USING A RISK-BASED APPROACH TO ALIGN SECURITY ARCHITECTURE WITH THE BUSINESS FOR DLP DEPLOYMENT

Jeff Bardin – VP, CSO
ITSolutions
jeff.bardin@itsolutions-llc.com

AGENDA

- What is Security Architecture
- Model for Security Architecture Development
- Role & Benefits of Enterprise Security Architecture
- Defense in Depth – A Military Comparison
- Sand Table Exercise
- What to Do Next

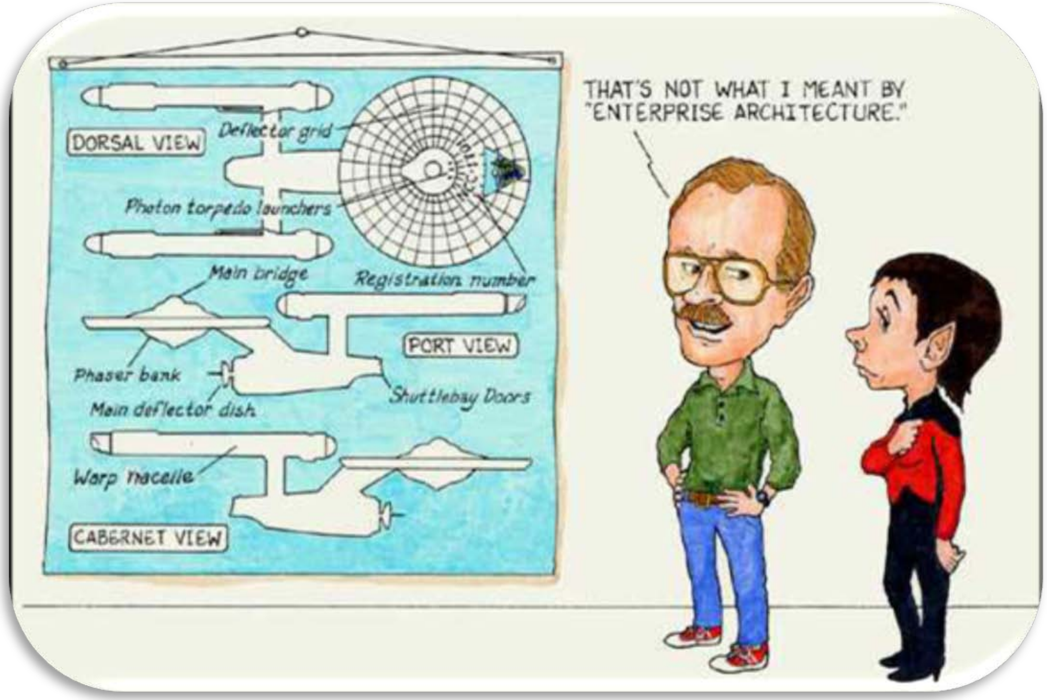
ITSolutions LLC
Interactive Technology Solutions

What is Security Architecture

WHAT IS SECURITY ARCHITECTURE?
WHO IS A SECURITY ARCHITECT?

- The art and science of designing and supervising the construction of business systems, usually business information systems that are:
  - Free from danger and damage;
  - Free from fear and care;
  - In safe custody;
  - Not likely to fail;
  - Able to be replied upon;
  - Safe from attack.

- A person qualified to design and supervise the construction of secure business systems, usually secure business information systems (using a risk-based approach).



THAT NEED TO BE ASKED

I KEEP six honest serving-men
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who.
I send them over land and sea,
I send them east and west;
But after they have worked for me,
I give them all a rest.

I let them rest from nine till five,
For I am busy then,
As well as breakfast, lunch, and tea,
For they are hungry men.
But different folk have different views;
I know a person small-
She keeps ten million serving-men,
Who get no rest at all!

She sends 'em abroad on her own affairs,
From the second she opens her eyes-
One million Hows, two million Wheres,
And seven million Whys!

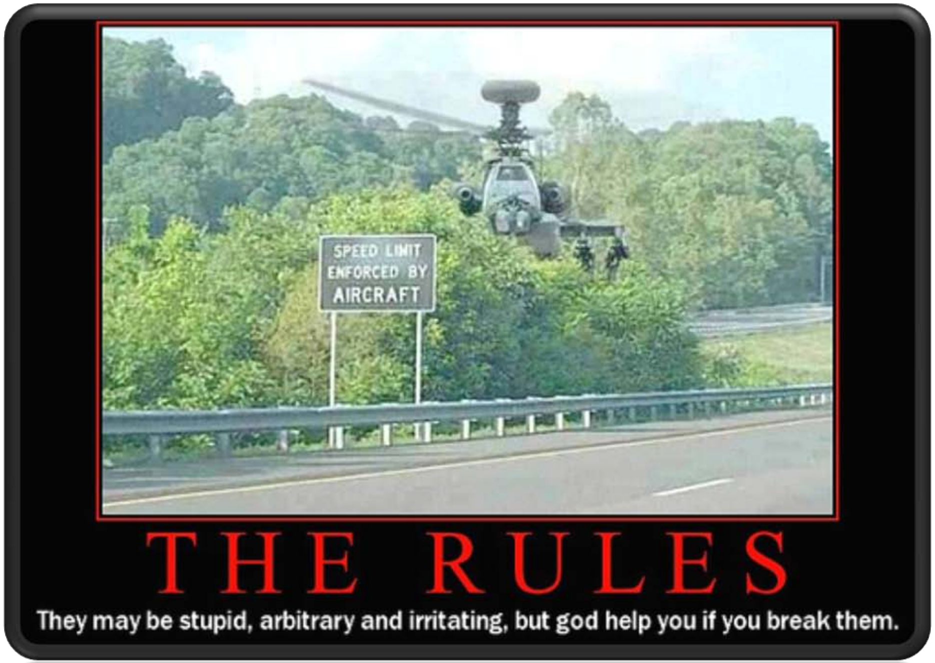
Kipling

- What type of information system is it and for what will it be used?
- Why will it be used?
- How will it be used?
- Who will use it?
- Where will it be used?
- When will it be used

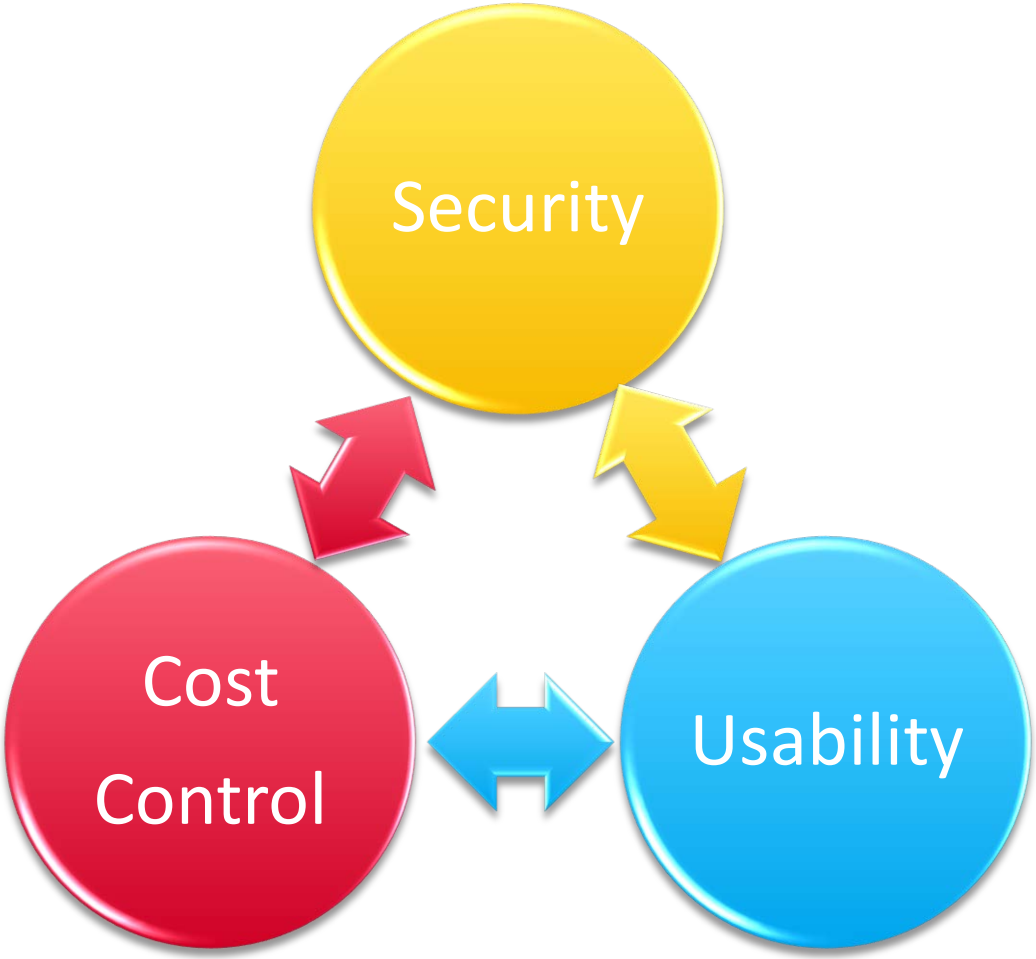
ITSolutions LLC
Interactive Technology Solutions

RULES TO LIVE BY

1. Listen to and Learn from the business
2. Lead Diplomatically
3. Your Area of Expertise
4. Repeatability
5. Market Awareness
6. Business Sense
7. Design Acceptance based upon business requirements and risk
8. Don’t Go to Extremes
9. Best Fit
10. Leverage Existing Investment


SPEED LIMIT
ENFORCED BY
AIRCRAFT
THE RULES
They may be stupid, arbitrary and irritating, but god help you if you break them.

CONFLICTING OBJECTIVES



What does the business want compared regulatory and organizational requirements?

Model for Security Architecture Development (Aligning with the Business)

WHAT, WHY AND WHEN, HOW, WHERE AND WHO?

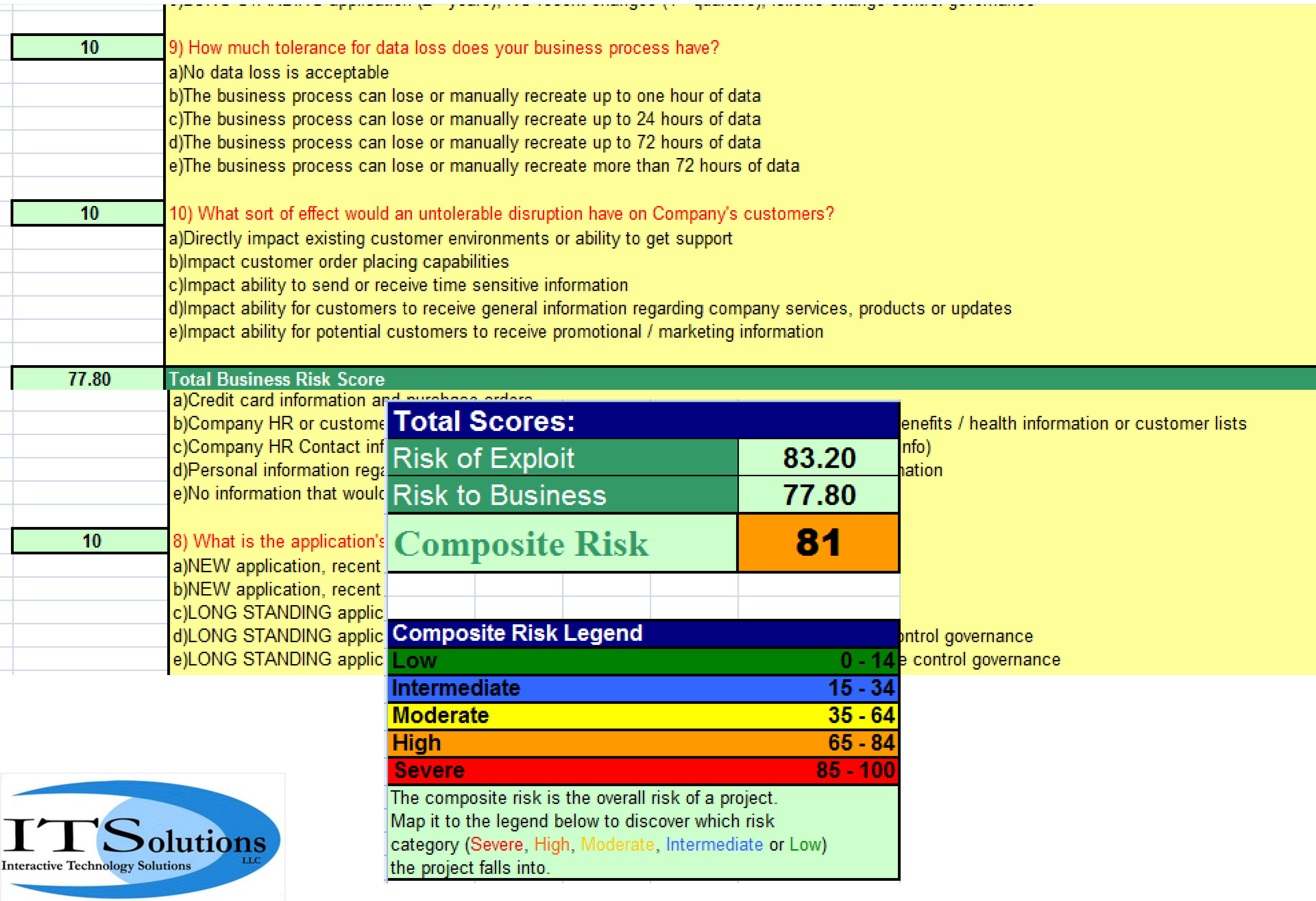
	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

SECURITY SERVICE MANAGEMENT – OPERATIONAL SECURITY ARCHITECTURE

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business Requirements Collection – Information Classification	Business Risk Assessment – Corporate Policy Making	Business-driven Information Security Management Program	Business Security Organization Management	Business Field Operations Program	Business Calendar and Timetable Management
Conceptual	Business Continuity Management	Security Audit, Corporate Compliance, Metrics, Measures & Benchmarks, SLAs	Change/Release Control, Incident Management , Disaster Recovery	Security Training, Awareness, Cultural Development	Security Domain Management	Security Operations Schedule Management
Logical	Information Security , System Integrity	Detailed Security Policy Making, Compliance, Monitoring, Intelligence Gathering	Intrusion Detection/Prevention, Event Monitoring, Security Process Development, Security Service Management, System Dev Controls, Config Management	Access Control Privilege and Profile Administration	Application Security Administration and Management	Applications Deadline and Cutoff Management
Physical	Database Security Software Integrity	Vulnerability Assessment, Penetration Testing, Threat Assessment	Rule Definition, Key Management, ACL Maintenance, Backup Admin, Computer Forensics, Event Log Admin, Anti-Virus Admin	User Support, Security HelpDesk	Network Security Management, Site Security Management	User Account Aging, Password Aging, Crypto Key Aging, Admin of Access Control Time Windows
Component	Product and Tool Security and Integrity	Threat Research, Vulnerability Research, CERT Notifications	Product Procurement, Project Management, Operations Management	Personnel Vetting, Supplier Vetting, User Admin	Platform, Workstation and Equipment Security Management	Time-out Configuration, Detailed Security Operations Sequencing

What is Data Loss Prevention

RAPID RISK – WORKING WITH THE BUSINESS



10 | 9) How much tolerance for data loss does your business process have?

a)No data loss is acceptable
b)The business process can lose or manually recreate up to one hour of data
c)The business process can lose or manually recreate up to 24 hours of data
d)The business process can lose or manually recreate up to 72 hours of data
e)The business process can lose or manually recreate more than 72 hours of data

10 | 10) What sort of effect would an untolerable disruption have on Company's customers?

a)Directly impact existing customer environments or ability to get support
b)Impact customer order placing capabilities
c)Impact ability to send or receive time sensitive information
d)Impact ability for customers to receive general information regarding company services, products or updates
e)Impact ability for potential customers to receive promotional / marketing information

77.80 | Total Business Risk Score

a)Credit card information and purchase orders
b)Company HR or custome … enefits / health information or customer lists
c)Company HR Contact inf … nfo)
d)Personal information rega … nation
e)No information that would

10 | 8) What is the application's

a)NEW application, recent
b)NEW application, recent
c)LONG STANDING applic
d)LONG STANDING applic … ntrol governance
e)LONG STANDING applic … e control governance

Total Scores:	
Risk of Exploit	83.20
Risk to Business	77.80
Composite Risk	81

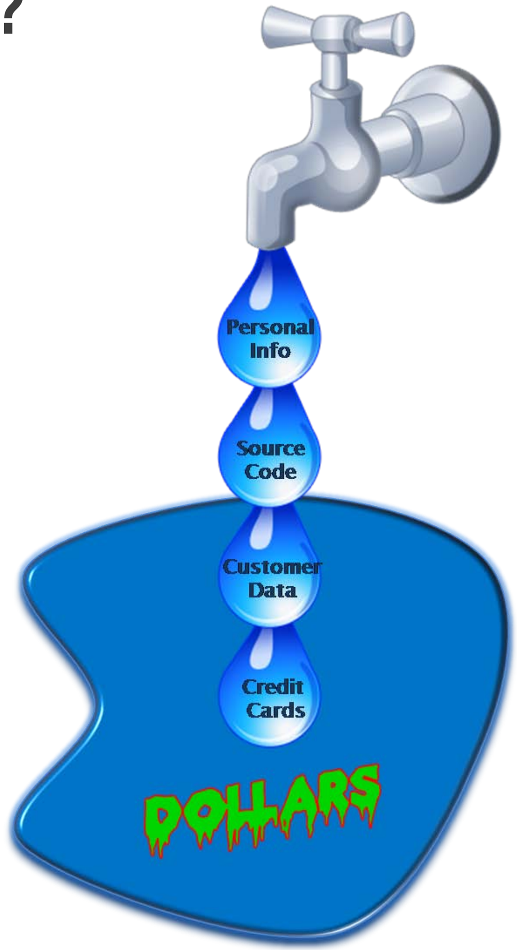
Composite Risk Legend	
Low	0 - 14
Intermediate	15 - 34
Moderate	35 - 64
High	65 - 84
Severe	85 - 100

The composite risk is the overall risk of a project.
Map it to the legend below to discover which risk
category (Severe, High, Moderate, Intermediate or Low)
the project falls into.

ITSolutions LLC
Interactive Technology Solutions

WHAT IS DATA LOSS PREVENTION?

- **Data Loss Prevention** (**DLP**) refers to systems that
  - identify,
  - monitor, and
  - protect data
    - in use (e.g., endpoint actions),
    - data in motion (e.g., network actions), and
    - data at rest (e.g., data storage) through deep content inspection and with a centralized management framework.
- The systems are designed to detect and prevent the unauthorized use and transmission of confidential information.



Data Protection Jeopardy

DLP CAN ANSWER 3 QUESTIONS

WHERE IS YOUR CONFIDENTIAL DATA AS DEFINED BY THE BUSINESS

HOW IS IT BEING USED BY THE BUSINESS

HOW TO BEST PREVENT IT'S LOSS

DID YOU EVER THINK ABOUT SELLING OUR CONFIDENTIAL DATABASE OF CUSTOMER INFORMATION?
www.dilbert.com scottadams@aol.com
IT WOULD BE MASSIVELY PROFITABLE WHILE VIRTUALLY UNDETECTABLE.
BUT HIGHLY UNETHICAL.
© 2004 Scott Adams, Inc./Dist. by UFS, Inc.
I DON'T KNOW YOU ANYMORE.
I'M YANKING YOUR CHAIN. WHEN DO WE START?

© UFS, Inc.

ITSolutions
Interactive Technology Solutions LLC

DLP CAPABILITIES - FOR THE BUSINESS (NOT FOR INFOSEC)

Discover

Find business specific data based upon their business rules

Create inventory of sensitive data (or not)

Determine if data cleanup is wanted

Protect

Proactively control data per business rules and policy

Prevent sensitive data from loss

Enforce business data policies

Monitor

Understand how the business uses their data

Understand the content in contextual form

Gain visibility into policy violations

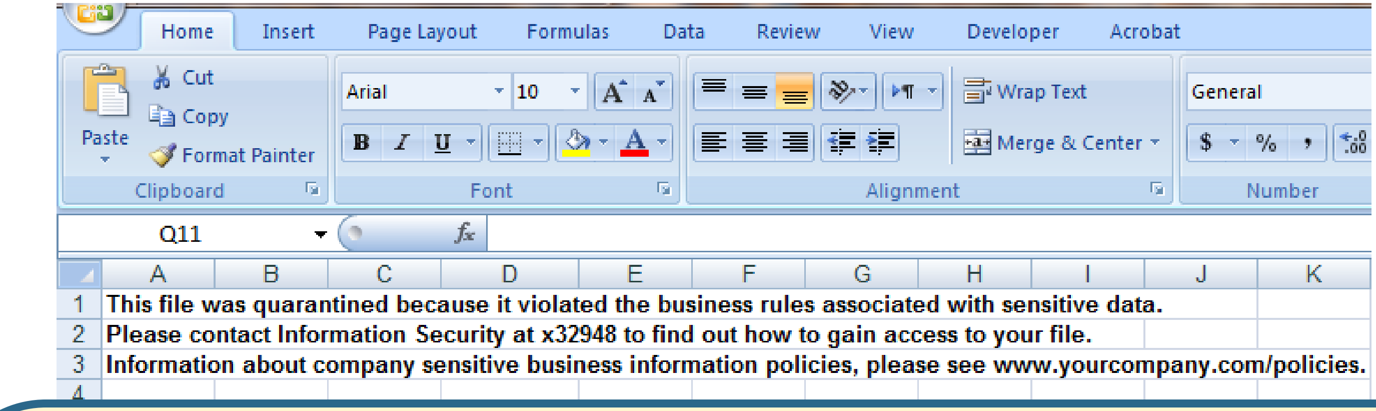
Manage

Define business data policies across the enterprise or as desired by the business

Report on and remediate incidents and issues

Detect business sensitive data accurately

DETECT, PREVENT, MEASURE, COMMUNICATE, ALIGN



1 This file was quarantined because it violated the business rules associated with sensitive data.

2 Please contact Information Security at x32948 to find out how to gain access to your file.

3 Information about company sensitive business information policies, please see www.yourcompany.com/policies.

Find it and fix it

Educate users with automated responses

Empower users to self remediate

Prevent copying to removable media

Block or allow based upon sensitive business rules

As defined by the business, for the business

ITSolutions LLC
Interactive Technology Solutions

WHO IS RESPONSIBLE? - RACI(S)

RACIS is an abbreviation for:

R = **Responsible** - owns the problem / project
A = to whom "R" is **Accountable** - who must sign off (**Approve**) on work before it is effective
C = to be **Consulted** - has information and/or capability necessary to complete the work
I = to be **Informed** -must be notified of results, but need not be consulted.
(**S** = can be **Supportive**) - can provide resources or can play a supporting role in implementation

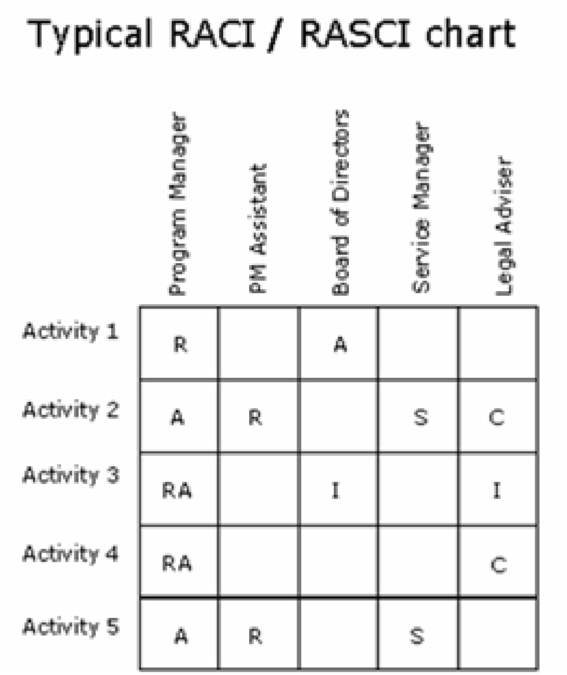
The technique is typically supported by a RACI chart (see figure) which helps to clearly discuss, agree and communicate the roles and responsibilities.

Typical **steps in a RACI process**:

1. **Identify all of the processes** / activities involved and list them down the left hand side of the chart.
2. **Identify all of the roles** and list them along the top of the chart.
3. Complete the cells of the chart: **identify who has the R, A, S, C, I for each process.**
4. **Every process should preferably have one and only one "R"** as a general principle. A gap occurs when a process exists with no "R" (no role is responsible), an overlap occurs when multiple roles exist that have an "R" for a given process.

5. **Resolve Overlaps** - Every process in a role responsibility map should contain one and only one "R" to indicate a unique process owner. In the case of multiple "R"s, there is a need to "zoom in" and further detail the sub processes associated with "obtain resource commitment" to separate the individual responsibilities.

6. **Resolve Gaps** - The simpler case to address is the resolution of a gap. Where no role is identified that is "responsible" for a process, the individual with the authority for role definition must determine which existing role is responsible or new role that is required, update the RASCI map and clarify with the individual(s) that assume that role.



Typical RACI / RASCI chart

	Program Manager	PM Assistant	Board of Directors	Service Manager	Legal Adviser
Activity 1	R		A		
Activity 2	A	R		S	C
Activity 3	RA		I		I
Activity 4	RA				C
Activity 5	A	R		S	

RESPONSIBLE, ACCOUNTABLE, CONSULTED, INFORMED, SUPPORTING

Data Loss Prevention

TASK	Security Services	ISSO/ISSM	Compliance Officer(s)	Internal Audit	HR/Employee Relations	Legal/Privacy Officer(s)	Investigations/Forensics	Business Managers	Department Heads	Executives	Project Manager(s)	Change Management	Configuration Management
Front line remediation													
Data classification													
Data owner													
Data custodian													
Data management													
Compliance and incident trends													
Risk scorecards													
Incidents that lead to employee sanctions													
Incident investigations													
Data flow - business process													
Involvement in escalated incidents													
Risk trends and key risk indicators													
Risk dashboards													
Quantification of risk appetite													
What type of information is in the system?													
Why will it be used?													
How will it be used?													
Who will use it?													
Where will it be used?													
When will it be used?													

R = RESPONSIBLE (Owns the project)
S = SUPPORTIVE (Supporting role or provides resources)
A = ACCOUNTABLE (Accountable for deliverable)
C = CONSULTATIVE (Provides information / input)
I = INFORMED (Notified of results)

Data Loss Prevention
What it means to you

DLP – Architecting a Risk Based Solution for the Business

As the Data Owner
As the Data Custodian
As the HR Director in charge of sanctions
As the Business Owner helping define key risk indicators

Data Loss Prevention - Podcast
'got Feedback?
Learn. Challenge. Explore. Connect.
Download
Get Training

Role & Benefit of Enterprise Security Architecture (With the Business in Mind)

ROLE OF ENTERPRISE SECURITY ARCHITECTURE

Architecture takes a wider more holistic approach to solving the business problem of security by ensuring that all of the components are specifically designed, procured, engineered, and managed to work together for the benefit of the business based upon risk. It considers:

Do we have all of the components?
Do these components work together?
Do they form an integrated system?
Does the system run smoothly?
Are we assured that it is properly assembled?
Is the system properly tuned?
Do we operate the system correctly?
Do we maintain the system?

ARCHITECTURAL CONSIDERATIONS FOR DLP

- What is the scope of creating and successfully implementing a DLP program?
- How will you determine the risk appetite of your organization?
- What policies do you need to establish or modify before you move forward
- Who will create the awareness and training plan?
- What will you do about data classification?
- Will you announce the DLP program to all employees?
- What are the key roles and responsibilities that need to be defined?
- How will you (or somebody) govern the process?

DLP Whitepaper

BENEFITS OF ENTERPRISE SECURITY ARCHITECTURE

Risk-Based Cost Benefit Effectiveness

Business Enabling

Adding Value to Core Business

Empowering Customers

Protecting Relationship and Leveraging Trust

Sound Management and Assurance Framework

Governance

Compliance

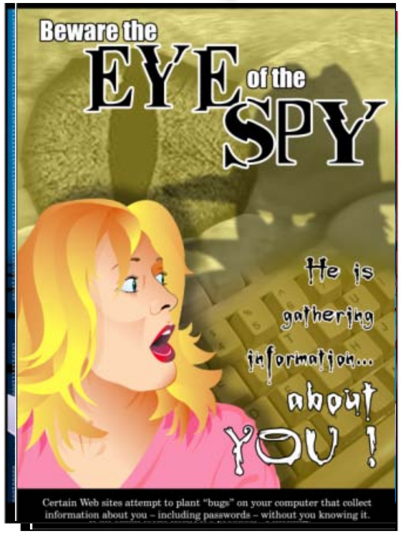
DLP AWARENESS – BASED UPON RISK

JEOPARDY!
Your email may not be secure
Do not send confidential information by unsecured email
Your email may not be secure
Do not send confidential Information by unsecured email
Gambling with our customers data?
Don't leave privacy to chance!

Multiple media types used for security awareness

- Seminars
- Awareness Day
- Annual testing
- Posters - Flash animation
- Email -Web postings
- Bookmarks
- Blogs
- Wikis
- Podcasts - Vodcasts
- Reward Positive Behavior
- Games
- Sandtables
- Twitter

Data Loss Prevention
What it means to you



Certain Web sites attempt to plant "bugs" on your computer that collect information about you – including passwords – without you knowing it.

Guidelines for Information Security and Internet Usage

Corporate Information Security

Enterprise information security architecture

From Wikipedia, the free encyclopedia

Enterprise information security architecture (EISA) is a part of enterprise ar

Contents [hide]

1 Overview
2 Enterprise information security architecture topics
2.1 Positioning
2.2 Goals
2.3 Methodology
3 High-level security architecture framework
4 Relationship to other IT disciplines
5 See also
6 References
7 Further reading
8 External links

Overview

Enterprise information security architecture (EISA) is the practice of applying a organization's security processes, information security systems, personnel and Although often associated strictly with information security technology, it relates architecture, performance management and security process architecture as we

Enterprise information security architecture is becoming a common practice wit security architecture is to ensure that business strategy and IT security are alig

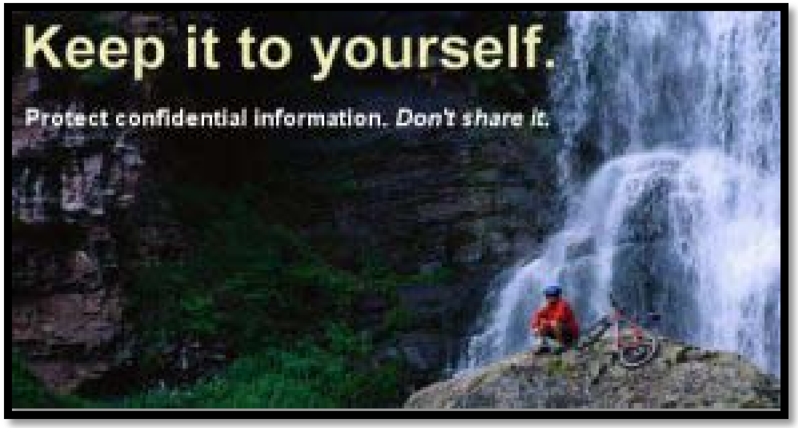
ITSolutions LLC
Interactive Technology Solutions

Defense in Depth – A Military Comparison

DEFENSE IN DEPTH

Examples of Layered Defenses

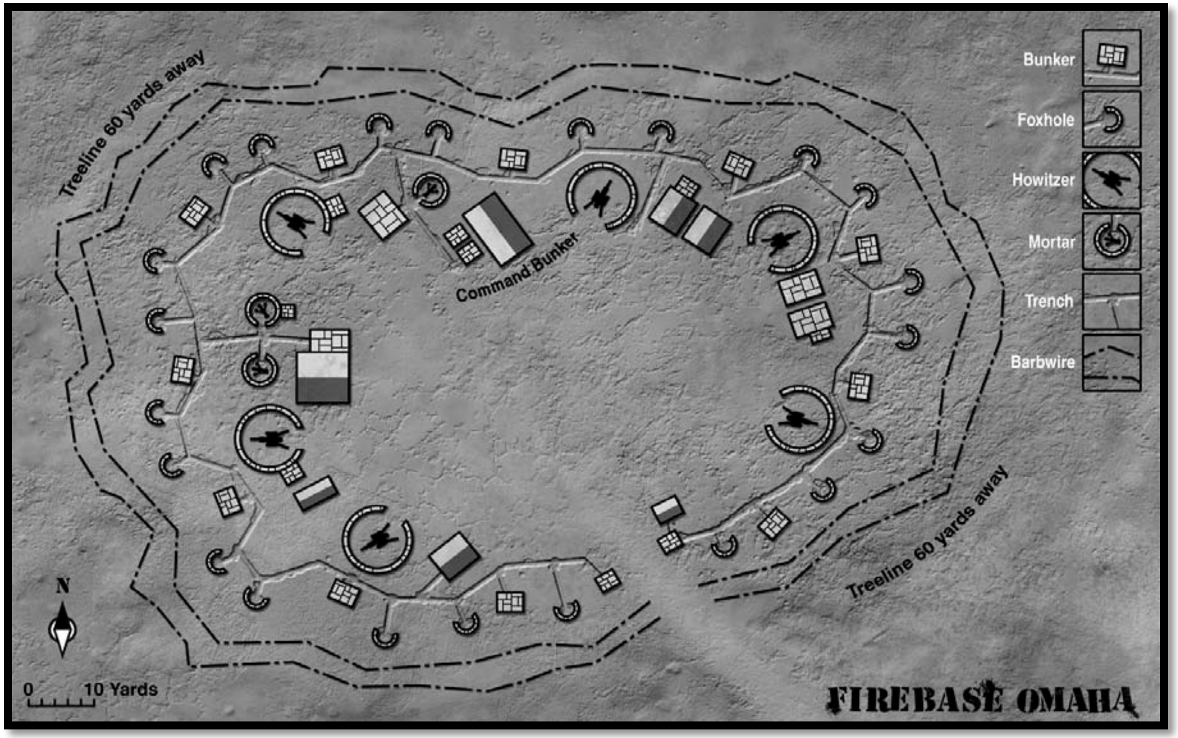
Class of Attack	First Line of Defense	Second Line of Defense
Passive	Link and network layer and encryption and traffic flow security	Security-enabled applications
Active	Defend the enclave boundaries	Defend the computing environment
Insider	Physical and personnel security	Authenticated access controls, audit
Close-In	Physical and personnel security	Technical surveillance countermeasures
Distribution	Trusted software development and distribution	Run time integrity controls



ITSolutions LLC
Interactive Technology Solutions

MILITARY DEFENSE IN DEPTH

The Firebase



THE COMPUTER IS MIGHTIER THAN THE PEN.
...MORE CAN BE STOLEN IN LESS TIME....
COMPUTER SECURITY... JUST DO IT!

ITSolutions LLC
Interactive Technology Solutions

HOW DOES THIS RELATE TO SECURITY ARCHITECTURE AND DLP?

WHAT TYPE OF SECURITY IS BEING USED?

WHAT TYPE OF THREAT IS THIS?

ITSolutions LLC
Interactive Technology Solutions

WHAT TYPE OF CONTROLS ARE BEING USED?

Sand Table Exercise

MOVE TO SAND TABLE FOR EXERCISE

- NOTE: a sand table representing a military firebase will be setup on a nearby table (sample picture below). Layers of physical defense will be compared to layers of virtual defense in this exercise.

ITSolutions LLC
Interactive Technology Solutions

What to Do Next

WHAT DO YOU DO NEXT?

- Acquire Enterprise Security Architecture skills
- Define your intent to your leadership
- Seek out like-minded people
- Understand your corporate process
- Assess the process for gaps
- Define the risk around information
- Listen to the business
- Examine data loss relative to business critical information
- Define what fits for your organization
- Do not force fit
- Focus on the business and business benefits
- Crawl, walk, run

ITSolutions LLC
Interactive Technology Solutions

SECURITY ARCHITECTURE

Jeff Bardin
ITSolutions
jeff.bardin@itsolutions-llc.com

Session ID: TUT-M51
Session Classification: Security Basics Boot Camp