

# The Future of Information Security and Risk Management What's Next?

Presented By:

**John P. Pironti**

CGEIT, CISA, CISM, CISSP, ISSAP, ISSMP

Chief Information Risk Strategist

Archer Technologies

# Agenda

- Why is Security So Difficult?
- Evolution of Information Security
- Risk Management Based Approach
  - Proactive data focused approach to Information Risk Management
- Evolving Threats
- Threat and Vulnerability Management
  - The challenges of Asset Identification
- Final Thoughts

# Why Is Security So Difficult?

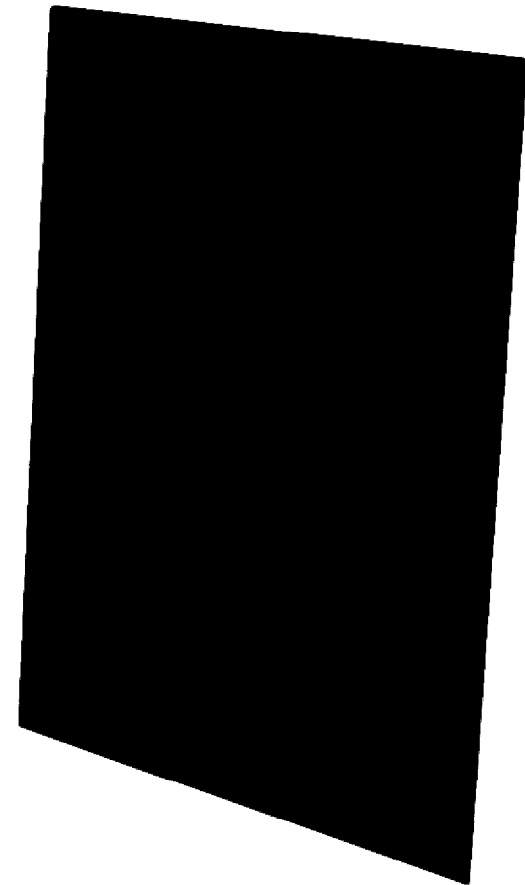
- Adversaries have extraordinary resources
- Adversaries need to master only one attack
- Defenders constrained by ethics and laws
- Defenders must serve business goals
- Defenders must win all the time



# Evolution of Information Security

## How Did We Arrive To This Point?

- **1970 – 1995**
  - Technology driven
  - Very few specialists
  - Limited threat landscape
- **1995 – 2001**
  - Technology driven
  - Adversary capabilities and knowledge grow
    - Status seeking, new tools, exploit disclosure
  - Expanding threat landscape
- **2001 - 2008**
  - Compliance driven
  - Worms, bots, malware...
  - Everyone becomes a security expert
  - Security is a specialized activity
- **2009 – and Beyond...**
  - Risk driven/data focused
  - Targeted threats
  - Consultative approach
  - Business unit within organization
  - Motivated and capable adversaries
    - Every user is a potential hacker...



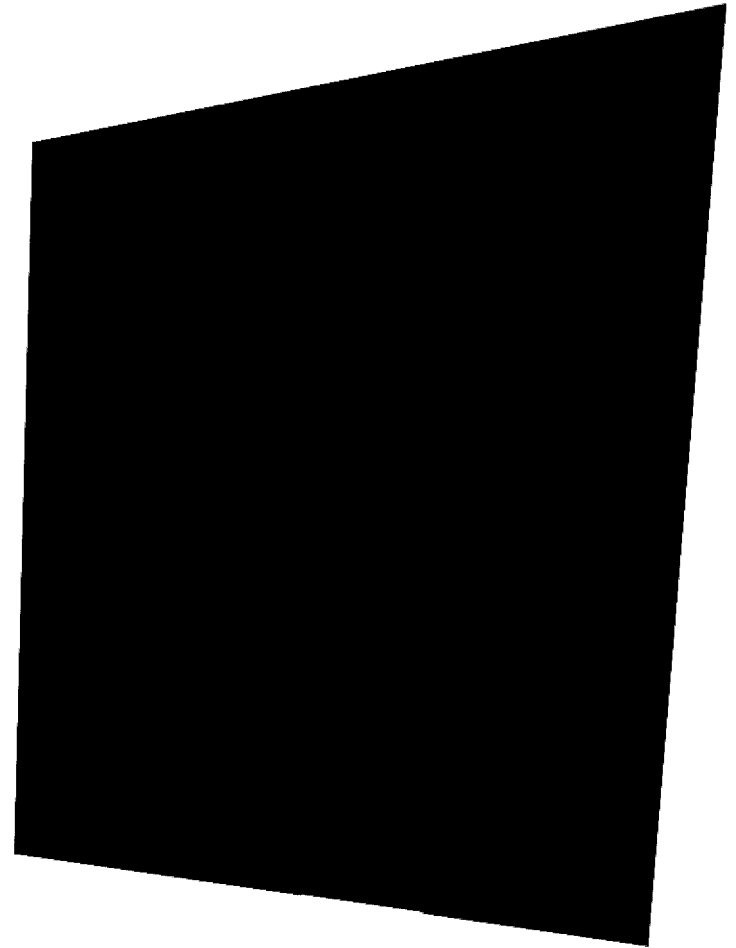
# What's Next: The Driving Force of Compliance

- Compliance continues to be the number one driver of investment
  - 10% to 13% of IT budgets being spent on compliance and compliance related activities
  - Security is falling to 5% - 7%
- Government regulation on the rise
  - Sarbanes Oxley, Basel II, EU Data Privacy and Security Directives, Disclosure Laws, GLBA
- Industry driven standards on the rise:
  - Payment Card Industry Standard (PCI)
- Common Themes:
  - You can no longer take risks that affect your customers or those outside of your organization
  - Risk is not transferrable to third parties



# What's Next: Information Security as a Consulting Organization

- Information security organization evolves
  - Becomes consulting organization
  - Aligns with risk management organization
  - Minimal operational activities
  - Information security program
    - Functional inventory of activities and capabilities
- Development of Risk Management Organization
  - Inclusive of information security program
  - Led by Chief Risk Officer
  - Provides 360 degree view of risk for organization



# Information Security Program Functional Inventory

## Functional Elements

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]		

## Organizational Interactions

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

# Information Risk Management Functional Inventory

## Functional Elements

[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]			

## Organizational Interactions

[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

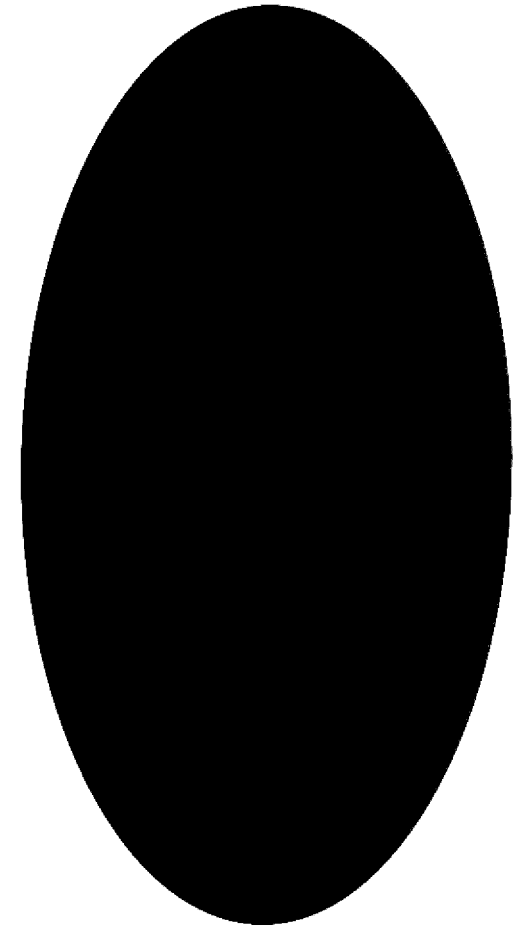
# What's Next: Threat and Risk Focused Approach

- Information security controls based on business aligned threat and vulnerability analysis
  - Business impact
  - Likelihood of occurrence
- Use of threat and vulnerability analysis and vulnerability management
  - Provides realistic threat and vulnerability intelligence to organization
- Integration into operational risk and business risk management activities
  - Allows for intelligent and business appropriate decisions



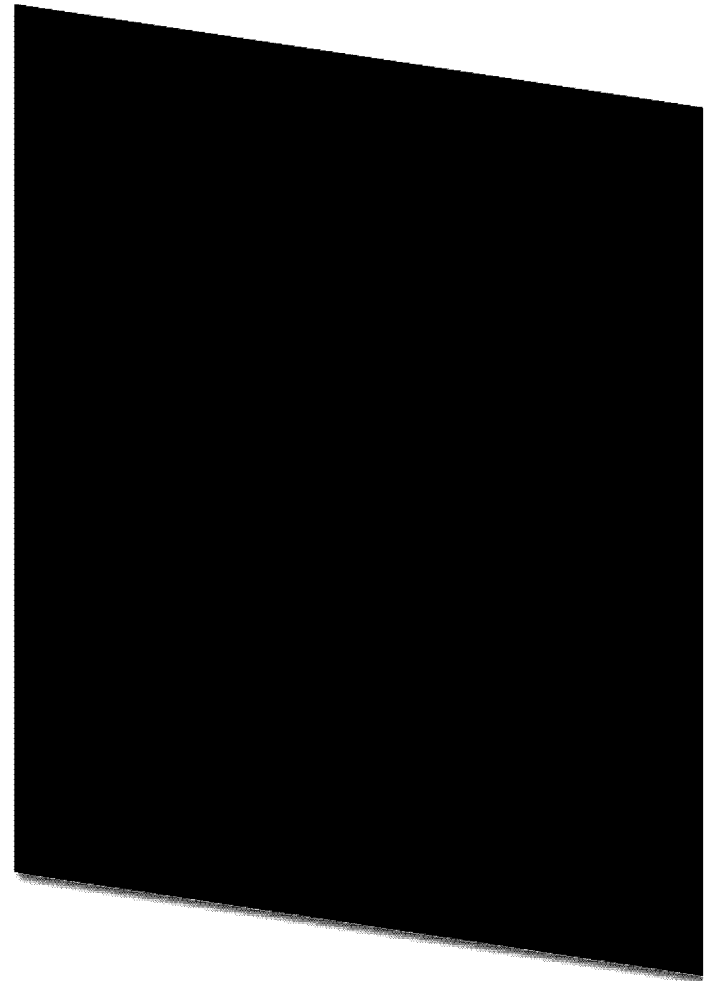
# What's Next: Logical and Physical Asset Identification and Classification

- Identification of all logical and physical assets
  - You cannot protect what you do not know
- Not all data needs to be secured the same way
  - Different data requires different controls
  - Classification system determines control requirements
- Data is pervasive and no longer easily contained
  - Four walls, a mainframe, and a LAN no longer exists
  - All business processes should be mapped for data flows and usage
- Must be kept current and accurate to be valuable
  - Stale information degrades integrity and confidence



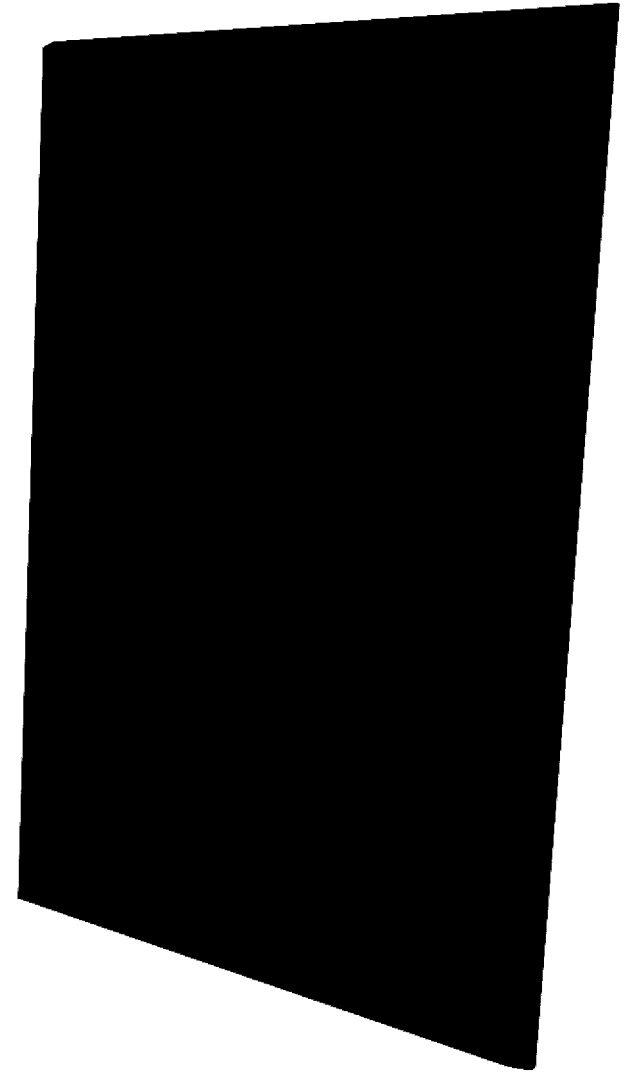
# What's Next: Evolving Threats

- Targeted attacks on the rise
  - Adversaries more interested in economic gains than fame
  - Identity theft becoming lucrative underground marketplace
- Adversary community becoming more capable
  - More tools and knowledge available
  - Financial support from organized crime
  - Publicly available tools and knowledge more powerful than ever
    - MetaSploit
    - Nessus
    - Google



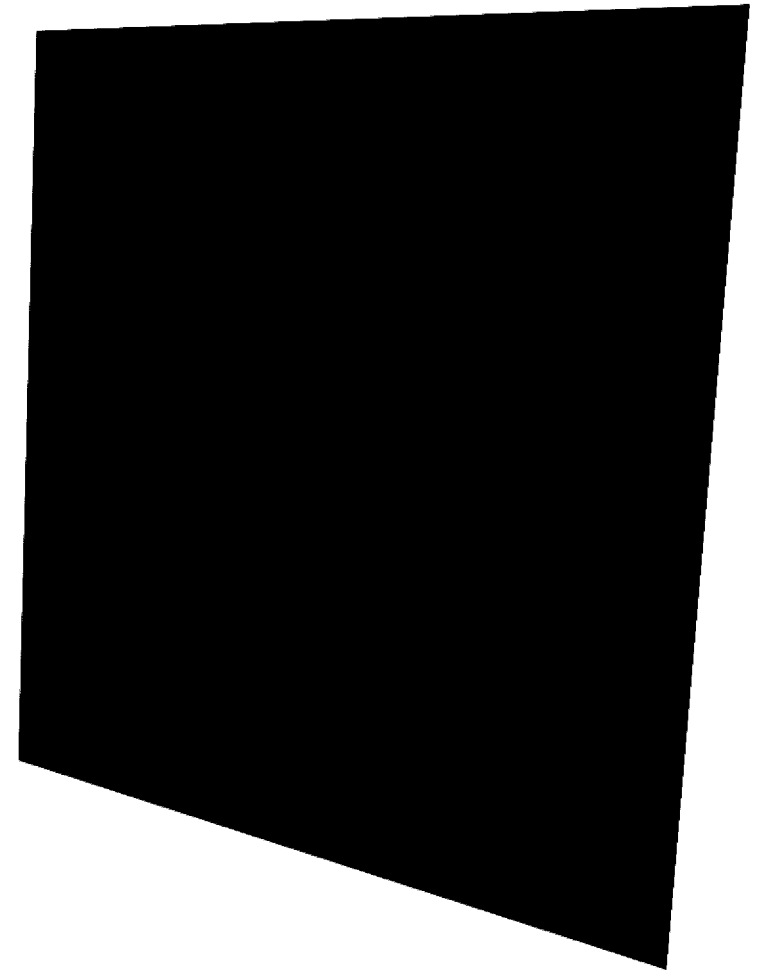
# What's Next: Threat and Vulnerability Management

- Protection of information infrastructure and information instead of information technology
- Expanded use of logical and physical asset inventory
- Use of Threat and Vulnerability Analysis to provide meaningful intelligence and insight
- Development of proactive countermeasure plans
- Understanding of realistic threat and vulnerability landscape
  - What are my realistic threats and vulnerabilities?



# Threat and Vulnerability Analysis Concept Overview

- Models a particular solution against attack scenarios and known vulnerabilities to evaluate its ability to repel attacks
- Output will produce information to create appropriate identification and countermeasure plans for identified attack scenarios
- Quantifies risk of identified threats and vulnerabilities to organization's information infrastructure
  - Likelihood of occurrence
  - Business impact on organization



# OSI+ Threat and Vulnerability Analysis Methodology Overview

## **Who**

Attacker Profiles

## **What**

What will be attacked

## **When**

When are you most  
vulnerable

## **Where**

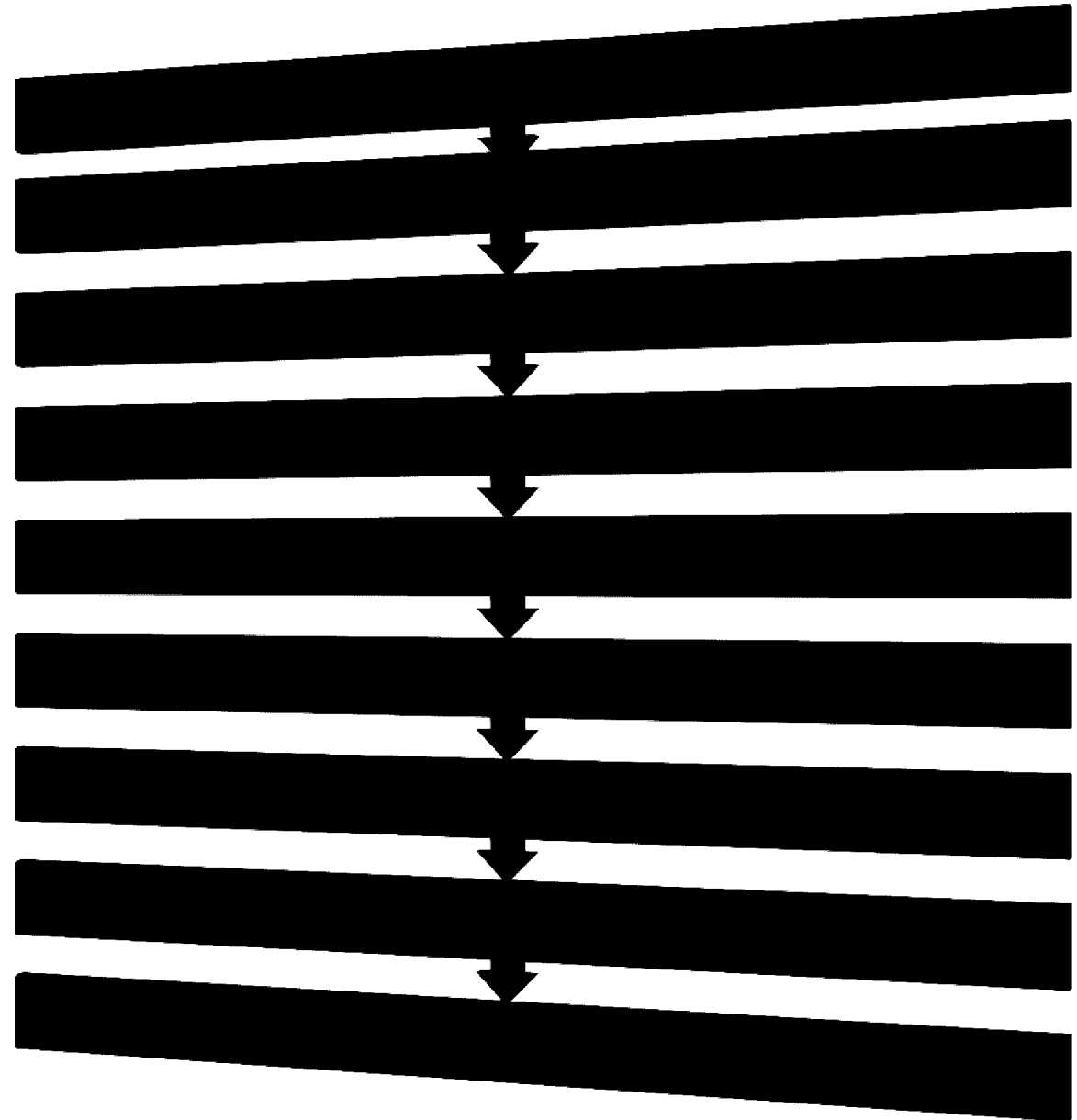
Where will you be attacked

## **Why**

The motivation for the  
attack

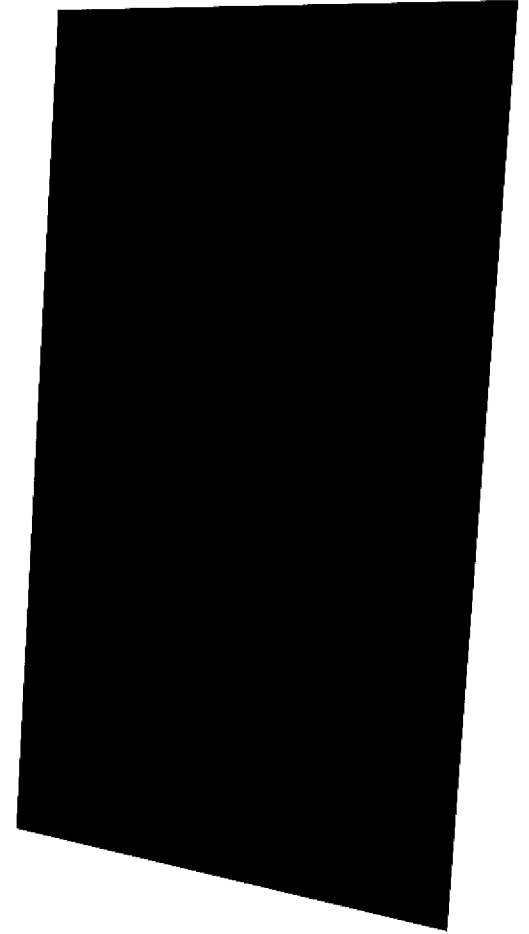
## **How**

How you will be attacked



# What's Next: How We Will Protect Information Infrastructure

- Countermeasure plans for identified threats and vulnerabilities
- Endpoint security solutions
  - Data focused solutions
- Enhanced authentication concepts
- Transparency to the general user
- Security knowledge management



# Final Thoughts

- Information security needs to be integrated as a business function to be successful
- Regulation will continue to grow until information is appropriately protected
- A risk based approach will drive business alignment and acceptance
- Threat and Vulnerability Analysis key to success
- Technological controls will mature but people, processes and procedures will still offer the greatest protection for information infrastructure and data

# Thank You for Your Time!



**John P. Pironti**

CGEIT, CISA, CISM, CISSP, ISSAP, ISSMP

Chief Information Risk Strategist

Archer Technologies

[John.pironti@archer-tech.com](mailto:John.pironti@archer-tech.com)