



O-ISC '07
Ohio Information Security Conference

Computer Forensics For The 21st Century: An Introduction to Active Forensic Intelligent Response Method

Bryan K. Fite

 Reed Elsevier

NOTICE



Everything you are about to see, hear, read and experience is for educational purposes only. No warranties or guarantees implied or otherwise are in effect. Use of these tools, techniques and technologies are at your own risk.

The views expressed in this presentation are entirely my own and do not necessarily reflect the views of Reed Elsevier.

WWW.AFIRM.ORG

Who Am I?

- Bryan Fite
- Global Security Architect
- Veteran Information Security Practitioner & Researcher
- Creator of AFIRM

WWW.AFIRM.ORG

- What Is AFIRM?
- Why Use AFIRM?
- How Is AFIRM unique?
- Putting It All Together
- Case Study (sneak peek)
- Q & A

What Is AFIRM?



Active Forensic Intelligent Response Method is the fusion of risk management, information security and forensic science practices. Its ultimate goal is to create secure audit friendly computing environments.

WWW.AFIRM.ORG

What Is AFIRM?

- It Is A Methodology
- It Is A Mindset
- It Is A Way Of Life ;)

WWW.AFIRM.ORG

Why Use AFIRM?

- It Works
- It Is Flexible
- It Is Practical
- Its Vendor Agnostic, Efficient and Cost Effective

WWW.AFIRM.ORG

How Is AFIRM Unique?

- Risk Management
- Information Security
- Forensic Science

WWW.AFIRM.ORG

Risk Management

- Is a business practice typically engaged in by legal, executive management, human resources and financial elements of an organization.
- Is interested in driving risk to an acceptable or “business reasonable” level.
- A mature discipline: Transfer, Reject, Reduce or Accept.

■ Traditional Approach:

- Blind to emerging threats
- Slow to react
- Isolated practice (financial, business and legal only) which is “culturally” biased

■ AFIRM Approach:

- Is Conscious of Emerging Threats And Context
- Is Real-time
- Is Holistic
- Is ***Business Reasonable***
- Focuses On The Relevant
- Is Proactive

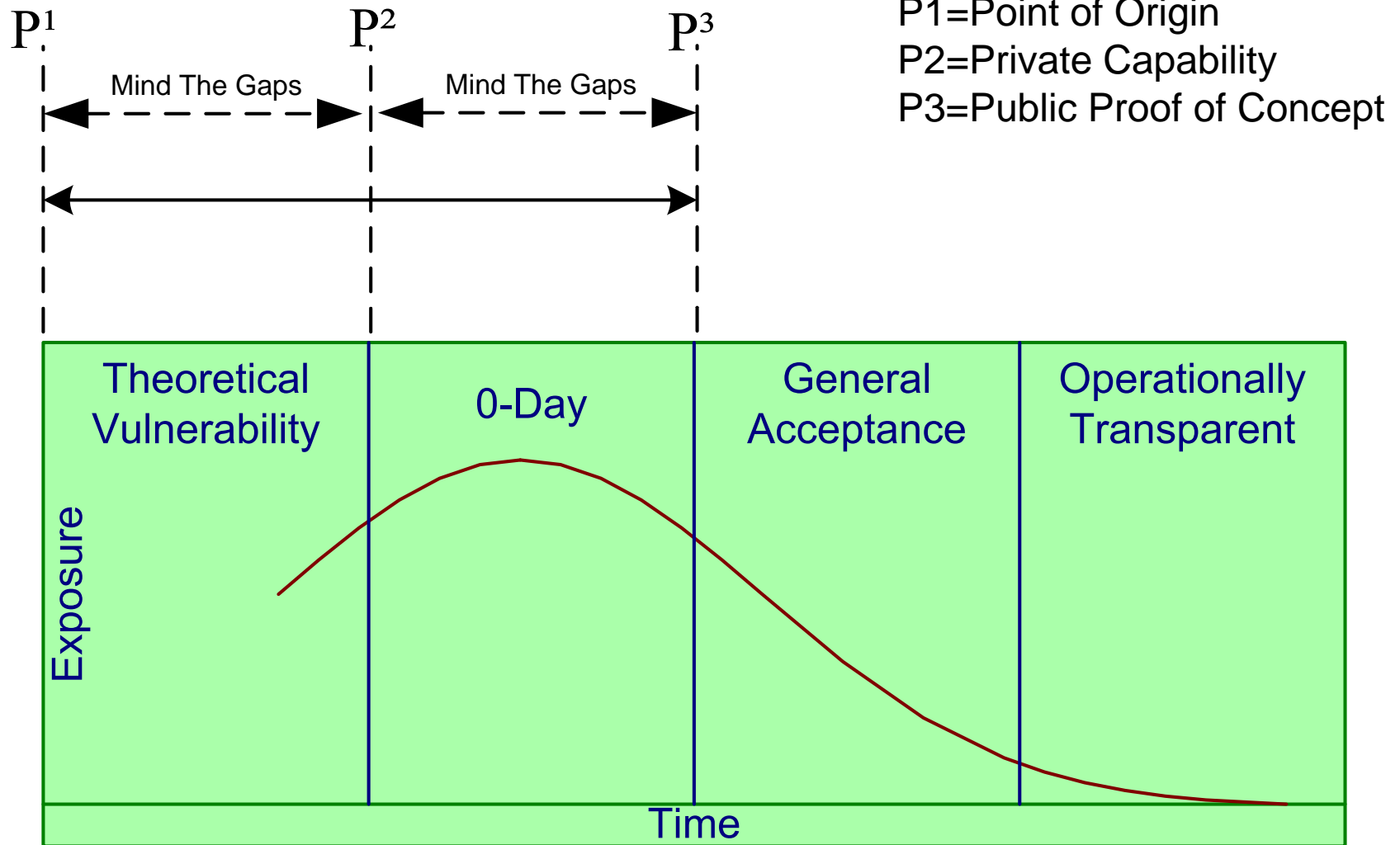
Risk Management



Risk = Threat * Vulnerability * Cost

WWW.AFIRM.ORG

Risk Management



■ 5 Basic Steps

- Define Assets & Owners
- Assign Asset Value (high, medium & low)
- Define Relevant Threats
- Identify Relevant Vulnerabilities
- Accept, Transfer or Mitigate

Information Security



- Is concerned with the Confidentiality, Integrity and Availability of Information Assets.
- Is a relatively new discipline based on ancient principles (secrets).
- Is typically obsessed with technical controls.
- Is reasonable in theory and but resisted in practice.

WWW.AFIRM.ORG

■ AFIRM Assertions:

- Security is a Pain
- There is no such thing as 100% security
- Ignorance & sloth are enemies of security
- Simple is better
- Information is power

■ AFIRM Approach:

- Governance
- Policies, Procedures, Guidelines and Standards
- People
- Technology

■ AFIRM Guiding Principles:

- Know Your Environment
- Know Your Enemy
- Trust Nothing, Verify Everything
- Practice Least Privilege Computing
- Leverage Everything (holistic efficiency)

Exposure = Motivation * Capability *
Vulnerability

Information Security



Control Matrix Dashboard

Attack Class:	Controls:						Exposure Index
	IPS	Client/Host	NACS	Encryption	Passwords	Operations	
Malware	1	1	0.5	0	0.1	0.8	43.33%
0-Day Malware	0.4	0.5	0.4	0	0.1	0.6	66.67%
DDoS	0.5	0.2	0.8	0	0	0.7	63.33%
Phishing	0.5	0.1	0.1	0	0.6	0.5	70.00%
Data Theft	0.2	0.3	0.8	0.2	0.6	0.3	60.00%

scale 0-1

0	not effective/ no affinity /inactive
0.5	effective or partially deployed
1	highly effective and fully deployed

Assumptions:

1. Controls are properly implemented and managed
2. Attacker is competent and motivated
3. Scores above 50% warrant a formal risk assessment

WWW.AFIRM.ORG

- Is concerned with the collection, preservation, analysis and presentation of evidence.
- Is most often viewed in a legal context.
- Follows a linear process.

■ Traditional Approach:

- Is Reactive
- Is A Cloistered Discipline (government, military and law enforcement)
- Is Unnecessarily Technical
- Is A Tactical Discipline

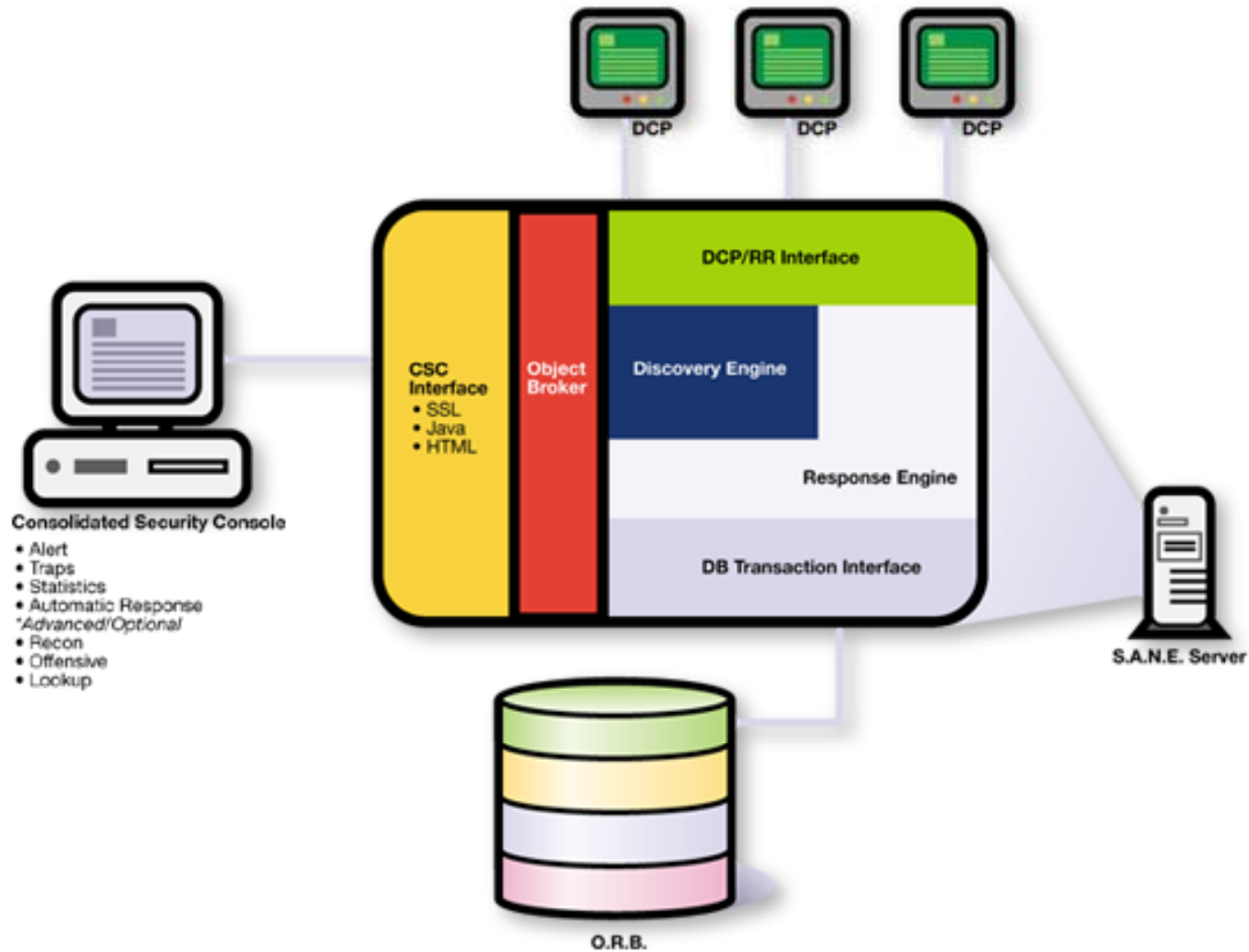
■ AFIRM Approach:

- Pro-Active (“Forensic Friendly”)
- Real-Time
- Contextually Aware
- Non-Reputable

■ ***AFIRM-DO*** (The Way)

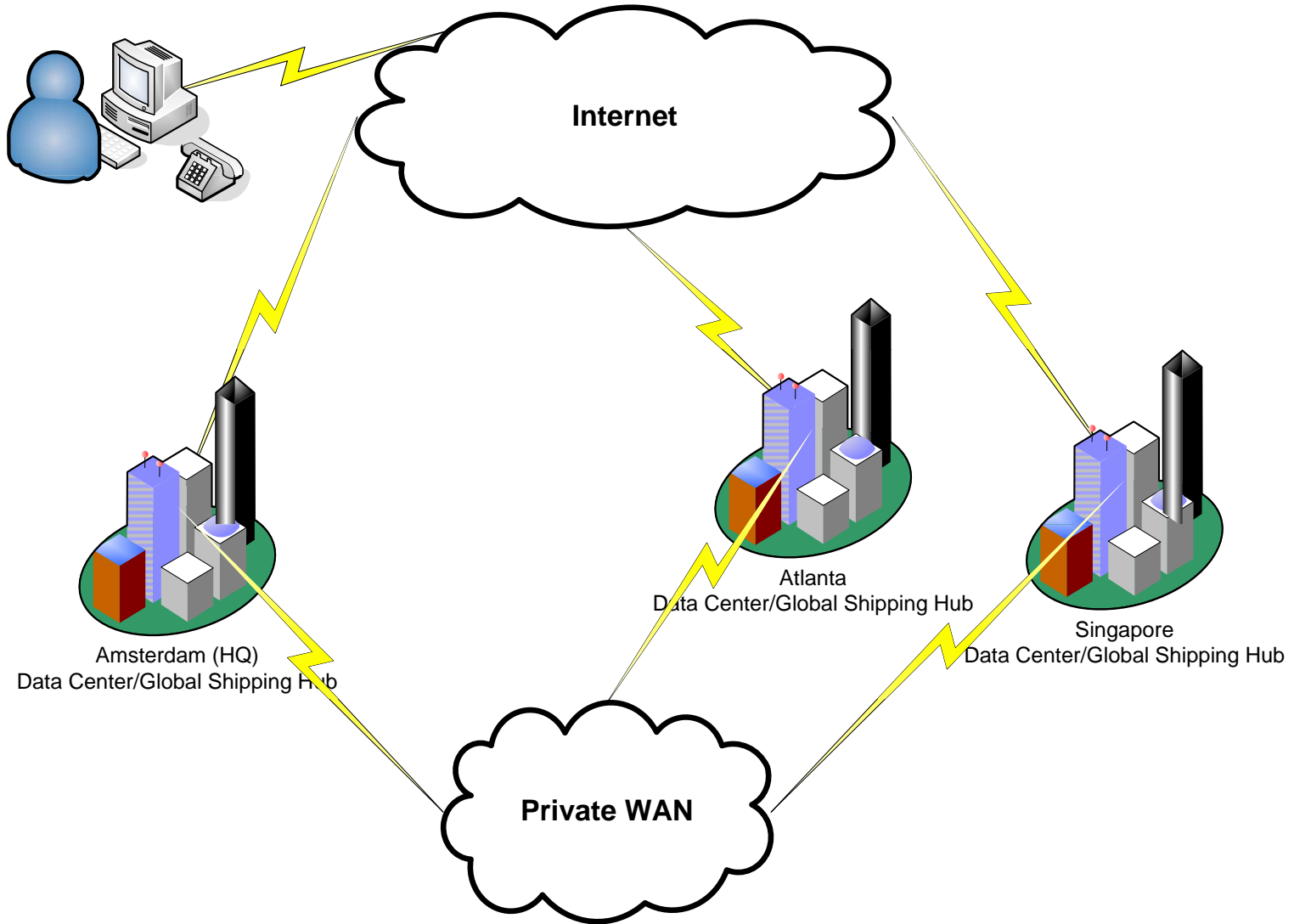
- User Friendly
- Agile Security
- Decision Support Tools
- Game Theory/Scenario Planning/Role Playing
- Virtualization
- Visualization
- Profiling/Modeling

Putting It All Together



WWW.AFIRM.ORG

Case Study



WWW.AFIRM.ORG

Questions & Answers

(bfite at afirm dot org)

WWW.AFIRM.ORG