#SHAREorg

SHARE
Technology · Connections · Results

Compliance Doesn't Mean Security Achieving Security and Compliance with the latest Regulations and Standards

Paul de Graaff
Chief Strategy Officer
Vanguard Integrity Professionals

March 11, 2014
Session 14976

SHARE in Anaheim

AGENDA

Current Threat Landscape

1

This part of the presentation discusses the current threat landscape and how enterprises are dealing with the challenges.

Regulatory Compliance

2

This part of the presentation discusses the challenges enterprises face with interpreting the regulatory requirement both domestic and international.

Security versus Compliance

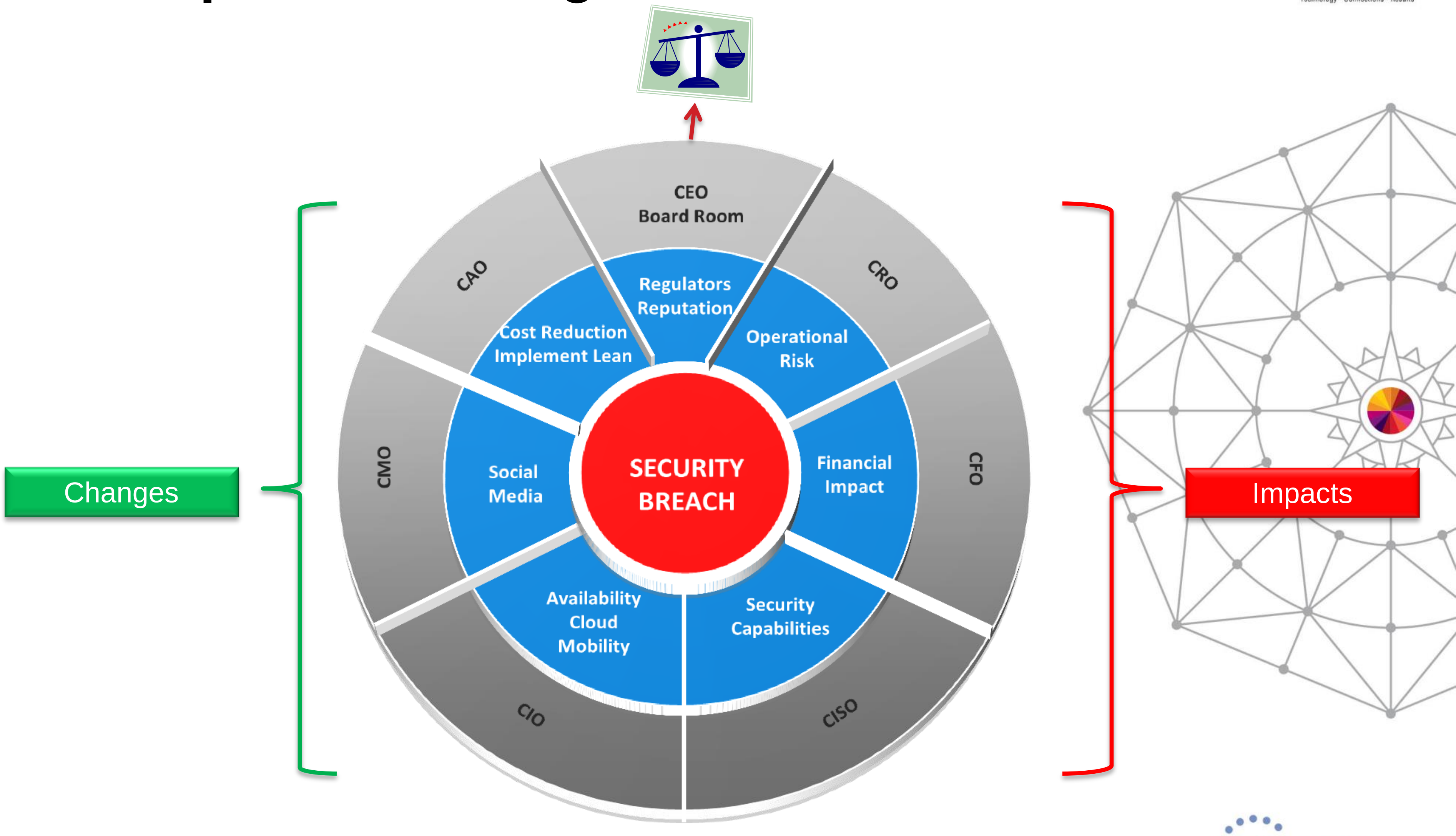
3

This part of the presentation discusses the "Security versus Compliance" debate and provides examples that without security there is no compliance

Setting the Scene

ENTERPRISE CHALLENGES

Enterprise Challenges



Security Challenges

Virtualization/Cloud

- Dynamic Workloads
- Cloud Bursting
- Elasticity

Security Intelligence

- Who wants to harm me
- What are they after?
- What methods are used?

Mobility/BYOD

- Explosion mobile devices
- BYOD seen as cost saver
- Data Loss inevitable

Impact

- Where is my "data"?
- Requires *Dynamic* Security Controls
- High Audit Requirements

Impact

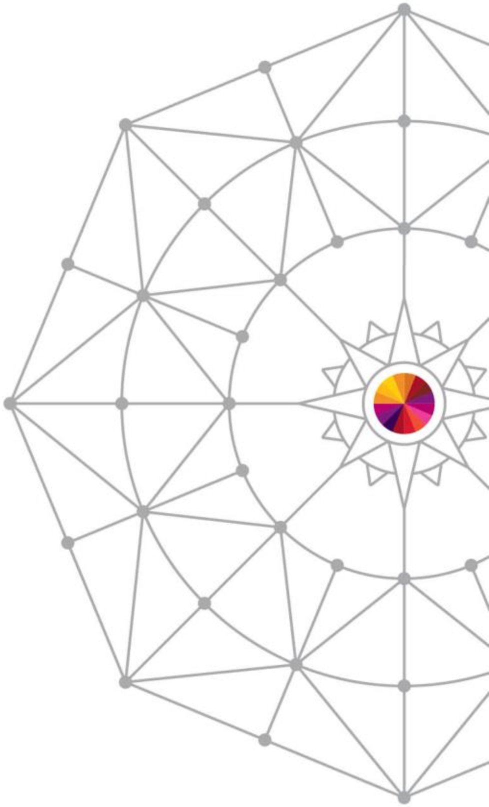
- Where is my IP?
- How is it protected and monitored ?
- Data Loss Prevention (DLP)

Impact

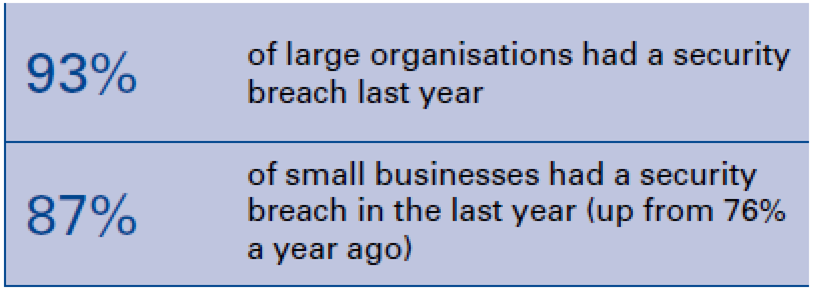
- Requires different set of IT services;
- Accelerates Cloud Adoption (Dropbox etc.)

Impact to Enterprises

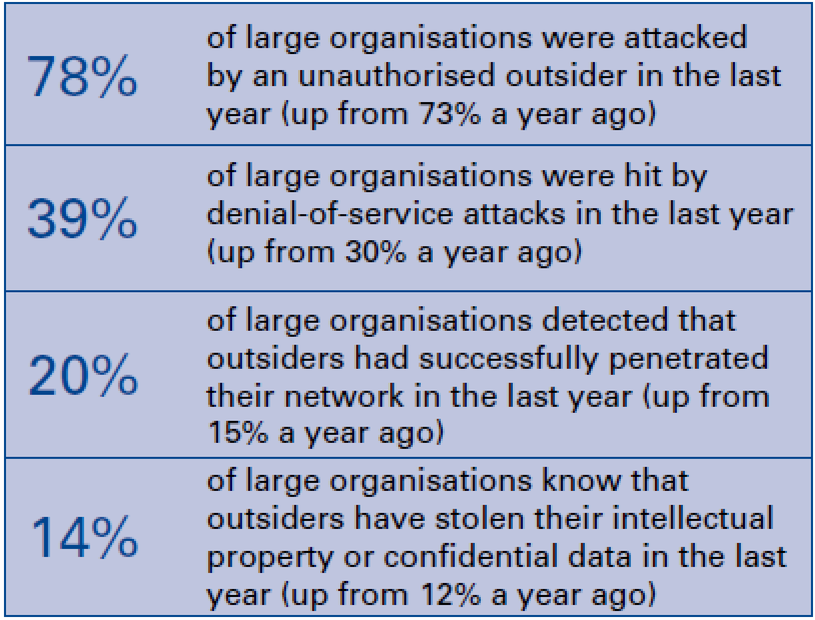
CURRENT THREAT LANDSCAPE



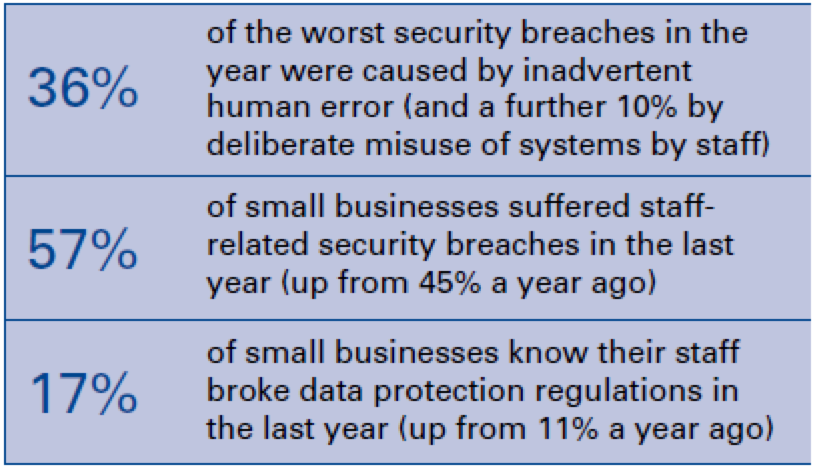
Statistics



93%	of large organisations had a security breach last year
87%	of small businesses had a security breach in the last year (up from 76% a year ago)



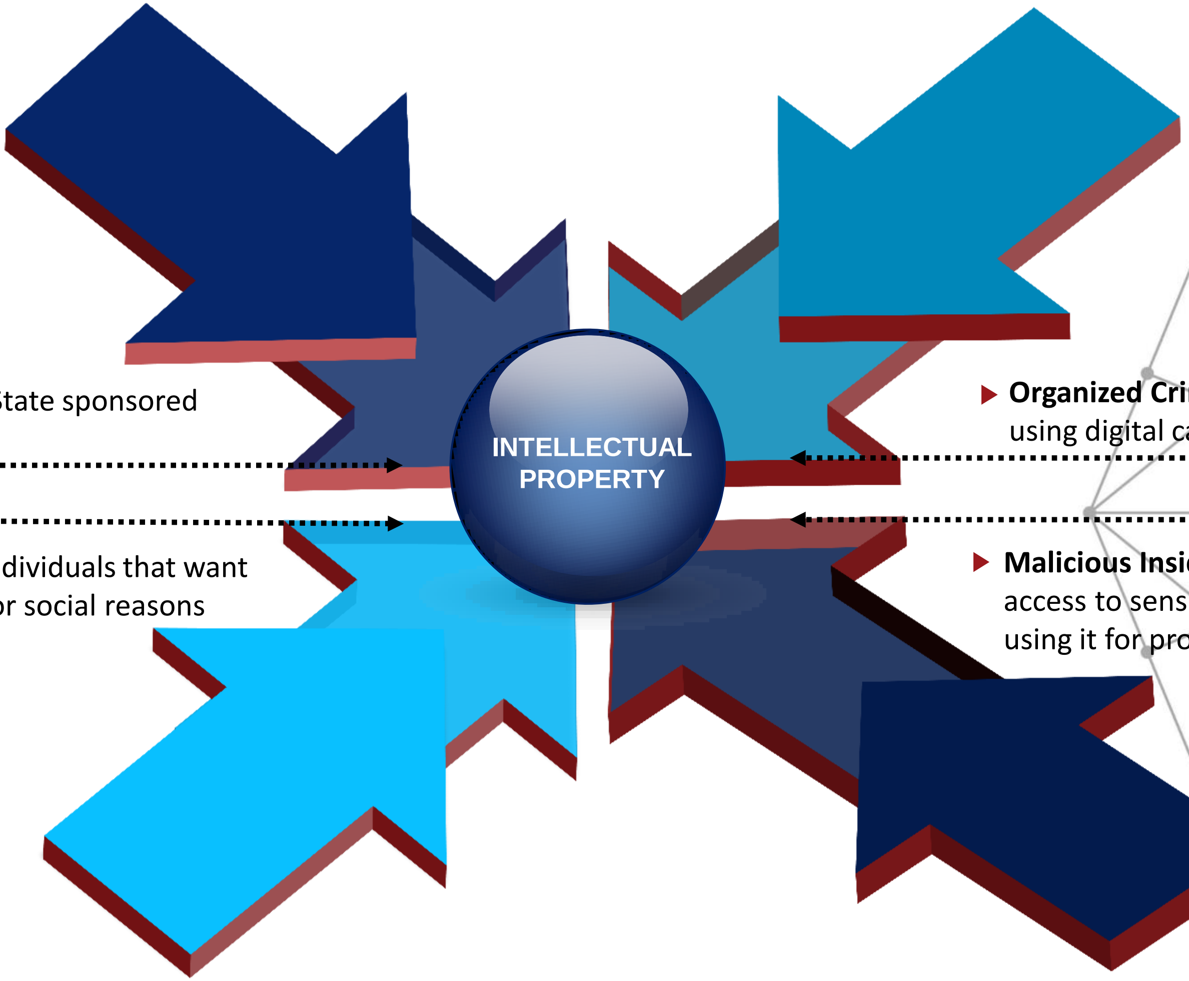
78%	of large organisations were attacked by an unauthorised outsider in the last year (up from 73% a year ago)
39%	of large organisations were hit by denial-of-service attacks in the last year (up from 30% a year ago)
20%	of large organisations detected that outsiders had successfully penetrated their network in the last year (up from 15% a year ago)
14%	of large organisations know that outsiders have stolen their intellectual property or confidential data in the last year (up from 12% a year ago)



36%	of the worst security breaches in the year were caused by inadvertent human error (and a further 10% by deliberate misuse of systems by staff)
57%	of small businesses suffered staff-related security breaches in the last year (up from 45% a year ago)
17%	of small businesses know their staff broke data protection regulations in the last year (up from 11% a year ago)

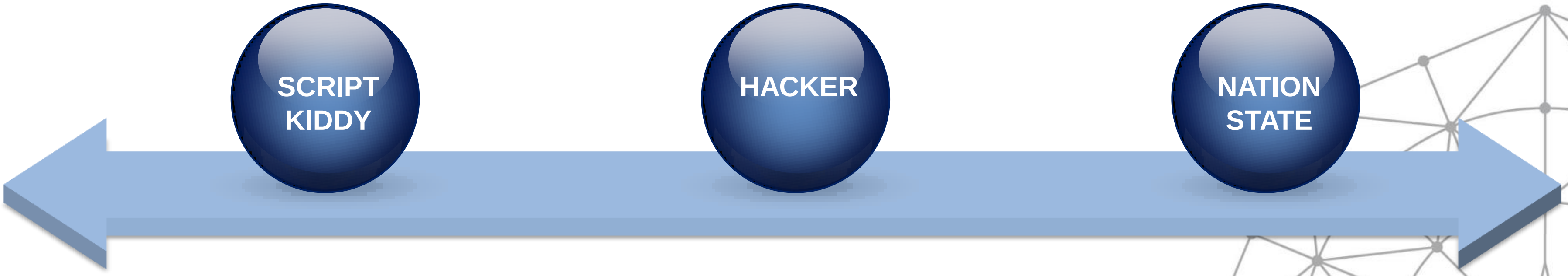
Note: 2013 Information Security Breaches Survey UK Department of Business Innovation & Skills

Threat Actors



- **Nation States:** State sponsored Cyber Warfare
- **“Hacktivism”:** Individuals that want to cause harm for social reasons
- **Organized Crime :** less expensive using digital capabilities than physical
- **Malicious Insider:** people with access to sensitive information and using it for profit or other ideals

Sophistication



SCRIPT KIDDY

HACKER

NATION STATE

Low Level

- **Motivation:** Fun, nothing else to do;
- **Target:** anybody
- **Funding**: None

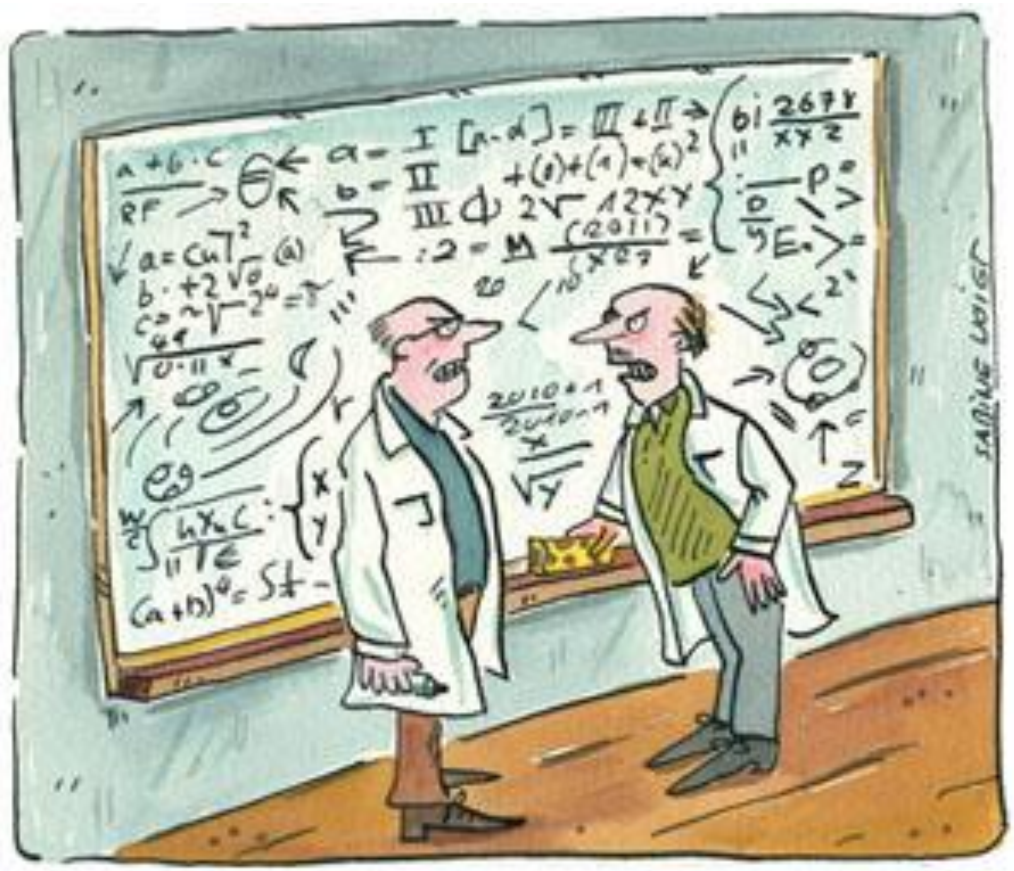
Medium Level

- **Motivation:** Reputation or Social;
- **Target:** Corporations, Governments, High Profile People;
- **Funding**: Limited funds but deep expertise;

High Level

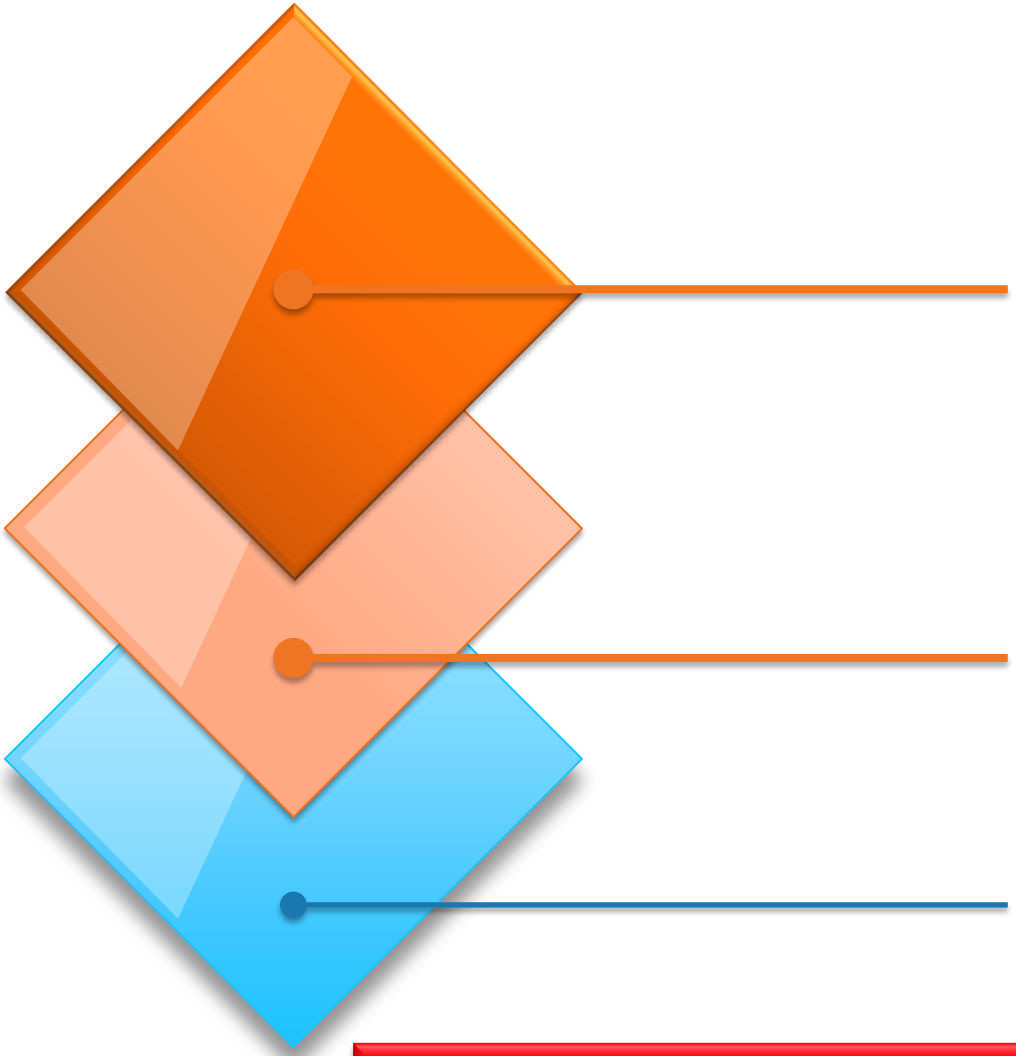
- **Motivation:** Espionage, Influence, Trade Secrets, Inside Information;
- **Target:** Government Agencies, Contractors, Think Tanks, Corporations
- **Funding**: Well funded and deep expertise;

Sophistication



"If you think <u>this</u> is advanced, how do you expect to deal with APT?"

Traditional Security - Set of Layered Defenses



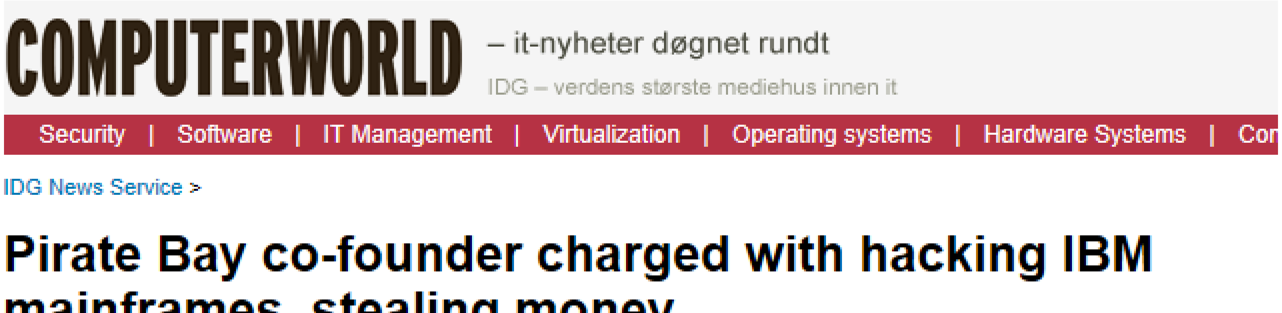
Preventive Controls
FW, IPS, WAF, DDoS, Awareness, Training

Detective Controls
IDS, AV, SIM, VA, etc

Corrective Controls / Response Procedures
IR Plans, BCP, DDoS

Why do we fail to detect / prevent APT type attacks?

Reality versus Ignorance



COMPUTERWORLD – it-nyheter døgnet rundt

IDG – verdens største mediehus innen it

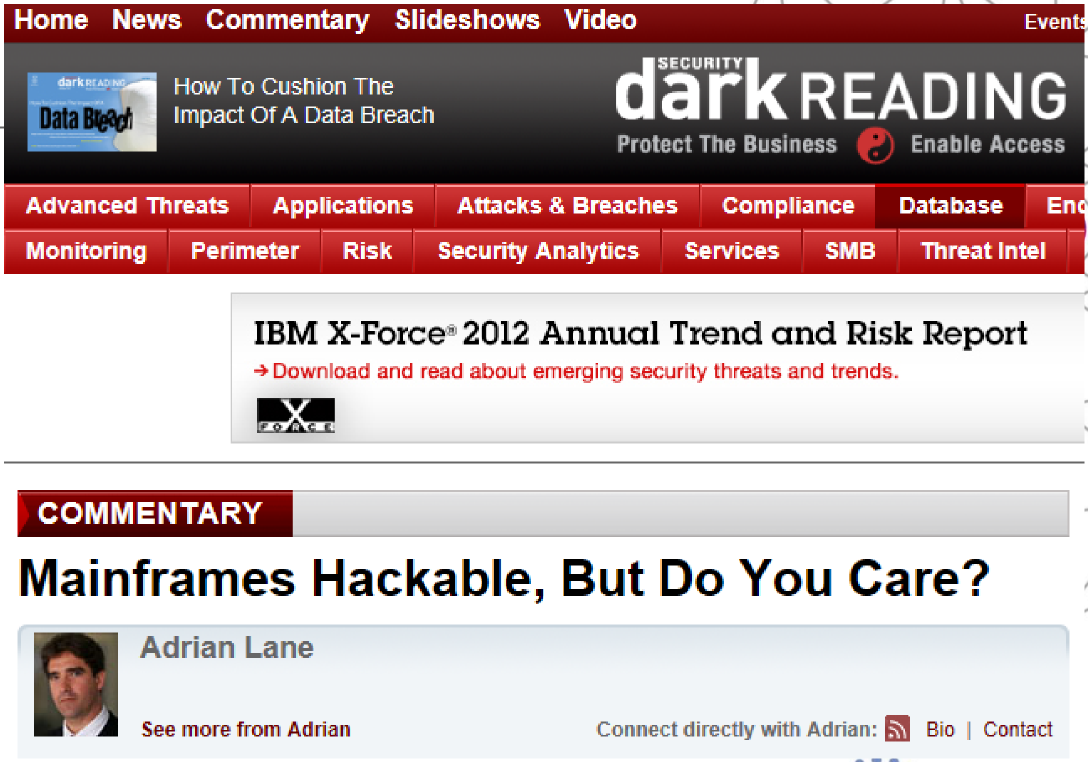
Security | Software | IT Management | Virtualization | Operating systems | Hardware Systems | Cor

IDG News Service >

Pirate Bay co-founder charged with hacking IBM mainframes, stealing money

o Loek Essers
16.04.2013 kl 16:02 | IDG News Service\Amsterdam Bureau

Reality



Home News Commentary Slideshows Video Events

How To Cushion The Impact Of A Data Breach

SECURITY dark READING

Protect The Business Enable Access

Advanced Threats | Applications | Attacks & Breaches | Compliance | Database | Enc

Monitoring | Perimeter | Risk | Security Analytics | Services | SMB | Threat Intel

IBM X-Force® 2012 Annual Trend and Risk Report

→ Download and read about emerging security threats and trends.

COMMENTARY

Mainframes Hackable, But Do You Care?

Adrian Lane

See more from Adrian

Connect directly with Adrian: Bio | Contact

Ignorance

The ever present “checklist”

REGULATORY COMPLIANCE

The World of Compliance

Laws

US State Privacy Laws
EU Privacy Laws
HIPAA
GLBA
FISMA
BASEL II/III
Solvency II

Industry Standards

PCI
FFIEC
HITECH
HITRUST
CSA

Common Practices

COBIT 4.1
ISO 27001
ISO 27002
NIST SP 800-53
ITIL
ISF

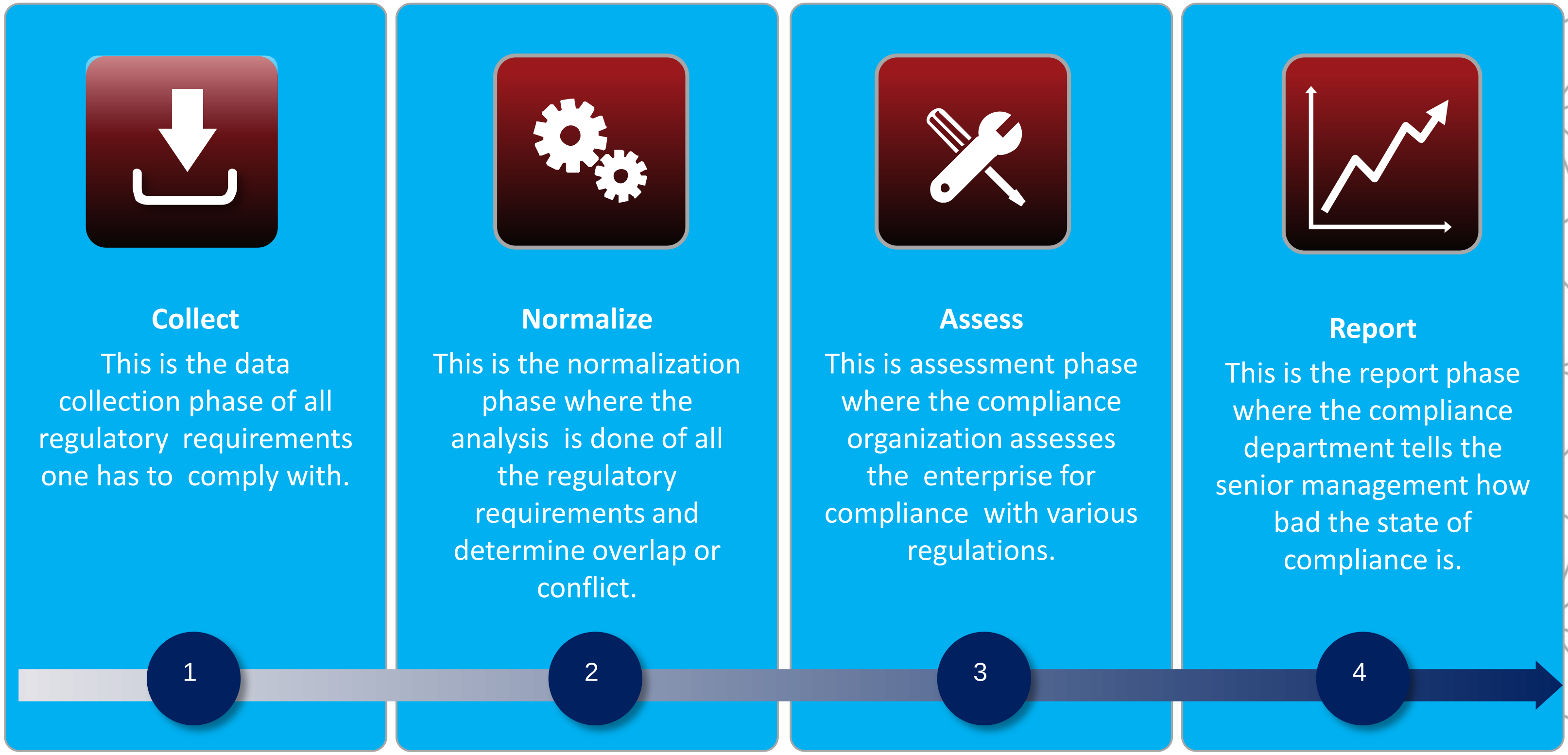
Internal Sources

Internal Documents that state security/privacy requirements (your company policies on security and privacu)

Contractual Requirements

Contractual agreements with 3rd parties you need to comply with. This may be application or system specific

Traditional Regulatory Compliance Approach



Collect

This is the data collection phase of all regulatory requirements one has to comply with.

Normalize

This is the normalization phase where the analysis is done of all the regulatory requirements and determine overlap or conflict.

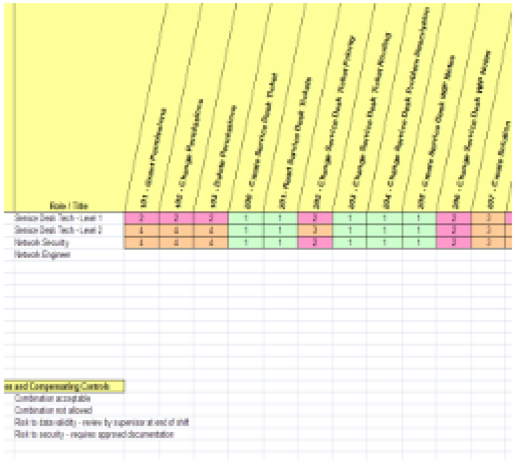
Assess

This is assessment phase where the compliance organization assesses the enterprise for compliance with various regulations.

Report

This is the report phase where the compliance department tells the senior management how bad the state of compliance is.

Compliance Assessment Methodologies

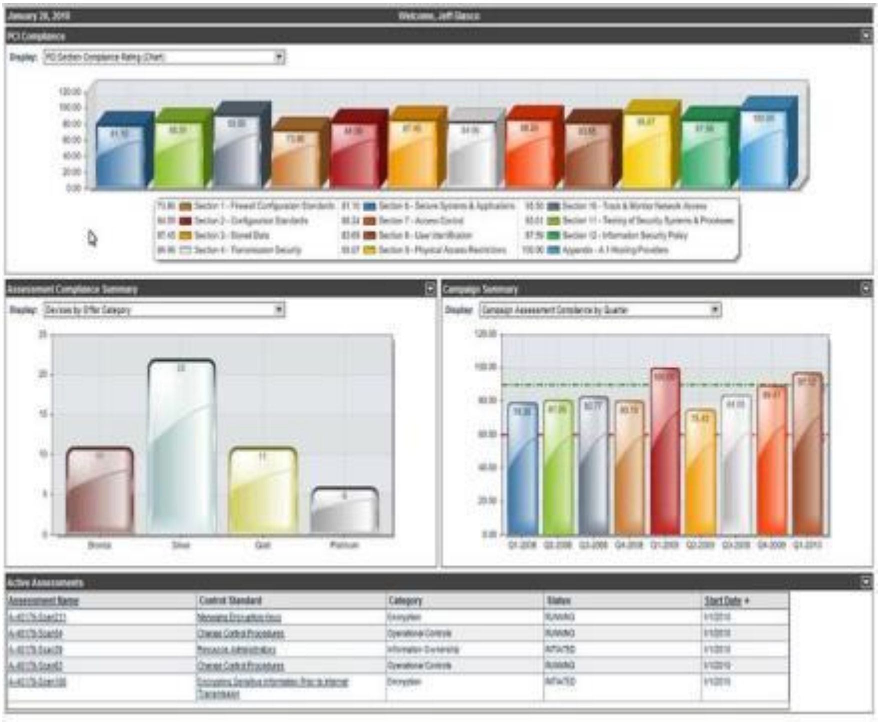


Role / Title	Grant Permissions	Change Permissions	Delete Permissions	Create Service Desk Ticket	Assign Service Desk Ticket	Change Service Desk Ticket Priority	Change Service Desk Ticket Routing	Change Service Desk Problem Description	Create Service Desk WIP Notes	Change Service Desk WIP Notes	Create Escalation
Service Desk Tech - Level 1	2	2	2	1	1	2	1	1	1	2	3
Service Desk Tech - Level 2	4	4	4	1	1	3	1	1	1	2	3
Network Security	4	4	4	1	1	2	1	1	1	2	3
Network Engineer											

es and Compensating Controls

1. Combination acceptable
2. Combination not allowed
3. Risk to data validity - review by supervisor at end of shift
4. Risk to security - requires approved documentation

Maturity



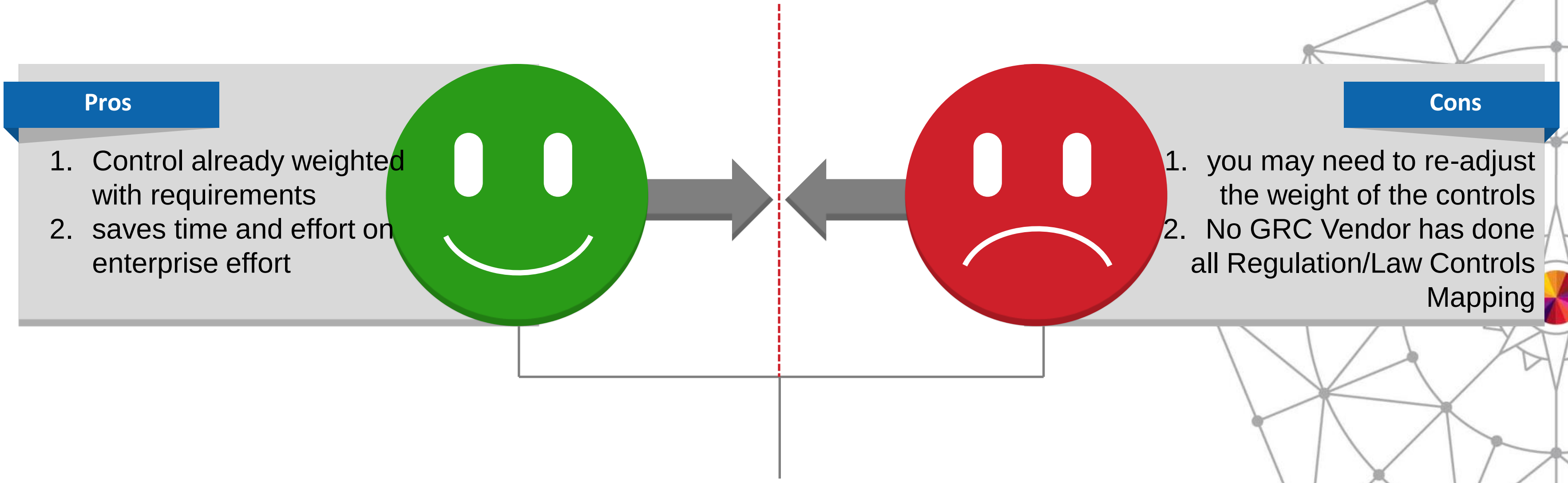
Active Assessments

Assessment Name	Control Standard	Category	Status	Start Date
[illegible]	Managing Encryption Keys	Encryption	RUNNING	1/1/2010
[illegible]	Change Control Procedures	Operational Controls	RUNNING	1/1/2010
[illegible]	Resource Administration	Information Ownership	INITIATED	1/1/2010
[illegible]	Change Control Procedures	Operational Controls	RUNNING	1/1/2010
[illegible]	Encrypting Sensitive Information Prior to Internal Transmission	Encryption	INITIATED	1/1/2010

Spreadsheet Model

GRC Solution

GRC Solution Benefits



Pros

1. Control already weighted with requirements
2. saves time and effort on enterprise effort

Cons

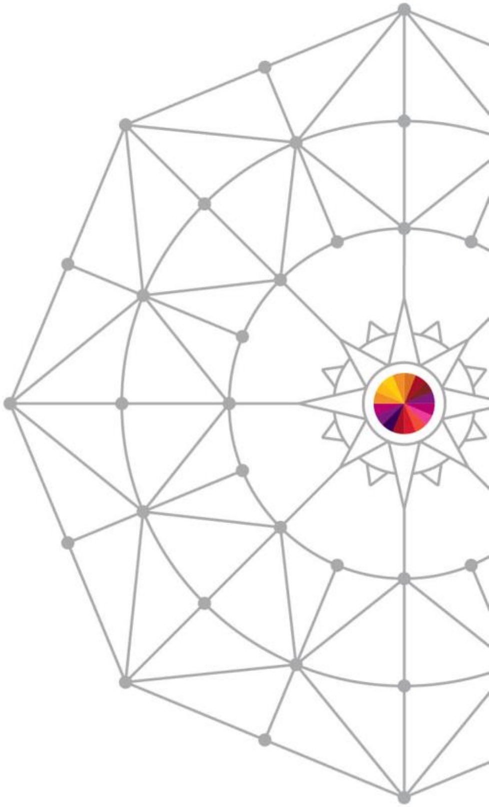
1. you may need to re-adjust the weight of the controls
2. No GRC Vendor has done all Regulation/Law Controls Mapping

Benefits

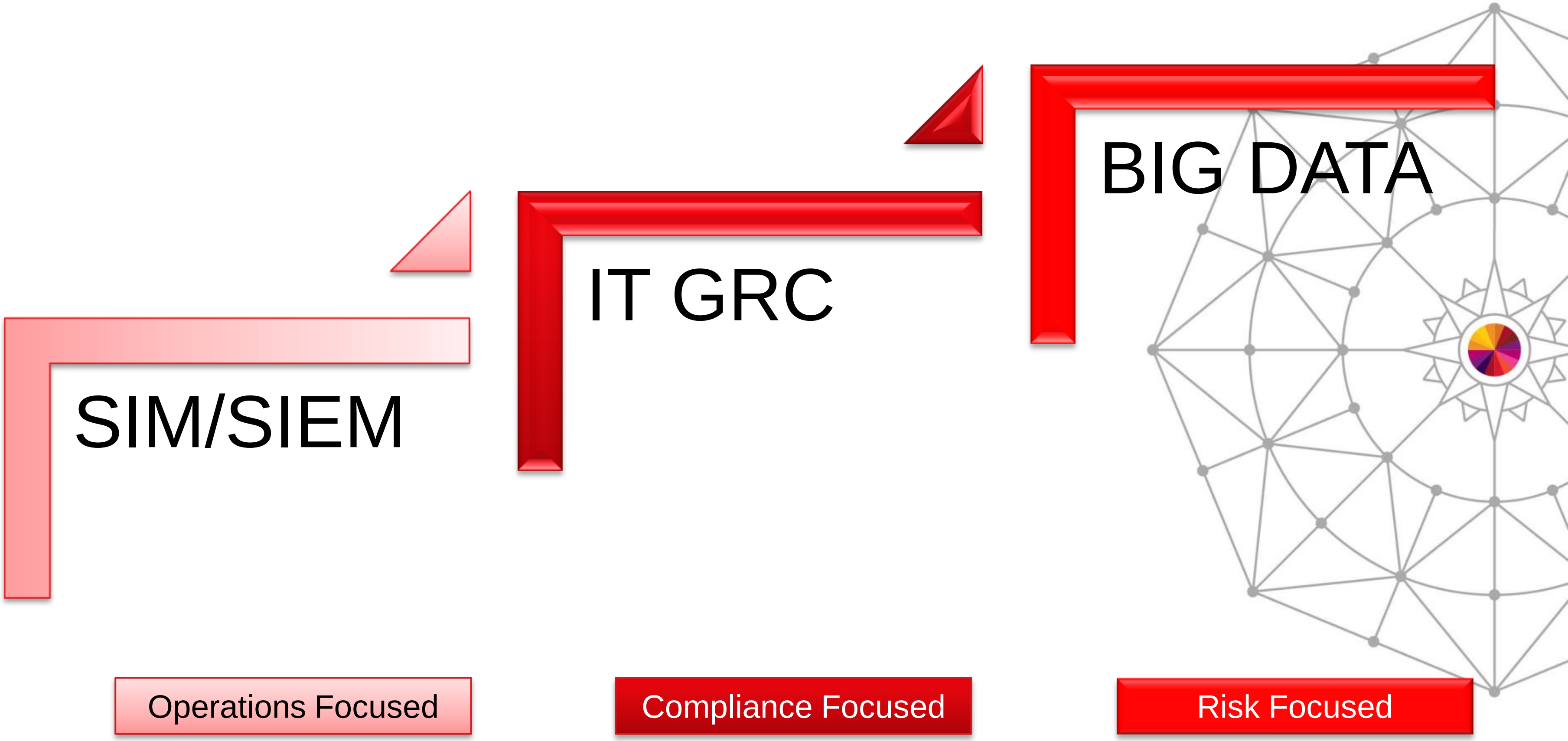
1. Controls Mapping Done With Various Regulations
2. Maintenance of Regulations done by GRC Vendor
3. Web Based Assessment Capabilities
4. Controls Testing (Vendor Integration)

No Compliance without Security

SECURITY VERSUS COMPLIANCE



Evolution of Security



SIM/SIEM

IT GRC

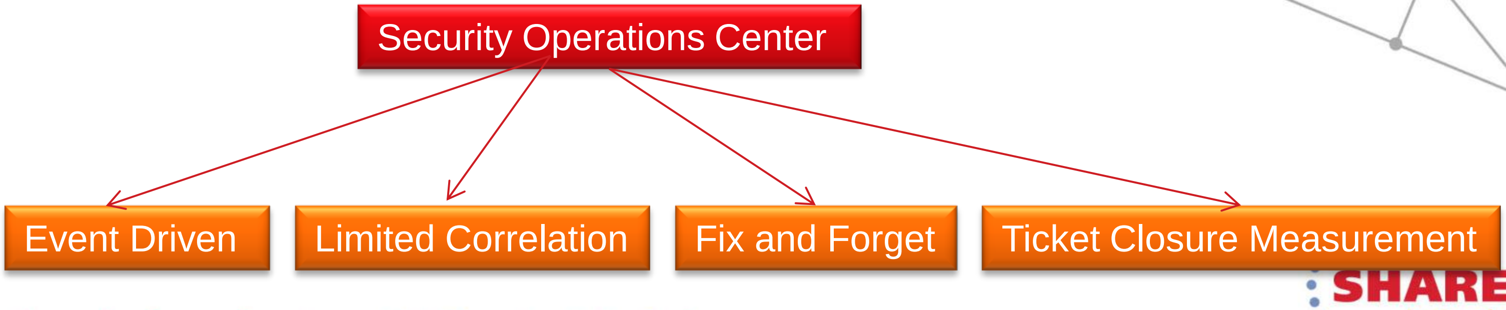
BIG DATA

Operations Focused

Compliance Focused

Risk Focused

Security Operations (SIM/SIEM)



Security Operations Center

Event Driven

Limited Correlation

Fix and Forget

Ticket Closure Measurement

“The Times They Are A-Changing”

Security Operations

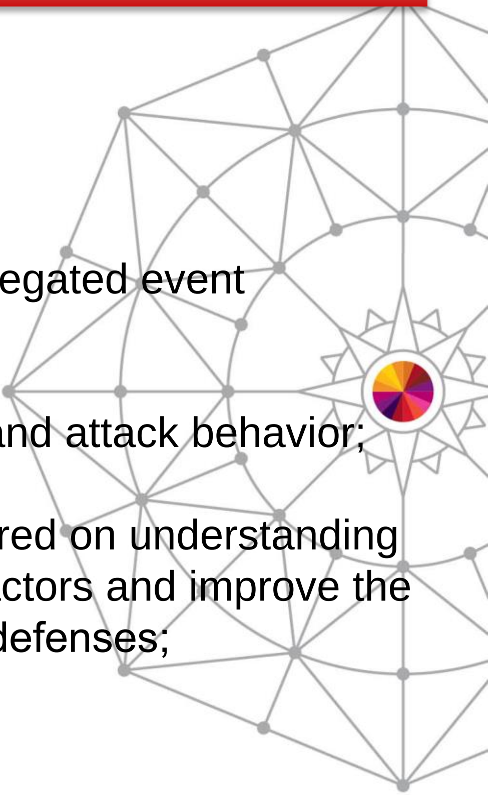
Traditionally:

- (security) event driven;
- limited correlation with other events;
- Fix and Forget;
- Team is/was measured on how many tickets closed within a certain SLA/OLA;

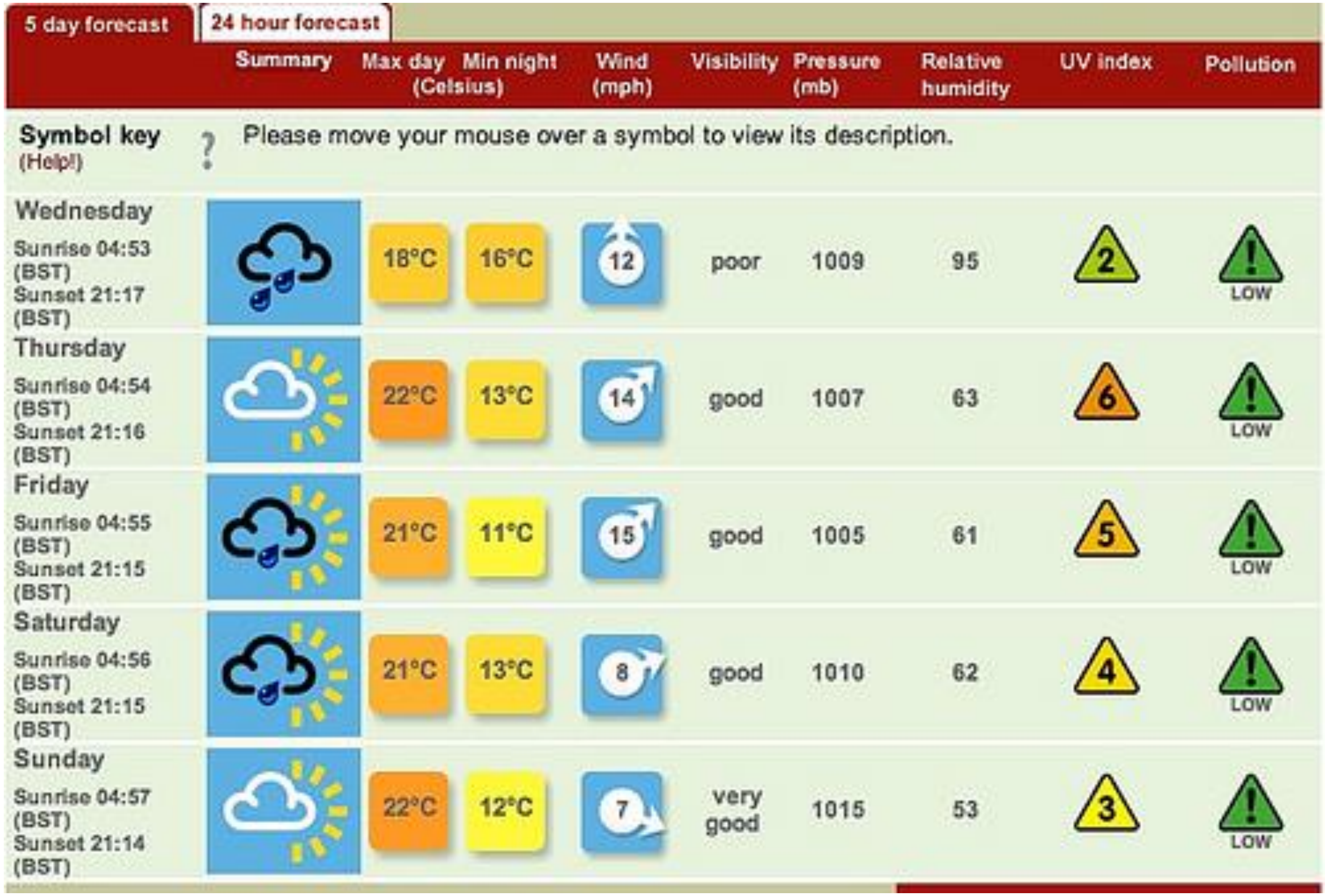
Security Intelligence

Now:

- Contextual aware;
- Correlated and aggregated event information;
- Isolate and understand attack behavior;
- Team is now measured on understanding attack vectors and actors and improve the company’s layered defenses;



Weather Report – Intelligence Example



5 day forecast | 24 hour forecast

Symbol key (Help!) ? Please move your mouse over a symbol to view its description.

	Summary	Max day	Min night	Wind (mph)	Visibility	Pressure (mb)	Relative humidity	UV index	Pollution
		(Celsius)							
Wednesday Sunrise 04:53 (BST) Sunset 21:17 (BST)		18°C	16°C	12	poor	1009	95	2	LOW
Thursday Sunrise 04:54 (BST) Sunset 21:16 (BST)		22°C	13°C	14	good	1007	63	6	LOW
Friday Sunrise 04:55 (BST) Sunset 21:15 (BST)		21°C	11°C	15	good	1005	61	5	LOW
Saturday Sunrise 04:56 (BST) Sunset 21:15 (BST)		21°C	13°C	8	good	1010	62	4	LOW
Sunday Sunrise 04:57 (BST) Sunset 21:14 (BST)		22°C	12°C	7	very good	1015	53	3	LOW

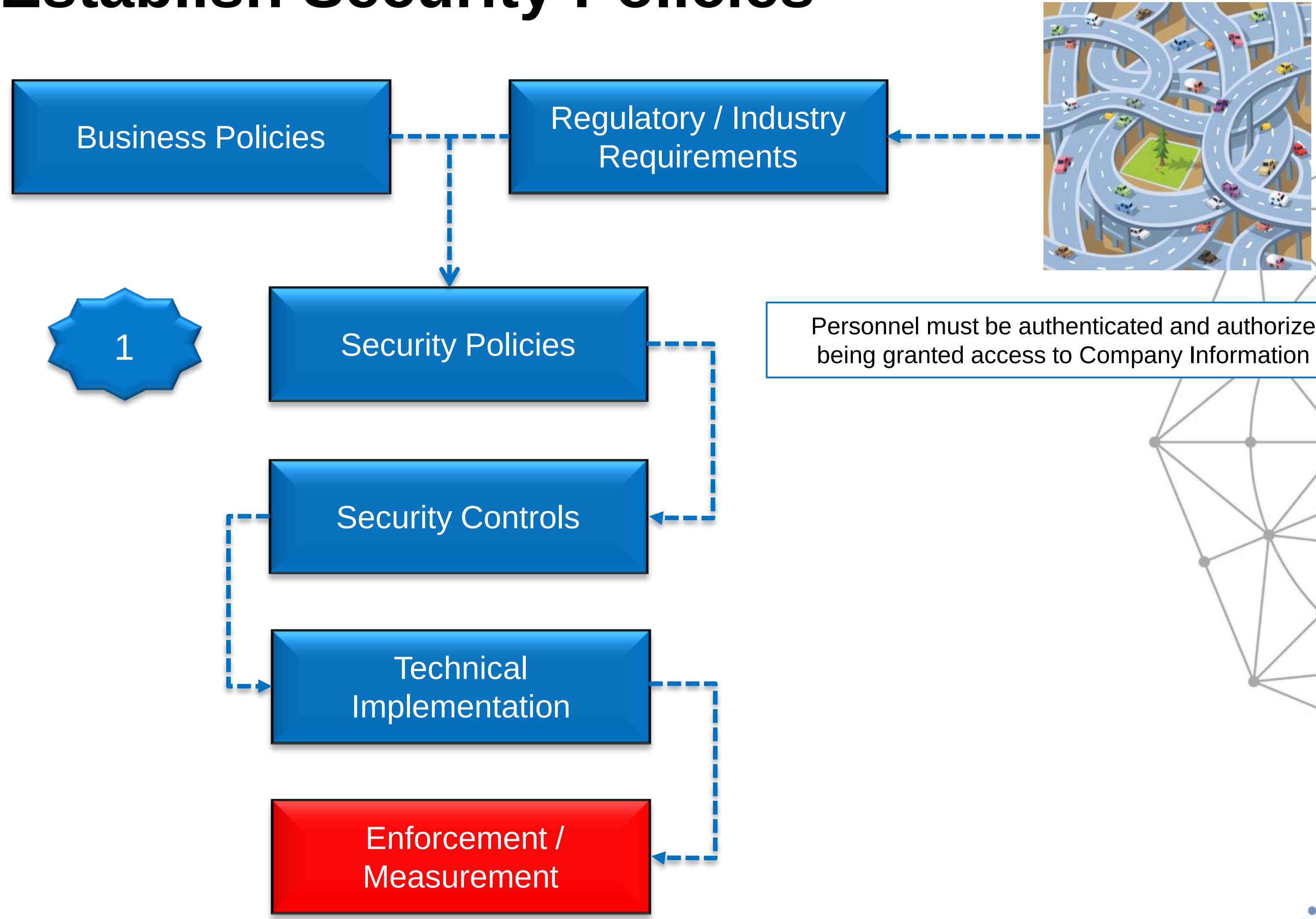
Most of us produce at best yesterday's weather report as it relates to security !!!!

Dashboard Opinions

DOGBERT CONSULTS
YOU NEED A DASH-BOARD APPLICATION TO TRACK YOUR KEY METRICS.
scottadams@aol.com
www.dilbert.com
THAT WAY YOU'LL HAVE MORE DATA TO IGNORE WHEN YOU MAKE YOUR DECISIONS BASED ON COMPANY POLITICS.
© 2007 Scott Adams, Inc./Dist. by UFS, Inc.
WILL THE DATA BE ACCURATE?
OKAY, LET'S PRETEND THAT MATTERS.

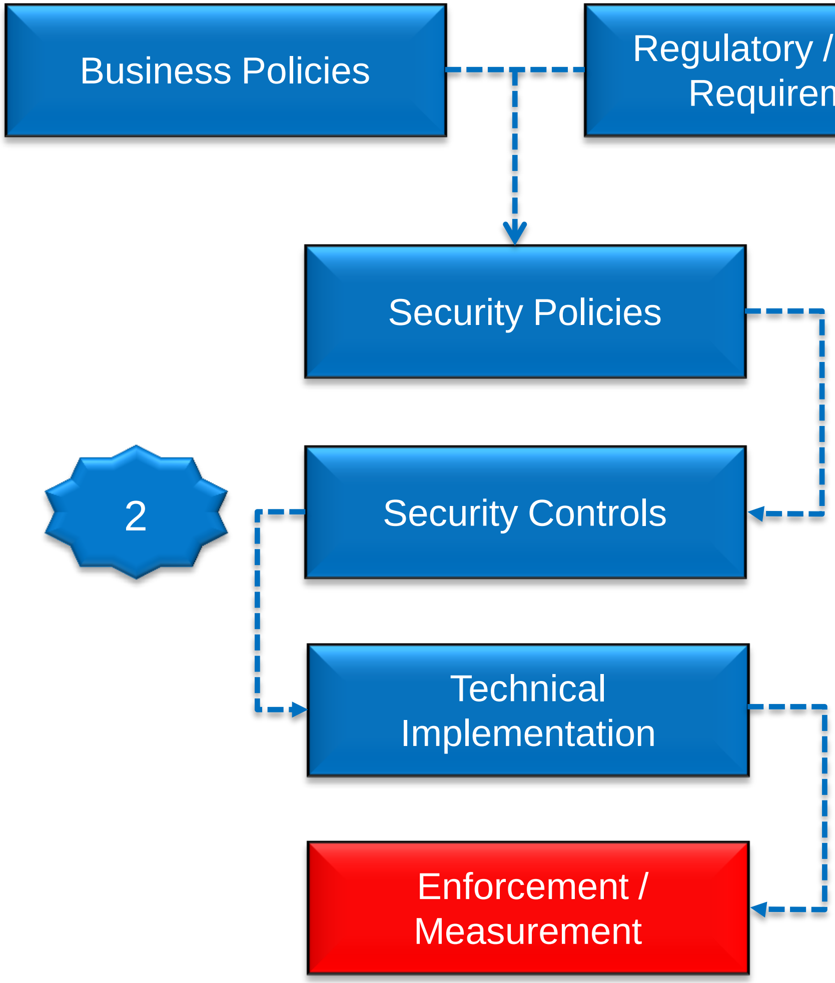
© Scott Adams, Inc./Dist. by UFS, Inc.

Security versus Compliance - STEP 1
Establish Security Policies



Personnel must be authenticated and authorized prior to be being granted access to Company Information Resources.

Security versus Compliance - STEP 2 Define related Security Controls



Business Policies

Regulatory / Industry Requirements

Security Policies

2

Security Controls

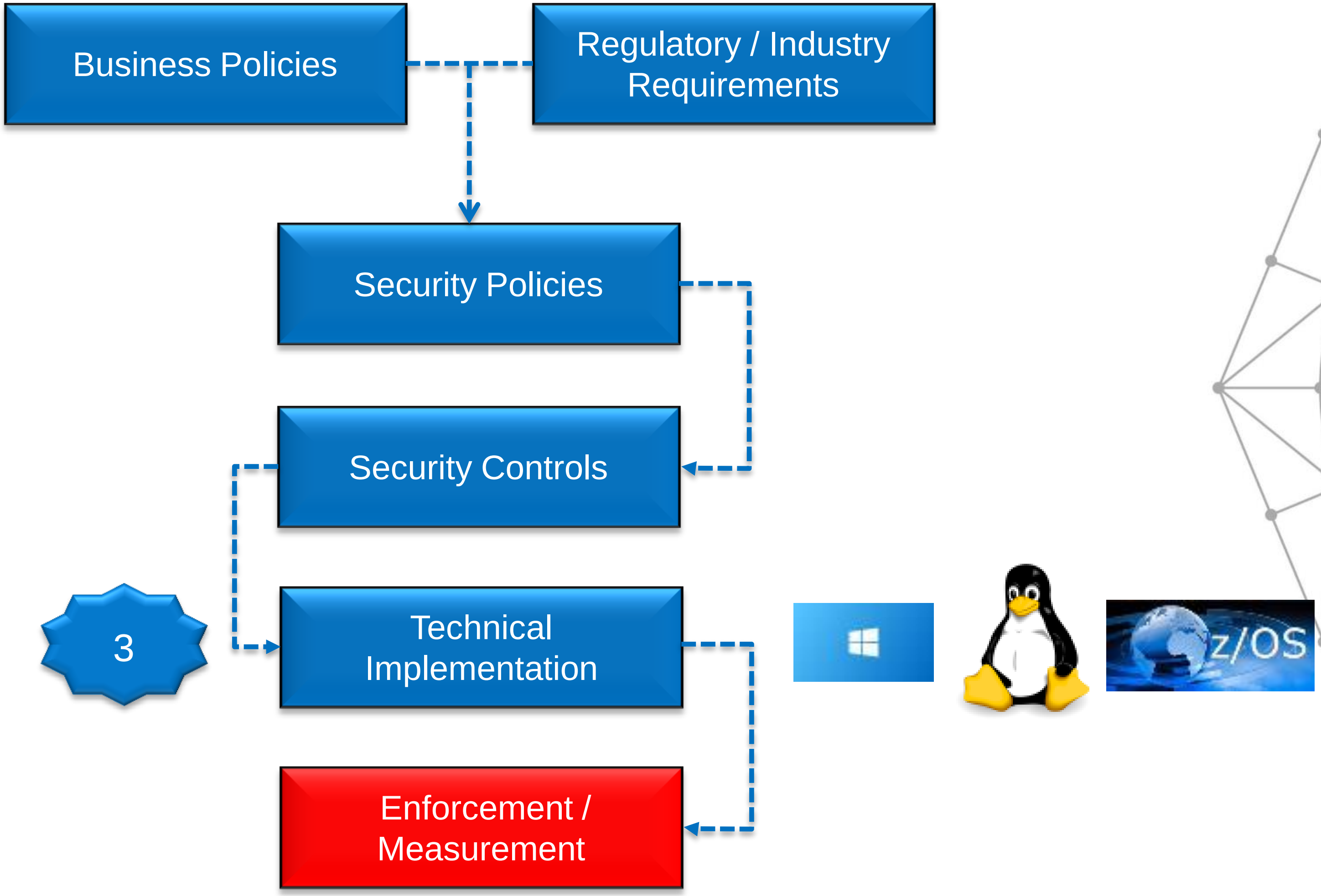
Technical Implementation

Enforcement / Measurement

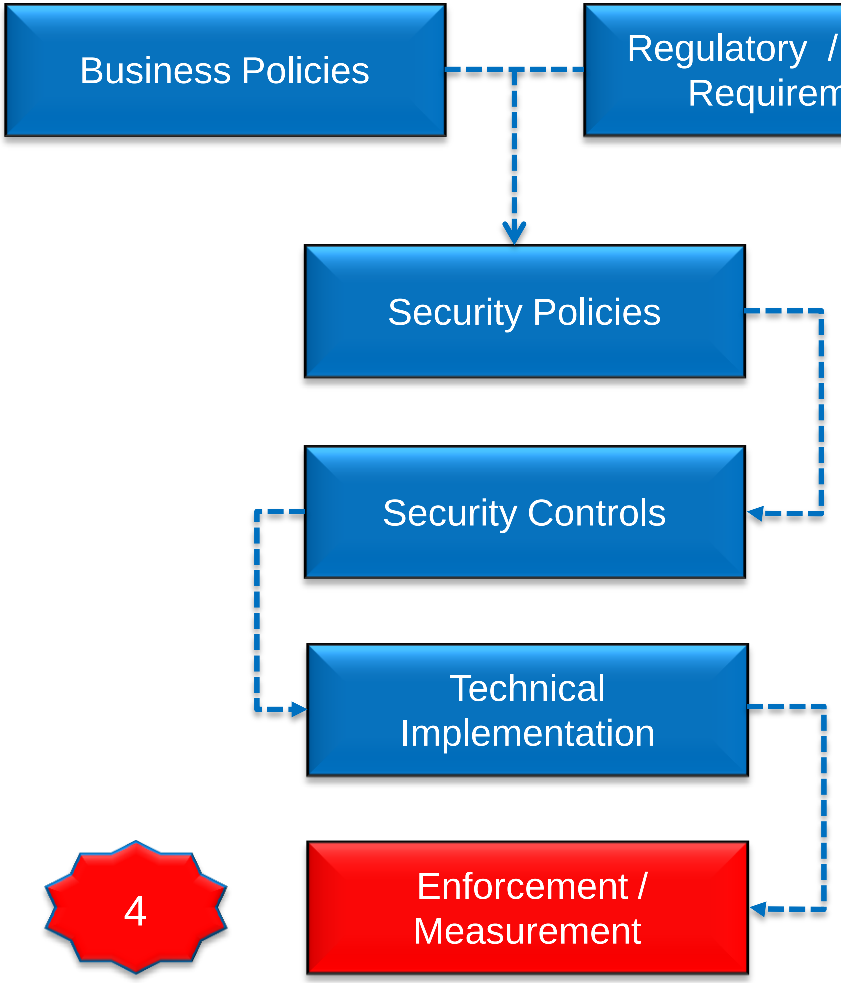
Access to Company Information Resources should be controlled by unique User IDs and use the following authentication methods: passwords, tokens or biometrics based on the risk identified

Passwords should be eight characters in length and contain at a minimum lower and upper case characters and one(1) numeric

Security versus Compliance - STEP 3 Implement Technical Controls



Security versus Compliance - STEP 4
Enforce Policy / Measure Compliance



Business Policies

Regulatory / Industry Requirements

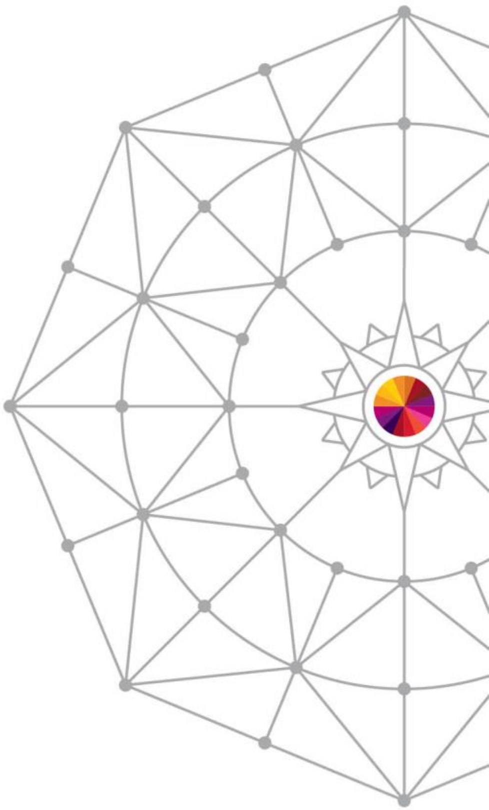
Security Policies

Security Controls

Technical Implementation

4

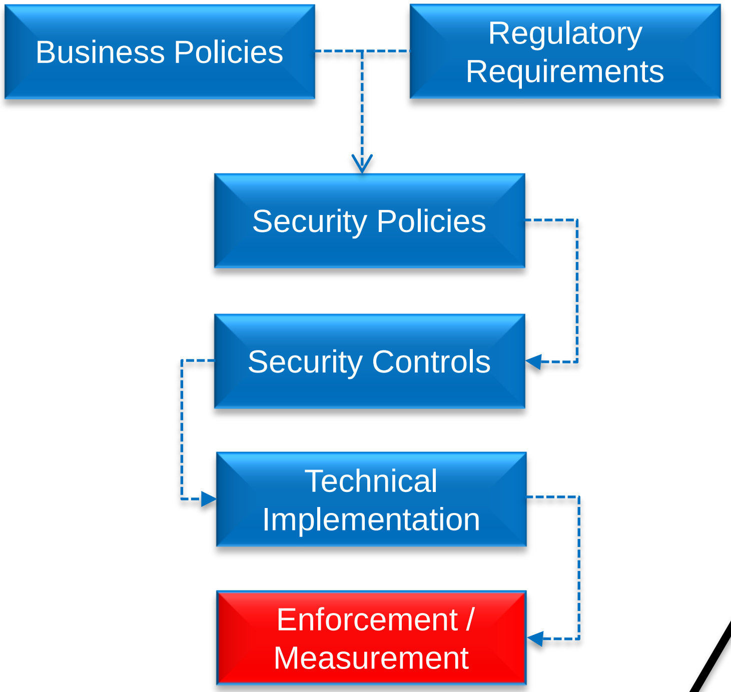
Enforcement / Measurement



Policy Enforcement Process

Change Management (ITIL) Process

Security versus Compliance
Auditors / Regulators


Business Policies

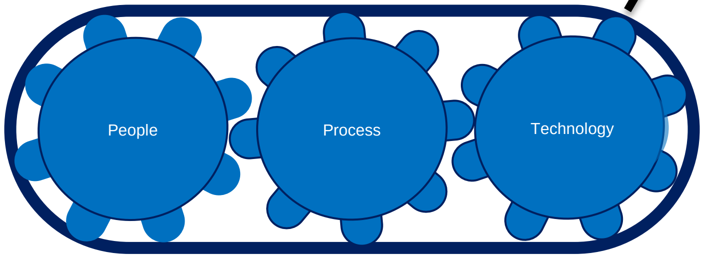
Regulatory Requirements

Security Policies

Security Controls

Technical Implementation

Enforcement / Measurement


People

Process

Technology

Data Access Governance Process
PCI Example

DATA LIFECYCLE PROCESS DIAGRAM

1

Discover
The first phase of the data lifecycle process is to discover where the PCI data in question resides;

2

Asses
The second phase of the data life cycle is to assess the protection of the PCI data discovered in Phase I;

3

Remediate
The third phase of the data life cycle is to remediate ACL's concerns with the PCI data protection assessed in Phase II

4

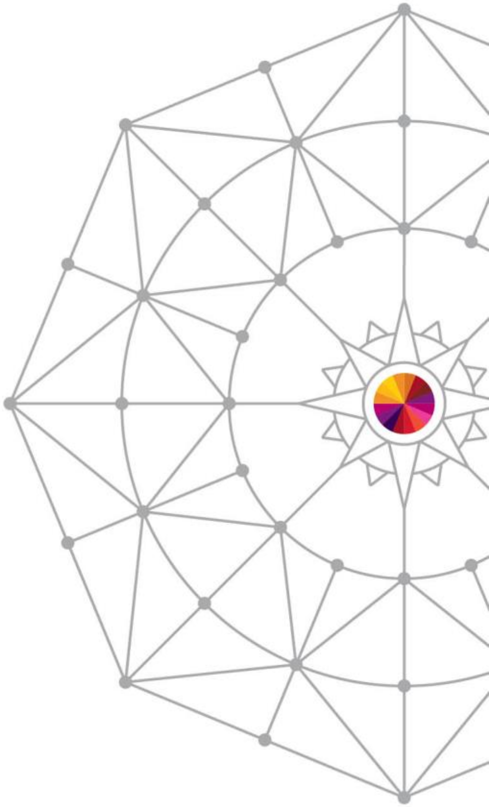
Enforce
The fourth phase of the data life cycle is to ensure no unauthorized changes are made to ACL's for the PCI data set profiles.

5

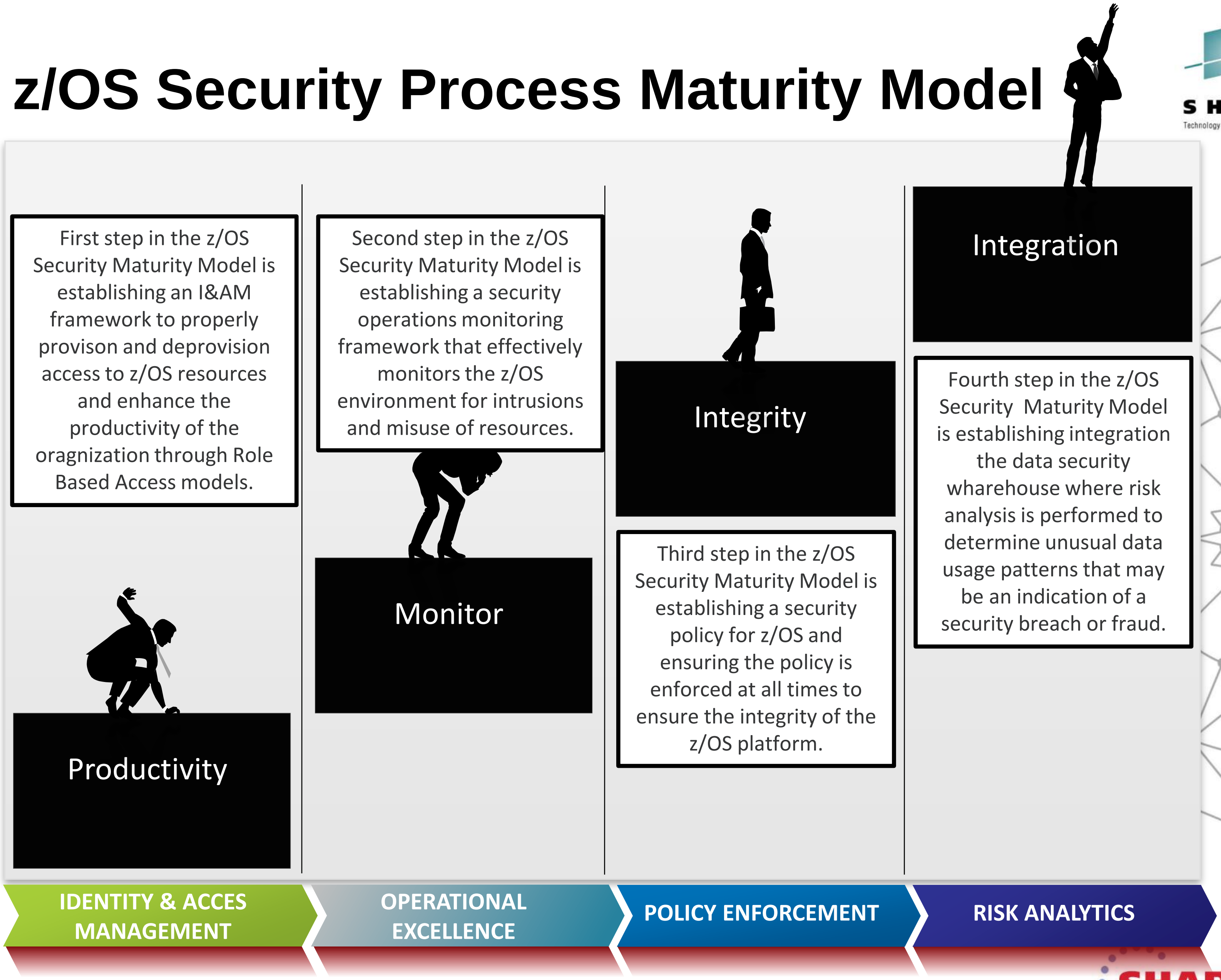
Monitor
The fifth phase of the data life cycle is the ongoing monitoring of access to the PCI data.

Wrapup

SECURITY VERSUS COMPLIANCE



z/OS Security Process Maturity Model



First step in the z/OS Security Maturity Model is establishing an I&AM framework to properly provison and deprovision access to z/OS resources and enhance the productivity of the oragnization through Role Based Access models.

Productivity

IDENTITY & ACCES MANAGEMENT

Second step in the z/OS Security Maturity Model is establishing a security operations monitoring framework that effectively monitors the z/OS environment for intrusions and misuse of resources.

Monitor

OPERATIONAL EXCELLENCE

Integrity

Third step in the z/OS Security Maturity Model is establishing a security policy for z/OS and ensuring the policy is enforced at all times to ensure the integrity of the z/OS platform.

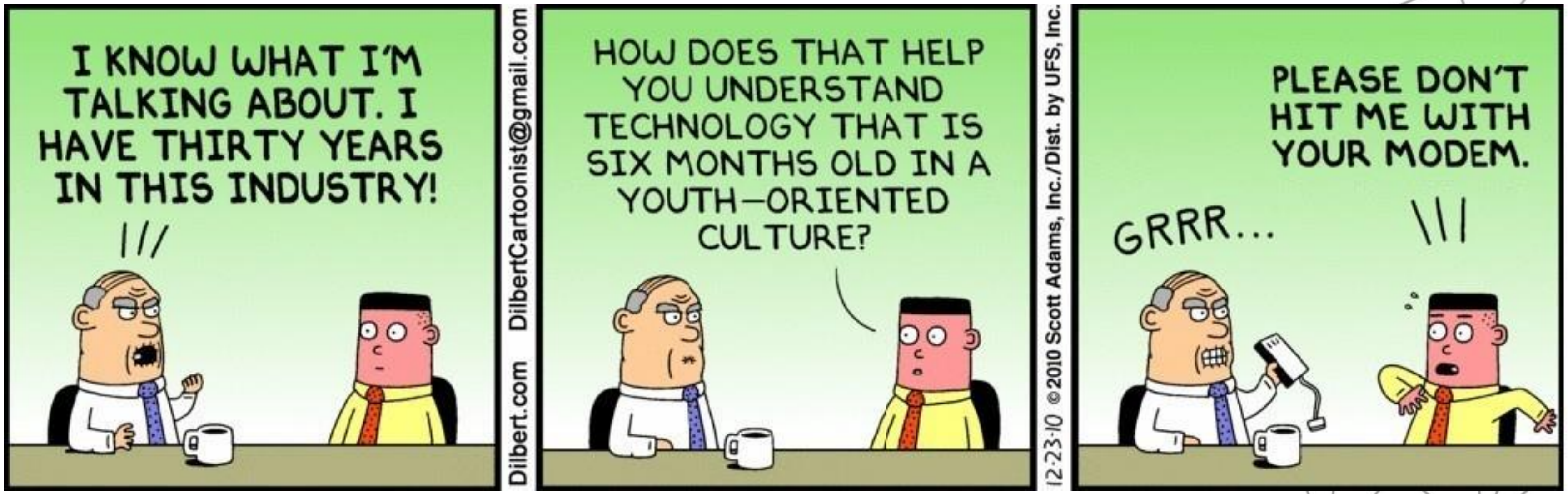
POLICY ENFORCEMENT

Integration

Fourth step in the z/OS Security Maturity Model is establishing integration the data security wharehouse where risk analysis is performed to determine unusual data usage patterns that may be an indication of a security breach or fraud.

RISK ANALYTICS

I must be getting old ……


I KNOW WHAT I'M TALKING ABOUT. I HAVE THIRTY YEARS IN THIS INDUSTRY!
Dilbert.com DilbertCartoonist@gmail.com
HOW DOES THAT HELP YOU UNDERSTAND TECHNOLOGY THAT IS SIX MONTHS OLD IN A YOUTH—ORIENTED CULTURE?
12·23·10 ©2010 Scott Adams, Inc./Dist. by UFS, Inc.
GRRR...
PLEASE DON'T HIT ME WITH YOUR MODEM.

Questions & Answers

Thank You
Call us at 800-794-0014 or email us at info@go2vanguard.com