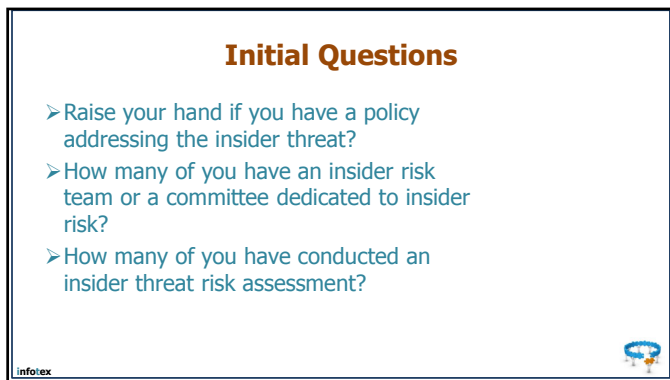
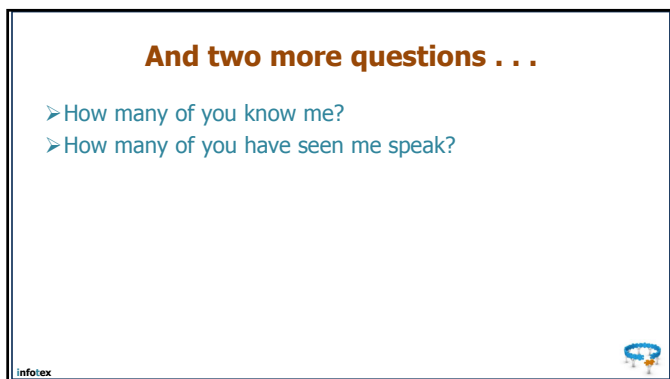




1



2



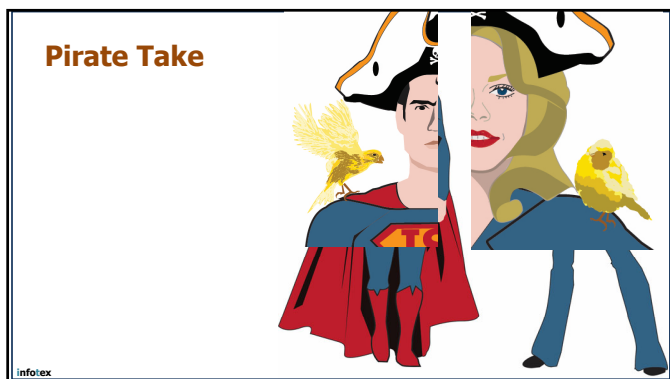
3



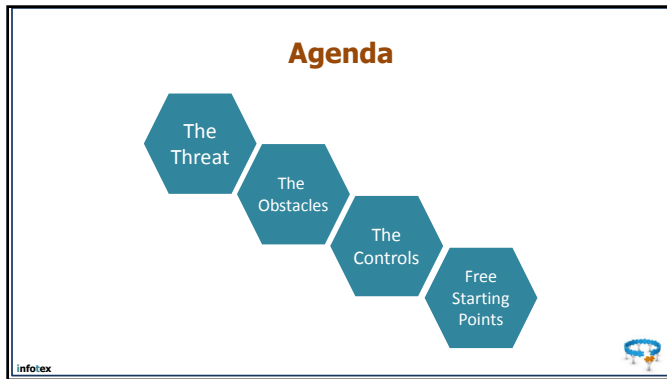
4



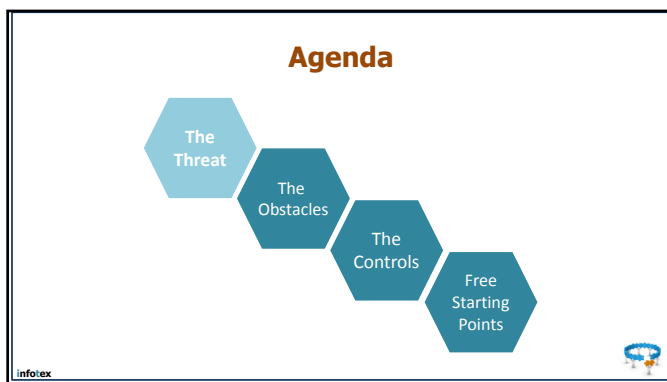
5



6



7



8

A question of viewpoints . . .


- How many of us think about user mistakes or policy enforcement issues when we hear "insider threat?"
- How many of us believe that the malicious insider threat is real?
- In *your* bank?

info:ex

9

Insider Threats

- Lack of Awareness
- Policy Enforcement
- Malicious



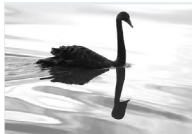
Hacker Guy

info/ex

10

But to the first two . . .


- 85% of breaches include a human element; usually social engineering. (Verizon Data Breach Report 2021)
- There are far more breaches in the first two categories than the third.



info/ex

11

First Bank of Nowhere



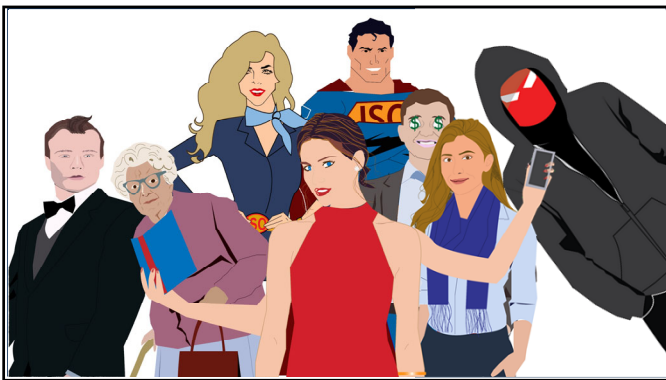
Bill Tookay Percy Nell Joan DePartmen Margaret De Target Mark Etting Jane ISO Joe ISO Hacker Guy

info/ex

12



13



14

Types of Malicious Insider Threats

- Workplace Violence
- Fraud
- Cybersecurity



info@ex


15

What is in common?

- There are always signs.
 - "We should have realized something was wrong when . . ."
 - These signs are almost always discoverable in the network traffic.
- Which is weird, because "it will never happen here" is also a commonality.



info:ex

16

The FFIEC



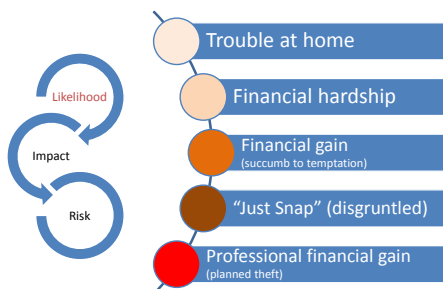
- Refers to "insider threats" as "Rogue Employees"
- I like this paradigm, cause it implies that an employee can "go rogue."



FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

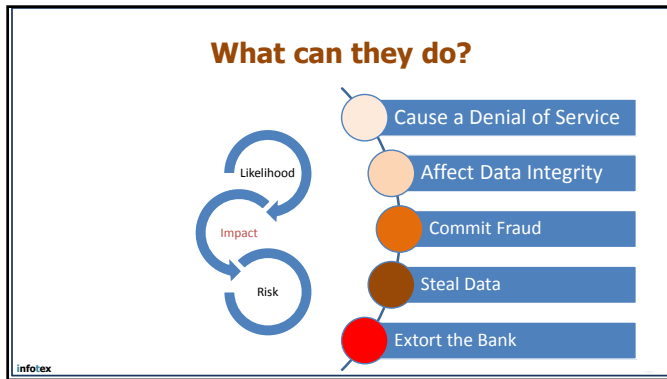
17

What makes them "go rogue"



info:ex

18



19

What the FFIEC says they can do . . .

- Alteration of data.
- Deletion of production and backup data.
- Misdirected data.
- Disruption of systems.
- Destruction of systems.
- Misuse of systems for personal gain or to damage the institution.
- Appropriation of strategic or customer data for espionage or fraud schemes.
- Extortion

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

20

Meanwhile, the government . . .

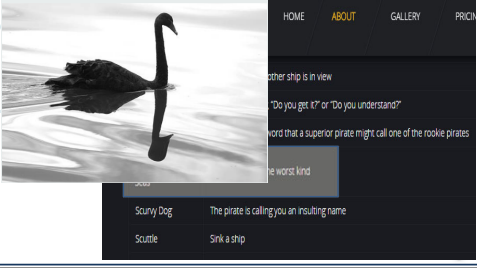
- In 2019, the FBI highlighted the insider threat as one of the leading new risks for 2020.
- OCC and FDIC both described "malicious insider threat" as one of the substantial new risks for 2020.
- The Cybersecurity Infrastructure and Security Agency published its risk assessment in 2021.

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

21

And, of course, the risk

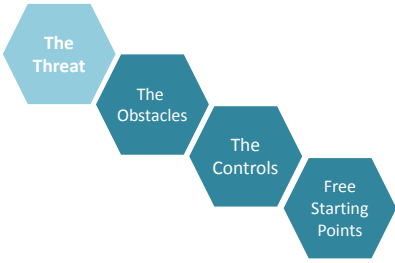
➤ Even if the likelihood is low, a person WE can't control can to HURT our customers . . . Black Swan I



info:ex

22

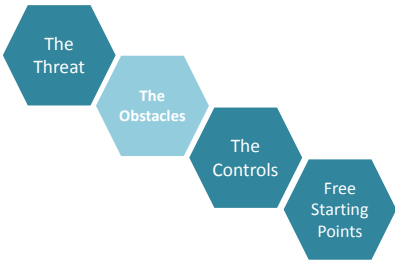
Agenda



info:ex

23

Agenda



info:ex

24

A few more questions

- How many have formally discussed the insider threat in the year?
- How many have informally discussed the malicious insider threat with somebody in your bank in the last year?
 - 6 months?
 - Last Week?

info:ex



25

Bank Insiders - The Scourge of The Seven Seas

SunTrust Bank

On April 20, 2018, SunTrust Bank announced a data breach that might have exposed the personal information of up to 10 million customers. The financial firm said it had received reports of unauthorized access to account numbers, security numbers, and other sensitive information. Fortunately, the security number was not compromised. In an investigation, the firm found that its data security controls were not strong enough to prevent the breach. The breach caused significant damage to the bank's reputation and financial performance.

May 12, 2021 by Extinction Rebellion

with a cyber-attack on the bank's systems. The breach was the result of a combination of factors, including a vulnerability in the bank's software and a lack of proper security controls. The breach was the result of a combination of factors, including a vulnerability in the bank's software and a lack of proper security controls.

Justice 100%

info:ex

26

Obstacles



- Awareness
- Legal Risk
- Operational Risk
- No Correlation of Physical Suspensions to Network Monitoring (**Integration**)

info:ex



27

Awareness "Dampeners"

- Awkwardness
- You-get-what-you-expect Risk
 - The Panopticon Effect?
- Trust as a control

The panopticon is a disciplinary concept brought to life in the form of a central observation tower placed within a circle of prison cells. From the tower, a guard can see every cell and inmate but the inmates can't see into the tower. Prisoners will never know whether or not they are being watched. Jul 18, 2017

<https://ethics.org.au/ethics-explainer-panopticon-what-is-...>

info:ex



28



29

Legal Risk

- Accusation Risk
- Employment at Will versus Fired for Stealing.
- Risk of others knowing why somebody was fired.




info:ex



30

Operational Risk

- Morale of team knowing a coworker was/is suspected.
- Morale of person under suspicion
- Morale of exonerated person.
- YOU-GET-WHAT-YOU-EXPECT-RISK




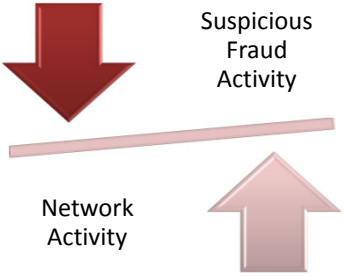
We often prove somebody did nothing wrong.

info/ex

31

Is there a correlation?





Suspicious
Fraud
Activity

Network
Activity

info/ex

32

Agenda

The Threat

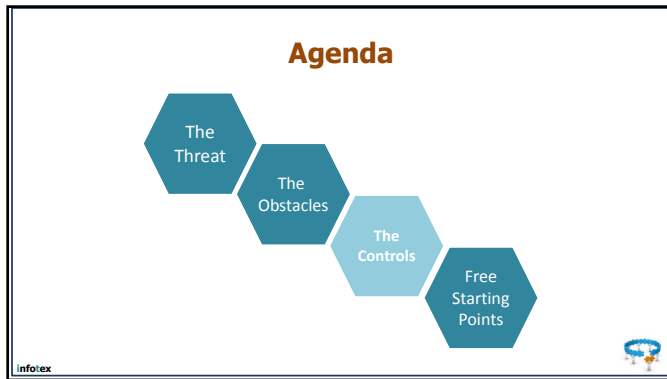
The Obstacles

The Controls

Free Starting Points

info/ex

33



34

More Questions to Ask

- Is there a risk profile on each employee?
 - Are you tracking employees by missed social engineering tests?
 - Is likelihood of malicious activity a part of that assessment?
- Do you monitor existing employees by risk profile?
 - Do your policies adequately secure your right to monitor network traffic, event logs, employee activities?
 - Do you have the ability to "put a watch" on specific employees?
 - Does doing this create legal risk?

info:ex

35

Potential Frameworks

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

info:ex

36

The FFIEC Control Suggestions

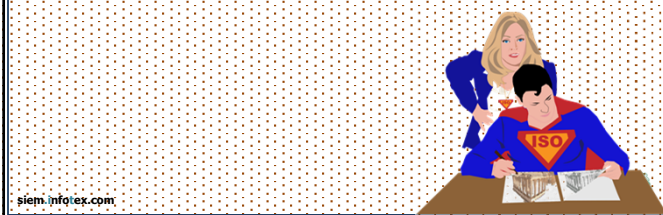
- Principle of least privilege
- Align job descriptions to access.
- Define user profiles.
- Ongoing access reviews / independent activity monitoring
- Timely notification of job changes, including terminations.
- Distribution of system administrator activities
- Cross-training



37

Takeaways and Boilerplates

- FFIEC Guidance Summary: The Insider Threat



38

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

[CYBERSECURITY](#)
[INFRASTRUCTURE SECURITY](#)
[EMERGENCY COMMUNICATIONS](#)
[NATIONAL RISK MANAGEMENT](#)
[ABOUT CISA](#)
[MEDIA](#)

CISA RELEASES NEW TOOL TO HELP ORGANIZATIONS GUARD AGAINST INSIDER THREATS

Original release date: September 28, 2021 | Last revised: October 05, 2021

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) released an [Insider Risk Mitigation Self-Assessment Tool](#) (for best results, please download and open with Adobe) today, which assists public and private sector organizations in assessing their vulnerability to an insider threat. By answering a series of questions, users receive feedback they can use to gauge their risk posture. The tool will also help users further understand the nature of insider threats and take steps to create their own prevention and mitigation programs.

"While security efforts often focus on external threats, often the biggest threat can be found inside the organization," said CISA Executive Assistant Director for Infrastructure Security David Mussington. "CISA urges all our partners, especially small and medium businesses who may have limited resources, to use this new tool to develop a plan to guard against insider threats. Taking some small steps today can make a big difference in preventing or mitigating the consequences of an insider threat in the future."

Insider threats can pose serious risk to any organization because of the institutional knowledge and trust placed in the hands of the perpetrator. Insider threats can come from current or former employees, contractors, or others with inside knowledge, and the consequences can include compromised sensitive information, damaged organizational reputation, lost revenue, stolen intellectual property, reduced market share, and even physical harm to people. CISA has a number of tools, training, and information on an array of threats public and private sector organizations face, including insider threats. Information on these resources can be found at [CISA.gov](#).

###

Topics: Infrastructure Security
Keywords: CISA, critical infrastructure, infrastructure security, infrastructure security tool, insider threat
Last Published Date: October 5, 2021

39

Please wait...

If this message is not eventually replaced by the proper contents of the document, your PDF viewer may not be able to display this type of document.

You can upgrade to the latest version of Adobe Reader for Windows®, Mac, or Linux® by visiting http://www.adobe.com/go/reader_download.

For more assistance with Adobe Reader visit <http://www.adobe.com/go/acrreader>.

Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries. Mac is a trademark of Apple Inc., registered in the United States and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.



40

Important to Keep In Mind

- CISA guidance is “industry agnostic”
- Guidance is often meant to scale up to very large organizations.
 - Though they are providing a separate question set for businesses under a million in revenues.
- Banking regulation is starting to point to CISA and NIST



41

What's in it

- Program Management Goals (and questions)
- Personnel and Training Goals (and questions)



42

Program Management Goals

1. An insider risk policy exists.
2. There is detect, identify, assess, and manage capability for insider incidents
3. Communication about insider risk events happens
4. Insider risk is integrated with the enterprise risk program (ERP) and/or security risk management program.
5. Mission-critical assets are known.

info:ex



43

Personnel and Training Goals

1. Organization-wide Participation
2. Multi-disciplinary Insider Risk Team
3. Insider Risk Team is Trained on Insider Risk
4. New Employees are made aware of the Insider Risk program as part of initial training.
5. Insider Risk Training is provided for all organization personnel
6. Role-based training provided to Insider Risk Team
7. Managers and supervisors receive training.

info:ex



44

Takeaways and Boilerplates

➤ CISA Insider Threat Assessment

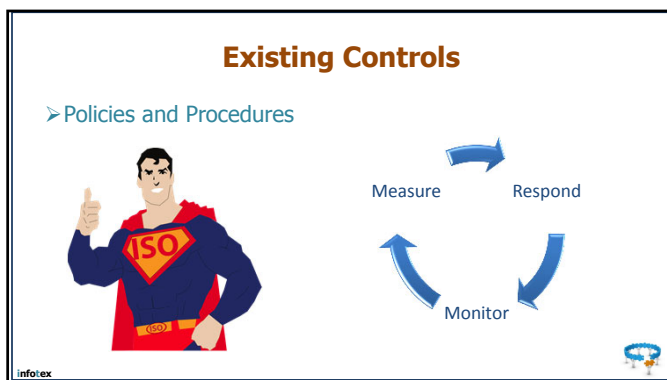
siem.info:ex.com



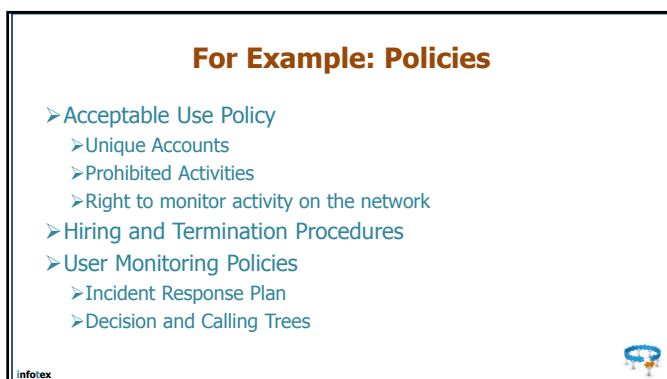
45



46



47



48

For Example: Policies

- Acceptable Use Policy
 - Unique Accounts
 - Prohibited Activities
 - Right to monitor activity on the network
- Hiring and Termination Procedures
 - How robust are your background checks, really?
 - How quick can you CONFIRM a termination is off all assets, really?
- User Monitoring Policies
 - Incident Response Plan
 - Decision and Calling Trees

info:ex



49

FFIEC AIO Booklet (2021)

ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS

Home | FF Booklets | Architecture, Infrastructure, and Operations | IT Governance and Risk Management Topics | AIO IT Asset Management | AIO IT Shadow IT

Architecture, Infrastructure, and Operations Booklet Contents

Introduction
Architecture, Infrastructure, and Operations
AIO Governance, Information, and Operations Governance
AIO Board and Senior Management Responsibilities
AIO IT Strategic Planning
AIO IT Enterprise Risk Management
AIO Other Roles and Responsibilities
AIO IT Management Responsibilities
AIO CISO Chief Architect
AIO CISO Chief Data Officer
AIO CISO IT Operations

II.B.3 Shadow IT

Shadow IT refers to IT devices, software, or services operating within the entity's environment without the knowledge, approval, or control of IT management. Shadow IT can also be identified within a third-party service provider's environment. Unapproved devices, software, or services should not be running at the entity, but there could be greater threat to the following:

- Business units to support their specific needs in contravention to the enterprise's needs.
- Third-party service providers to support services provided to the entity or to collect data for the service providers.
- Individuals (internal or external) for convenience to allow them to use entity resources (e.g., address unmet need for malicious purposes (e.g., to steal data or processing power).
- Incomplete decommissioning process for legacy systems (e.g., business unit systems that were never decommissioned because of software compatibility limitations).

Failure to address the risks of shadow IT may lead to an unknown attack vector due to management's lack of awareness of unapproved devices, software, or services. Therefore, management should understand and communicate the following risks of shadow IT to the entity's governance:

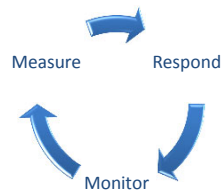


FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

50

Existing Controls

- Policies and Procedures
- Network Security



info:ex



51

Network Security Controls (insider)

- Password Policies
- Privileged Account Management
- Endpoint Security
 - Data Loss Prevention
 - Email Filtering and Monitoring
- Network Monitoring
 - Monitoring of specific assets or users



info/ex

52

More Questions

- How many of you have a SIEM or a SIM at your bank?
- How many of you simply don't know?
- How many know what a SIEM does?

info/ex

53

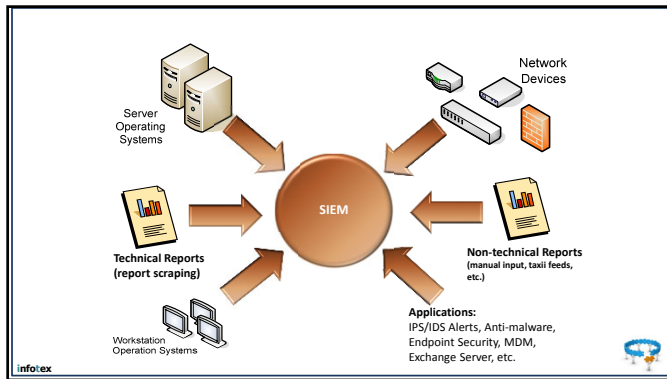
High Level

- A **Security Information and Event Management System**:
 - Is a network monitoring tool used by most banks.
 - Hard to be at bank without it.
 - Watches (and collects) all network events and event logs
 - Knock on the door
- A SIEM is usually
 - A **Security Operations Center** from the network
 - An MSSP or "Managed Security Service Provider"
 - 24x7x365

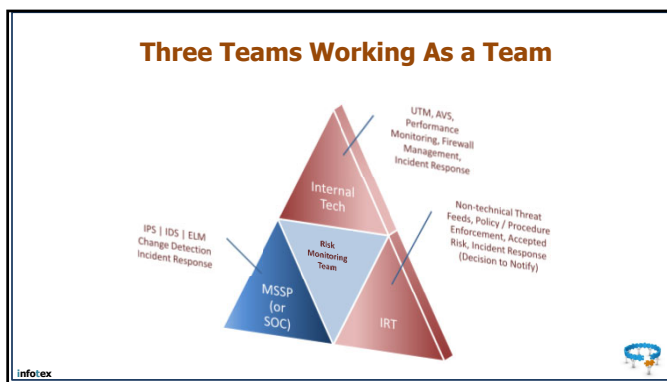


info/ex

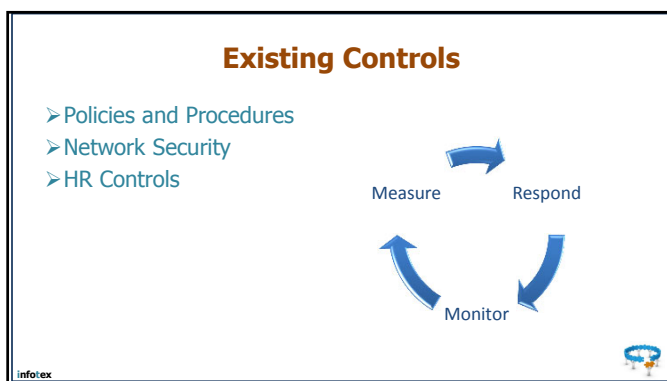
54



55



56



57

HR Controls

- Termination Procedures
- Fraud Monitoring
- Segregation of Duties
- Vacation Policy



info:ex

58

At a minimum

- Work on those termination procedures!!



info:ex

59



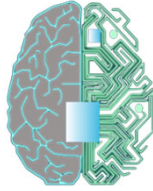
New Control: Integration?

info:ex

60

Integration

- Technology Risk Management with Enterprise Risk Management
- Insider Threat with Enterprise Risk Management (CISA)
- Fraud monitoring with Network Monitoring
- Physical Surveillance with Logical Surveillance



info:ex



61

What a SIEM sees . . .

- Legitimate Activity
- Illegitimate Activity
- Legitimate Illegitimate Activity



info:ex



62

How to add MIT to visibility

- Add your Fraud Team or person to your Incident Response Team.
- Be sure the Fraud Team or person is on the calling tree / daily report distribution for appropriate purposes.
- Train your Fraud Team on the capabilities of your SIEM

info:ex



63

How to add MIT to visibility

- Establish a secure line of communicate between your fraud person and the M-SOC or SOC.
- To mitigate legal risk, this cannot be visible to the IT Team
 - They have to be listed in the contacts database, and create a pass phrase (or opt for the call-back)
 - Requires a phone call to NOC Line
 - Requires the recipient of the PAW to receive the PAW Reports via secure messaging.

info/ex



64

Other New Controls



info/ex



65

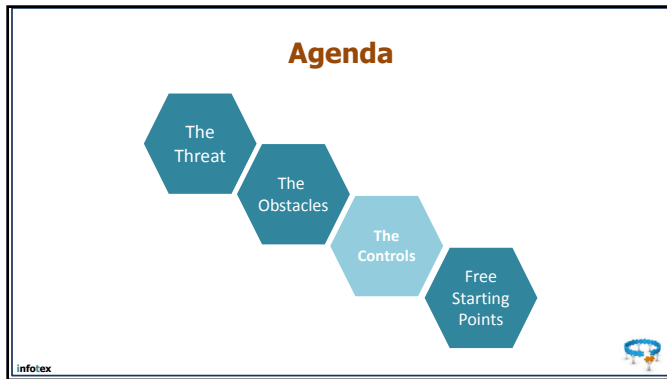
At a minimum

- Teach your incident response team to escalate heightened threat scenarios to your SOC or MSSP.
- They will add it to their "threat hunting" activities.

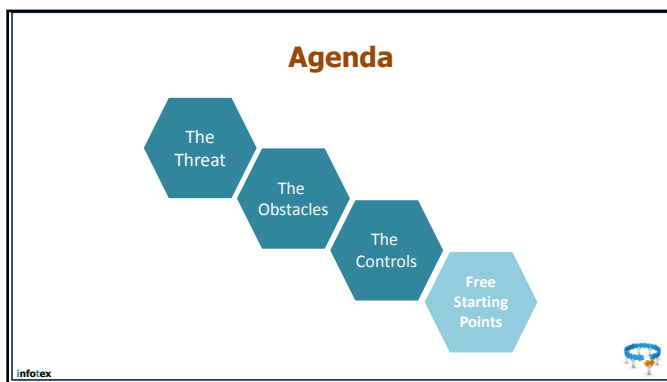


info/ex

66



70



71



72

Free Giveaways

- Policy Excerpts
- Guidance summary
- Example Insider Threat Tabletop Test Scenario
- Includes comprehension exercises

The Threat

The Obstacles

The Controls

Free Starting Points

siem.infotex.com

boilerplates.infotex.com

73

Free Giveaways

➤ my.infotex.com/insider

The Threat

The Obstacles

The Controls

Free Starting Points

siem.infotex.com

boilerplates.infotex.com

74



75

Mitigation in 5 Steps

1. Security Culture – talk to your board about the threat.
2. Beef up Background Check and Termination Procedures.
3. Put physical and/or fraud on the incident response team.
 - Develop a private channel for Fraud Monitoring
4. Learn how your SIEM looks for insider threats.
 - Escalate to your SOC or MSSP when conditions warrant
 - Termination Procedures
5. Tabletop Test the Insider Breach.

infotex



76

More Information



- Article with Reports and Studies:
 - <https://my.infotex.com/insider-threats/>
- The seven-step process:
 - <https://my.infotex.com/seven-insider-threats/>

infotex



77



infotex

78



79
