



State of the Art

CSO
Perspectives

State of the Art: Fraud Detection

Michael Theis
Executive Director of Insider
Threat Strategies
Raytheon



Cyber Threat Management Strategies



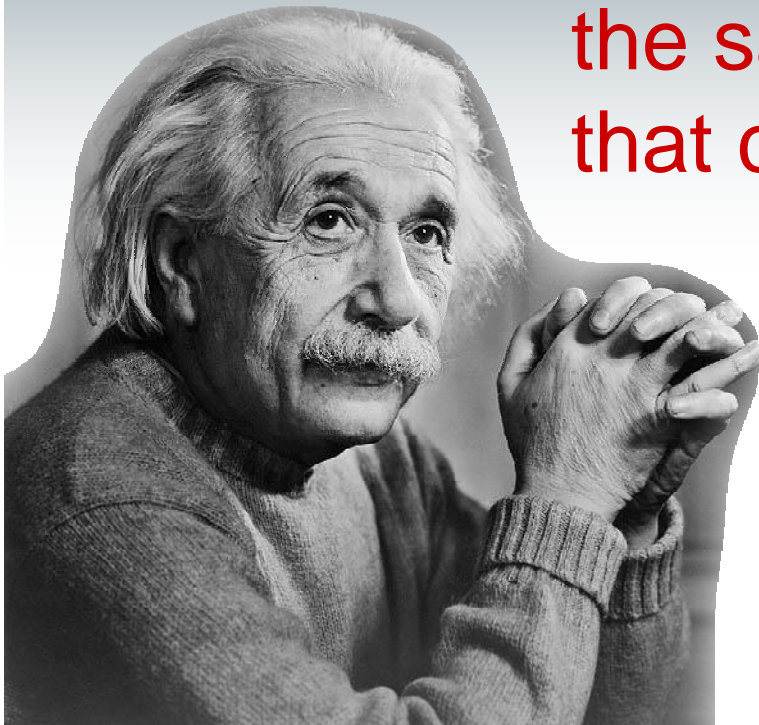
Meeting the Challenges
of the Trusted Insider Threat

7 April 2010

Creative Thinking

“Problems cannot be solved at the same level of consciousness that created them.”

- *Albert Einstein*



Creative Thinking

- Son of Irish immigrants; born 1962
- Entered USAF in 1980 – retired in 2000
- Detailed to NRO from 1995 to 2000
- A SIGINT specialist with broad access
 - Cryptography training
- Lived in Bowie, MD
- Father of four
- Worked for TRW, pending clearances for renewed access to NRO

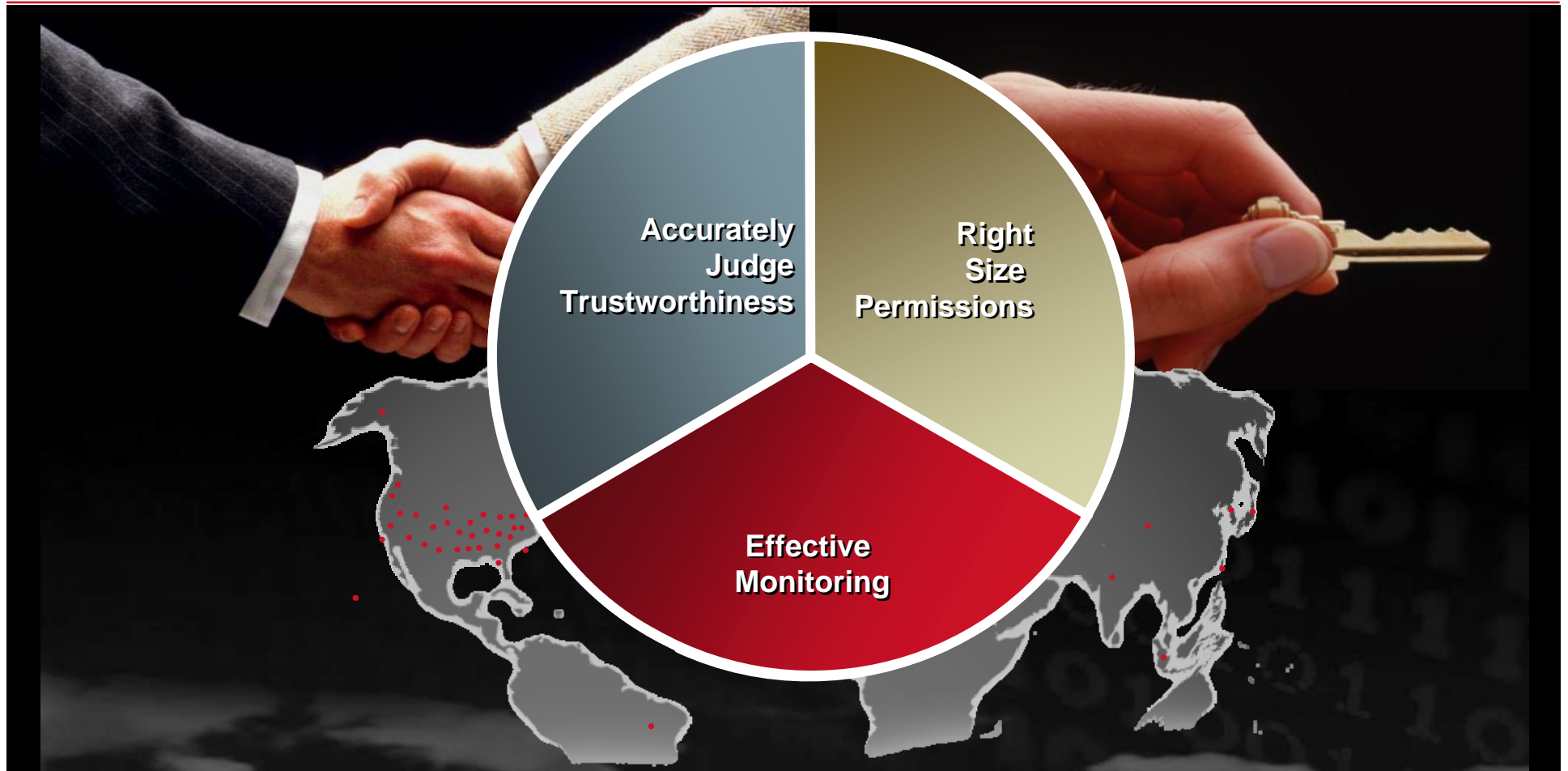


Creative Thinking



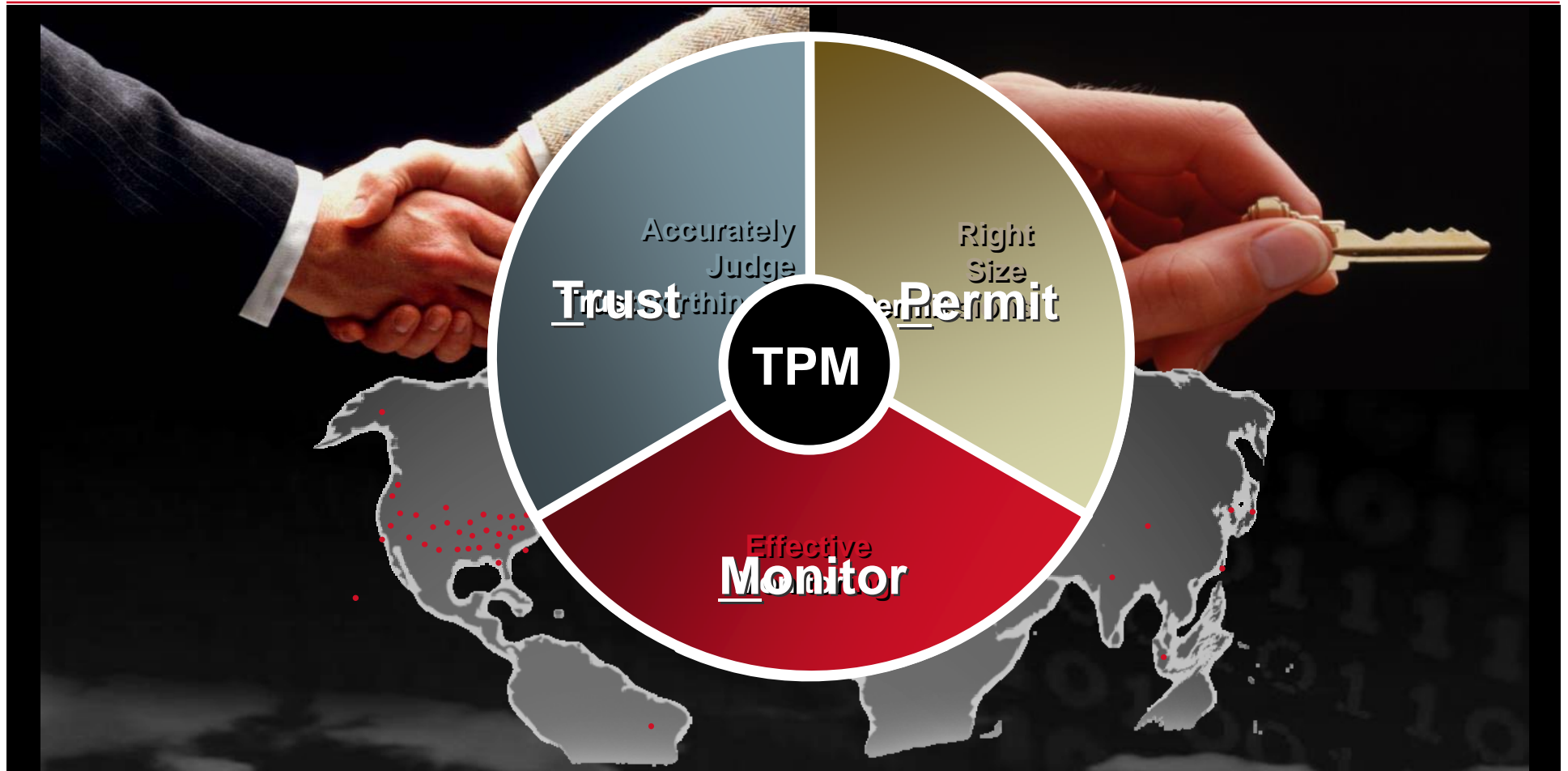
“All important company secrets are in a computer...somewhere.”

Protect From Cyber Threats



If you can't do all of them equally
then you have to compensate in other areas

Protect From Cyber Threats



If you can't do all of them equally
then you have to compensate in other areas

Accurately Judge Trustworthiness

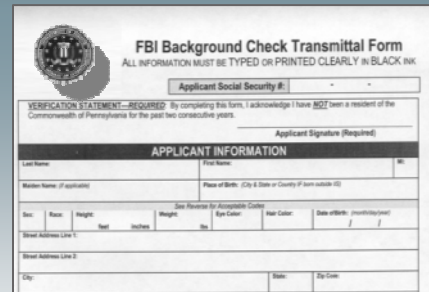


- People
 - Employees
 - Contractors
 - Service providers
 - Anyone with legitimate access to the computer

- Software & Hardware
 - All software runs at the privilege level of the user who clicked it or started it
 - Hard drives, USB, etc. attached to the machine run at the privilege level of the computer system itself

Accurately Judge Trustworthiness

- Standard measures
 - Incentives for new-hire referrals
 - Criminal background check
 - Reference check
 - Financial check
 - Periodic reviews
 - Academic verification
- Technology measures
 - RSA
 - PKI
 - SSL
- Aggressive Measures
 - Polygraph
 - Full Scope Background investigation



FBI Background Check Transmittal Form
ALL INFORMATION MUST BE TYPED OR PRINTED CLEARLY IN BLACK INK

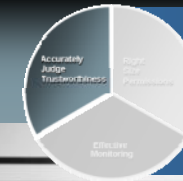
Applicant Social Security #: _____

VERIFICATION STATEMENT—REQUIRED: By completing this form, I acknowledge I have **BDZ** been a resident of the Commonwealth of Pennsylvania for the past two consecutive years.

Applicant Signature (Required): _____

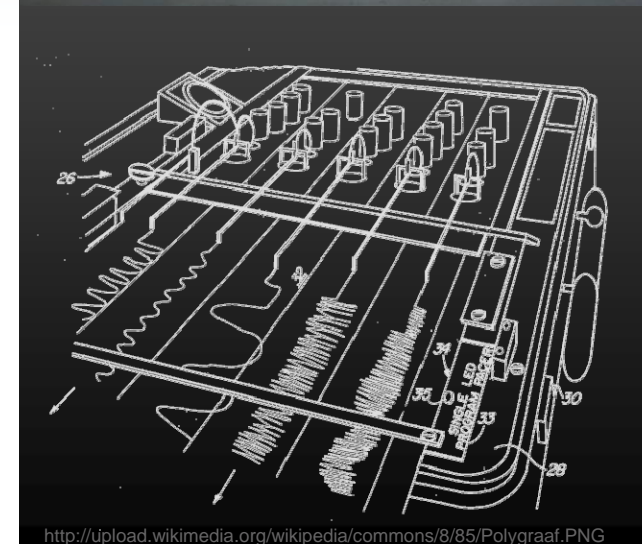
APPLICANT INFORMATION

| | | |
|-------------------------------|------------|---|
| Last Name | First Name | MI |
| Middle Name (if applicable) | | Place of Birth: City & State or County if born outside US |
| Sex | Race | Height |
| Weight | Eye Color | Hair Color |
| Date of Birth: month/day/year | Test | Defense |
| SSN | DOB | DOB |
| Street Address Line 1 | | |
| Street Address Line 2 | | |
| City | State | Zip Code |



Accurately
Judge
Trust

TPM



Accurately Judge Trustworthiness

Paradigm shift



Accurately
Judge
Trust

TPM

“Judging trustworthiness is currently geared only to evaluating behavior in the Brick & Mortar world.”

- *Dr. Joseph Krofcheck*

What behavioral shifts might we be missing?

Accurately Judge Trustworthiness

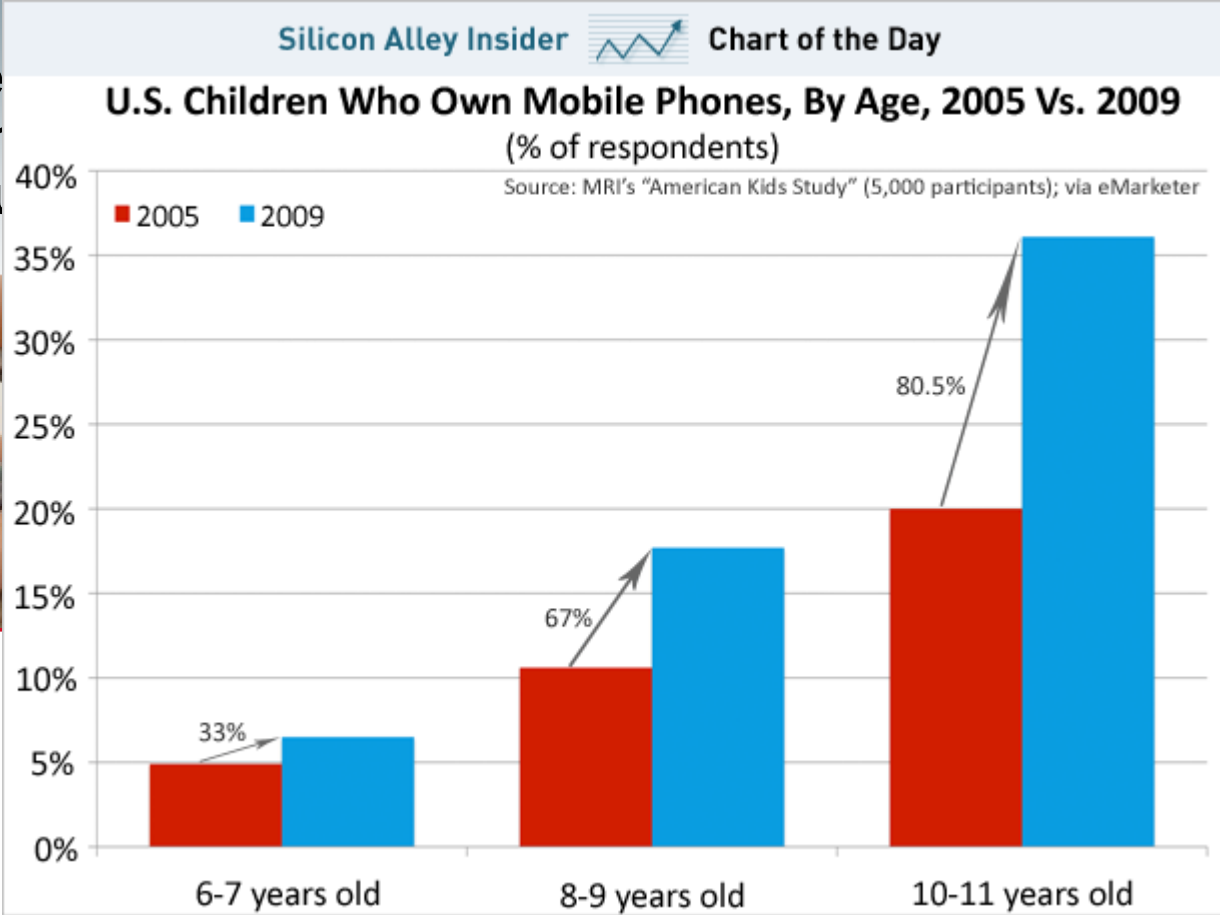
Behavior Shift



Accurately
Judge
Trust **TPM**



Le
kir
mu



“Coul

ole the

Accurately Judge Trustworthiness



Accurately
Judge
Trust **TPM**

Behav

- Sexting
- "Frie
- Onlin

No Pants 2010 NYC Reports

Published on January 10, 2010 in News. 234 Comments

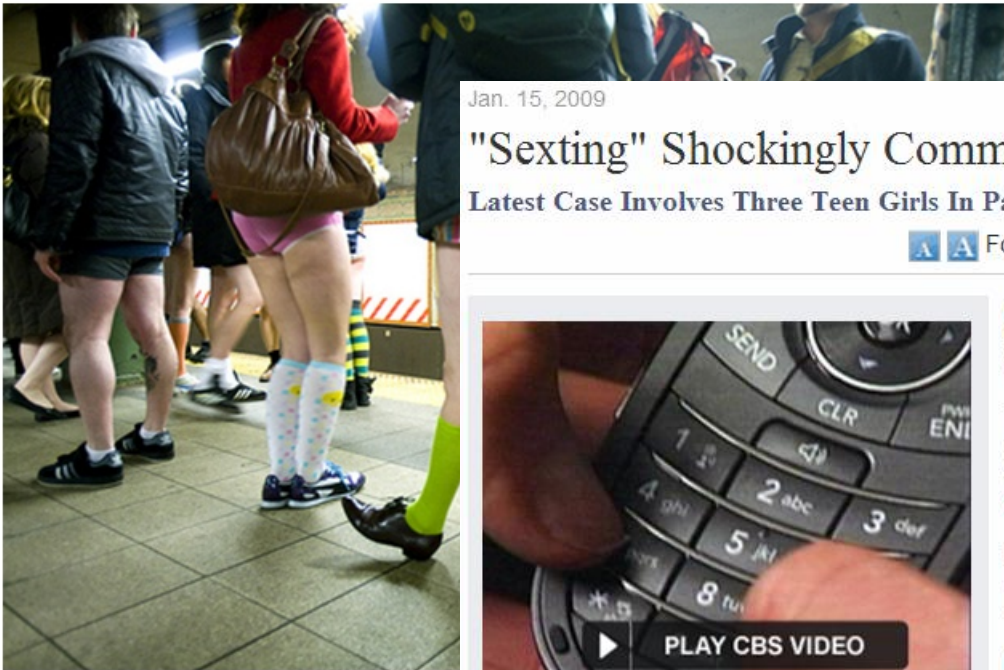


Photo by Katie Sokoler

The 9th Annual [No Pants Subway Ride](#). It's tough to count, but we're guessing met at meeting points spread out all c The high was 28 degrees. There were also No Pants rides in [43 other cities around the world in 16 countries!](#)

Jan. 15, 2009

"Sexting" Shockingly Common Among Teens

Latest Case Involves Three Teen Girls In Pa. Who Sent Nude Pics To T

Font size Print E-mail



VIDEO

Dangers Of Teen 'Sex-ting'

What teens call "sex-ting" is the act of sharing nude or partially nude photos via cell phone text message. As Harry Smith reports, few realize they are breaking the law.

(CBS/ AP) While it may be shock sending nude pictures via text me for high schoolers around the cou

This week, three teenage girls wh cell phone pictures of themselves western Pennsylvania high schoo with child pornography.

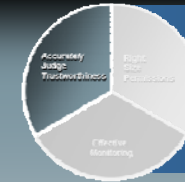
In October a Texas eighth-grader detention center after his football cell phone that a fellow student se

Roughly 20 percent of teens adm according to a [nationwide survey](#) Support Teen and Unplanned Pre

"This is a serious felony. They co **CBS News legal analyst Lisa Bl** Pennsylvania.

But, **Bloom** added, "What are we

Accurately Judge Trustworthiness



Accurately
Judge
Trust

TPM

Behavior Shift 2008-2009

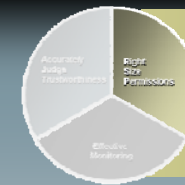
- 59% of employees who lost or left their jobs took electronic versions of confidential data with them
- 88% of IT Administrators said they would take data with them if they were laid off or fired
- Predictive Injustice



What Can be Done?

Hope is NOT a Strategy!!

Right Size Permissions



*Right
Size
Permissions*

TPM

- Standard measures
 - Badge access
 - Password Protection
 - Role-based security
- Aggressive Measures
 - Mandatory access controls
 - Biometrics
 - Security Stations



**Provide the amount of permission necessary
to securely accomplish the required task**

Right Size Permissions



Right Size Permissions

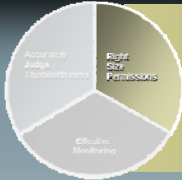


Right
Size
Permissions

TPM



Right Size Permissions



Right
Size
Permissions

TPM

BusinessWeek

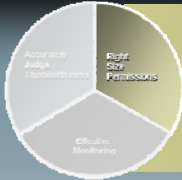
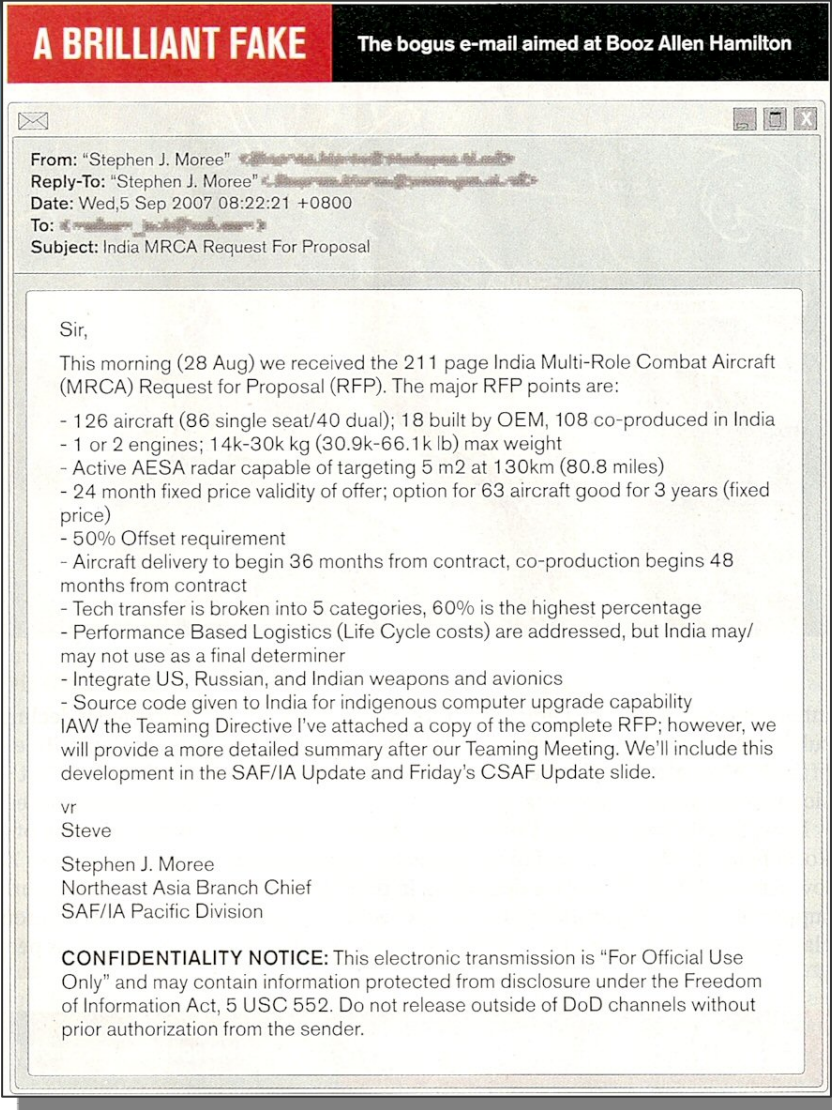
E-SPIONAGE

A BUSINESSWEEK **INVESTIGATION**

The U.S. military created the Internet. Now the Web may be turning against its maker. As America fights to protect itself, we uncover **startling new instances of cyber spies targeting the government** and trace the path of a pernicious attack aimed at defense consultant Booz Allen.

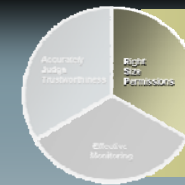
94-99 163
0 73361 18248 7

Right Size Permissions



Right
 Size
 Permissions

TPM



*Right
Size
Permissions*

TPM

JUST-IN-TIME CYBER SECURITY

- Supplants draconian cyber security measures
- Maximizes cyber technological capabilities
- Protects pro-actively (before incident response)
- Reduces the security tax
- Protects company's investment in employees

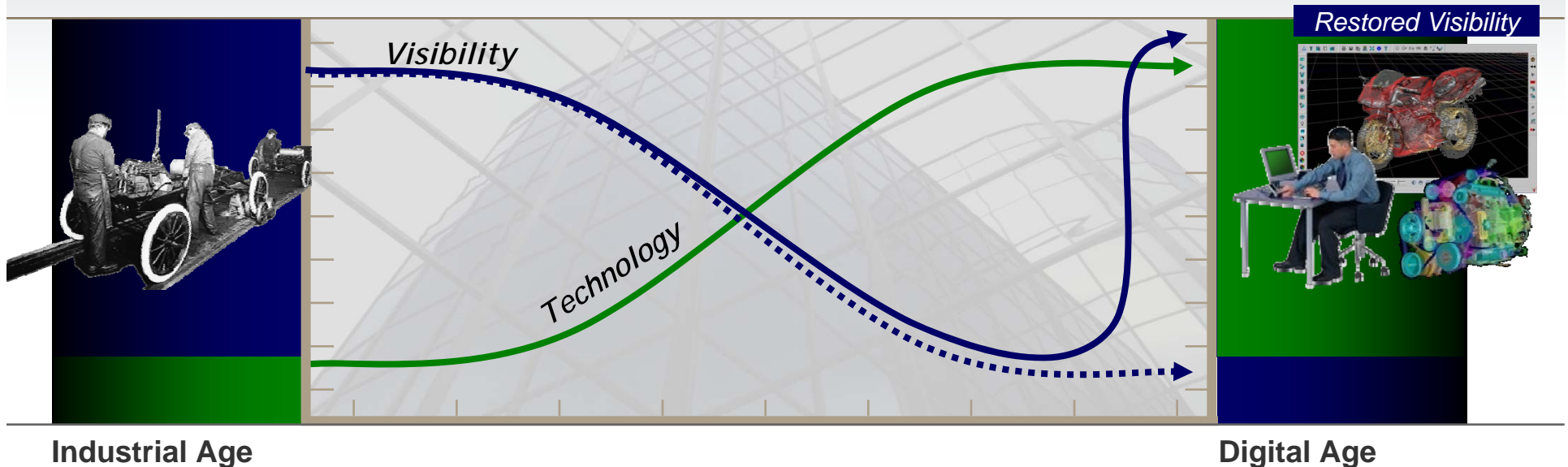
Effective Monitoring

“If your CSO says that you have not been penetrated [no security breaches] you need to get a new CSO”

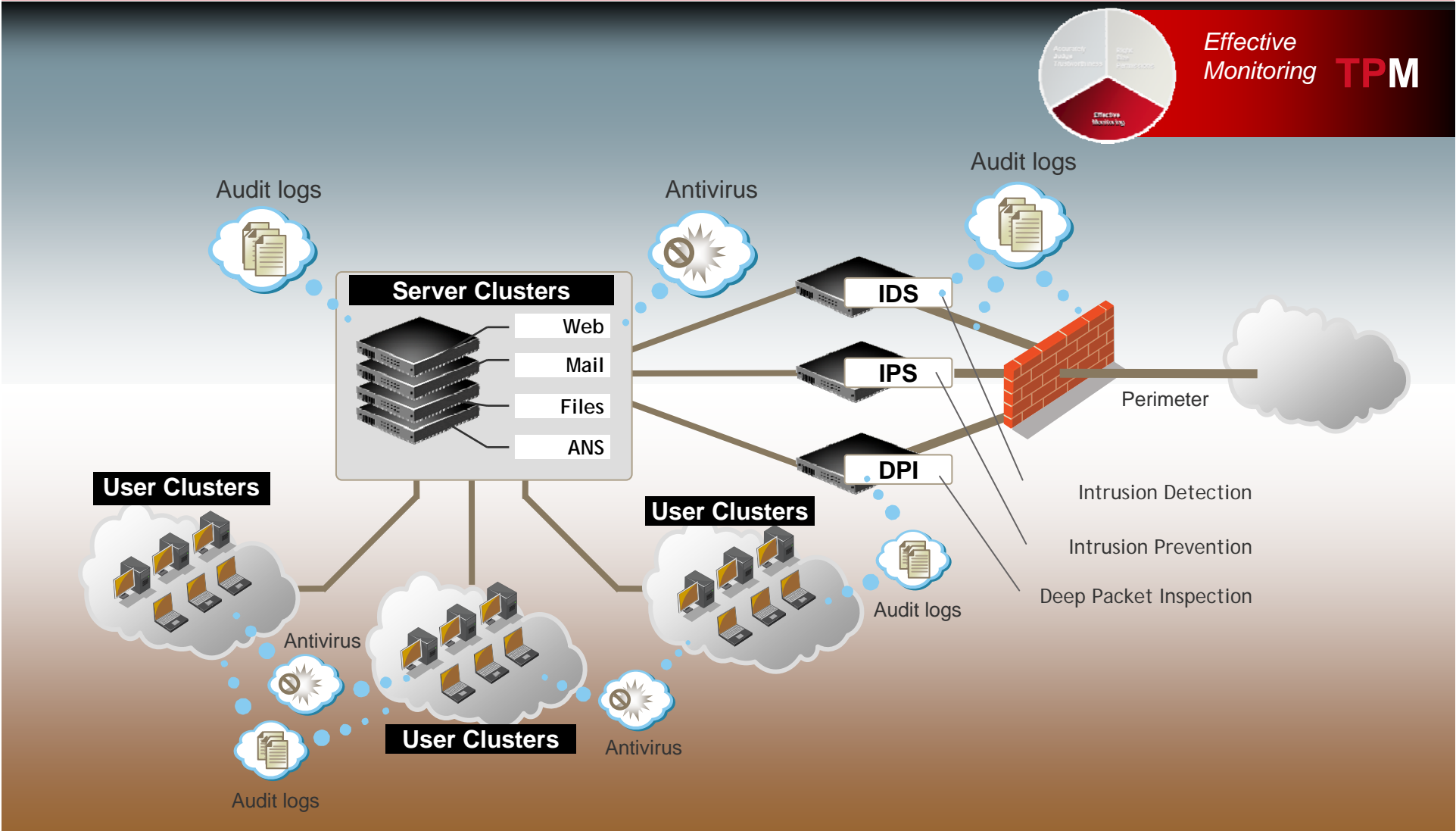


Effective
Monitoring **TPM**

-General Pace (former Chairman, Joint Chiefs of Staff)



Effective Monitoring

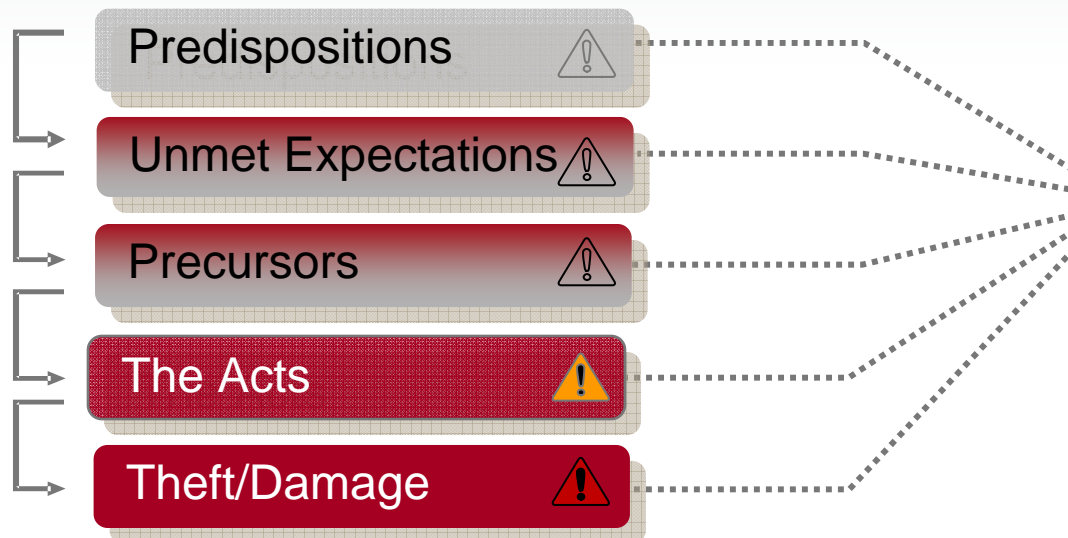


Effective Monitoring

Carnegie Mellon

■ SEI Insider Threat Workshop

– http://www.cert.org/insider_threat/



Effective
Monitoring **TPM**



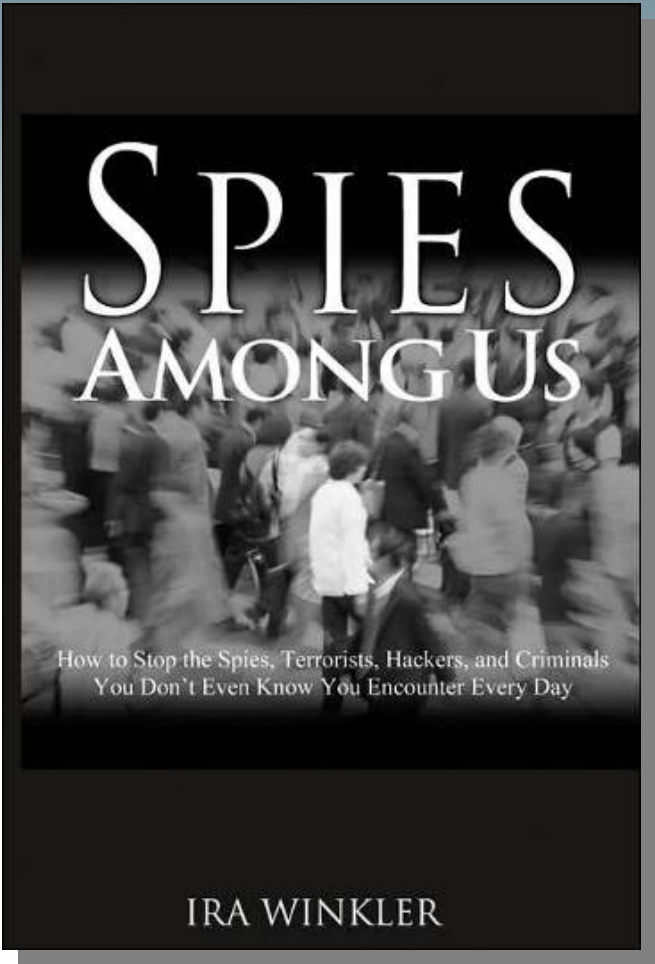
! Technical Observables

Understanding that technology is an enabler

Effective Monitoring



Effective
Monitoring **TPM**



Effective Monitoring



Effective
Monitoring **TPM**

■ **Social Engineering** – Through many avenues

- Email
- Instant Messaging
- Chat Rooms
- Blogs
- Online Gaming
- Online Dating
- Hardware

**Can adversely
affect computer
security**

Effective Monitoring



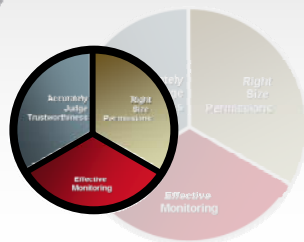
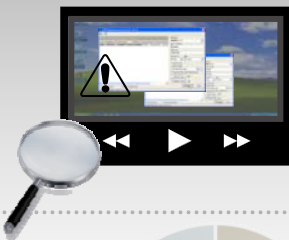
Effective
Monitoring **TPM**

Why is it hard to catch a cyber spy?

Effective Monitoring

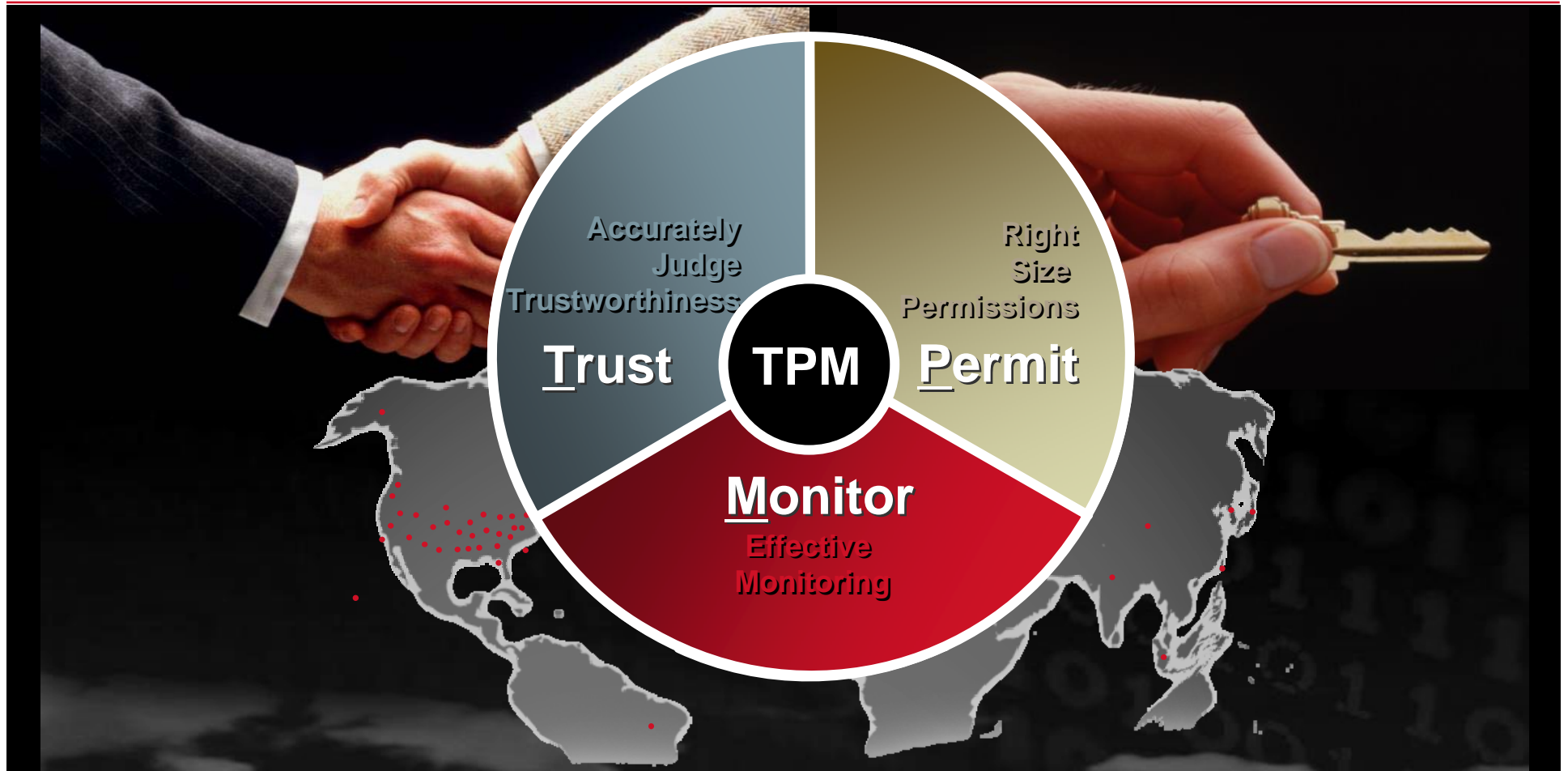


Effective
Monitoring **TPM**



- **Must provide unambiguous and irrefutable attribution for all user activity**
- **Must provide context to discern malicious or benign user activity**
- **Must recreate user activity that is normalized for review by non-technical people**
- **Must support judging trustworthiness and right-sizing permissions**

Protect From Cyber Threats



**If you can't do all of them equally
then you have to compensate in other areas**

Thank you.