EVOLVE
An HCM Growth Summit

Payroll and Security

2024 Asure Reseller Partner Conference

Presented by Joshua Gohman, CISSP

Asure

Speaker Introduction

Joshua Gohman, CISSP

VP, Information Security

Over 20yrs IT, Cybersecurity, and Risk Management experience beginning in the US Army and continued in civilian career leading security consulting teams conducting technical security assessments, security and compliance audits, and security program implementations for companies of all sizes from startups to Fortune 500 companies.

Joined Asure in 2018 led the security team in developing a world class information security program establishing security best practices, implementing security tooling to protect systems, and leading our Incident response to security and disaster recovery events.

Session Agenda

01 Introduction

02 Why Security?

03 Payroll Fraud

04 Defense in Depth: Preventing Payroll Fraud

05 Regulatory and Compliance


EVOLVE
An HCM Growth Summit
Why Security?

Security Stats*

- 68% of Breaches involve a human element
- Phishing and Pretexting account for 73% of social engineering attacks
- 50% of social engineering attacks result in stolen creds

Gen AI will continue to improve social engineering attack vectors

*2024 Verizon Data Breach Investigation Report

Security Best Practices

01

Security Program

- Have a written program
- Defined onboarding/Offboarding process
- Role Based Access Controls
- Information Security Awareness Training

02

Security Best Practices

- Implement MFA on ALL accounts
- Test users on phishing monthly
- Endpoint Protections (AV, EDR)
- Quarterly Access Reviews
- Provide awareness to customers

03

Incident Response

- Have a Written plan
- Business Continuity Plan
- Rehearse the plan annually
- Law enforcement contacts

EVOLVE
An HCM Growth Summit

Payroll Fraud

Payroll Fraud

01

New Client Setup Fraud

RCA:

Gaps during new client setup

02

Client Compromise

RCA:
Insufficient security at the client

Fail to validate customer requests

03

CSR Phished (EE Request)

RCA:

Lack of training of the CSR

04

EE Compromise

RCA

Insufficient security on the EE acct

Attack Scenarios

01 User Email Compromise

1. Phishing Attack – Credential Harvesting
2. Compromise user email accounts
3. Resets user's password in the payroll system via self service password reset
4. Attacker Logs in and Updates bank info
5. Waits until regular payday

02 Phishing Attack

1. Phishing Attack – Credential Harvesting
2. Compromise client email accounts
3. Change rules to deliver mail from SBO to separate folder
4. Urgent request to setup new EE/1099
5. Out of Cycle Payment or Payroll

03 New Client Setup

1. New client setup
2. Fake EE and company docs
3. Goes through implementation
4. Once moved to DD, NSFs company payment

Preventing Payroll Fraud

01 Security is a Team Sport

Train your people and educate your clients

02 Defense in Depth

Secure your accounts

Monitoring/Reviews

Set Limits on per Payroll/per Check

03 Validation

Out of Band checks – Call the customer

Second person review

Have a defined process

04 Separation Duties

Roles based on not what a person does but what a Role/Job Title does

Manual reviews


EVOLVE
An HCM Growth Summit
Q & A

Resources & Contact

Joshua.Gohman@asuresoftware.com

Fernando.munoz@asuresoftware.com

https://www.ic3.gov/

https://www.secretservice.gov/investigation

EVOLVE
An HCM Growth Summit

Thank You!

2024 Asure Reseller Partner Conference

Asure