

AI UNCHAINED

Accounting Intelligence. No boundaries. No limits.

2024



CHECK IN: 1010CTI

Securing Your Firm in a Cyber-Threat Landscape

AI UNCHAINED

Accounting Intelligence. No boundaries. No limits.



INTRODUCTIONS



Travis Cherry
Chief Technology Officer
Botkeeper



Matt Geary, CISSP, CRISC, CISA
Senior Director Information Security & IT
Botkeeper

TABLE OF CONTENTS

01 **Cybersecurity Landscape**
Dystopian State of Affairs

02 **Evergreen Security Strategies**
Current trends

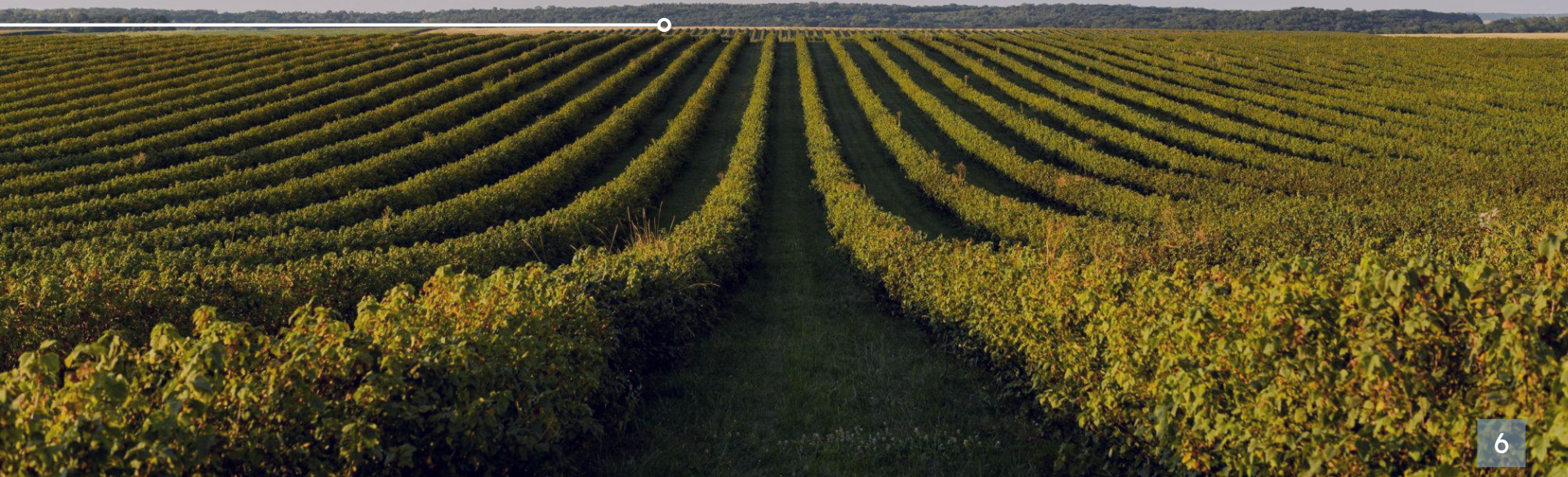
03 **SOC 2 Compliance**
Topics to review at your firm

04 **Securing Software**
Building and deploying securely

05 **Recent Case Study**
AWS .env Attack

01

CYBERSECURITY LANDSCAPE





The global cost of cybercrime is

\$24 TRILLION A YEAR

From a period of 2022 to 2027, cybercrime will increase 182%.

THE FOUR DIGITAL HORSEMEN

Maybe you have heard of these headlines in the news or at work?

Doom (War): “WW3 will be caused by a cyber attack”

Breach (Pestilence): “Everyone’s data is already out, it’s too late”

Sophistication (Death): “It can’t be stopped”

Resources (Famine): “There isn’t enough money or people”



THE STATE OF SECURITY

1,210 Organizations

Impacted by ransomware **every week**

43% of Attacks

Aimed at SMB's **under 100 employees**

60% of Businesses

Close down after a significant cyber attack

500,000 Unfilled Roles

In the U.S. **Over 4,000,000 openings worldwide.**





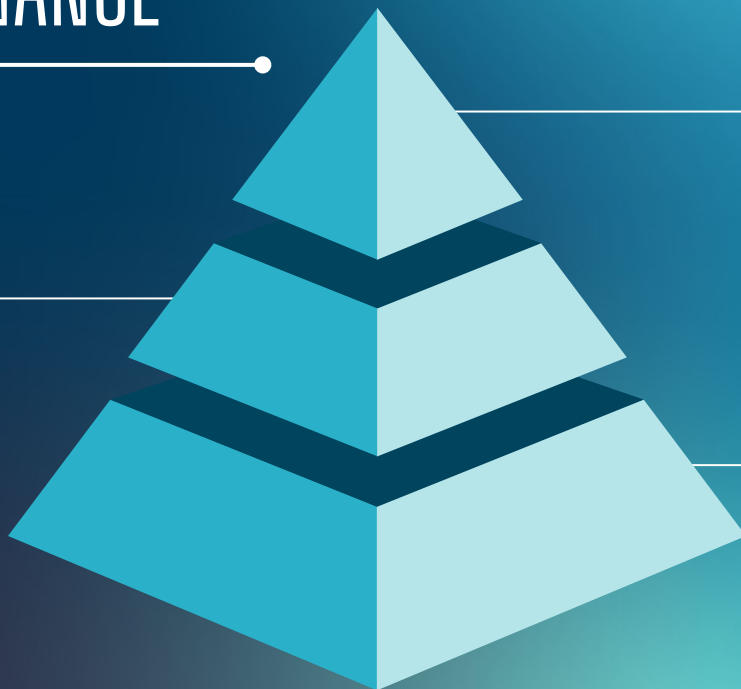
POLL 1

Do you know of anyone who has had a security incident in the past year?

THE STATE OF FINANCE

Fraudulent Schemes

Alter billing information of clients, invoices, bank access, etc.



30% Higher Risk For Attacks

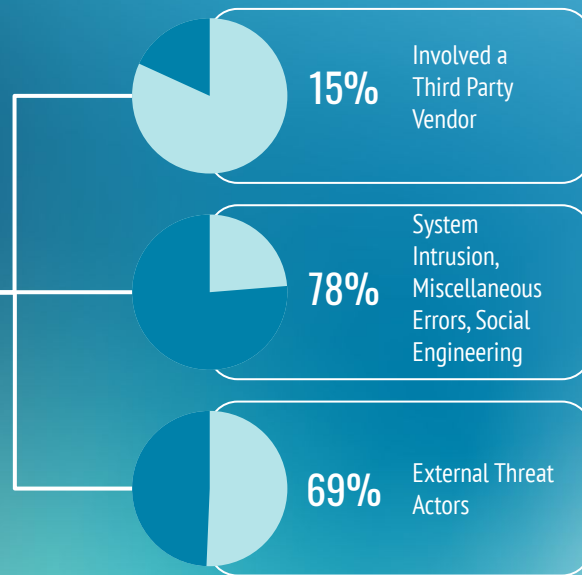
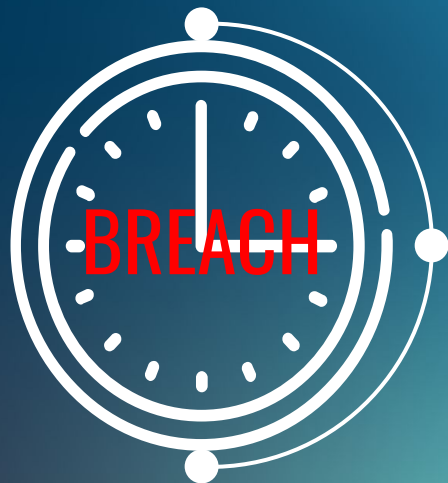
1 Tax season! Phishing to businesses and consumers increase. Stolen identities committing tax fraud.

Revealing & Sensitive Data

3 Many different compliances, fake compliance audits. Membership of AICPA code of ethics - integrity of data, confidentiality of clients, etc.

TIME BOMB – THIRD PARTY RISK

“In short, these are the breaches an organization could potentially mitigate or prevent by trying to select vendors with better security track records. We see this figure at 15% this year, a **68% increase from the previous year** [...]”
- Verizon Data Breach Investigation Report, 2024



EVERGREEN SECURITY STRATEGIES



DO'S and DON'TS

Tips To Implement

Traps To Avoid



RISK MANAGEMENT

Governance, Risk, Compliance “GRC”

Incident Response

DO's

Apply The "Ransomware Discount Code"

According to a study by IBM, companies saved \$470,000 in average costs of a breach compared to those that chose not to involve law enforcement.

Legally Privilege Your Penetration Tests

If you have a breach and are sued (and you will be) your known issues protected by ACP could result in huge savings of both money and reputation.

Champion Your Information Security Team

Every time those slight inconveniences security imposes, like multi-factor, say YES! Your culture is invaluable to your Information Security team.

DON'Ts

Dismiss The Risk & Say, "I Have Cyber Insurance"

Policy gaps like social engineering / loss of device "Duty to Defend" and are you covered by D&O Also, hackers love to know you are insured!

Let "Reasonable" Be The End of Discussion

Only one in three breaches were detected by internal security teams/tools. Data breaches disclosed by the attacker cost nearly \$1 million more on average.

Think Checking A Compliance Box Means Secure

Riding a motorcycle wearing a helmet and no other protection meets legal requirements, but not necessarily smart.

INFOSEC RISK MANAGEMENT 101

01

ASSETS

People, Hardware, Data, Intellectual Property, etc

02

POLICIES

Administrative, Technical Controls and Configurations, Physical Security

03

MONITORING

Are Assets + Policies aligned? Are audits as expected?

04

RESPONSE & RECOVERY

If Yes, Continual Improve
If No, Incident Response

EXAMPLES

01

ASSETS

UEM for Devices & Installed Apps & EDR
iDP for Employees
SSPM for Cloud Software

02

POLICIES

GRC Tool to document & track against
AUP & Training & Phishing
Group Policy, DLP, Encryption, etc

03

MONITORING

SIEM ingesting logs
Threat Hunting & Threat Intelligence
Event Viewer "Advanced" Auditing

04

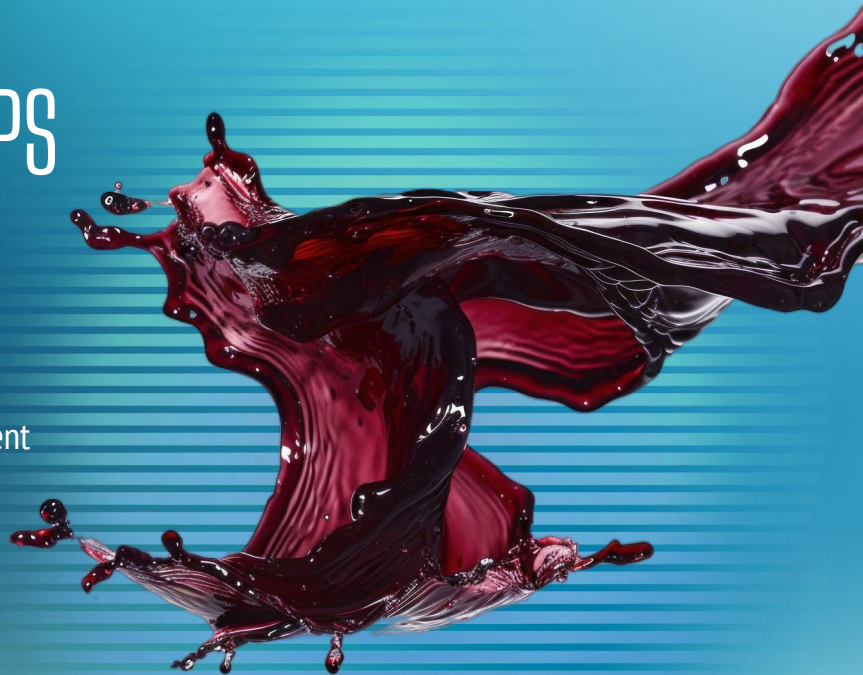
RESPONSE & RECOVERY

Incident Response Procedures
BCP With Recent DR Procedures
Infosec Professional To Lead

INCIDENT RESPONSE & TABLETOP TIPS

Some questions you may want to bring to your team:

- Incident response team - internal vs external, tracking reimbursement
- Who to contact first? Law Enforcement? Lawyer? Cyber Insurance?
- Are “Out Of Band” Communications set up?
- How are you simulating weeks / months?



AI SECURITY TIPS

- Broad exclusion claims but limited liability cap
- Upstream indemnification
- Copyright law requires human authorship
- Developer code generation (reciprocal open source licenses used in training the model can cause licenses to trigger against your codebase)
- Employees/Customers “Escaping The Matrix” of an AI chat
- PII, Secrets, other data leakage
- Vendor solutions can rely heavily on third-party LLMs and put your data at risk





POLL 2

Has your firm created an AI policy?

03

SOC 2

SOC 2 TYPE 2 THINGS TO KNOW

AUDITOR OPINION

Qualified opinions need to be read carefully!

NOT BINDING

SOC is not a contract. Have a list of expectations to reconcile against.

ARE YOU THE AUDIENCE?

If you do not understand the report, it is not for you.

SOC For Goods

SOC 2 is for Service only!
“SOC for Supply Chain” is for goods

SHADOW IT

Not everyone in the organization will think of SOC 2 before they break a control

REMOTE WORK

SOC 2 has nothing to do with geography, unlike ISO 27001. Perimeters may be different for remote workers



POLL 3

Do you regularly perform SOC 2 report reviews of vendors your firm utilizes after the initial review?



04
SECURING SOFTWARE

OWASP Top 10

Broken Access Control

Cryptographic Failures

Injection

Insecure Design

Security Misconfiguration

Vulnerable and Outdated Components

Identification and Authentication Failures

Software and Data Integrity Failures

Security Logging and Monitoring Failures

Server-Side Request Forgery



Web Application Security

Trusted Tools & Frameworks

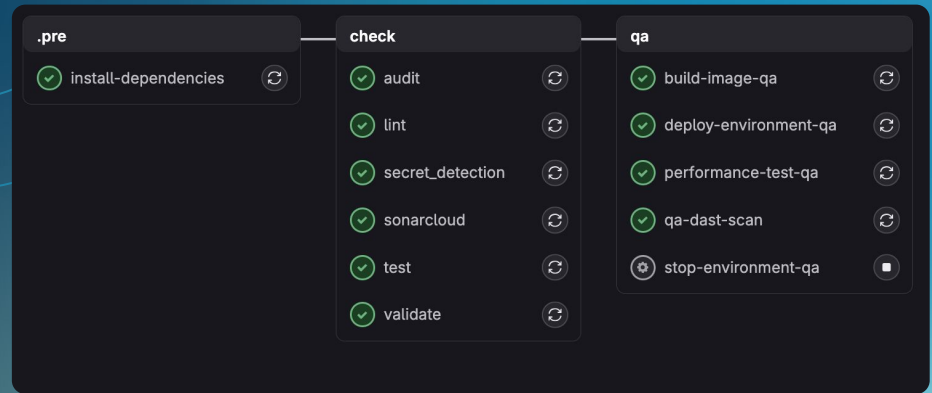
- Trusted user Identity & Access Management (IAM)
- Trusted Data Sources (e.g. Financial Aggregator)
- Validated integrations (e.g. adhering to marketplace standards)
- Mature coding frameworks that prevent XSS & SQL injection

Secure by Design

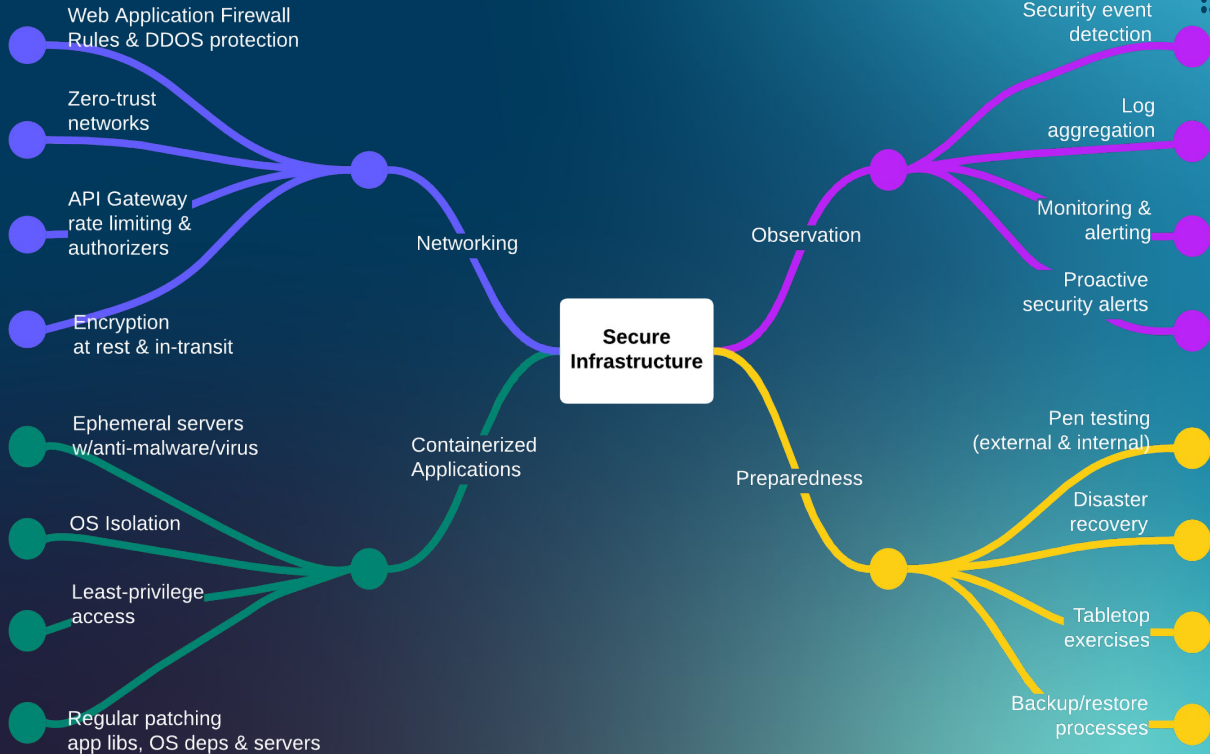
- SSO and/or 2-factor and step-up authentication
- Fine-grained user roles & per entity provisioning
- Antivirus scanning of uploaded files in isolation
- Secure coding training and security awareness

Secure Software Development Lifecycle (SDLC)

- Continuous integration & shifting left - identify and remediate asap
- Dependency audits for known vulnerabilities
- Linting - enforce style and secure coding structure
- Secrets detection and exclusion from deployed codebase
- Code-based security bug detection
- Unit testing with minimum coverage %
- DAST Scans in ephemeral environments
- Mandatory code reviews and approvals



Securing Infrastructure






05

Recent Case Study

AWS .env Attack

Recent Amazon Web Services .env Attack

- In August of '24, an attack against AWS accounts was uncovered by Unit 42 researchers that targeted inadvertent credential exposure via insecurely stored .env files on servers
- The exposed files held AWS access keys, API & access keys and database credentials
- The attack impacted 110,000 domains, exposing over 90,000 environment variables including API keys and more
- Enforce best practices to minimize risk:
 - .env exclusions from deployed images
 - Secret detection in codebase within audit phase
- Deploy defenses:
 - AWS Web Application Firewall (WAF) with bot detection & managed rules
 - AWS API Gateway with rate limiting and authorizers
- Enable proactive alerting to detect incidents:
 - AWS Guard Duty - privilege escalation detection
 - Elastic SIEM - detect outliers and suspicious behavior
- Formalize incident response plan rehearsal and activation process



“ Don't Worry. We won't get hacked. That's illegal!

– SOMEONE THAT WAS EVENTUALLY HACKED

CHECK OUT: 1010CTO

QUESTIONS?

CONNECT ON LINKEDIN!

@travischerry
@mattkylegeary

SUPPORT

Come check our booth out to learn more as to how we're a secure vendor for you!

THANK YOU!