your users access to the payroll system
- Regularly audit payrolls
- Review all notices
- Make it easy to report payroll fraud

Tips for Verifying Pay



- Preview your payroll
- Verify Employee count
- Verify totals on Payroll Register. (Do the hours and dollars look reasonable? Compare to previous payroll)
- Check all new hires. Reference New Employee and Change Audit Report
- Check the Exceptions Report
- Verify overtime and bonuses
- Verify tax amounts
- Check bank account changes.
- Check pay rate changes.
- Have more than one person verify the payroll. Keep everyone honest...

Client ID:	MME - Ann Moonshine Magic Inc	EXCEPTIONS	Ann Moonshine Magic Inc	Period Begin Date:	12/24/2022
Pay Group:	Bi-Weekly			Period End Date:	1/6/2023
Check Date:	1/11/2023			Pay Period:	1
Run Date:	1/13/2023	Run Number:	44	Payroll Type:	Regular Payroll

Exception Type	Exception Description
Missing Tax ID - Maryland	Tax ID is missing for the tax Maryland - EE W/H
Missing Tax ID - Nevada	Tax ID is missing for the tax Nevada - ER UI
Missing Tax ID - Nevada	Tax ID is missing for the tax Nevada - Modified Business
Invalid Tax ID - New Jersey	Tax ID APPLIED FOR does not match a valid EIN format for tax agency New Jersey - EE W/H
Missing Tax ID - New York	Tax ID is missing for the tax New York - ER UI
Missing Tax ID - New York	Tax ID is missing for the tax NY- MCTMT
Missing Tax ID - Ohio	Tax ID is missing for the tax OH- Akron
Missing Tax ID - Ohio	Tax ID is missing for the tax OH- RITA
Missing Tax ID - Ohio	Tax ID is missing for the tax Ohio - School District
Missing Tax ID - Oregon	Tax ID is missing for the tax Oregon - UICNTY
Missing Tax ID - Oregon	Tax ID is missing for the tax OR- Statewide Transit Tax
Missing Tax ID - Pennsylvania	Tax ID is missing for the tax PA- Findlay TWP, Allegheny W/H
Missing Tax ID - Pennsylvania	Tax ID is missing for the tax PA- Findlay TWP, Allegheny LST
Missing Tax ID - Pennsylvania	Tax ID is missing for the tax PA- Franklin Park BORO, Allegheny W/H
Missing Tax ID - Pennsylvania	Tax ID is missing for the tax PA- Greensburg City (Greensburg Salem SD), Westmoreland W/H
Missing Tax ID - Pennsylvania	Tax ID is missing for the tax PA- Greensburg City (Greensburg Salem SD), Westmoreland LST
Missing Tax ID - Pennsylvania	Tax ID is missing for the tax PA- Sharpsburg BORO, Allegheny W/H
Missing Tax ID - Pennsylvania	Tax ID is missing for the tax PA- Sharpsburg BORO, Allegheny LST
Missing Tax ID - Pennsylvania	Tax ID is missing for the tax Pennsylvania - EE W/H
Missing Tax ID - Pennsylvania	Tax ID is missing for the tax Pennsylvania - ER UI

New Hires NOT Included in New Hire File (Include in New Hire Report not selected):					
Location	Department	Employee ID	Name	Hire Date	Status
03	90	1019	Lester Butterman	12/12/2022	Active

Deductions & Garnishments not taken due to insufficient net pay:							
Location	Department	Employee ID	Name	Type	Title	Calculated	Taken
02	90	1015	Richard L Barnes	Pre-Tax DED	401k	150.00	.00
		1025	James bolyog	Pre-Tax DED	Medical Pre-tax	100.00	.00

* Variance is due to Tips and/or GTL.

solved EXCEPTIONS Page 1
Created on: 1/13/2023 12:05:57 PM



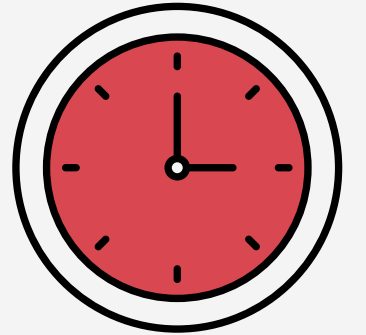
Thank You!

Feel free to reach out today or in the near future

Scan for Free Gap Analysis



Schedule Time with Us



Marc Malloy

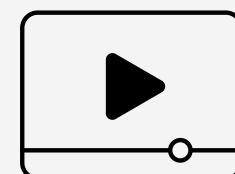
412-335-0477

marc.malloy@blackbottle.io

John Hensberger

412-303-1339

John.hensberger@blackbottle.io



blackbottleit.com

