AUDITOR PANEL

Hot Takes: Soapbox Opinions from Security Auditors

KEYS 2026 HORIZONS

1

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the presenters' opinions.**
  Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.

KEYS

2

Andrew Hettick
Information Security Officer
CoNetrix, LLC

Bret Mills
Audit & Security Consultant
CoNetrix Security

Benjamin Taylor
Audit Manager
CoNetrix Security

Cole Daniel
Security Support Technician
CoNetrix Security

KEYS

3

SESSION AGENDA

1. Passwords are Outdated
2. Another Risk Assessment?
3. All My Vendors are Critical
4. Filling Out Request List Items

KEYS

4

Passwords

KEYS

5

"**Passwordless** authentication is an authentication method in which a user can log in to a computer system **without entering a password** or any other **knowledge-based secret.** In most common implementations, users are asked to enter their public identifier and then complete the authentication process by providing a **secure proof of identity through a registered device, biometric method, or token.** Passwordless authentication methods typically rely on **public-key cryptography** infrastructure, where the public key is provided during registration to the authenticating service."

KEYS

6

PASSWORDS

- Are password managers a good solution?
- Enable multi-factor authentication (MFA).
- Stay current with key based infrastructure changes.

KEYS

7

```
# The practice of representing info in a way that is not obvious on initial examination

# Allows any digital media to become an obfuscation layer

# Not mathematically secure

# Discovery of info depends on knowledge of its existence

# Exists in many places we're not aware of

# Modern example: Cicada 3301
```

KEYS

8

IT Audit Risk Assessment

KEYS

9

IT AUDIT RISK ASSESSMENT

Criticality	Definition	Frequency
Insignificant	A deficiency could cause **negligible** adverse effects.	Situationally Based Only
Low	A deficiency could cause **limited** adverse effects.	18 - 24 Months
Medium	A deficiency could cause **serious** adverse effects.	12 Months
High	A deficiency could cause **severe** adverse effects.	6 Months
Extreme	A deficiency could cause **catastrophic** adverse effects.	3 Months

Audit Area	Criticality
IT Infrastructure Management	Medium
IT Audit Independence	Low
Business Continuity Planning	Medium
Cyber Incident Response	Medium
IT Oversight, Strategy & Policy	Medium
IT Staffing, Security Training & Company Culture	Insignificant
IT Risk Management & Risk Assessment	Medium
Vendor Management	Medium
Access & Data Management	High
Physical Inspections	Low
Cyber Monitoring, Alerting & Review	Medium
External Vulnerability Scanning	Extreme
Internal Vulnerability Scanning	High

KEYS

10

IT AUDIT RISK ASSESSMENT

- Identifies areas of most concern
- Determines best use of audit resources
- Helps you plan your audit schedule

KEYS

11

```
+-----------------------------------------------------------+
| the power of                                              |
|          ____ | | __ _(_)_ __     ___(_) __ _| |__ | |_  |
|         | '_ \| |/ _` | | '_ \   / __| |/ _` | '_ \| __| |
|         | |_) | | (_| | | | | | \__ \ | (_| | | | | |_  |
|         | .__/|_|\__,_|_|_| |_| |___/_|\__, |_| |_|\__| |
|         |_|                             |___/             |
+-----------------------------------------------------------+
```

```
# File format permissivity (polyglots)

# Overlooked text patterns

# Realtime visual decoding (spectrograms)
```

KEYS

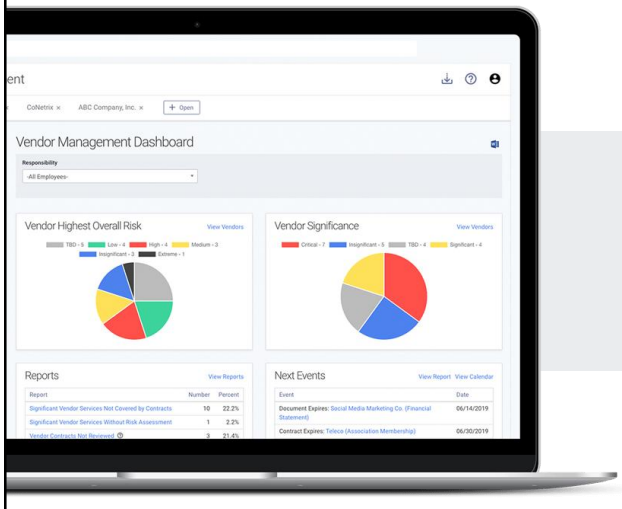
12

Vendor Management

KEYS

13

KEYS



Tandem Vendor Management Software

14

VENDOR MANAGEMENT

- What data do they have? Where is it?
- Are the risk/significance ratings appropriate?
- What due diligence documents do I really need?

KEYS

15


```
# Garnered popularity in 2013

# Led by an anonymous group with unknown goals

# Began with an image and spread across numerous mediums

# ARGs use similar tactics
```

KEYS

16

Request List Items

KEYS

17

"Audits should **review every aspect** of the information security program, the environment in which the program runs, and outputs of the program. Audits should assess the **reasonableness and appropriateness** of, and compliance with, policies, standards, and procedures; **report** on information security activity and control deficiencies to decision makers; **identify root causes and recommendations to address deficiencies**; and test the effectiveness of controls within the program. "

FFIEC Information Security Handbook

KEYS

18

REQUEST LIST ITEMS

- The deeper we go, the more secure you are.
- The tool in the toolbox.
- Yes, we need them on time!!!

KEYS

19

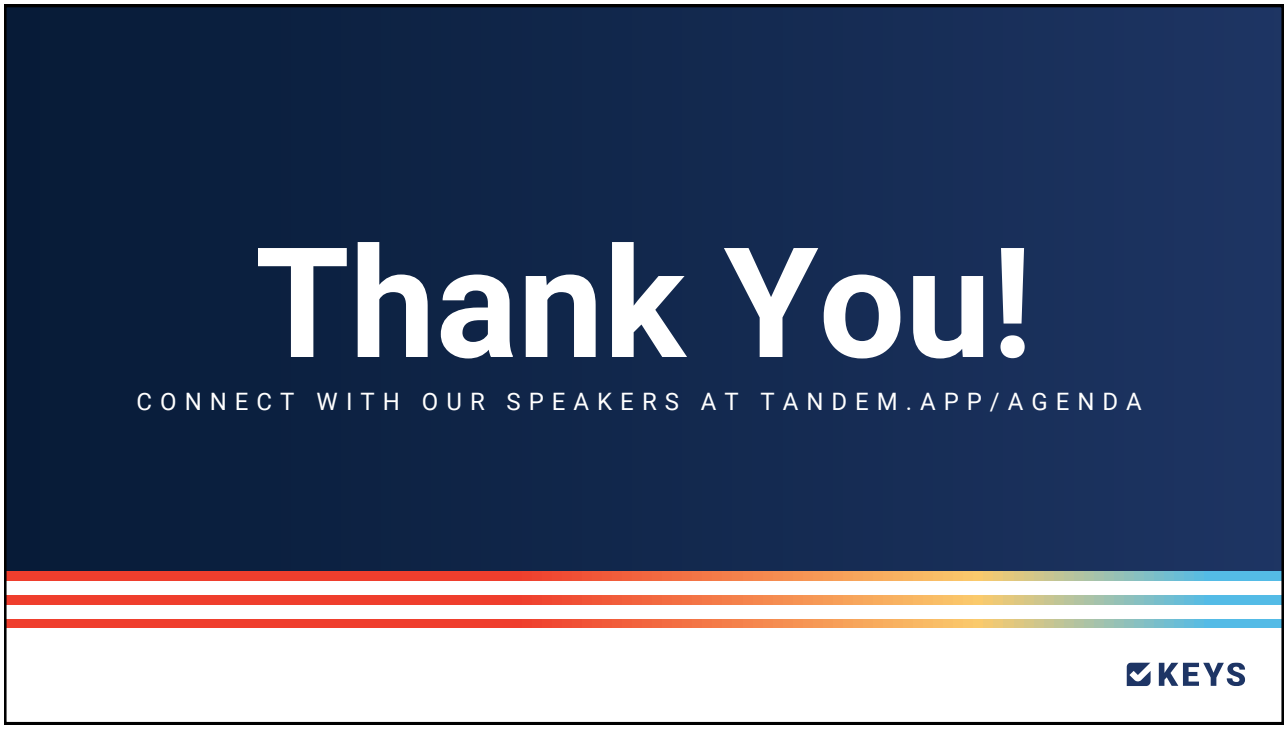
```
  # Doesn't depend on information from external sources

  # Uses multi-layer obfuscation to avoid brute-forcing

  # Homage to Jim Sandborn's Kryptos Code
```

KEYS

20

21

22


Thank You!
CONNECT WITH OUR SPEAKERS AT TANDEM.APP/AGENDA
KEYS

23