Nebraska CERT Conference

Security Methodology / Incident Response

Patrick Hanrion

Security Center of Excellence

Sr. Security Consultant

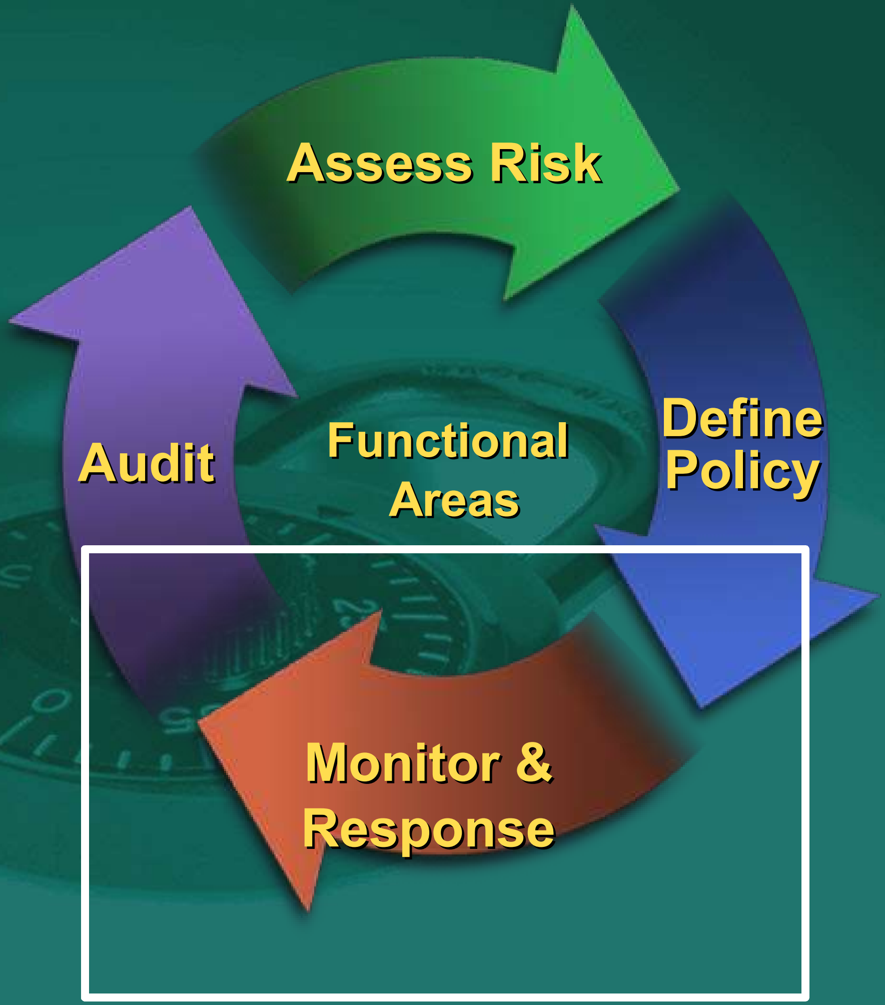
Agenda

- Security Methodology
  - Security Enabled Business
    - Framework methodology
- Incident Response
  - Incident Response methodology
  - IR lifecycle
    - Proactive
    - Reactive
    - Remediation
    - Measurement
  - Incident Remediation

Security Enabled Business

Information Security Mission

Manage IT security risks to an acceptable level by systematically assessing, communicating and mitigating risks to digital assets



Security Enabled Strategy & IT Governance

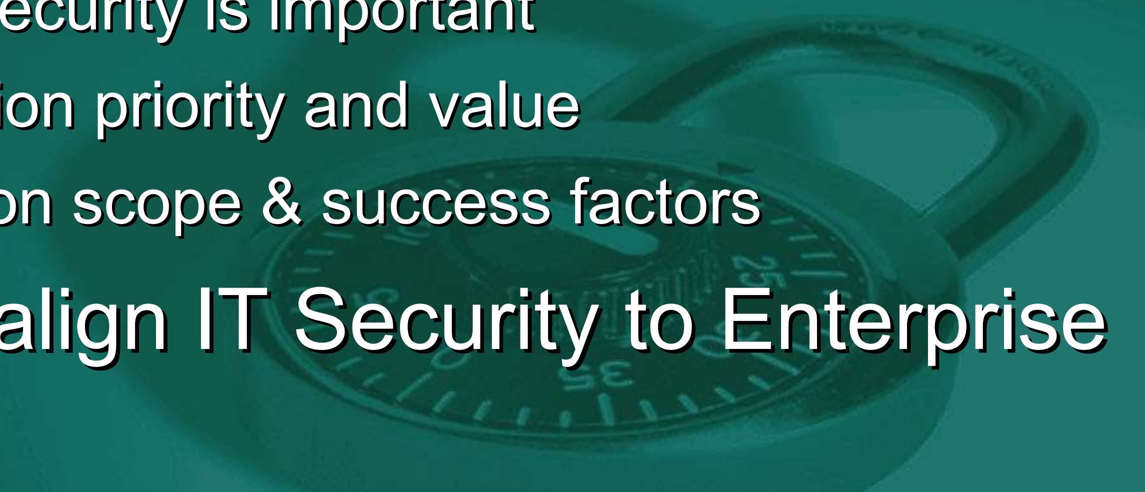
- A word on governance...
- Security Strategy is a subset, not a substitute, for overall IT Governance
- IT Governance sustains and extends enterprise strategies and objectives*
  - Strategic Alignment
  - Risk Management
  - Resource Management
  - Performance Measurement
- IT Governance is essential, but out of scope here
  - This briefing focuses on identifying specific security strategies to help you manage IT risk

* source: Institute for IT Governance, 2003

Why We Discuss Security Strategy

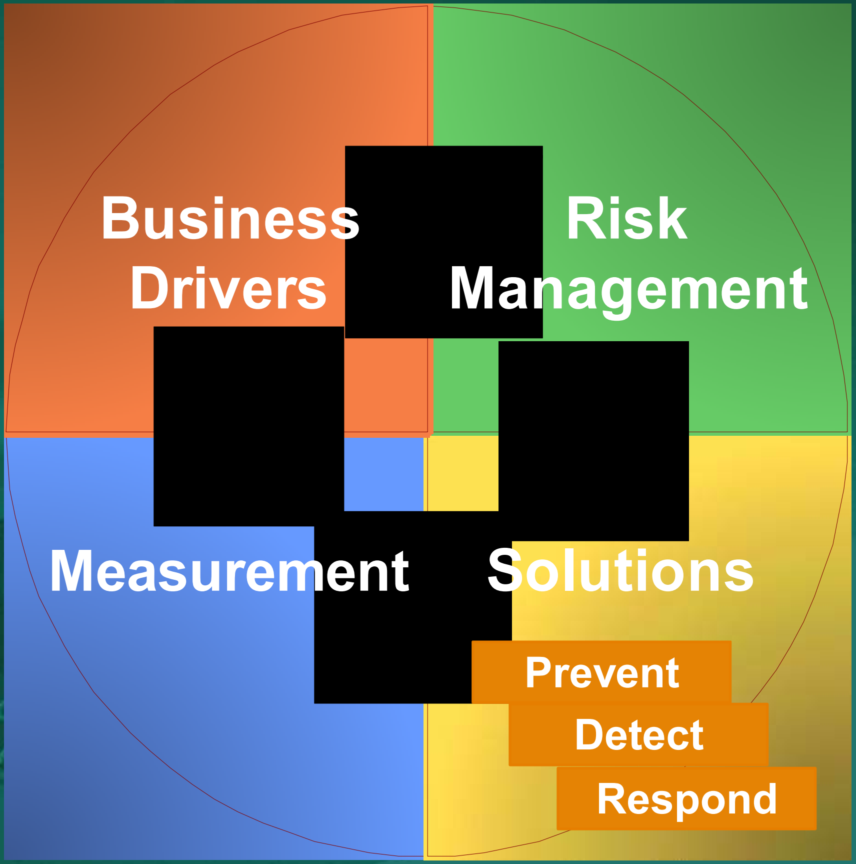
Security Strategy is:

- A foundation for deploying tactical solutions to manage risks
  - Define why security is important
  - Identify solution priority and value
  - Define solution scope & success factors
- Needed to align IT Security to Enterprise objectives
- Blueprint for a comprehensive IT security program
  - Including Incident Response



IT Security Strategy

- **Executing on the Mission**
  - Business Drivers
    - Why is security important?
  - Risk Management
    - What are the priorities?
  - Control Solutions
    - How best to mitigate?
    - How best to respond?
  - Measure
    - How effective are we?



Security Enabled: Business Drivers

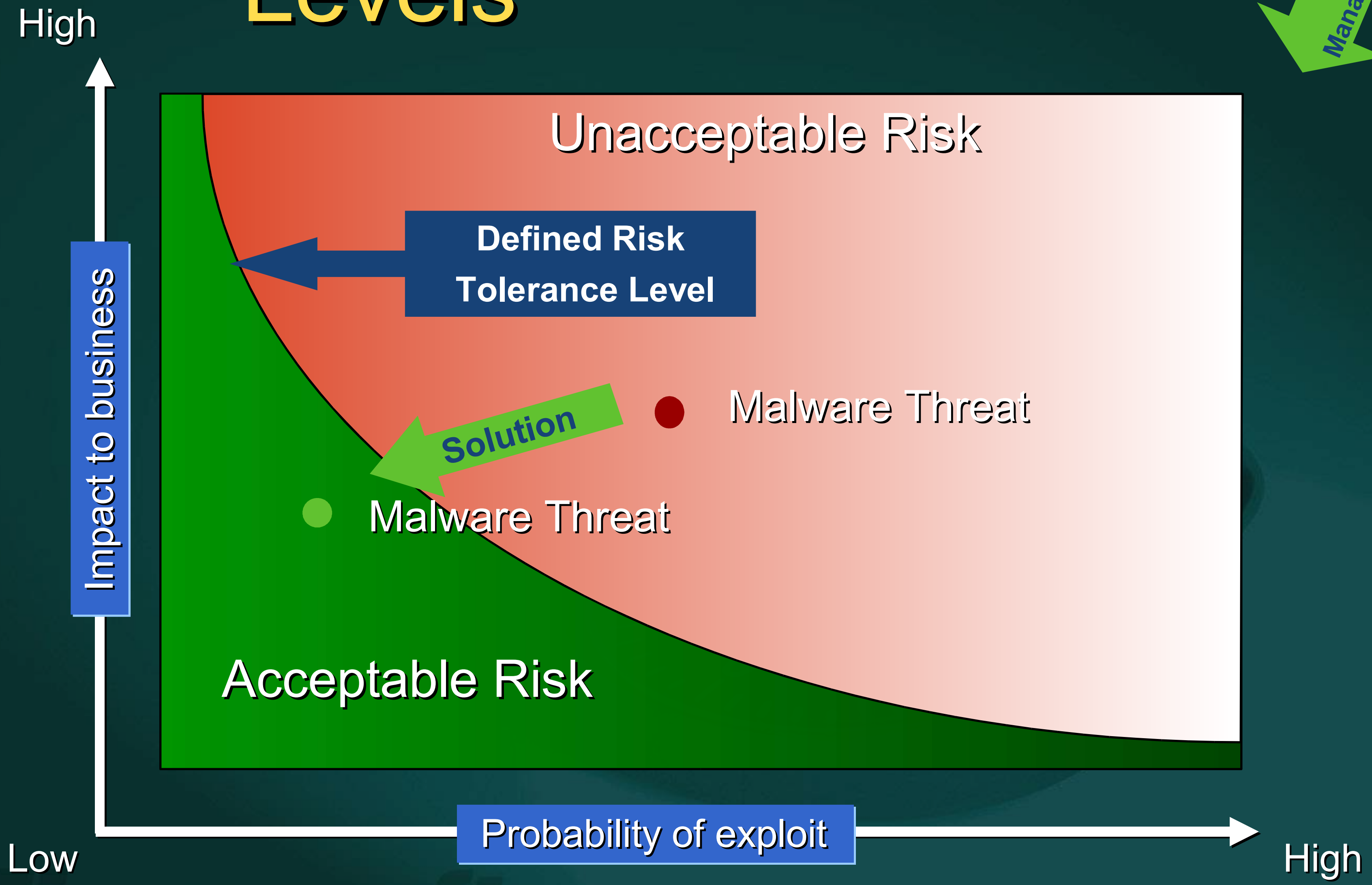
- Align with overall Business Objectives
  - Communicates “why” security is important to the business:
    - Reduce Cost
    - Protect Assets
    - Regulatory Requirements
    - Enable the Business
- Drivers defined at executive level
- Defines primary inputs into Risk Management Process
  - Identify Critical Assets & Business Functions
  - Define Risk Tolerance i.e. Acceptable Risk
  - Acceptable levels of business risk against cost of IT

Security Enabled: Risk Management

- Goal
  - Prioritize IT security risks
  - Select and justify expenditures – Develop ROI
- Risk Management Process
  - Identify threats & vulnerabilities
  - Determine impact
  - Estimate likelihood
  - Enable cost/benefit analysis to select best solution to mitigate risk
- Risk Management Outputs
  - Current security risks
  - Optimal Security Solutions to mitigate risk

Understanding Risk Levels

Risk Management



Security Enabled: Solutions

- Solutions encompass people, process, technology to manage risk
- Microsoft Solutions include
  - Microsoft Products, Services, and Training
  - Microsoft Partner Products and Services as needed
  - Solutions can be mapped to ISO 17799
    - Because 17799 provides comprehensive IT Security view
- Solutions can be organized into standard control buckets
  - Prevention
- Detection
- Response

Security Solutions Framework

	ISO/ISE 17799:2005(E) Security Control Clauses									
	Security Policy	Security Org.	Asset Mngmnt.	HR Security	Physical Security	Comm. & Operations	Access Control	System Dev/Mntc.	Incident Mngmnt.	Business Continuity	Compliance
Malware Protection	S,G	S,G	P,S,G			P,S,G	P,S,G	P,S,G	S,G		S,G
Internal abuse	S,G	S,G	P,S,G			P,S,G	P,S,G	P,S,G	S,G		S,G
External Intruders	S,G	S,G	P,S,G			P,S,G	P,S,G	P,S,G	S,G		S,G
Regulatory Reqs.			P,S,G			P,S,G	P,S,G	P,S,G	S,G		S,G
Business to Employee	S,G	S,G	P,S,G			P,S,G	P,S,G	P,S,G	S,G		S,G
Business to Business	S,G	S,G	P,S,G			P,S,G	P,S,G	P,S,G	S,G		S,G
Business to Consumer	S,G	S,G	P,S,G			P,S,G	P,S,G	P,S,G	S,G		S,G
Application Dev.	S,G	S,G	P,S,G			P,S,G	P,S,G	P,S,G	S,G		S,G

LEGEND

P – MS PRODUCTS

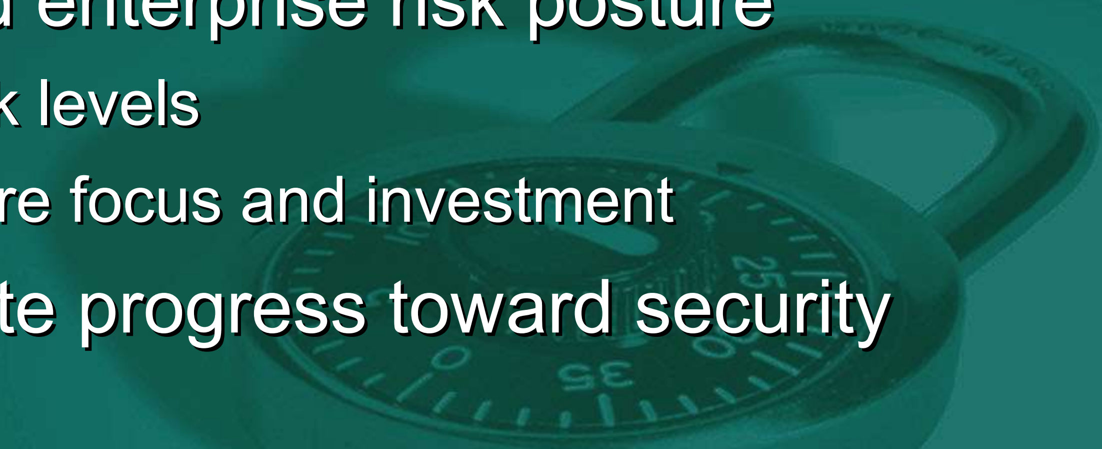
S – MS SERVICES & SUPPORT

G – MS GUIDANCE & TRAINING

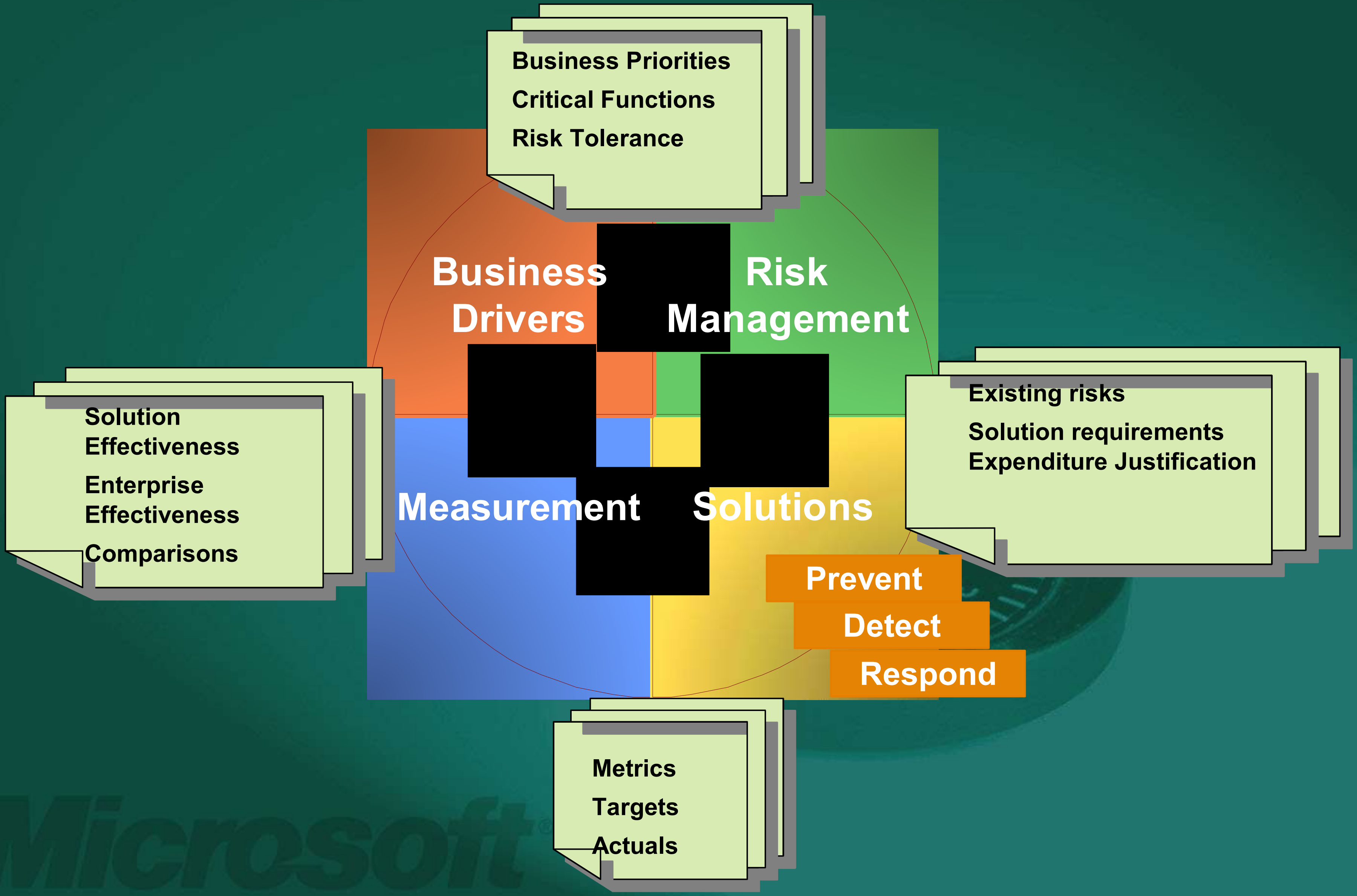
MS PARTNER OFFERINGS AVAILABLE

Security Enabled: Measurement

- Measure effectiveness of specific security solutions
  - Monitor return on security investment
  - Scorecards for executive summaries
- Understand enterprise risk posture
  - Current risk levels
  - Drives future focus and investment
- Demonstrate progress toward security objectives
  - Internal gap and trend analysis
- Compare against Best Practices
- External analysis across industry and standards



Security Strategy Deliverables



Business Priorities
Critical Functions
Risk Tolerance

Business Drivers

Risk Management

Measurement

Solutions

Solution Effectiveness
Enterprise Effectiveness
Comparisons

Existing risks
Solution requirements
Expenditure Justification

Prevent
Detect
Respond

Metrics
Targets
Actuals

Incident Response

Why do we need Incident Response?

- IT Security Mission: manage risk, not eliminate risk
  - Incidents will happen
- Incident response is a control strategy to deal with security events
  - Events that were deemed “acceptable”
  - Unforeseen events
  - Control failures

Incident Categories

- Denial of Service—an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- Malicious Code—a virus, worm, Trojan horse, or other code-based malicious entity that infects a host
- Unauthorized Access—a person gains logical or physical access without permission to a network, system, application, data, or other resource
- Inappropriate Usage—a person violates acceptable computing use policies
- Multiple Component—a single incident that encompasses two or more incidents.

Incident Detection

- Network and host based IDS(Intrusion Detection Systems)
- Antivirus software
- File and system integrity checking software
- System service and application log files
- Network device logs
- Honeypots
- Exploit databases and alert tools
- Security aware system administrators
- Security aware users
- Outsource partners

Incident Lifecycle

- Analysis
  - Before you can act you need to understand the attack
- Containment
  - Segmentation, Removal, Monitoring
- Reporting
  - Communicate to management
- Planning
  - Plan how to remove the intruder
  - Remediate the incident

Analysis

- Forensics
- Support organizations
- Government
- Intrusion Detection

Containment

- Segmentation
- Antivirus
- IPSec
- Firewalls
- Disconnect
- Rebuild infected systems

Reporting

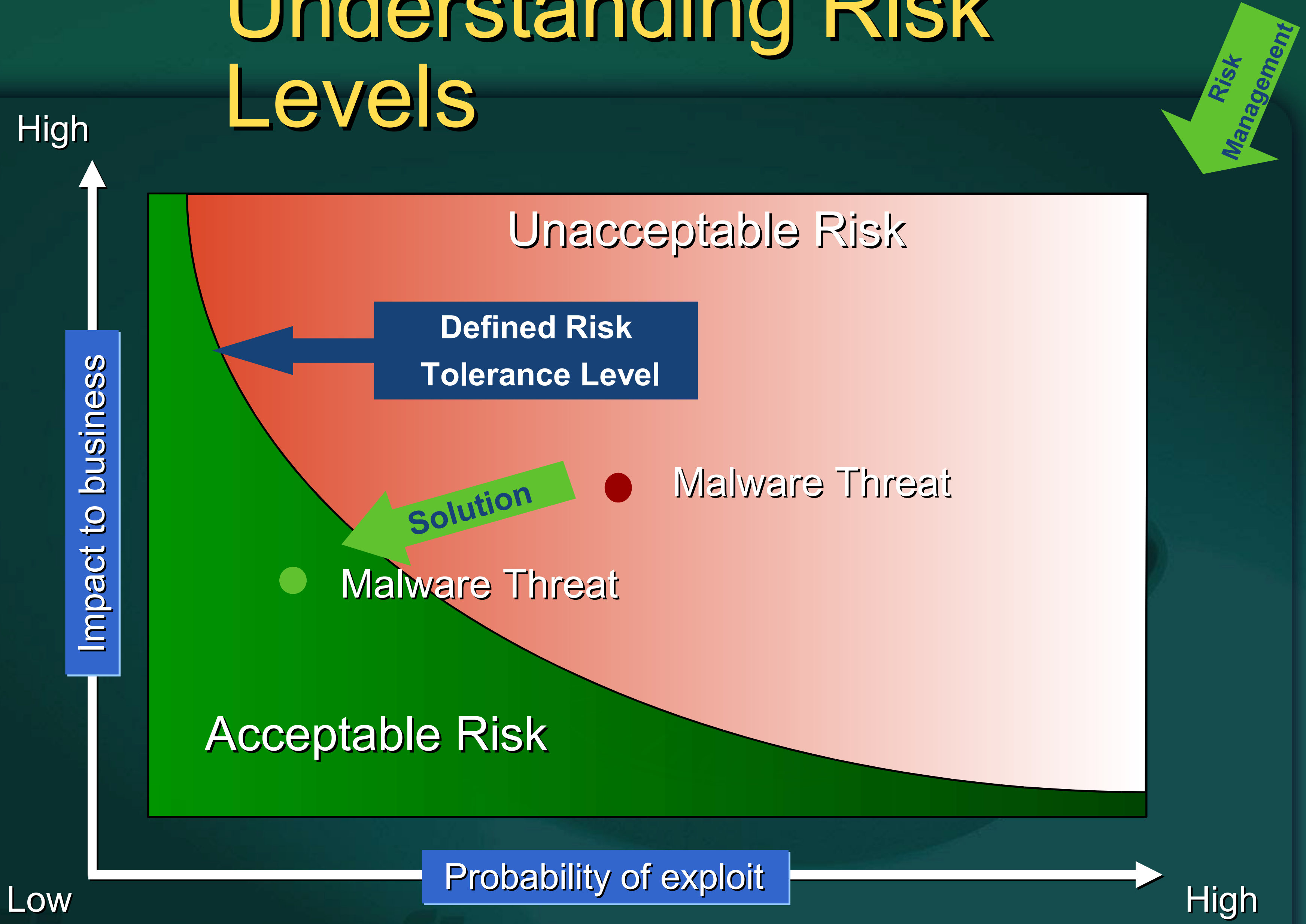
- Communication to:
  - Management
  - Press
  - Government

Planning

- Remove the intruder
  - Understand exploit
  - Stop attack vectors
- Remediate the incident
  - Create a trusted zone

Incident Remediation

Understanding Risk Levels



Remediation

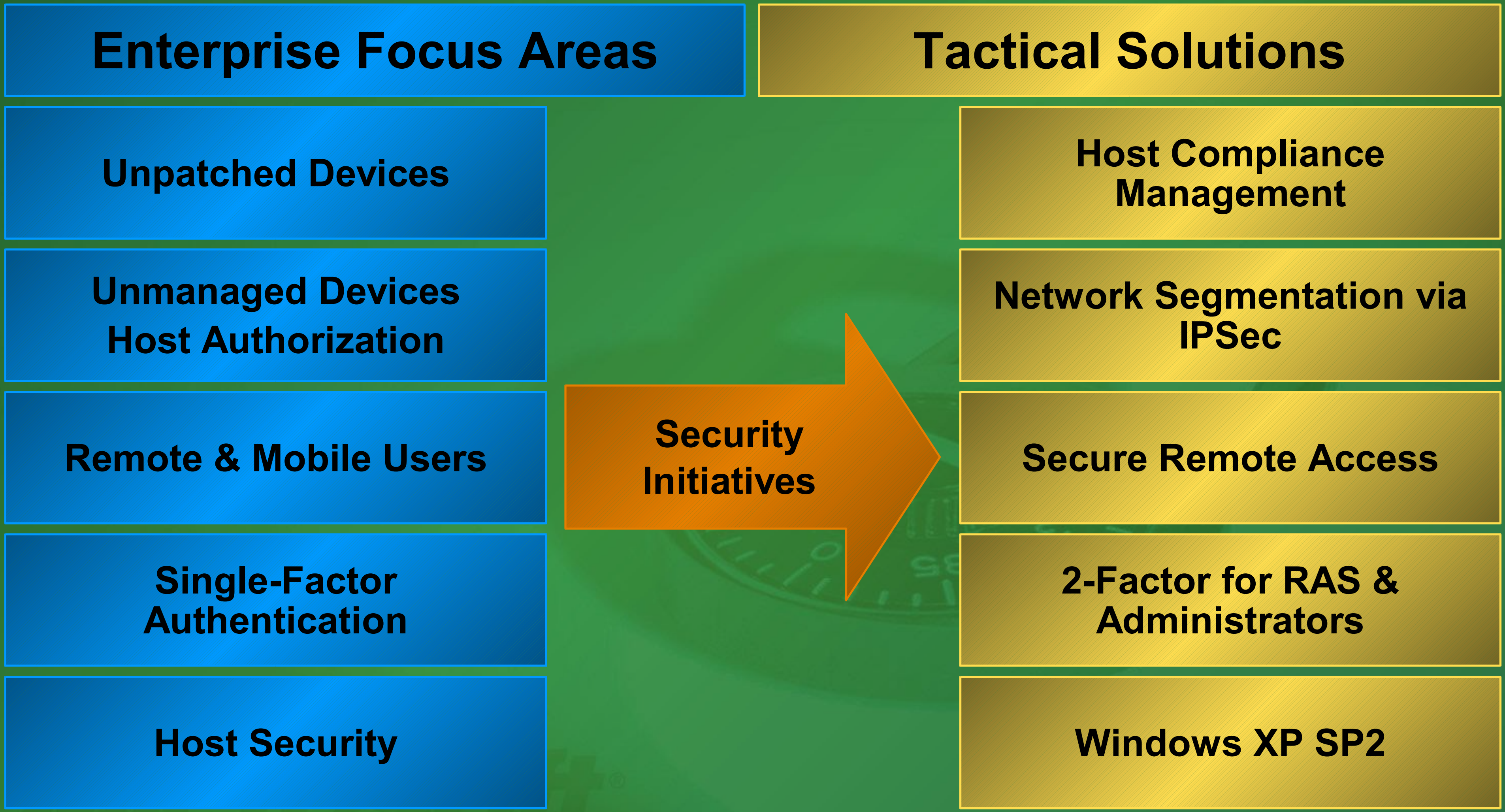
- This is where you actually fix the problem
  - Install AV
  - Remove exploits
  - Rebuild systems
    - Some times the hardest for organizations to accept

Proactive

- Monitor and prevent incidents
  - Monitor
    - IDS
    - Log Management
    - Systems Management
    - Etc…
  - Prevent
    - FW
    - IPSEC
    - Certificate usage
    - Etc…

MS IT approach to identified risks

MS IT Primary Risks and Tactics



Enterprise Focus Areas

- Unpatched Devices
- Unmanaged Devices Host Authorization
- Remote & Mobile Users
- Single-Factor Authentication
- Host Security

Security Initiatives

Tactical Solutions

- Host Compliance Management
- Network Segmentation via IPSec
- Secure Remote Access
- 2-Factor for RAS & Administrators
- Windows XP SP2

Success Factors

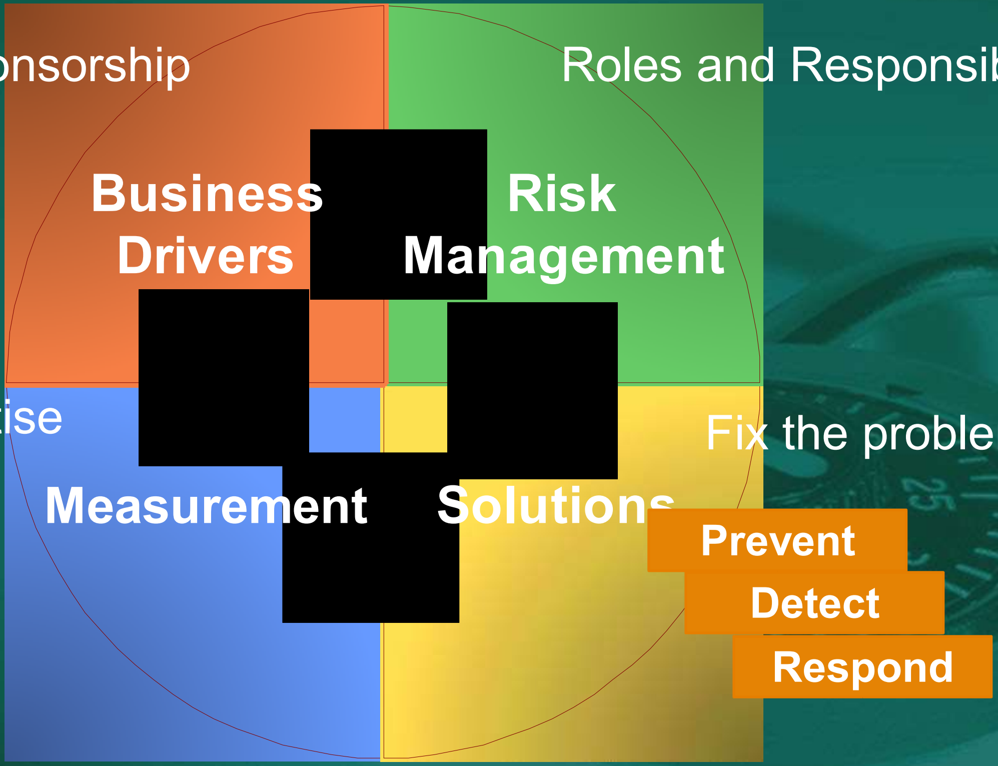
- Executive sponsorship
- Overcome denial and blame
- Fix the problem
- Internal expertise
- Roles and Responsibilities

Success Factors

Overcome denial and blame

Executive sponsorship

Roles and Responsibilities



Business Drivers

Risk Management

Measurement

Solutions

Prevent

Detect

Respond

Internal expertise

Fix the problem

Case Study

You’ve been Hacked!

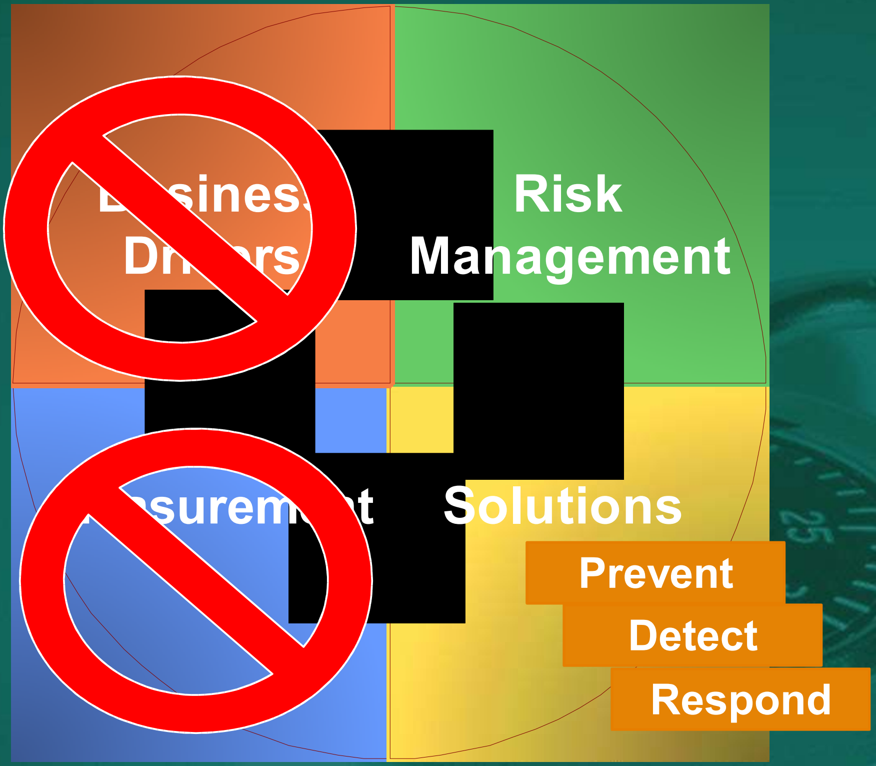
Company X Scenario

- We have 4 subsidiaries in the company
  - Sub 1 makes bombs for the government
  - Sub 2 makes consumer electronics
  - Sub 3 makes shoes
  - Sub 4 makes fishing poles
- We outsource most of our sub 1 infrastructure to a third party, All other subs manage their own infrastructure
- Our infrastructure outsourcing company has discovered a root kit on some key servers in sub 1
- The outsourcer has invited a few other consulting partners in on this incident and they have spent the past few months watching the hacker make moves on honey pots etc

Company X scenario continued

- They have identified that the hacker entered the infrastructure via sub 3
- Security consultants are invited to help with this incident by the outsourcing partner, after 2 months pass with no resolution
- The outsourcing partner was frustrated because they were blamed for the incident but were not able to resolve the issues because the initial breach was not under their control.
- One of the 4 consulting companies has worked to take a leadership role in the engagement and proposes a 5 firewall 3 DMZ model which they say will resolve the issue

Company X situation



Business Drivers

Risk Management

Measurement

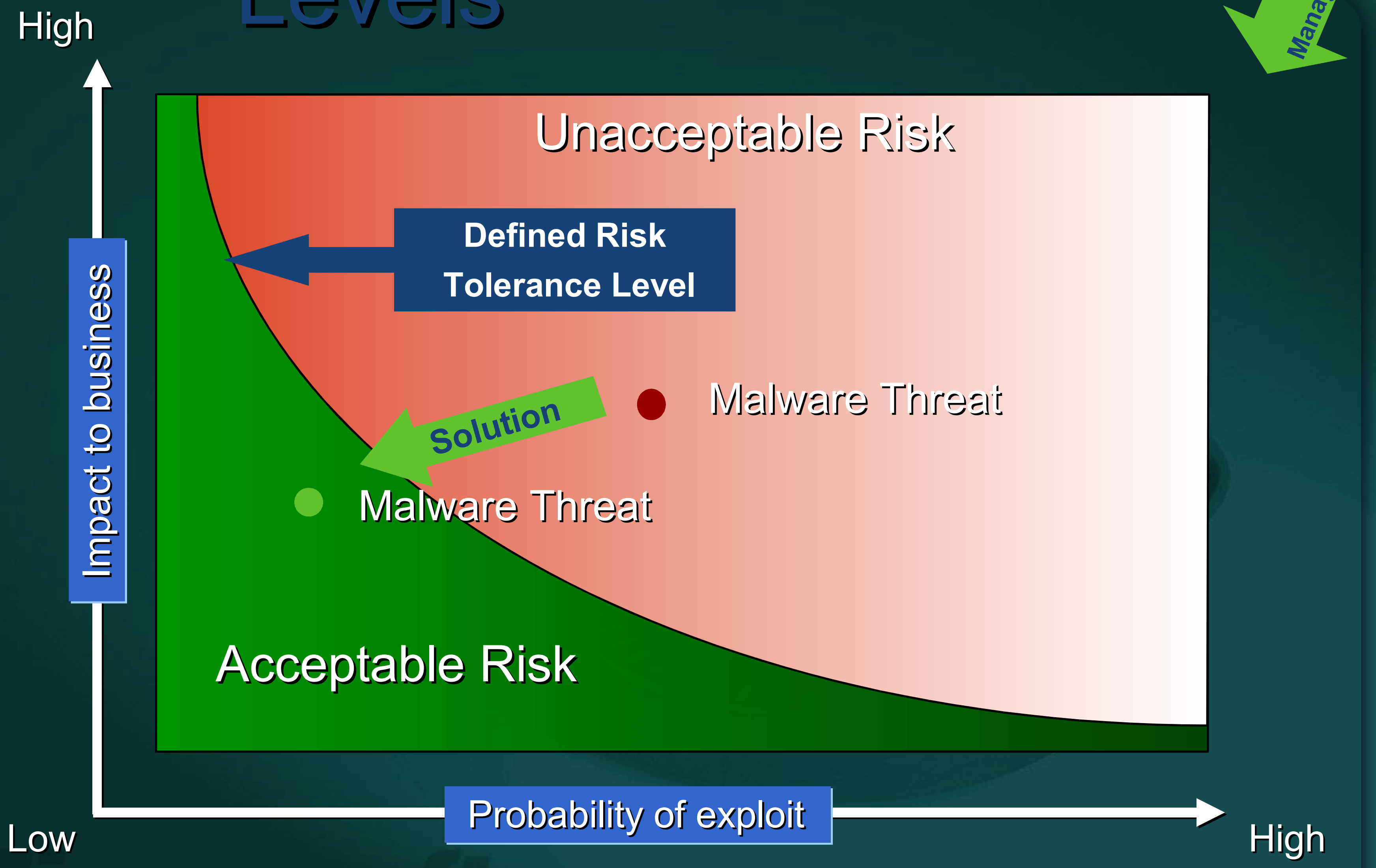
Solutions

Prevent

Detect

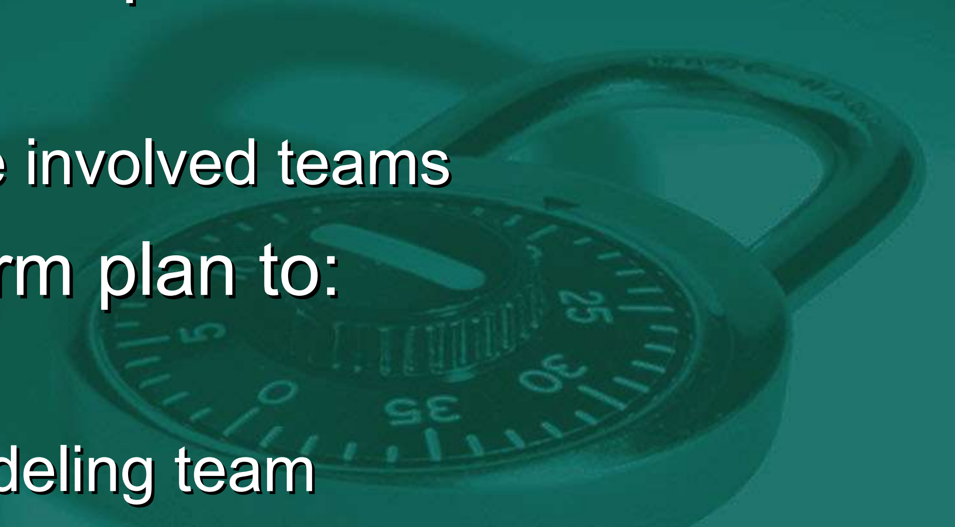
Respond

Understanding Risk Levels

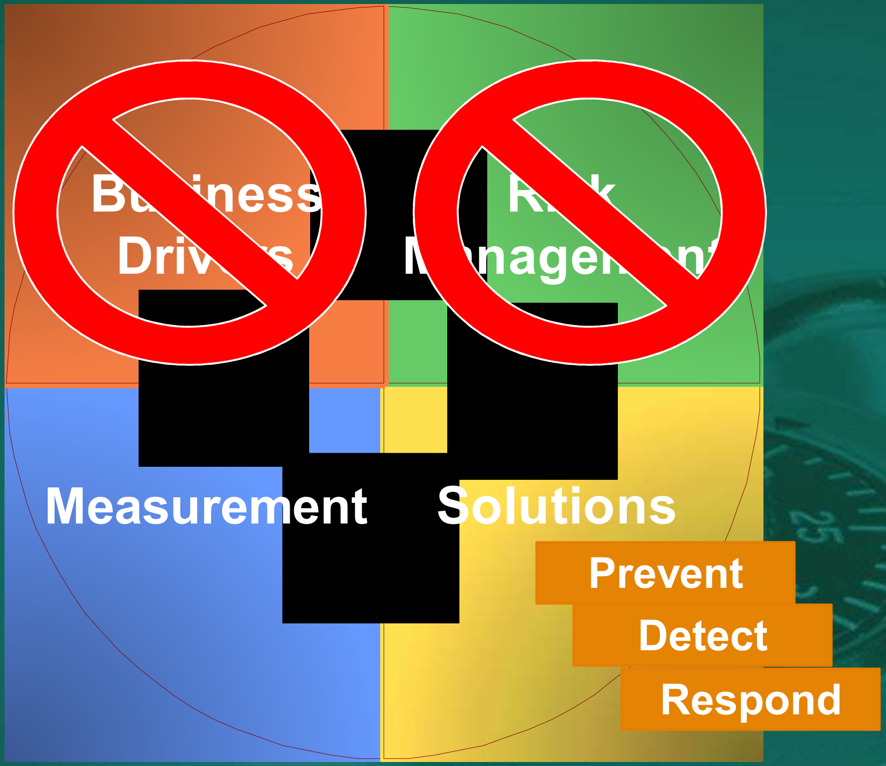


What was the resolution?

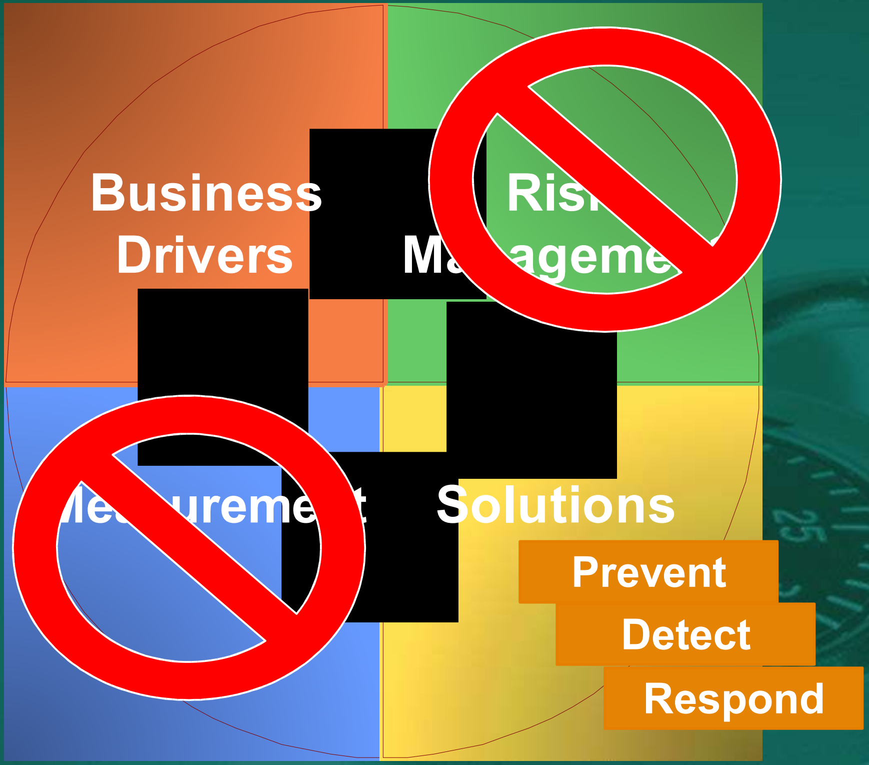
- Roles and Responsibilities need to be solidified
  - Someone needs to take responsibility for the overarching security of the system and manage both sub 1 and 3.
- Create a short term plan to:
  - Stop the breach
  - Manage all of the involved teams
- Create a long term plan to:
  - Rebuild systems
  - Create a risk modeling team
  - Create a risk management program
  - Create an incident response program



Company Y situation



Company Z situation



Reference

- CSIRT Handbook
  - http://www.sei.cmu.edu/publications/documents/
- COBIT
  - http://www.isaca.org/cobit
- Microsoft security
  - http://www.microsoft.com/security