SECURIFY

Security Centric Management of Planned Change

June 2003

Taher Elgamal, PhD
Chairman and CTO

Carl Wright
VP Federal Operations

Agenda

SECURIFY

Security Issues in today's networks

Security-Centric Management of Planned Change

The Objectives

SECURIFY

A safer network for business:

- More trust between business partners
- More consumer trust in the infrastructure

Protection of the critical infrastructure

- Slowing down malicious behavior on the Internet

"Homeland security"

Fighting terrorism

Security manageability is THE big problem!

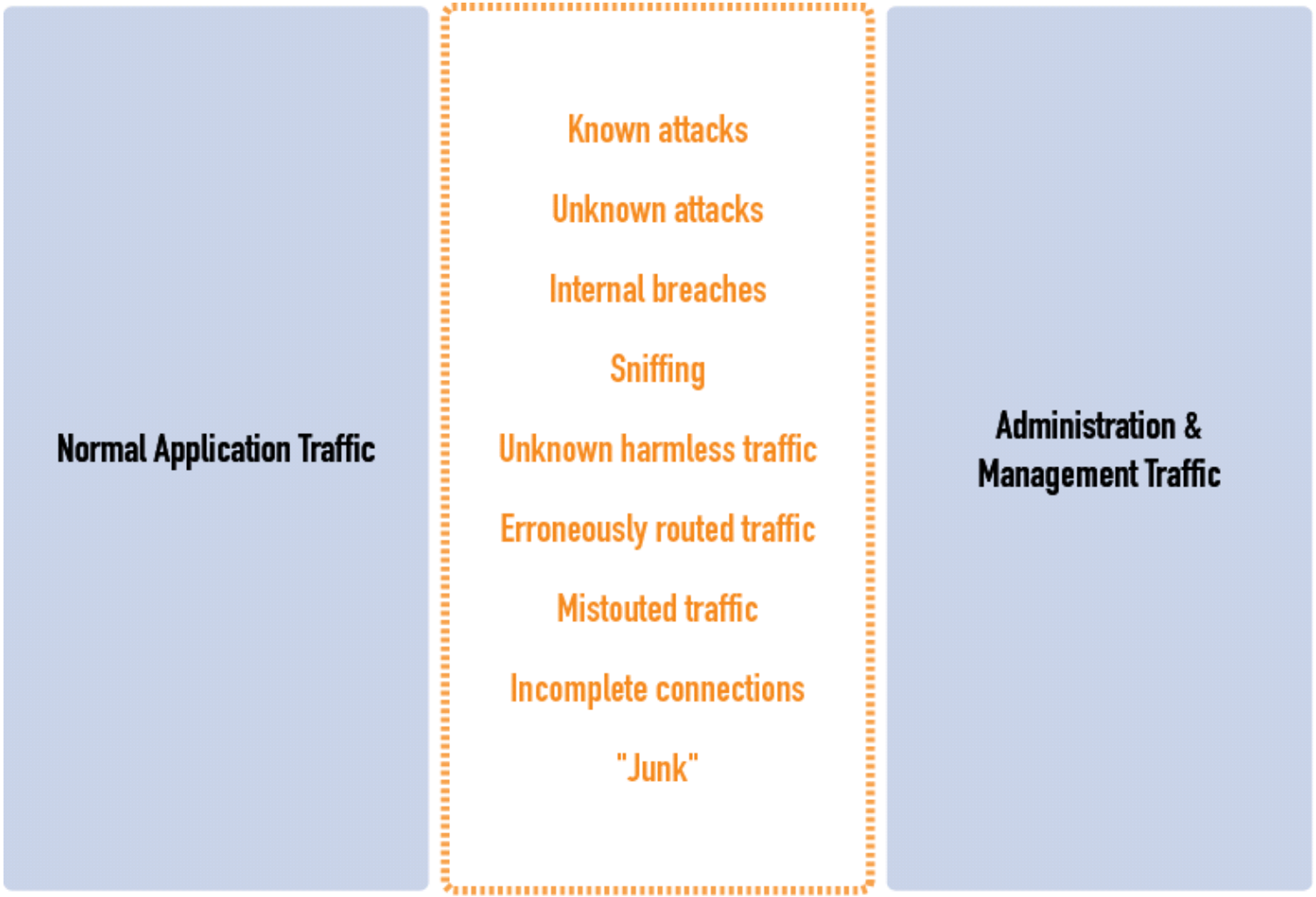
The Top Issues with Security

SECURIFY

- Lack of understanding of the overall picture
- Security is not integrated in any business process
- User identities not associated with access to resources
- Numerous products, versions, patches
- Lack of expertise and / or continuity
- Cost that may not be unjustified – desperate projects with no overall objective

What Happens on the Network

SECURIFY



Issues Facing Security Officers

SECURIFY

- Justifying and understanding IT Security investments is extremely hard
- No way of understanding level of policy compliance
- No effective way of enforcing policies
- No way of measuring effectiveness of security or improvement
- No effective way of understanding the high level view of the network security
- Very difficult to assign priorities to the various tasks

Issues Facing Network Ops

SECURIFY

Very difficult to validate the configurations to the policies

Communicating information about the network function is very technical

No effective way to communicate with the security officer and staff

Very hard to map network operations into an effective, priority-driven actions

Issues Facing Security Professionals

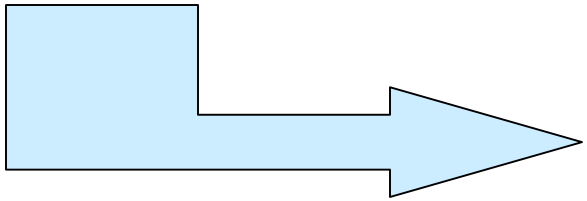
SECURIFY

- Extremely hard to focus on important, architectural, or policy-related issues
- Hard to justify security investments
- Too many details without enough priorities
- Always "fire-fighting"

The Complexity Problem

SECURIFY

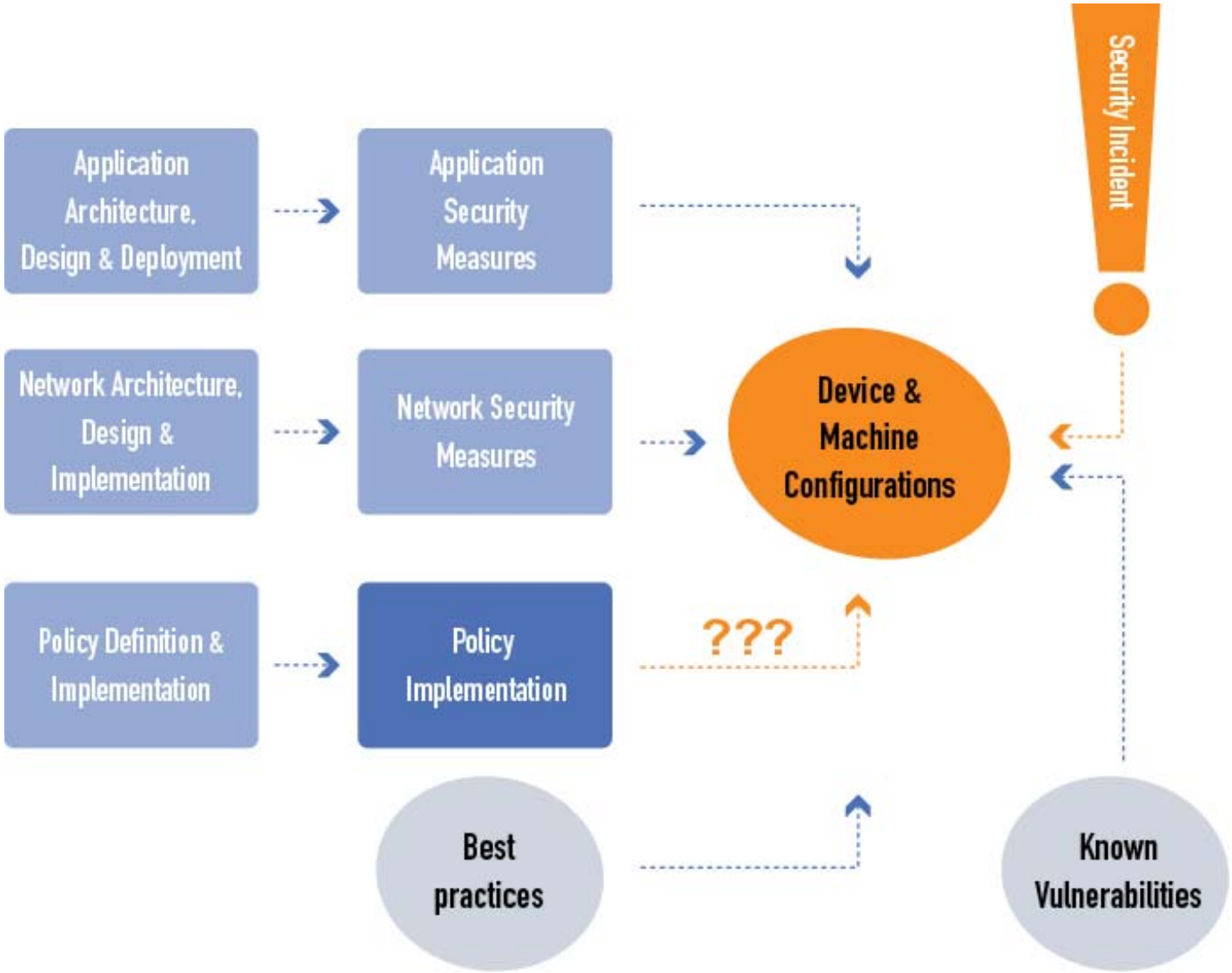
- Large number of machines, users, …
- Connectivity to other networks
- Interaction between machines very difficult to understand
- General purpose machines allow many un-necessary functions
- Configurations, patches and vulnerabilities
- Lack of IT security staff



Unmanageable amount of logs, alerts and data to manage

Security Workflow Today

SECURIFY



The Problem -- summary

SECURIFY

We don't manage networks like we manage the rest of the business – No visibility

No way of measuring improvements or evaluating effectiveness of security – No measurability

Large amount of data to manage without enough context – No priority

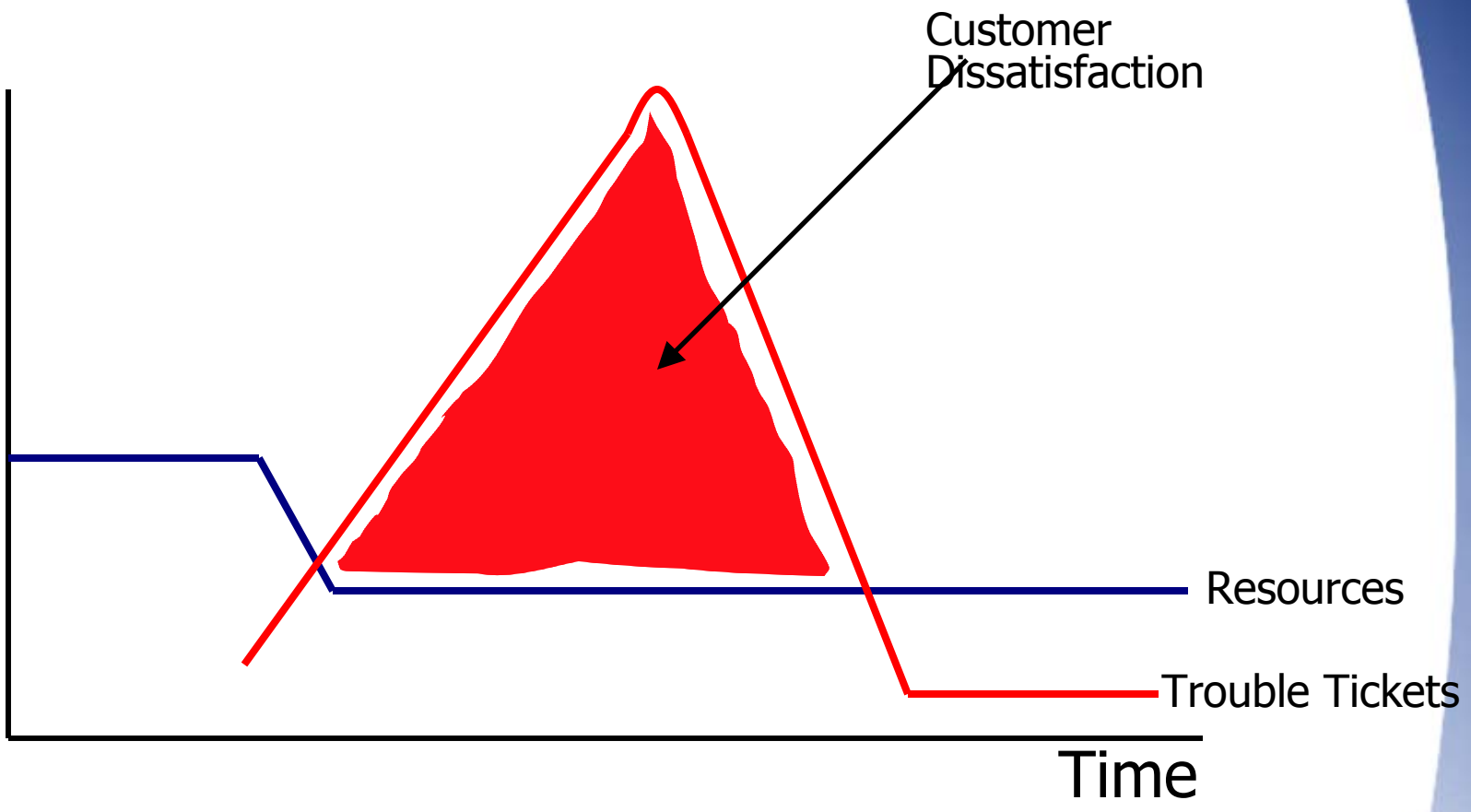
Network security remains a mystery – done as a craft – No manageability

SECURIFY

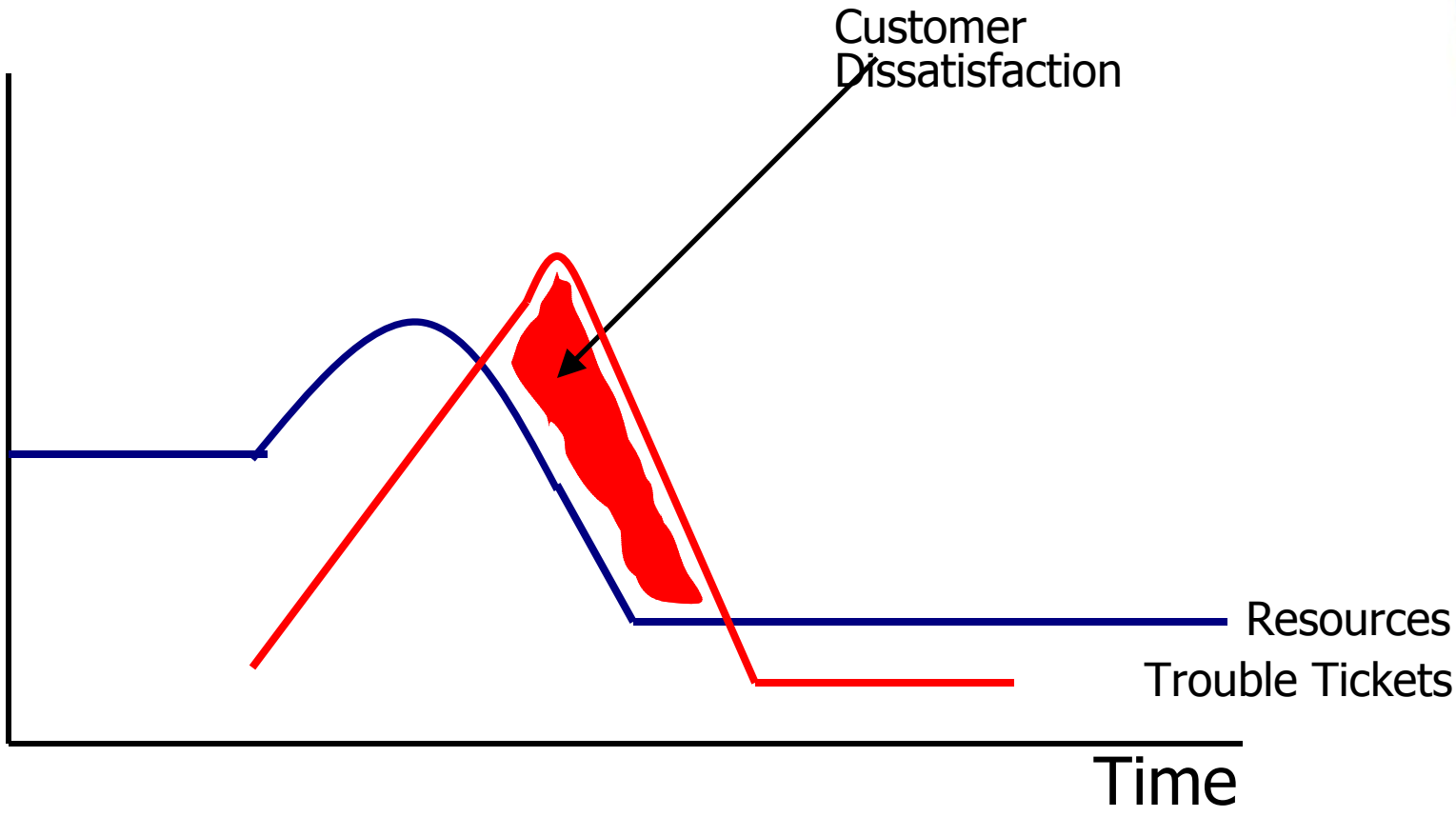
Why is this so hard?

- DoD invented B2B
- Impacts long standing core business processes that support mission
- Balancing act between acceptable risk and capability
  - Is the capability strategically aligned with organizational objectives?
- Directly impacts the culture and politics

Causality of Planned Change



Causality of Planned Change



SECURIFY

Accomplishing the Objective

Macro Level Outsourcing Model Change Framework

- Near Perfect Information of AS-IS Information Technology States
  - Information Technology Management principles are implemented enterprise wide [Standards based Configuration Control]
  - Network and Information Architectures are documented and aligned with strategic organizational objectives
- Define TO-BE States
- Define Transition Parameters Predicated on Operational Requirements
  - Business process predicated on organizational objectives and variables

SECURIFY

The MCEN Case Study

- In the Beginning – free love and peace
- Bringing Discipline to the Process
- Evolutionary Change at Revolutionary Rates
- Expanding Services and Configuration Management
- From Transition to Steady State Mode
- The Next Step Forward

SECURIFY

The MCEN Case Study

In the Beginning

- Mainframe Services always centrally provisioned and managed
- 1990-1991 Banyan Vines deployed at the enterprise level – Centrally controlled by Regional Automated Service Centers and Quantico CDPA
- 1993 USMC deploys Vines IP enabled devices
- 1994 - 1996 USMC deploys distributed client server architectures and native IP enabled devices, not centrally controlled
  - Client/Server Applications begin to proliferate
  - Organizations manage their own IT and NIPRnet PoPs

Legacy Applications

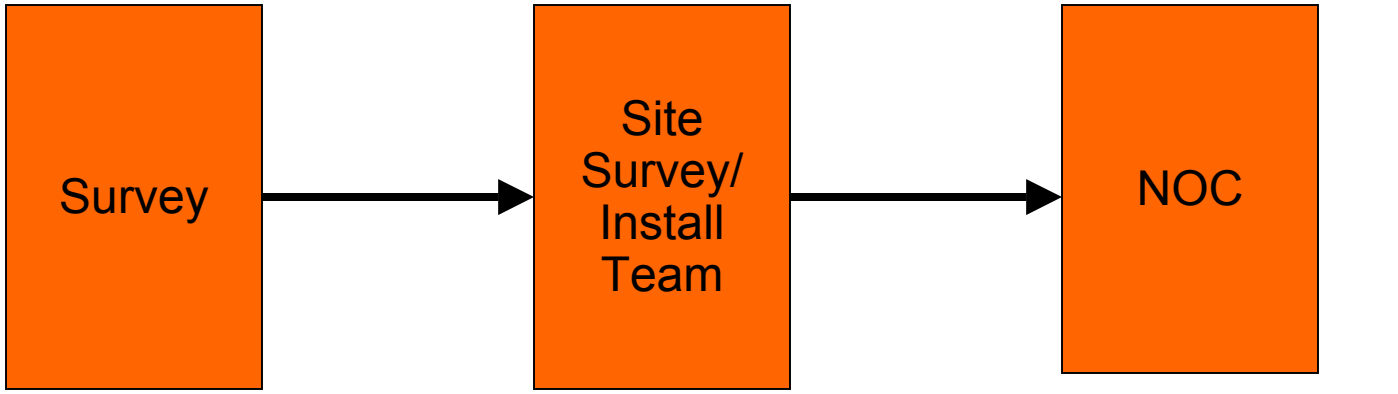
SECURIFY

During the initial transitions, it became readily apparent that although the Marine Corps ultimately **desired a completely secure enterprise network** from the initial onset and resource investment, due to the mission criticality of many of the legacy applications the Marines would **have to be satisfied with an incremental security posture** transitional change rather than the **draconian transition** originally planned. This was done in order to facilitate and ensure the continuity of existing operations, operations for which many of the most offensive legacy applications were critical. As a result, **legacy applications that did not immediately comply with organizational policy** were segregated into three simplistic categories.

- **Category 1:** Legacy applications that were non-compliant with organizational security policies and for which an immediate mitigation solution existed (e.g. migrated to the DMZ)
- **Category 2:** Legacy applications that were non-compliant with organizational security policies and for which no immediate mitigation solution was available. Legacy application is deemed mission critical to operations and the DAA has accepted the risk, waiver approved for a period of time until resources could be identified to correct application security deficiencies. Category 2 applications were to be tracked for progress and eventual compliance.
- **Category 3:** Legacy applications that were non-compliant with organizational security policies and for which no immediate mitigation solution was available. DAA does not accept the risk, waiver not approved. Application life cycle terminated. (There were not many in this category, because each base had a physical DMZ, mitigation solutions were usually found)

MCEN Transition Process

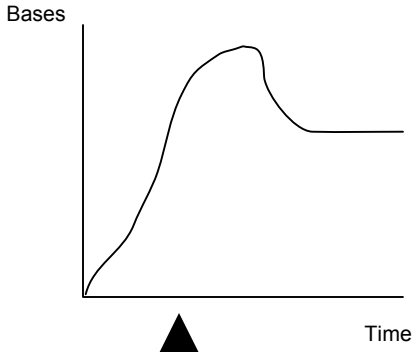
SECURIFY



-Mailed Out
-Phone Interviews
-P4 ->25% reported

-NAI Sniffer Analysis
-Local IT staff

3-5 days allotted
8-25 days actual
60% traffic compliancy



Failed to allot sufficient time to ascertain Legacy Apps communication requirements. This resulted in a huge spike in trouble tickets at the NOC [250 at any one time].

SECURIFY

The MCEN Case Study

Summary

- Took over 3 years to get to a steady state mode for ~100,000 users, ~5000 servers, 268 Extranet TCP/IP Legacy Applications
- We failed to initially address LA management of planned change from a security-centric life-cycle perspective – **we did not know what we did not know**
- We inflicted significant pain on our user communities and impacted operations
- We did eventually succeed, but was there a better way?

Lessons Learned

SECURIFY

- During times of transition, organizations are at the greatest risk. It is important that the organization move through certain phases of the transition as quickly as possible in order to maintain continuity of operations. Follow-on objectives can be achieved with additional phased approaches that require less initial enterprise impact during high-risk periods.

- Security change must be incremental in order to insure continuity of operations. That is not to say that the organization should assume avoidable risk or reduce risk when possible. It is simply a statement that the aircraft carrier should not be expected to turn on a dime, but is should be expected to turn.

- Do not underestimate the "Christmas" effect associated with many aspects of a technology change/deployment. Marketing the positives of the program are as important as addressing the problems. It is easy to focus only on the problems during the initial phases of the transition. Specific to legacy applications, sometimes situational awareness of risk is enough to start with.

Security Centric Management of Planned Change

SECURIFY

- **Critical Success Factors**
  - Target clearly defined end state & objective that is achievable in a phased approach
  - Communication, communication, communication
    - Marketing is a must
  - Information Management during transition
    - Fluid environment – users, networks, and applications are not static by their nature

Policy Driven Situational Awareness

SECURIFY

Security is about configuration management and configuration control

- Must scale based on complexity
- Policy simplifies complexity

The risk to your organization is highest during the transition. The enemy knows this.

- Imperative that during this time you have the highest situational awareness and visibility into NETOPS that you can