


Information Security Management

Approaches to Managing an
Information Security Program

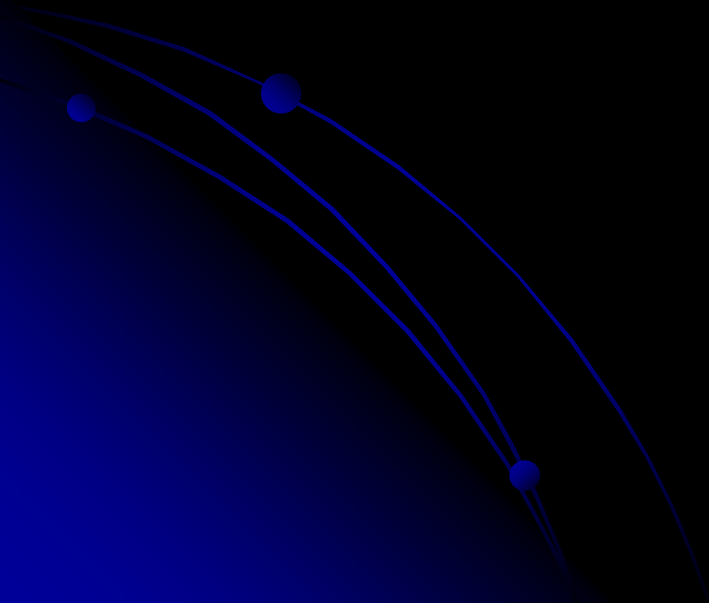
Daniel Charboneau



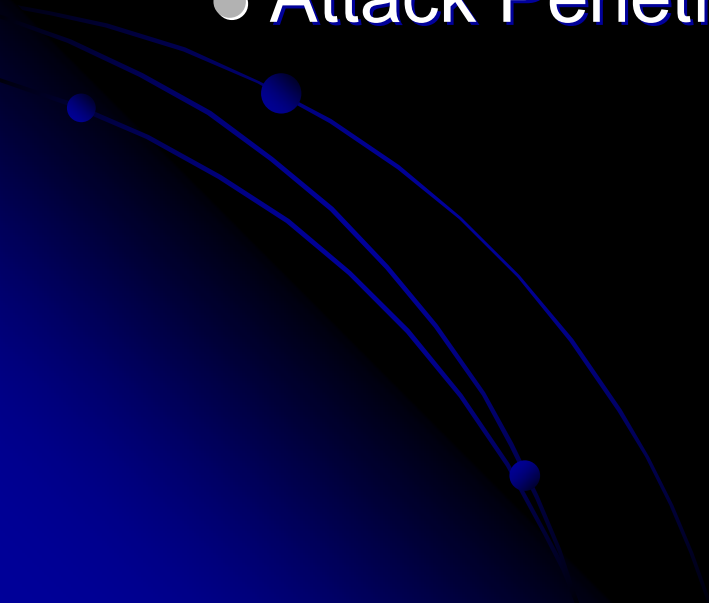
Agenda

- Models for creating Security Programs
 - Program Management Primer
 - What constitutes a Security Program
 - Where to Start
 - Metrics
 - Closing
 - Discussion on Security Information Management Solutions
- 


Models for creating Security Programs



“A Vision Without Resources is a Hallucination”

- Approaches to developing an Security Program
 - Consultative
 - Academic
 - Attack Penetration
- 

Consulting Approach

- Identify processes or systems with the highest risk to the company
 - Create attack maps for all relating systems
 - Implement protection strategies for each attack vector
 - Time, Quality, Cost ?
- 

Academic Approach

- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- OCTAVE is **different from typical technology-focused assessments**. It focuses on organizational risk and strategic, practice-related issues, balancing operational risk, security practices, and technology.
- Time intensive,
- Requires business understanding and “Buy in”
- Works well in already established Security Programs moving to the next level.
- Once again, From the creating a base security program, Using just this approach with out a management program in place introduces risk.

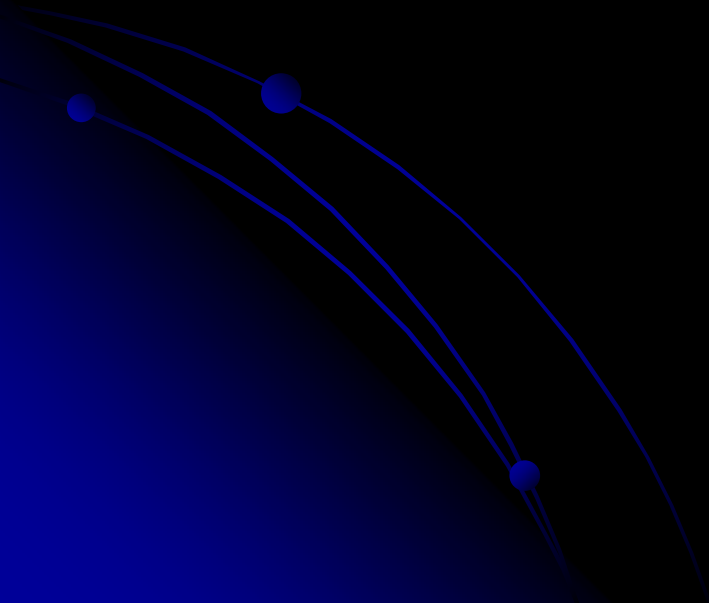
Attack Penetration Method

- Continuously attack and assess the effectiveness of controls in place.
- Doesn't directly address the Policy and Program Aspect of the Information Security Program
- Requires skilled staff or consultants
- Is generally better left as part of a Information Security strategy, It should not drive the program.
- Ignores the Support Maintenance and Operational concerns of a program

Issues With Existing Models

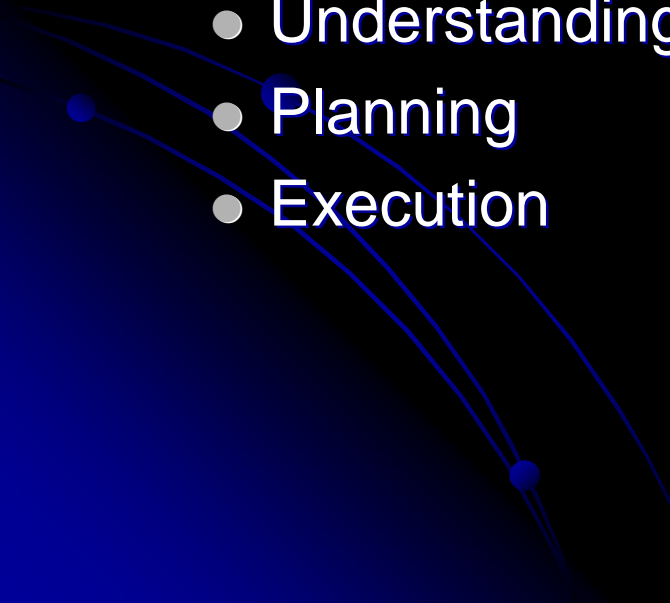
- Existing Models work are based on basic protection mechanisms and Support Maintenance and Operations in place.
- The do not Address the overall Program Aspect from existing workload and SMO
- Realistically can generally only be used in Mature environments.
- What happens to the Security Posture of the company while you execute? What will get you fired today.

Program Management Primer



Managing a Program

“Hope is not an Action Plan”

- Without a well defined management philosophy the best security policies and technologies in the world are not enough to secure an environment.
 - Demand Management
 - Capacity Management
 - Understanding of Time investments (Time Control)
 - Planning
 - Execution
- 

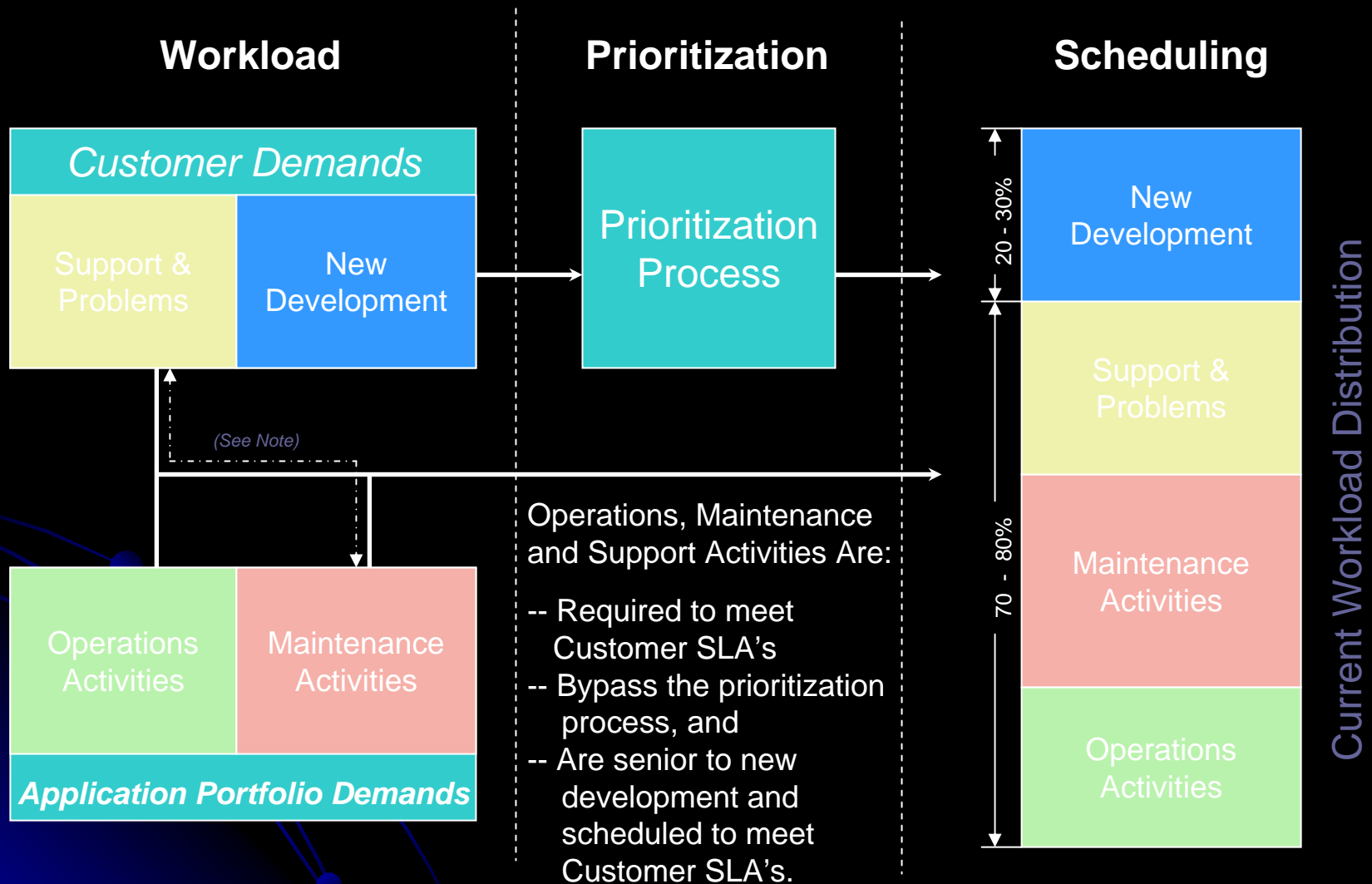
Critical Success Factors

- Strategy Drives Process Drives systems
Drives Solutions
 - Understand the Building blocks of the program and where you want to be
 - Create a road map based on Capacity, Demand and other constraints to provide a realistic security approach
 - METRICS!!! Ensure that the security strategy aligns with the business.... CONSTANTLY prove Value

Understand your Workload

- To effectively manage a program, a philosophy / strategy must exist.
- Understand your constraints
- Understand your Capacity
- Understand your Workload and Time investments
 - Four Categories of work:
 - Support – Maintains Value
 - Operations – Maintains Value
 - Maintenance – Maintains Value
 - New Work – Value Add

Workload Management



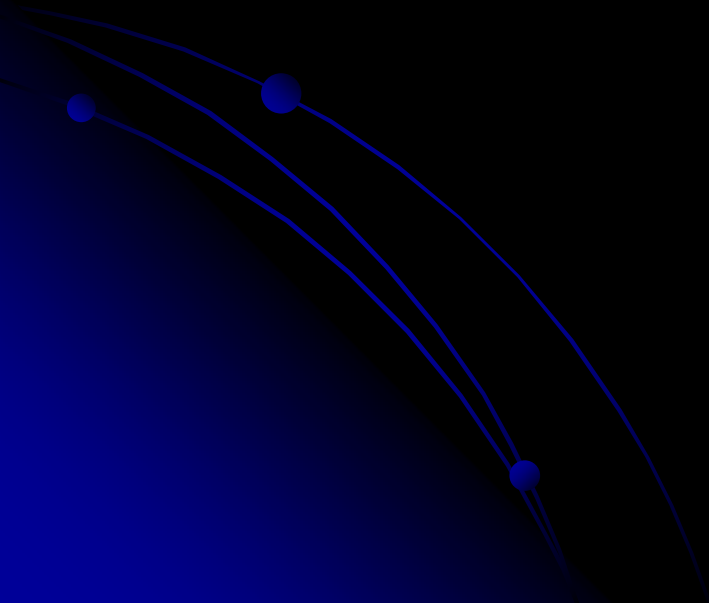
Note: Some support & problems are reported from the customer but are in reality maintenance issues.

Workload Management

Workload Distribution Target



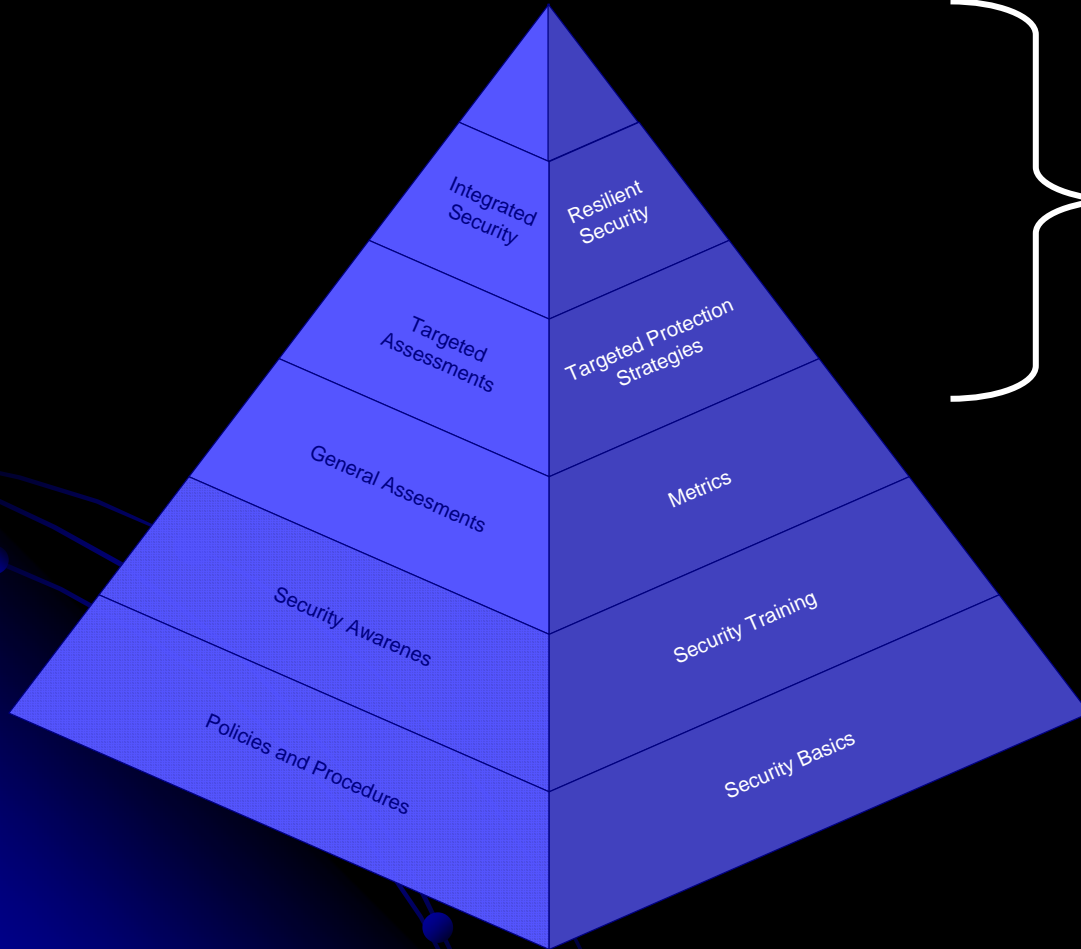
What constitutes a Security Program



Definitions

- **Defense In Depth – General Protection Strategy**
 - Layered Technical Security Controls to establish a Secure Infrastructure
- **Targeted Security**
 - Additional Layers of Technical and Administrative Security Measures created to protect specific critical assets
- **Integrated Security**
 - Administrative, Technical, and Cultural changes working together to create a coherent security program.
 - Executives and Business partners thinking about security first
 - Users aware of Security Implications
 - Technology enabling secure transportation, storage, and access control to critical assets
 - Enterprise wide visibility for Information Security issues

Program Breakdown

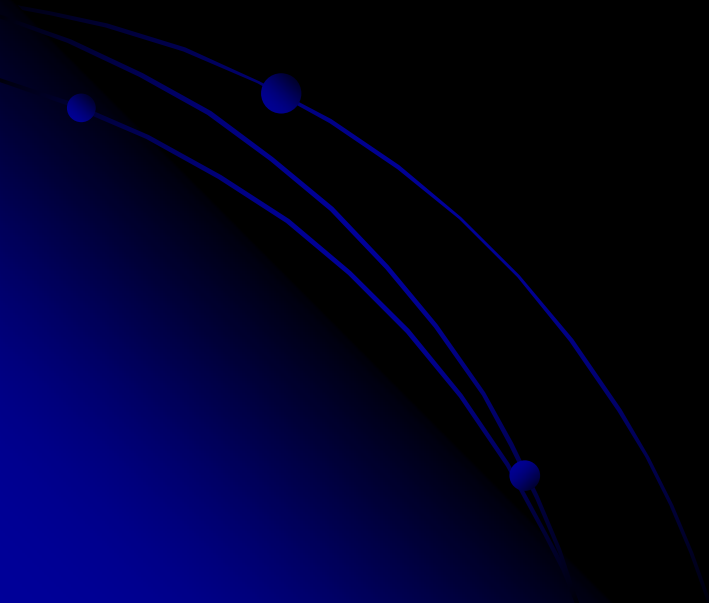


Dependent on Execution of Level 1 & 2

<u>Cost</u>	<u>Value</u>
20%	80%
80%	20%

Foundation needs to be built first

Where to Start



Foundations

- Ensure the Minimal Operational Security Measures are in Place and Have Policies
- Base/General protection Strategies
 - These are tools or process that provide equal protection across your environment such as:
 - Antivirus
 - Patch Management
 - Change Control
 - Anti-SPAM
 - These controls need to be in place and policies written and enforced immediately. General Protection Strategies are what constitute the BASE or minimum protections upon which you can build a security program and provide value.
- Policy
 - Create a Holistic Policy set concurrently with Basic Operations
- Incident Response PLANS in place and tested!
- FIX / Maximize the BASE first. While the largest risk is the Data or Intellectual property that a company possesses, It is impossible to protect the critical assets without a strong foundation in place.

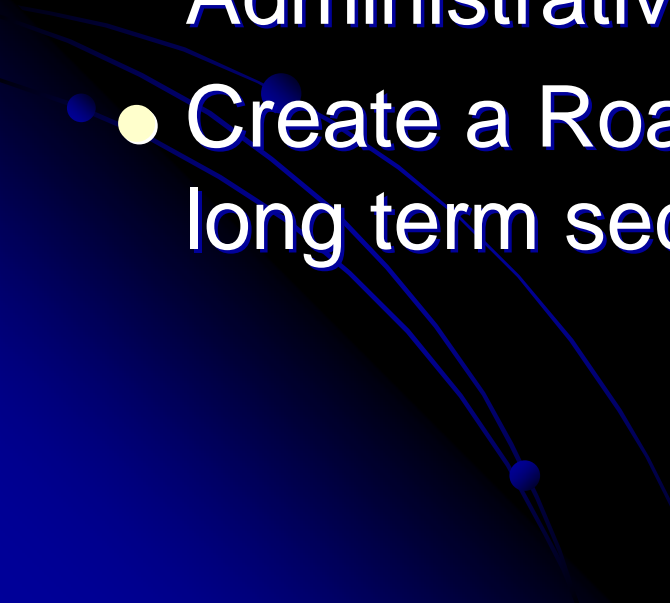
CMMI for InfoSec

- Capability Maturity Model Integrated (CMMI) is a concept/methodology to gauge how well any function is performed. There are six Levels:
- CCM – 0 Not Performed
- CMM – 1 Performed Informally
- CMM – 2 Planned and Tracked
- CMM – 3 Well Defined
- CMM – 4 Quantitatively Controlled
- CMM - 5 Continuously improving

Workload Matrix

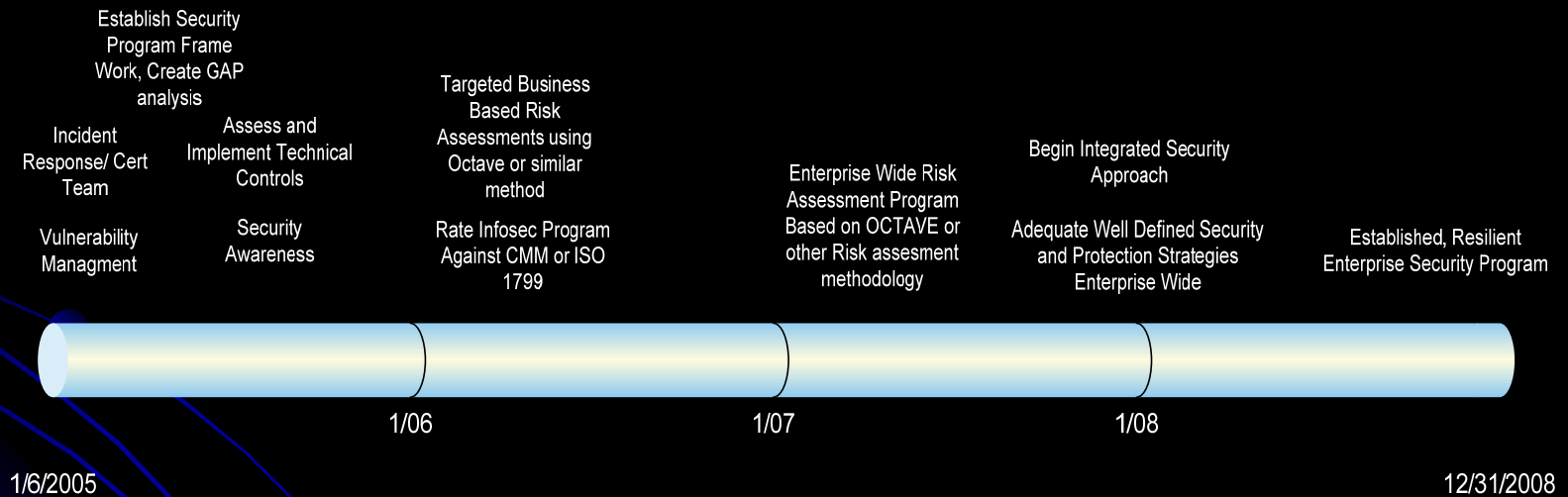
<i>Activity</i>	<i>Responsible Group/Person</i>	<i>D ai ly</i>	<i>We ekly</i>	<i>Mon thly</i>	<i>Quar terly</i>	<i>Semi- Annually</i>	<i>Ann ually</i>	<i>Estimat ed Time</i>	<i>Po lic y</i>	<i>Process Document</i>
Review Antivirus Logs	Information Security Administration Group							N/A		
Review Virus Activity	Information Security Administration Group	X						20min		4.1.7.2 Malicious Software and Anti-virus.doc
Review Dat Compliance Rate	Information Security Administration Group	X						20min		4.1.7.2 Malicious Software and Anti-virus.doc
Review AV install Compliance Rate	Information Security Administration Group	X						20min		4.1.7.2 Malicious Software and Anti-virus.doc

Next

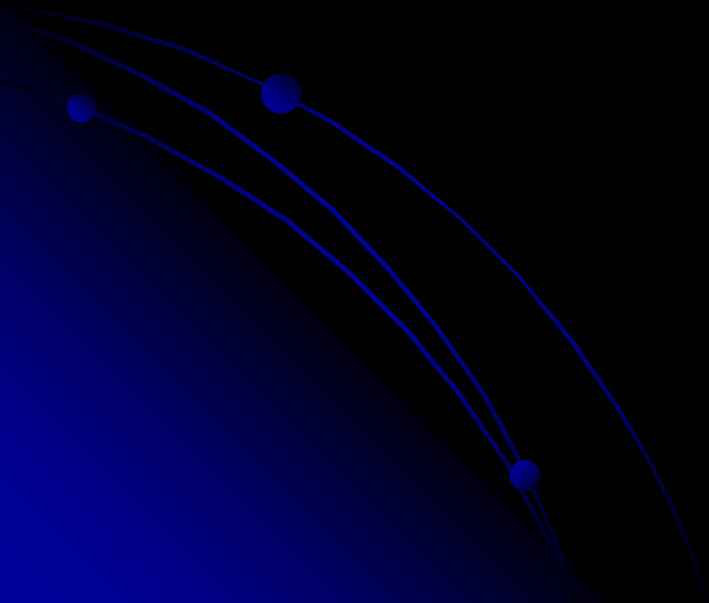
- Only after the Basics are in place and you have a functional operational framework can you think strategically.
 - Assess the current Technical and Administrative Security Architecture.
 - Create a Roadmap for implementing your long term security strategy...
- 

Where are you going and how do you plan to get there?

Information Security Roadmap



Metrics



Metrics What?

- The most often overlooked part of a successful security program is ensuring you can prove that you are Successful.
- Metrics in Information Security are generally readily apparent. Start with what you can track and impact.
- Antivirus, WebFiltering, AntiSpam, etc.
 - Tie these metrics to Costs from realistic potential loss
 - Tie metrics back to Operational Gains in productivity
 - Helpdesk Calls
 - Storage
 - Wasted Productivity
- Strong Metrics are the fastest way to get in front of the Board or Executive Staff.

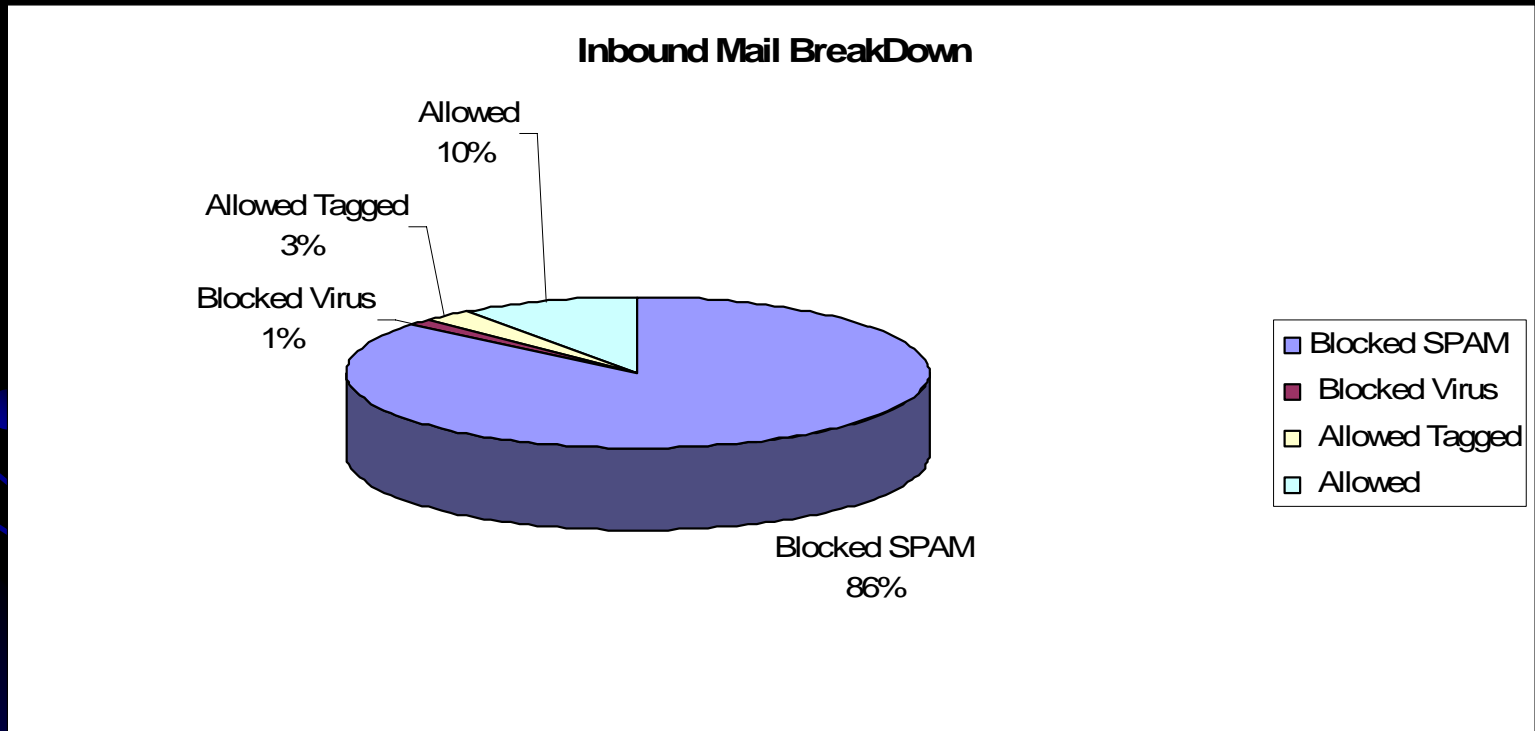
Key Metrics

- SPAM
 - Risk
 - Lost Productivity
 - Wasted Storage
 - Virus
 - Phishing – Loss of confidential information, personal, or business related.
- Antivirus
 - Risk
 - Loss of confidential information
 - Downstream Liability (Infecting other companies or clients)
 - Lost Productivity (Sasser Outbreak in April of 2004 took 3 days to resolve and estimated cost of \$40,000 dollars over three days)
- Websense
 - Risk
 - Lost productivity
 - Network Bandwidth waste
 - Legal Liability (HR, Security, Etc)
 - Virus, Phishing, Security violations, Spyware infection due to browsing habits.

Key Metric: SPAM

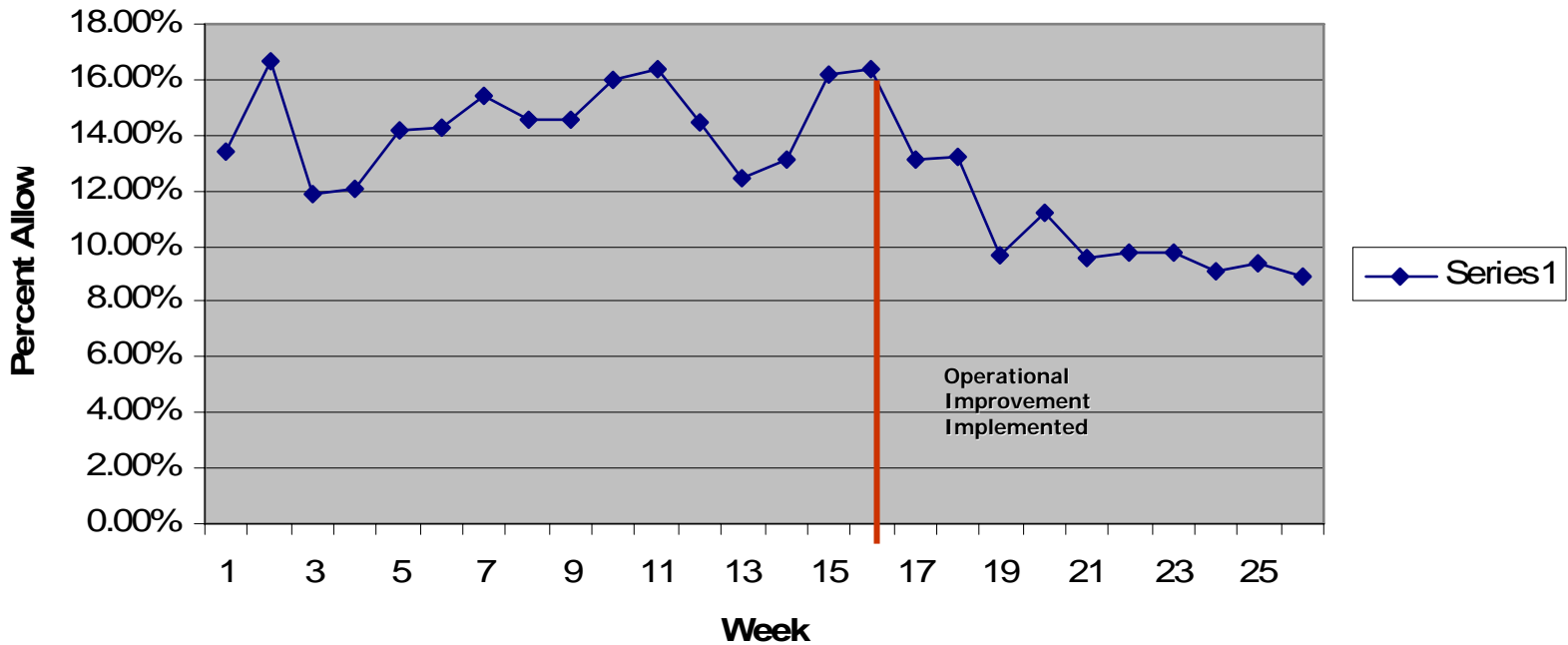
- **Year to Date Cost Avoidance of \$1,145,000**
- Weekly Cost Avoidance of \$60,000
- Reduced Inbound Spam by 90% for most users. This equates to one Spam Message a day per user.
- Inbound Mail Stats
 - 10% of all inbound mail is accepted.
 - 1% of all Mail is blocked due to Viruses
 - 3% Is tagged as possible SPAM.
 - 86% Is blocked as SPAM
 - Average number of messages inbound a week is 800,000 Messages.
- Average time to Managed the SPAM Filter is 6 hours a week.

Spam – Inbound Mail breakdown Year to Date



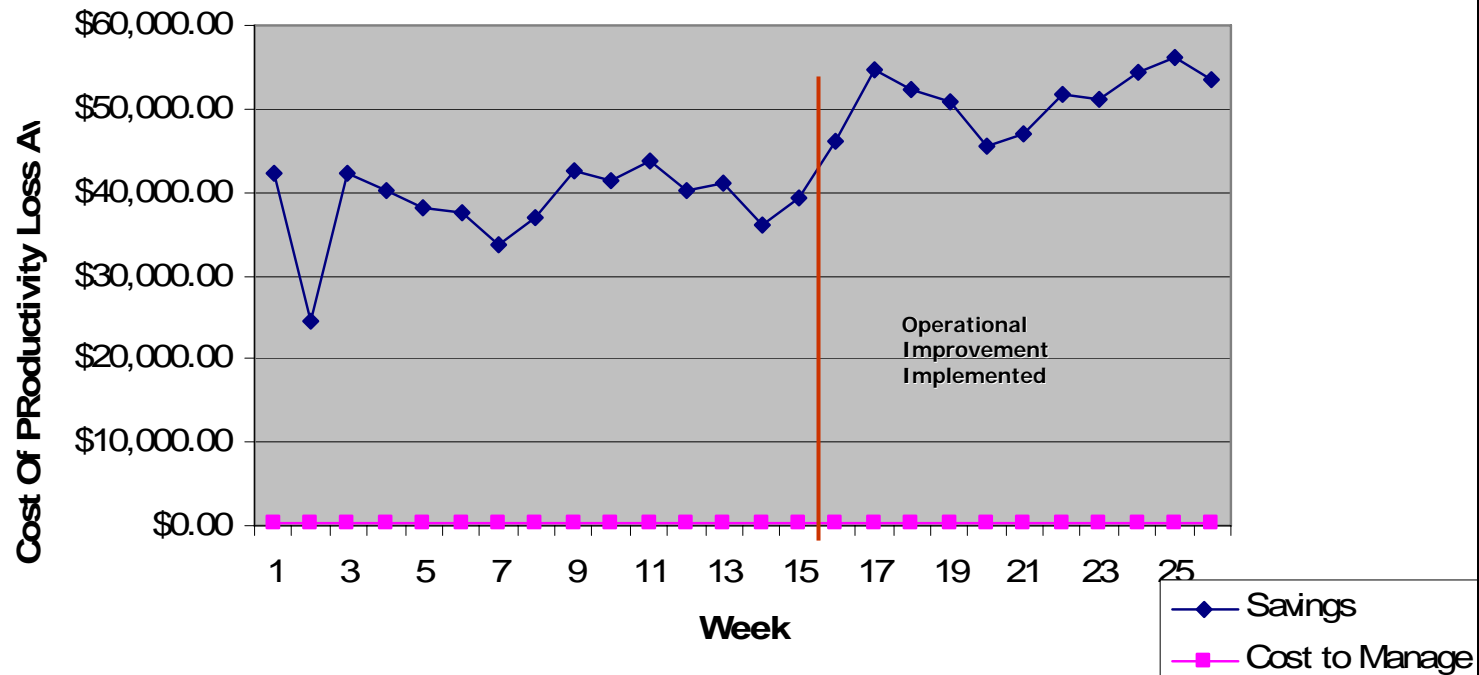
SPAM – Improvements

Percentage of Inbound Mail Allowed



Spam – Cost Avoidance

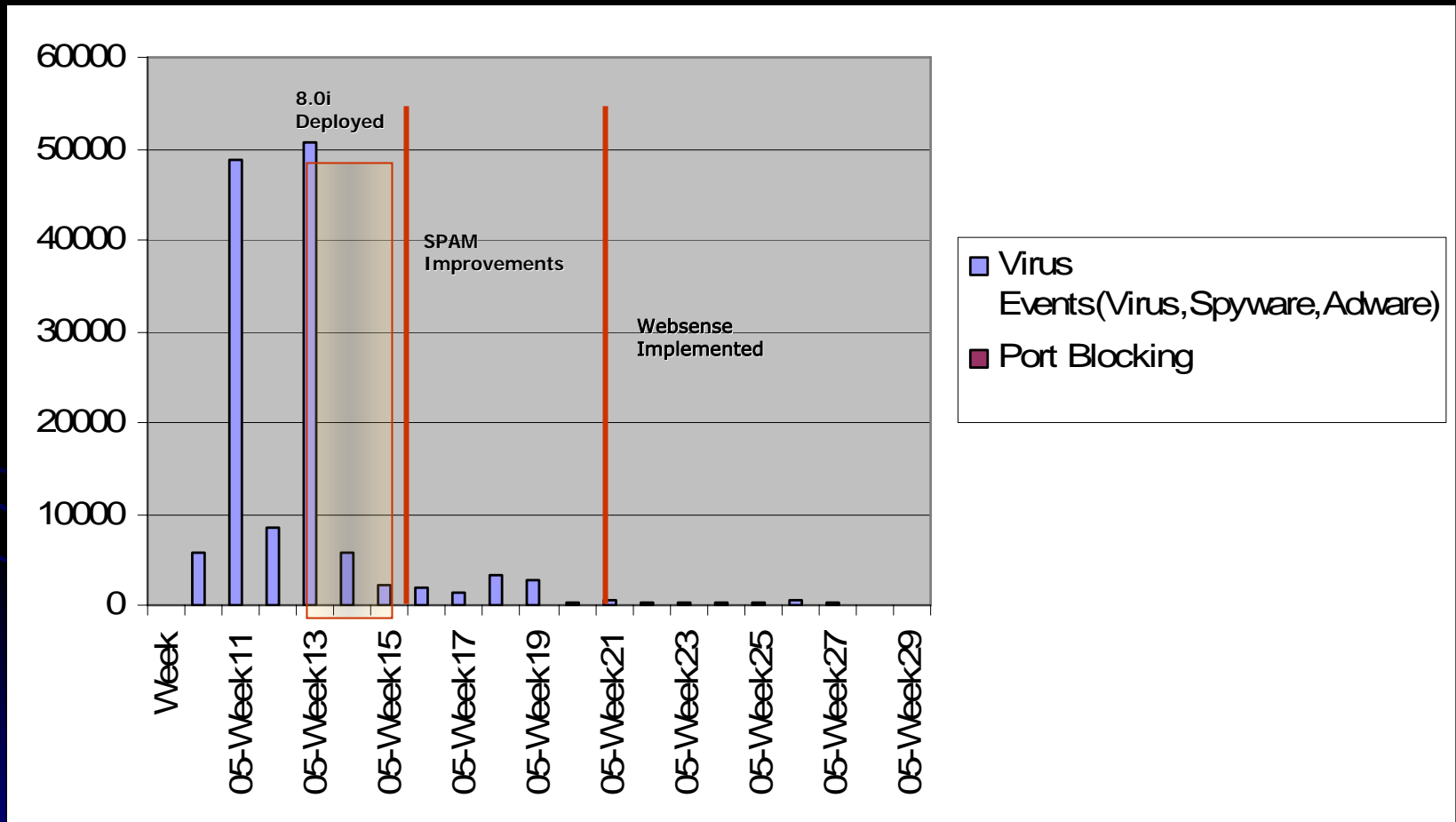
Cost Avoidance Saving of Spam Blocked



Key Metric: Antivirus

- Average number of detected or prevented attacks is 210 down 90% from 1,000 a week last year.
- Average Deployment rate is 95% of all workstations.
- Average time to update new Pattern files across the network is 90% in one hour.
- Estimated cost Avoidance due to Virus, Spyware, or Adware incidents is \$10,000
- 3 Non Adware/Spyware events have been detected at a workstation in the past 6 months.
- On Average Spyware event is handled a month.

Antivirus – Trends



Key Metric: Websense

- Estimated Cost avoidance of \$5,000 Dollars a month.
- Reduced detections of Spyware/Adware attempts by 90%.
- Reduced Bandwidth Utilization as much as 40% in some locations resulting in more available bandwidth for work related applications and an 80% reduction in Trouble tickets related to Internal Applications.
- Reduced [company X]'s risk relating to Employee browsing habits (Human Resources, Security, etc)

Overall Cost Avoidance of Protective Measures

Antivirus Monthly: \$10,000

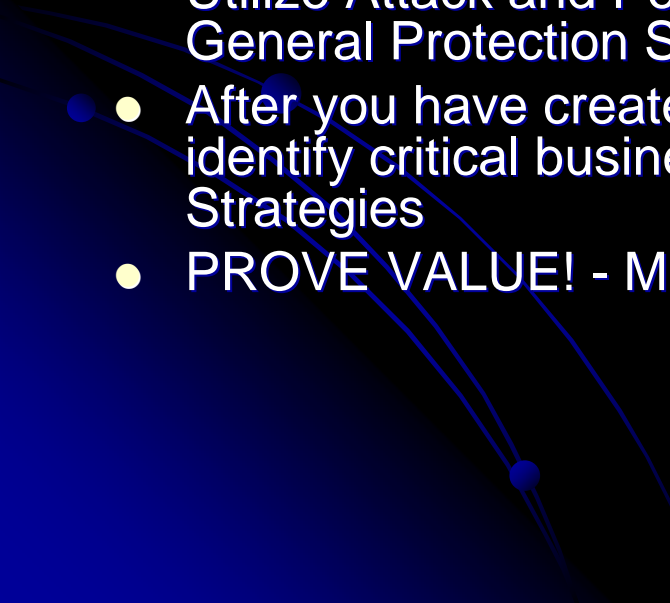
Websense Monthly: \$5,000

SPAM Protection Monthly: \$240,000

Total Monthly Cost Avoided: \$255,000

Year to Date: $\begin{array}{r} \times \quad 8 \\ \hline \end{array}$ \$2,040,000

Conclusion

- Start with the Basics:
 - Policy
 - Patch Management
 - Antivirus
 - IPS
 - Change Control – Desktop, Server, Network
 - Have a Strategy and Vision to ensure your Support Maintenance and Operations are Reduced or Streamlined with CMMI Concepts. Utilize Attack and Penetration Testing to further develop your General Protection Strategies
 - After you have created an Established base utilize OCTAVE to identify critical business risk and create targeted protection Strategies
 - PROVE VALUE! - Metrics
- 

Resources

- OCTAVE – www.cert.org
- CMMI for InfoSec www.iatrp.com
www.sei.cmu.edu/cmmi/
- **The Executive Guide to Information Security** by Mark Egan with Tim Mather, Symantec Press

System Hierarchy

Today

Level 4 Security Intelligence

This is **ASPRIRATIONAL** until levels 1,2 and 3 are in place

- Product Line Profitability
- Warranty Analysis
- Market Share Analysis
- Customer Satisfaction
- Sales – Product/Channel

- Manual analysis
- Pay Premium for Operational elasticity
- Difficulty Integrating Acquisitions
- Near Teams Planning focus
- Little Decision support
- Management Information

A lot of data, no information to make decisions

Dependent on Execution of Level 1 & 2

Level 3 Operating, Planning & Control Systems

- Supply Planning
- Demand planning
- Shop Scheduling
- Inventory Control
- Maintenance Scheduling
- P&Ls
- Production planning
- Distribution planning

- Work-around Ad Hoc systems
- Continually Bridge systems
- Single Purpose interface
- No Process ownership
- Inconsistent Data
- Expensive to Grow and Maintain

Spend too much of our time reconciling and justifying data

Cost	Value
20%	80%

Level 2 Transactional Management

- AV Alerts
- IDS/IPS Alarms
- Work Orders
- Log Parsing
- Claims
- Payments / Invoices
- Serial Numbers

- Extensive Manual interfaces
- Untimely Delivery cycle
- System instability
- Inflexibility

80%	20%
-----	-----

Foundation needs to be built first

Data is the foundation, timeliness and accuracy are critical

Level 1 Core Technical Security Management

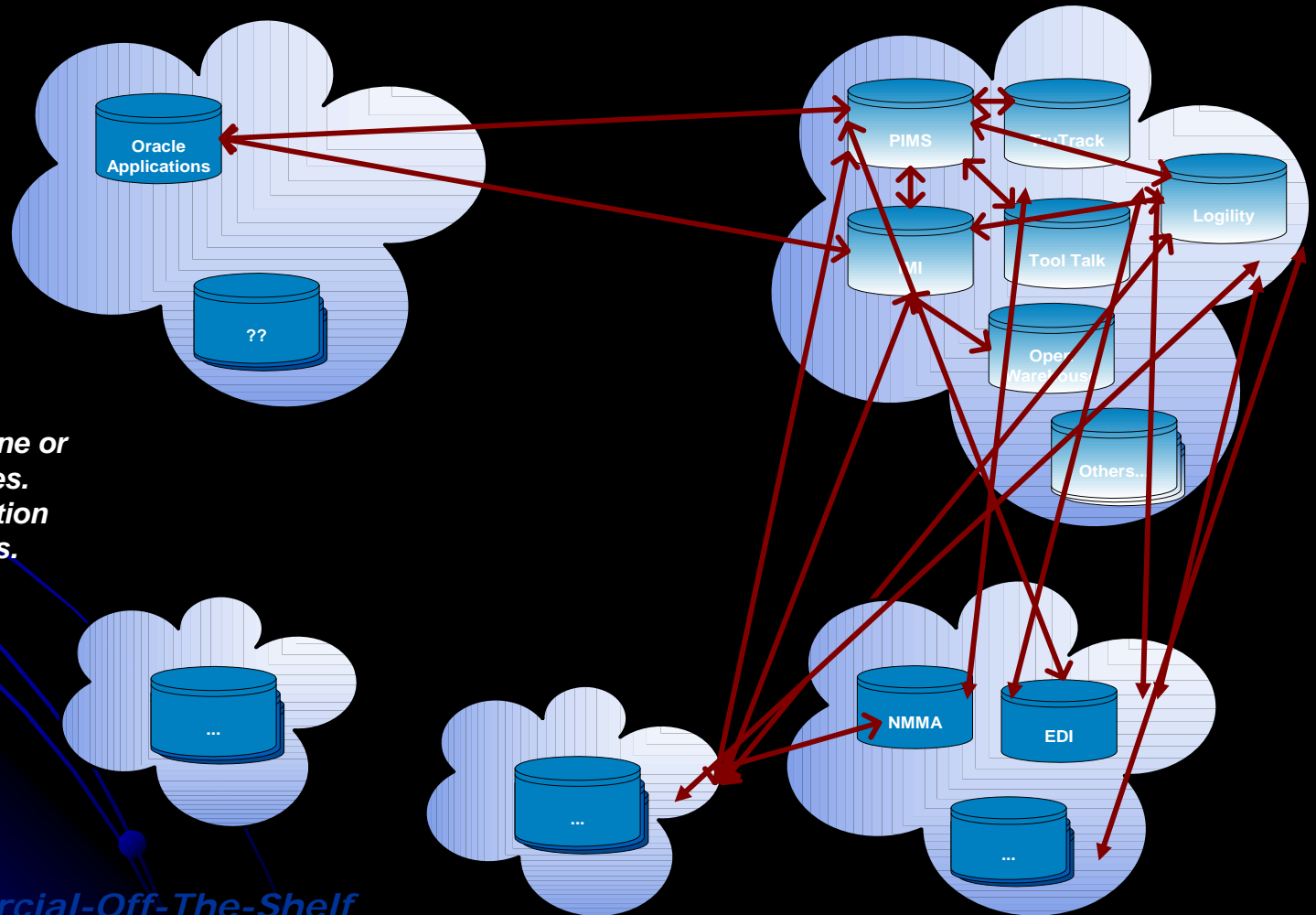
- IDS
- IPS
- Anti-X
- Firewalls
- HIPS
- Routers, Switches

- Multiple Vendors
- Suspected Data moved across
- Multiple platforms
- Unmanaged Data Sources

Common Security Model

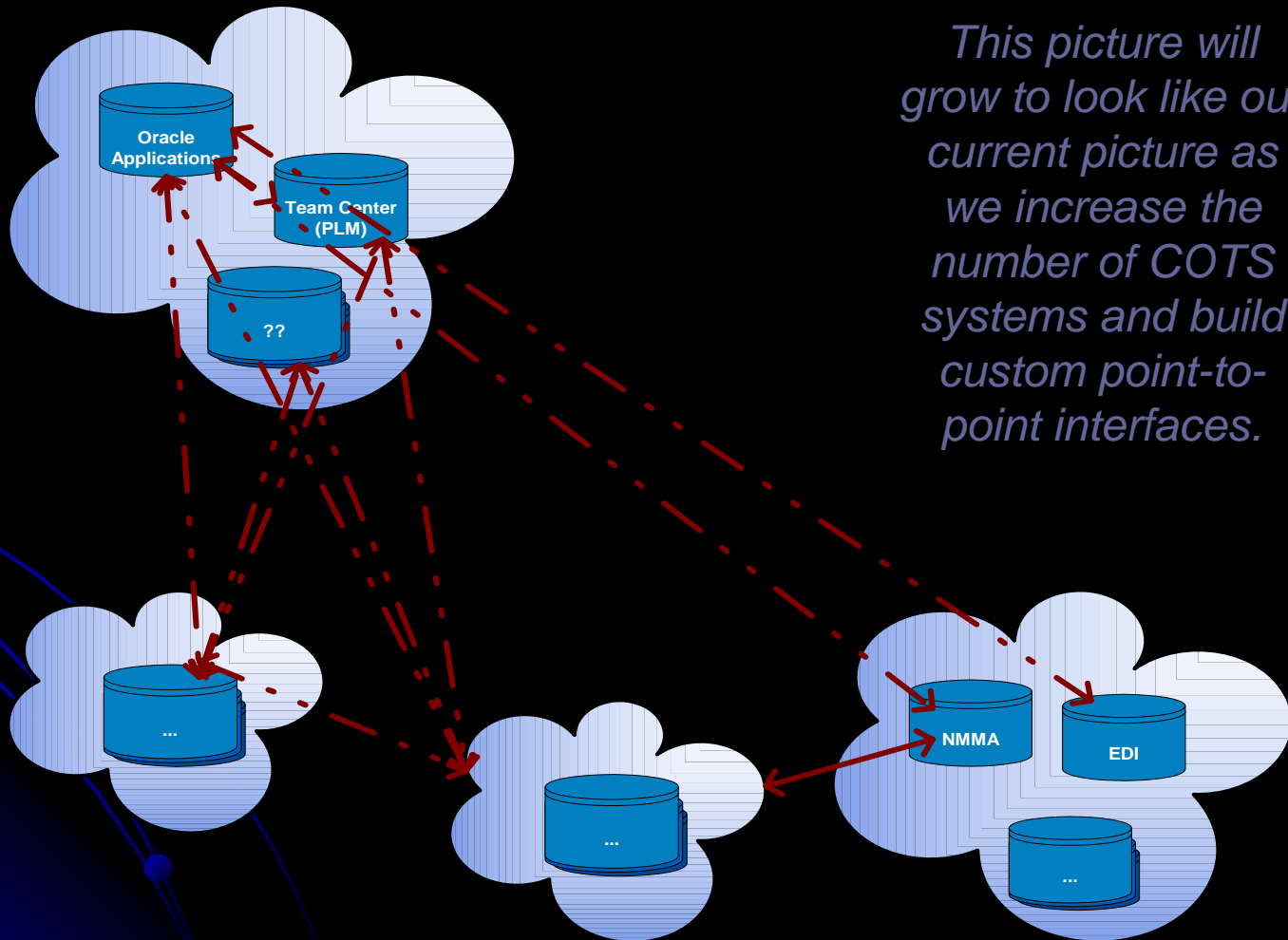


As-is Integration (the problem space)



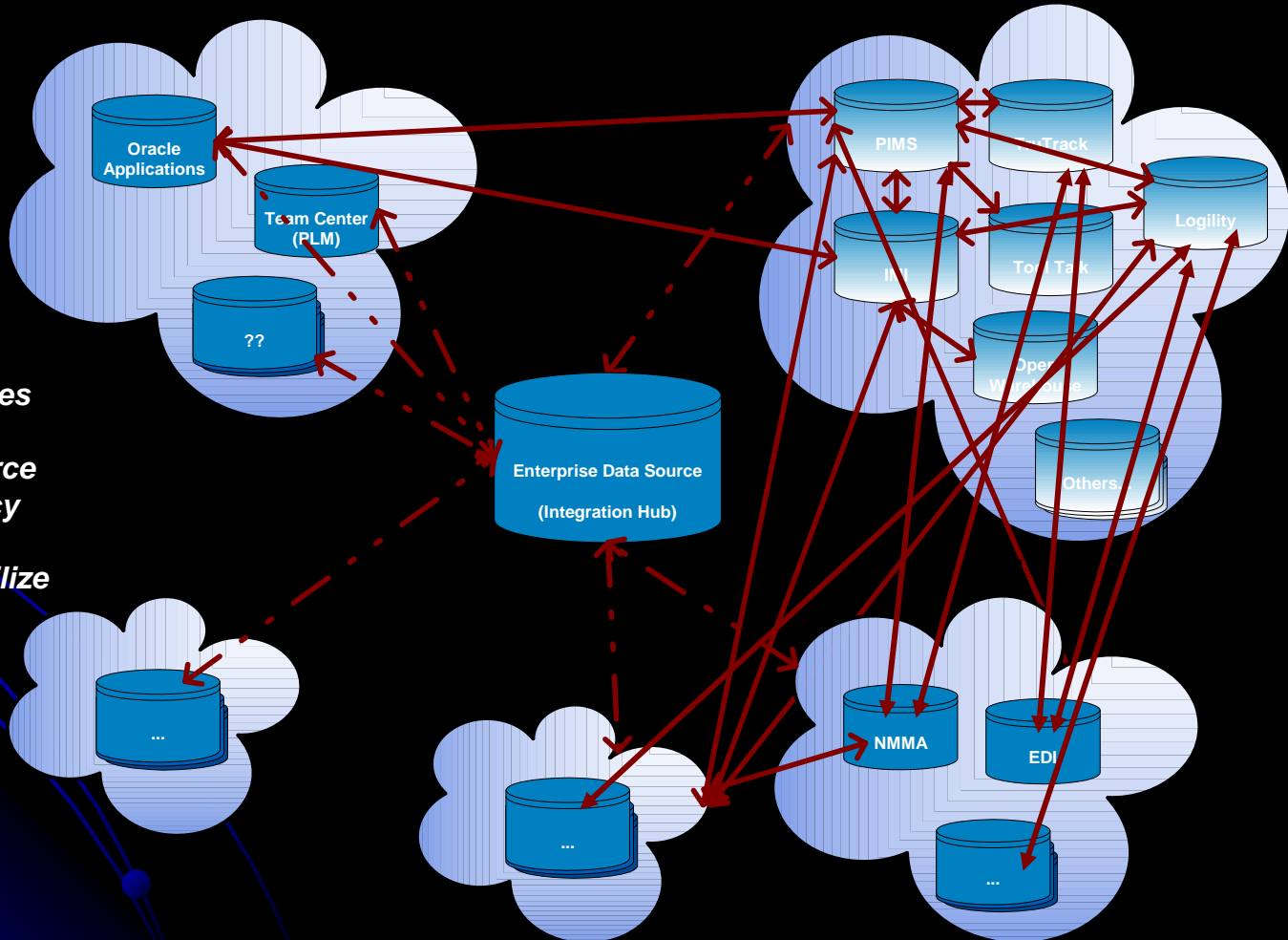
Each line represents one or more types of interfaces. Data flows in the direction indicated by the arrows.

If we continue to build interfaces the way we have in the past.



This picture will grow to look like our current picture as we increase the number of COTS systems and build custom point-to-point interfaces.

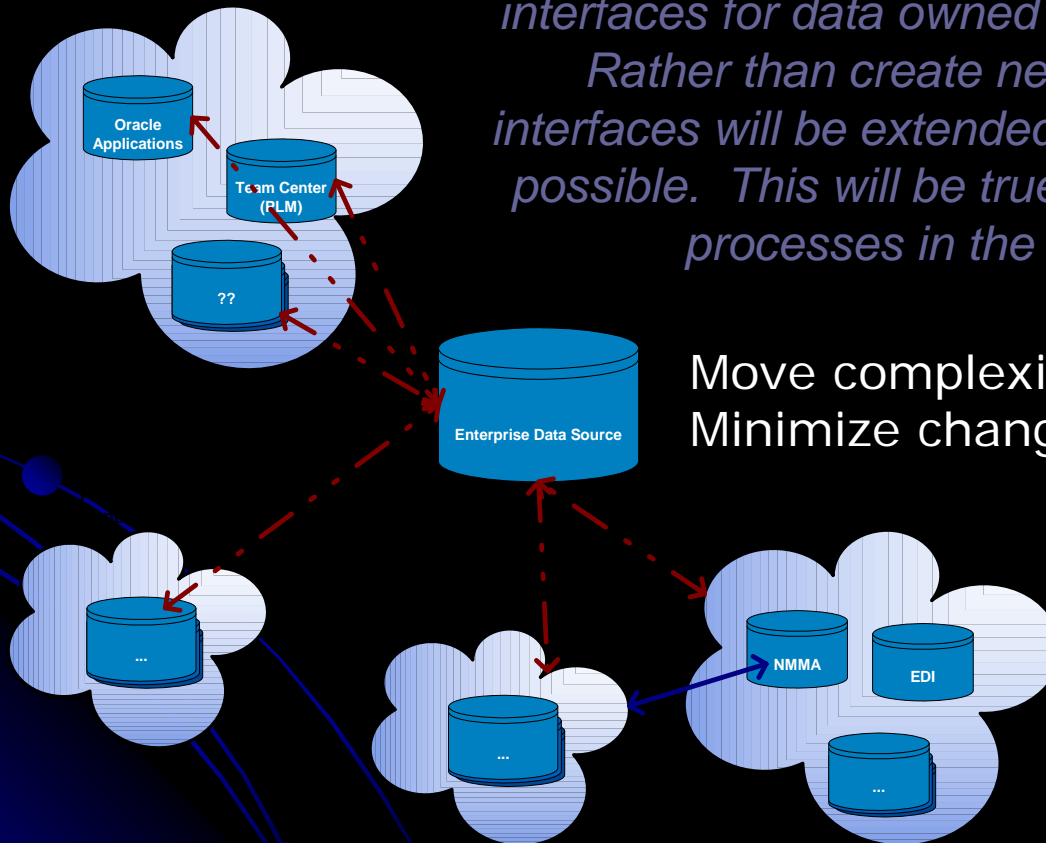
The transition must be managed, SO...



New integration pieces are built using the Enterprise Data Source (an EAI HUB). Legacy data required for integration would utilize the Enterprise Data Source (EAI HUB).

In the end we have clean and managed integration environment

Each new COTS system will add additional interfaces for data owned within the COTS system. Rather than create new interfaces, existing interfaces will be extended and/or reused whenever possible. This will be true not only for data but for processes in the future (i.e. SOA)



Move complexity to the center.
Minimize changes to legacy systems.

