Metrics: Practical Ways to Measure Security Success

Pete Lindstrom, CISSP
Research Director

Spire Security, LLC
www.spiresecurity.com
petelind@spiresecurity.com

What entity is most/least secure?

- **Bank of America**
- **T-Mobile**
- **Choicepoint**
- **Wells Fargo**
- **[your name here]**

What platform is most/least secure?

- **Microsoft Solutions**
- **Linux Servers**
- **SymbianOS Smartphones**
- **IBM Mainframe**
- **Cisco Network Devices**

The state of security

- **We can’t define “good security” (as a group)**
- **We can’t tell the difference between “strong” and “lucky”**
- **We don’t know how to measure success**
- **One incident doesn’t necessarily mean “failure”**

In other words…

Agenda

- Information Assets Value
- **Usage (Transactions)**
- **Risk Metrics**
- **Control Metrics**
- **Resource Management Metrics**

Calculate asset value

- **Basic premise: Your assets are worth at least as much as your support costs plus usage costs plus direct revenue.**
- **Support Costs (an indirect valuation)**
  - **Ops & Maintenance – salaries, maintenance, consulting.**
  - **Current Capital Expenses – hardware and software.**
- **Usage/Productivity Costs**
  - **End User salaries and wages * amount of computer use**
- **Direct Revenue (Supply Chain)**
  - **Product Manufacturing**
  - **Sales**

Types of info asset losses

- **How much value would be lost under the following conditions?**
- **Information-centric Loss**
  - **Modified data (Integrity)**
  - **Copied data (Confidentiality)**
  - **Deleted data (Availability)**
- **System/App-centric Loss**
  - **Resource Availability (Productivity)**
  - **Resource Misuse (Liability)**

Estimating loss

- **How much are you spending on it?**
  - **Can you "lose" this?**
- **How much could be lost/stolen without knowing it (or caring)?**
  - **Revenue, Liquid Assets**
  - **Materiality, shrinkage**
- **How much could be lost if unavailable?**
  - **Revenue, Productivity, Supply Chain**
- **Tolerance is a key ingredient (don't overestimate)**

How much can you lose?

- **Lost information asset value**
  - **Productivity**
  - **Revenue**
  - **Other IA Value**
- **Incident costs**
  - **IT Productivity x 2**
    - **Costs incurred**
    - **Opportunity costs**
  - **Legal / Regulatory Costs**
  - **Other (non-labor) Recovery Costs**

Legal/regulatory costs

- **Lawsuits –**
  - **Privacy suits**
  - **Downstream liability**
  - **Legal fees**
- **Regulatory issues –**
  - **Regulatory fines**
  - **Remediation costs**

How do we calculate losses?

Understand Information Asset Value

	Read	Modify	Delete	Avail	Misuse
IT Prod.	**H** (forensics)	**M**	**M** (restores)	**M**	**L**
User Prod.	**M**	**H** (recon)	**H** (mistakes)	**H** (worms and viruses)	**L**
Legal/ Fines	**M/H** (Privacy)	**H** (regulated)	**L**	**L**	**?**
Revenue	**L**	**H** (robbery)	**H**	**H** (snowstorm)	**M**
Liquid Assets	**L**	**H** (trust)	**H**	**M**	**M**
IP	**H** (compete)	**M**	**H**	**L**	**L**

Information assets – getting started

- **Pick top 5 key applications**
- **Calculate asset value**

$$\text{Info Asset}_{min} = \text{IT Salary \& Wages} + \text{Current Capital Expense} + (\text{Org Salary \& Wages})*\text{Usage \%} + \text{Direct IT Revenue} + \text{Intellectual Property}$$

- **Add legal/regulatory fines**
- **Identify the types of loss that are most significant for each app**
- **Factor in tolerance (this is a value reduction)**

Core elements of security metrics

- **Information assets**
- Usage (Transactions)
- **Risk**
- **Controls**

Usage / events

- **Objective: to identify discrete events that can be evaluated as success/fail from a security perspective.**
- **These are all computer usage events, NOT control events.**
  - **They are the source of value and threat within the computing environment.**
- **Identify events at various discrete layers:**
  - **Network layer**
  - **Host layer**
  - **Application layer**
  - **Data layer**

Usage / events

- **Network layer: flows**
  - **Source IP, Dest IP, Dest Port**
  - **Inbound and/or Outbound**
- **Host Layer: sessions**
  - **Sessions under management**
  - **Number of logins**
- **Application layer: program operations**
  - **System calls**
  - **Application calls**
- **Data Layer: transactions**
  - **Messages**
  - **Business events (financial trades, purchase orders, published articles, etc.)**

Usage / events getting started

- **Turn netflow on**
- **Identify average number of active users and/or IP addresses.**
- **For Top 5 key applications, identify major transactions (data layer)**

Core elements of security metrics

- **Information assets**
- **Usage (transactions)**
- Risk
- **Controls**

Quantifying risk

- **Risk: The likelihood that something unwanted will happen.**
- **About probability, not possibility**
- **Yes, Virginia, you can quantify risk (but it ain't gonna be easy)**

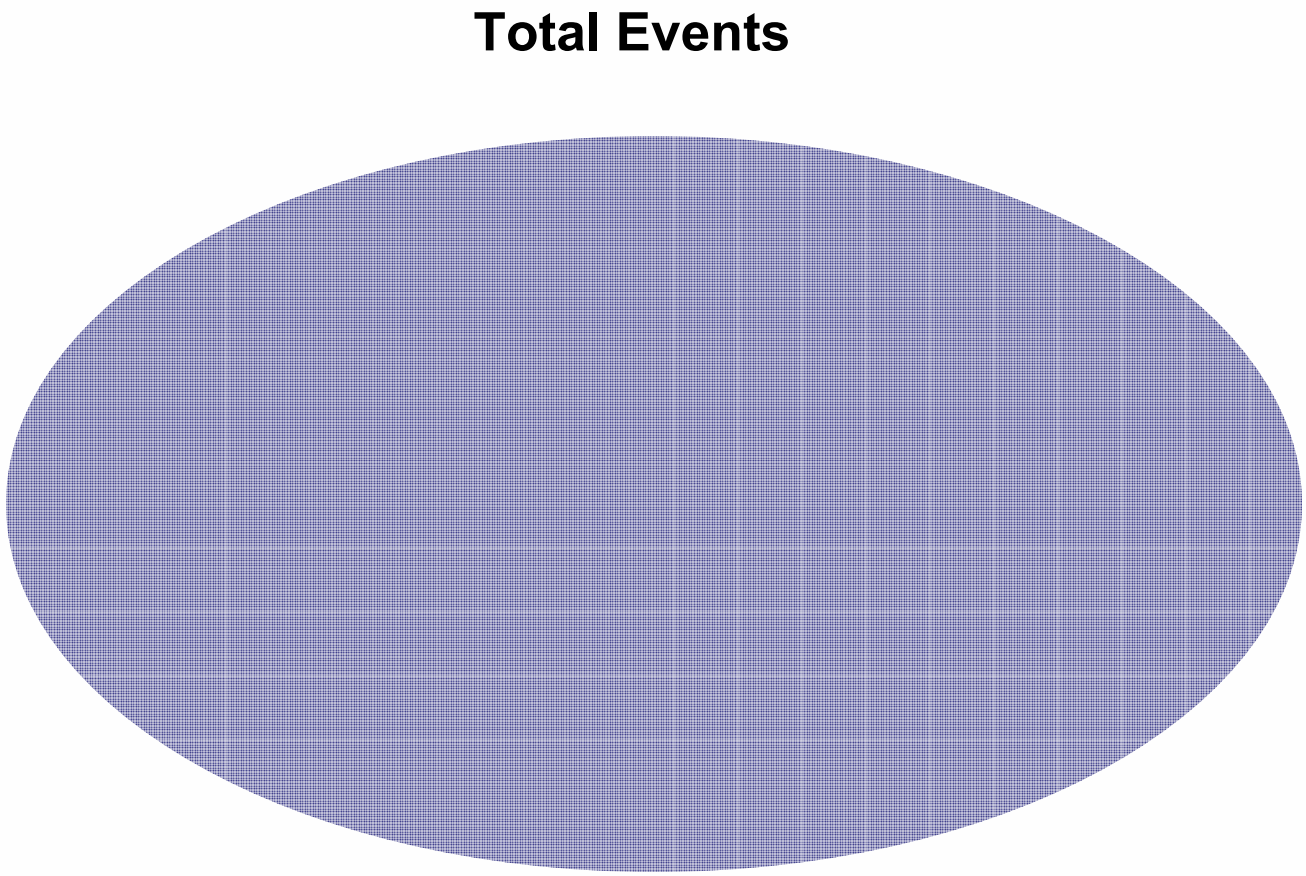
Types of risk

- **Manifest Risk - Events occurring within the computing environment. (Actual)**
- **Inherent Risk - Combinations of events that may occur within the computing environment. (Possible)**
- **Contributory Risk - Risk associated with control processes.**

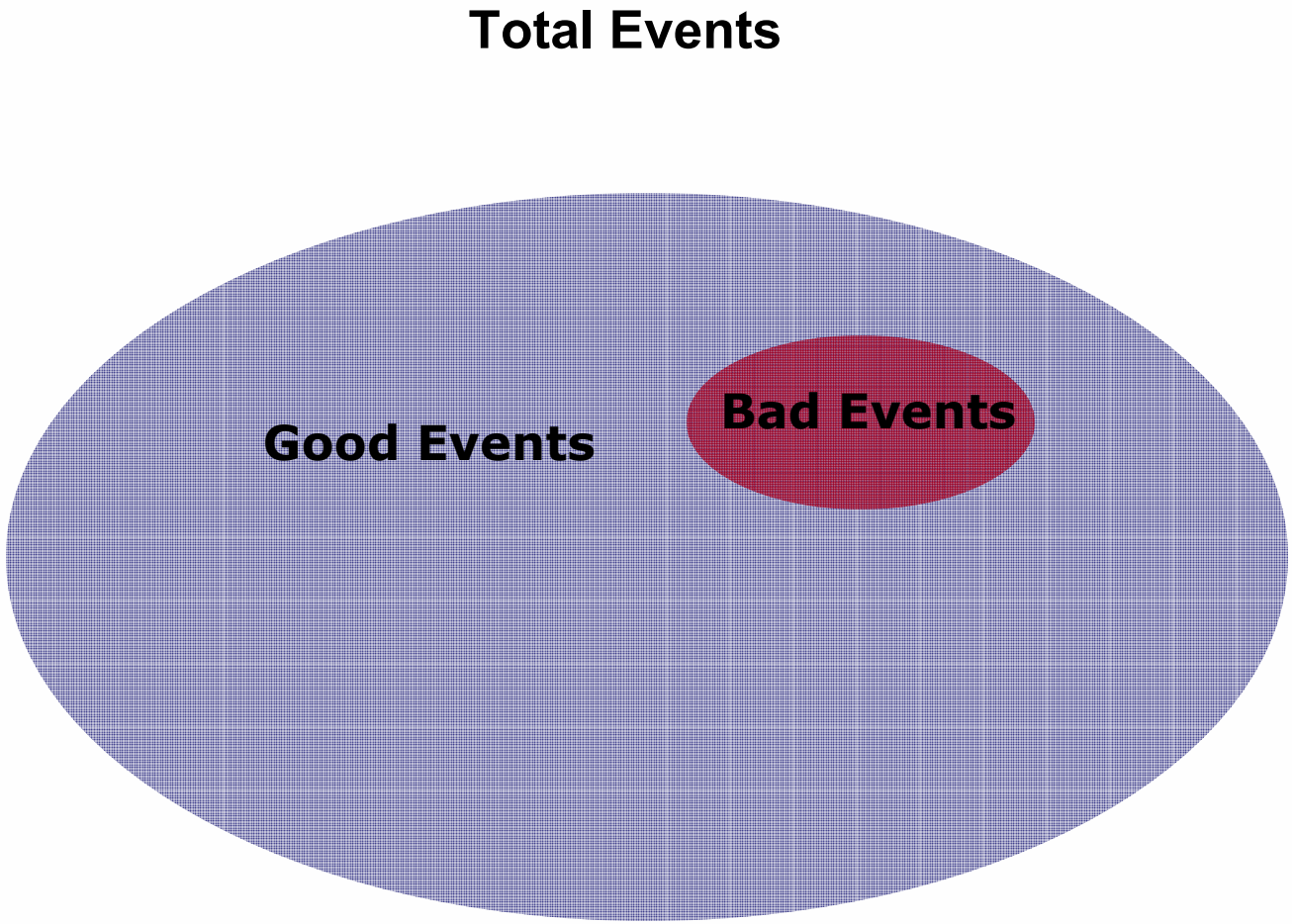
Manifest risk

- **Events occurring within the computing environment. (Actual)**
- **Philosophy: A compromise can't occur without online event.**
- **Count discrete events.**
  - **Actual Flows (network)**
  - **Actual Sessions (system)**
  - **Actual Program Operations (application)**
  - **Actual Transactions (data)**
- **Count number of "bad" activities.**

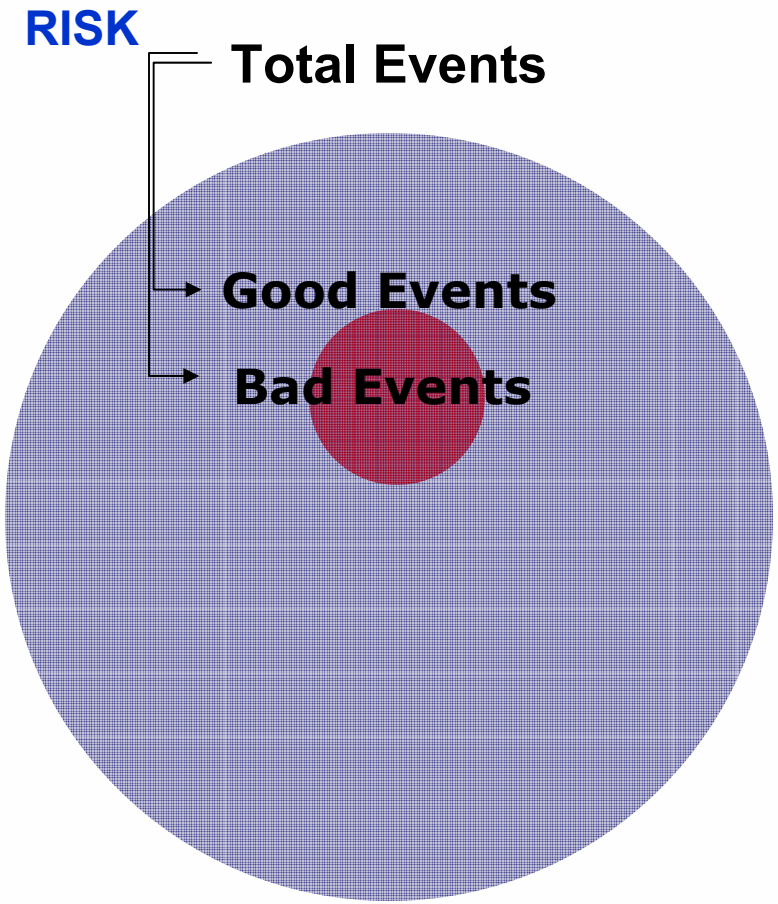
Quantifying risk



Quantifying risk



Quantifying risk



$$\text{Risk} = \frac{\text{Bad Events}}{\text{Total (Good + Bad) Events}}$$

$$\text{Risk} = \frac{\text{Bad Emails}}{\text{Total (Good + Bad) Emails}}$$

$$\text{Risk} = \frac{\text{Bad Flows}}{\text{Total (Good + Bad) Flows}}$$

What is a "bad" event?

- **Anything that results in an incident (some unwanted outcome)**
- **A denied event from security control that doesn't result in a help desk call.**
- **E.g. Failed logins, spam, viruses, leaked IP, etc.**

Manifest risk – getting started

- **For top 5 applications, define what is "bad"**
- **Add the concept of good and bad to the event data being collected.**
- **Start quantifying risk!**

Inherent risk

- **Combinations of events that may occur within the computing environment (Possible)**
- **Philosophy: Even without events, we are exposed when we make computing resources available**
- **Calculate potential activities**
  - **Possible Flow – number of unique source IPs x number of open ports**
  - **Possible Sessions – number of unique user sessions x number of applications**
  - **Program Commands – not recommended**
  - **Transaction – not recommended**
- **Use as a relative reducer to manifest risk Multiply the total number of known**
  - **i.e. reducing the number of possible flows by 50% results in a reduction of 50% manifest risk**

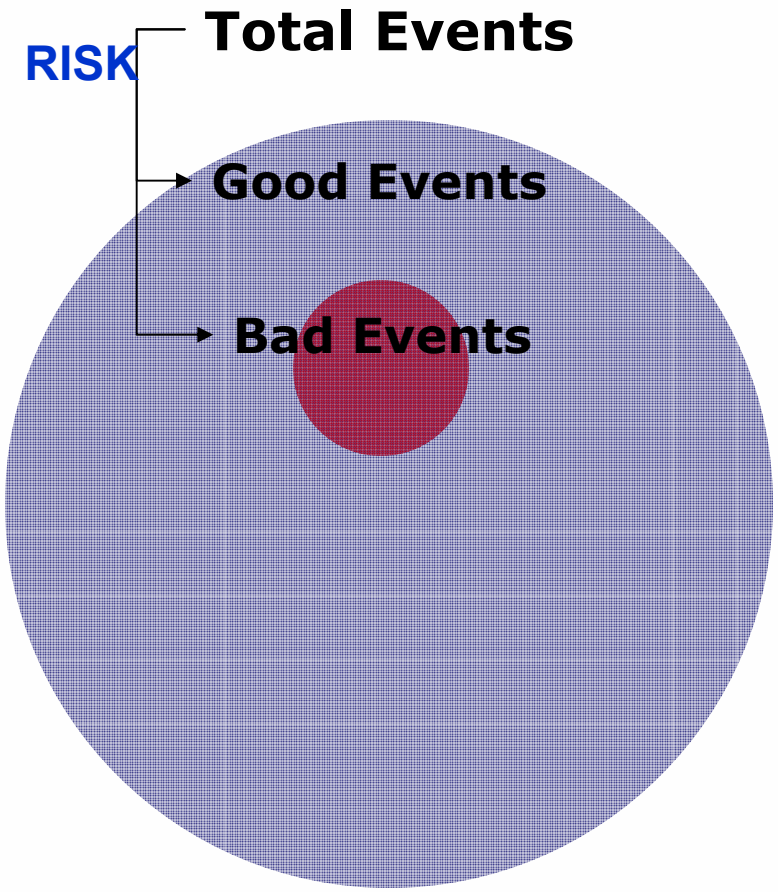
Contributory risk

- **Risk associated with control processes**
- **Philosophy: Security is about process, not product**
- **At best, there is an indirect relationship between contributory risk and actual compromises**
  - **That's why "you can't measure risk"**
- **Caveat: This risk is more clearly associated with regulatory requirements**

Core elements of security metrics

- **Information Assets**
- **Usage (Transactions)**
- **Risk**
- Controls

Recall: quantifying risk

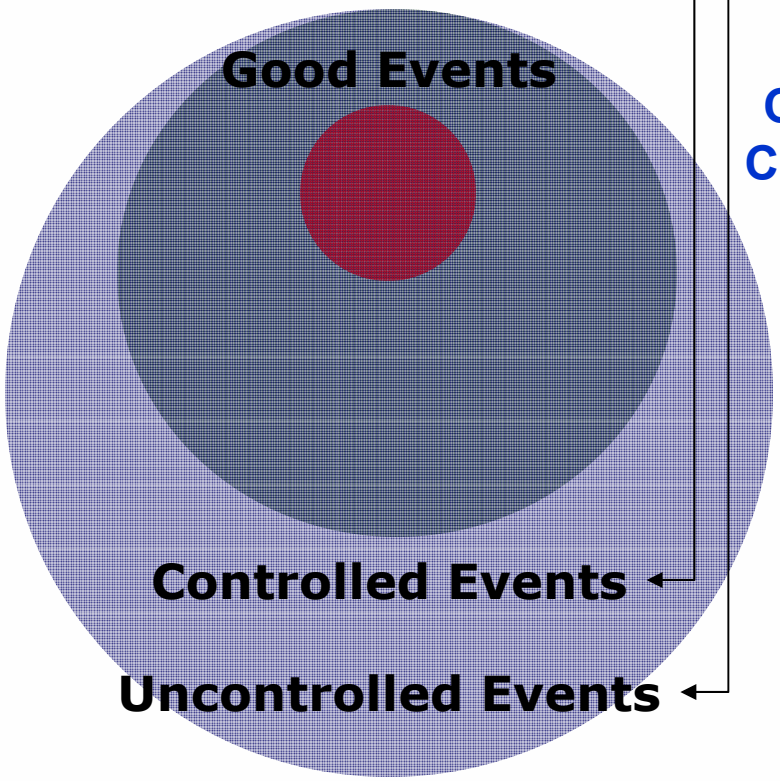


$$\text{Risk} = \frac{\text{Bad Events}}{\text{Total (Good + Bad) Events}}$$

$$\text{Risk} = \frac{\text{Bad Emails}}{\text{Total (Good + Bad) Emails}}$$

$$\text{Risk} = \frac{\text{Bad Flows}}{\text{Total (Good + Bad) Flows}}$$

Applying controls: coverage

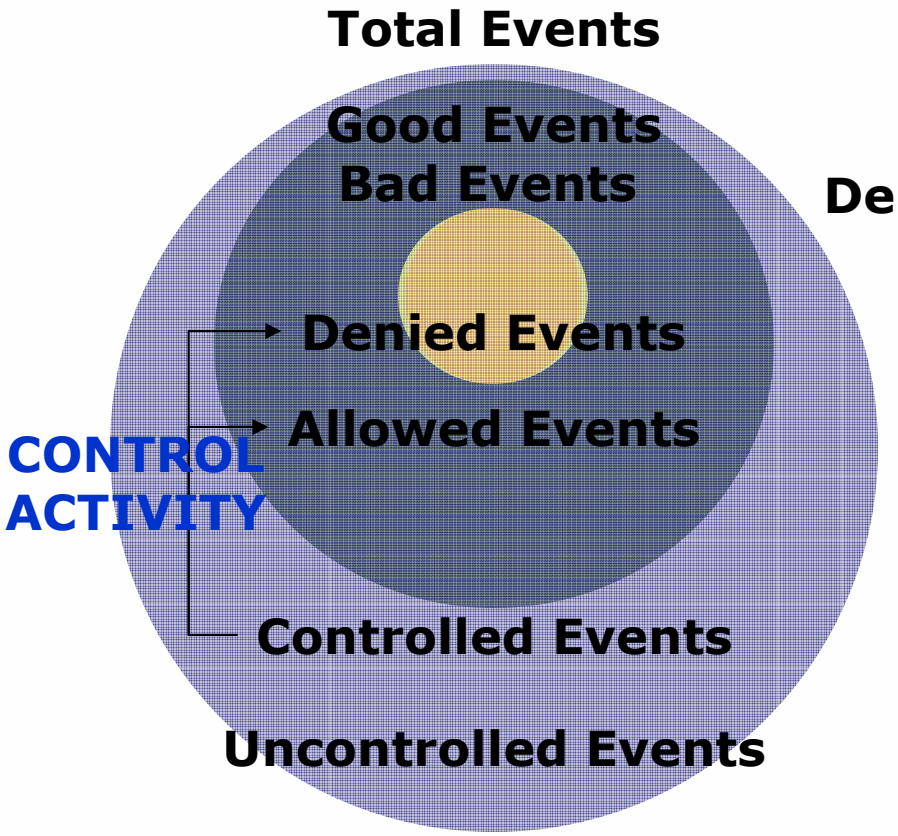


CONTROL COVERAGE

$$\text{Coverage} = \frac{\text{Controlled Events}}{\text{Total Events}}$$

Acceptable Risk = (Bad/Total) * Uncontrolled Events

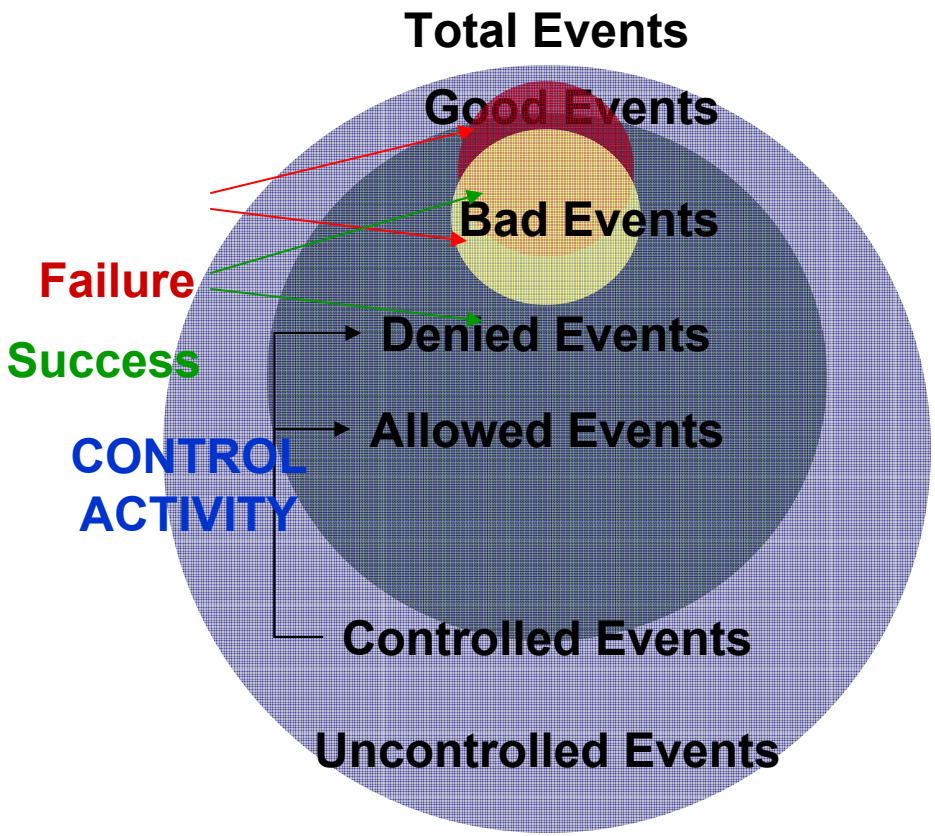
Applying controls: activity



Security Ratio = Denied Events : Allowed Events

Note: Both legitimately denied events and legitimately allowed events are control successes, though they may be policy failures.

Applying controls: errors



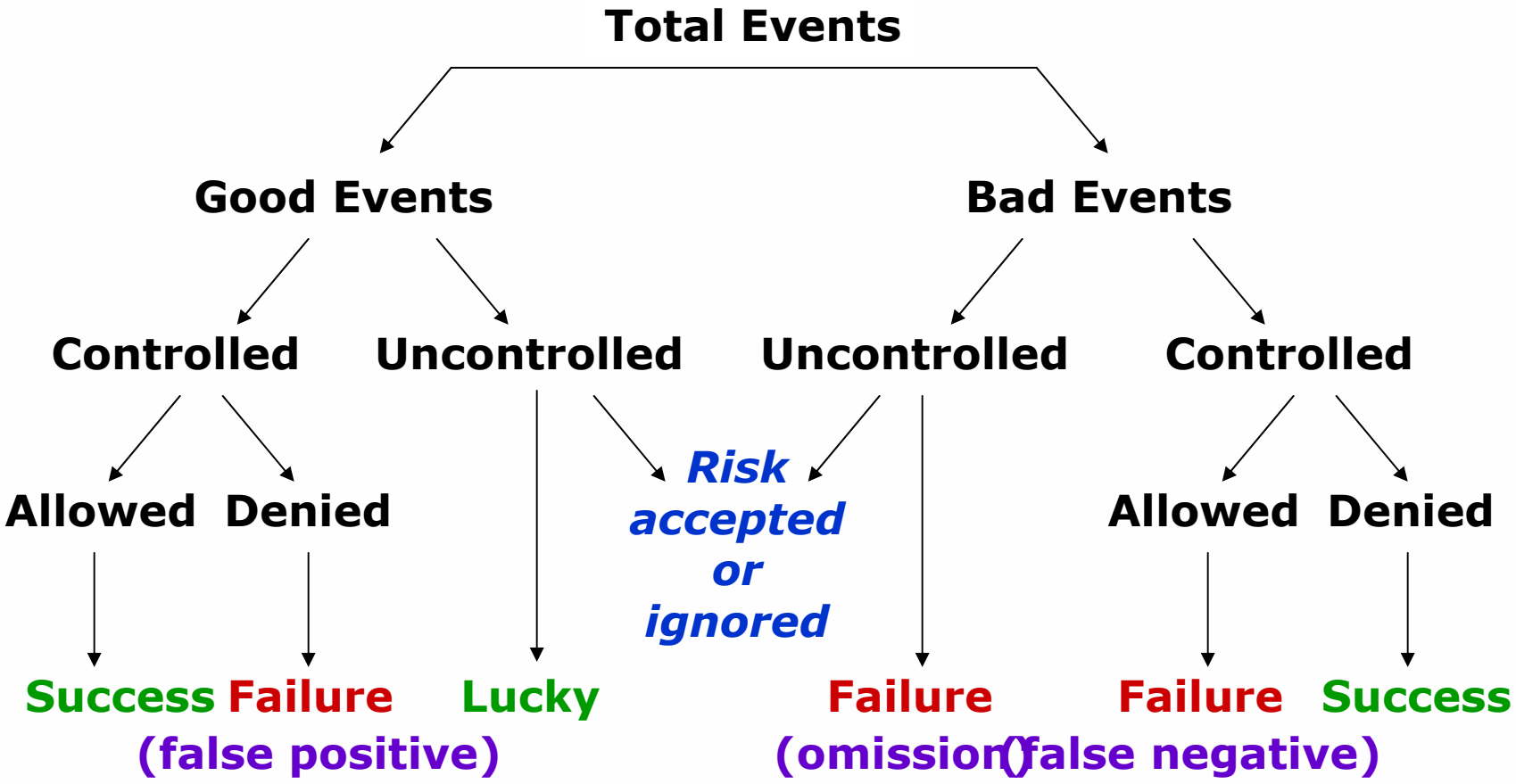
Control Successes:
Denied bad events
Allowed good events

Control Failures:
Denied good events
Allowed bad events

Accepted Risk:
Uncontrolled bad events

Luck:
Uncontrolled good events

Risk & control taxonomy



"Other" security metrics

Security Mgt - what to count

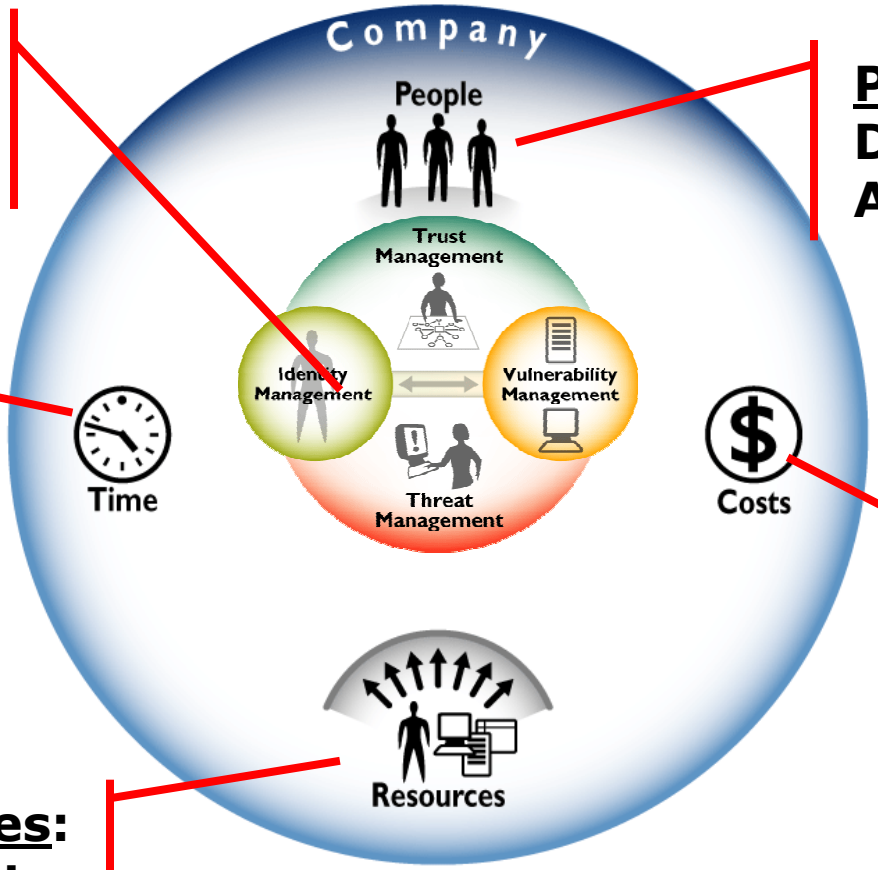
Activities: Four Disciplines

People: Departments Admins

Time: Hr/Day Month/Yr

Costs: Salaries, Consulting HW, SW, Maint.

Resources: User accts, systems, apps

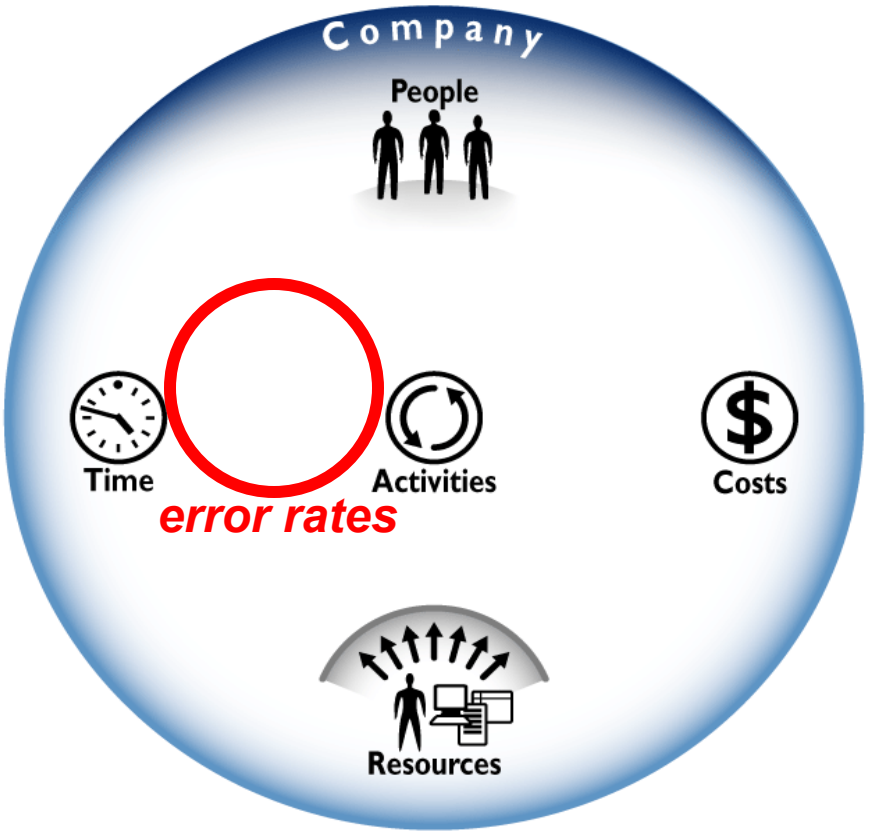


Process effectiveness metrics

"doing things right"

Key Elements:
- **Activities**
- ***errors***

Examples:
- **Acct request errors**
- **Remediation errors**
- **False alarm rate**
- **Policy exceptions**



Process effectiveness

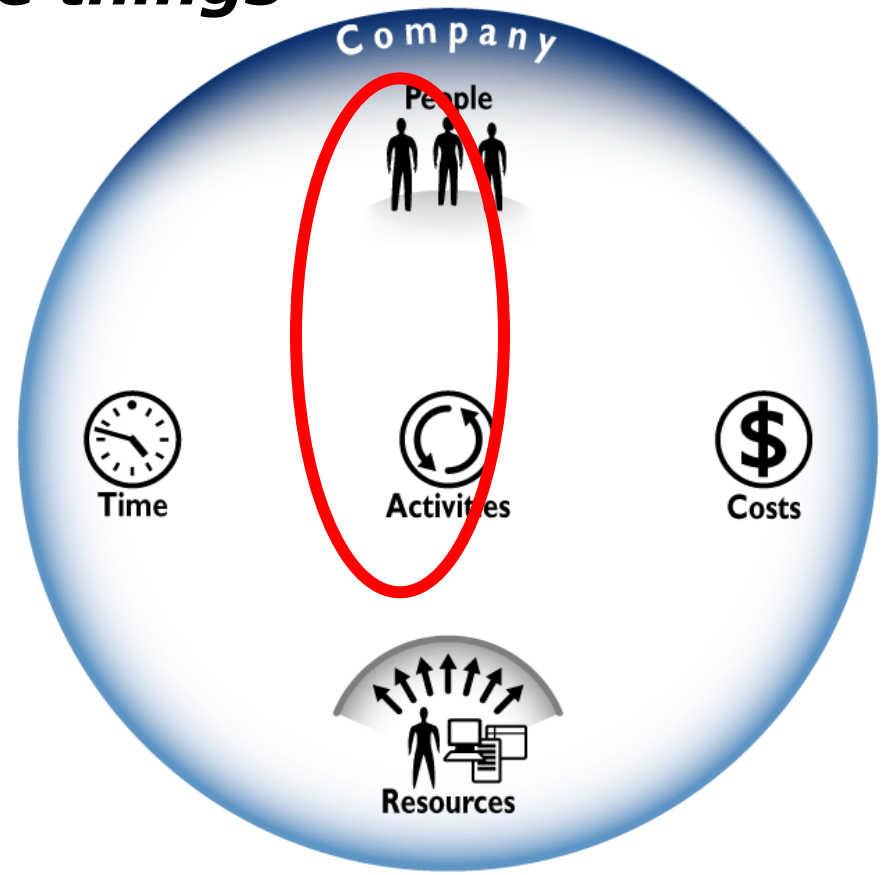
- **Measure quality by identifying error rates of activities**
- **Identity Management**
  - **User account request errors**
- **Vulnerability Management**
  - **Vulnerabilities not remediated**
- **Threat Management**
  - **Improper incident management**
- **Trust Management**
  - **Policy violations**

Staff productivity metrics

"people doing more things"

Elements:
- **People**
- **Activities**

Examples:
- **Accts per person**
- **Vulns per person**
- **Patches per person**



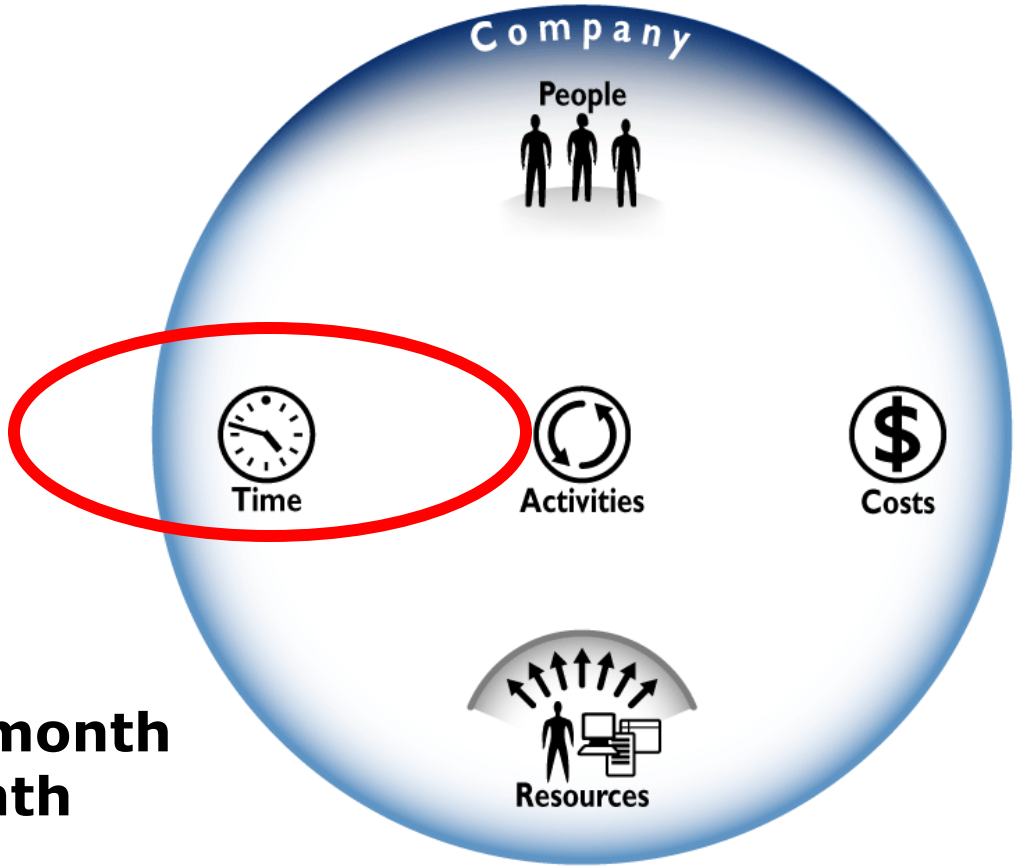
Staff productivity

- **Productivity and workload for all manual activities (activities/people)**
- **Identity Management**
  - **Requests per administrator**
  - **Account disablements per admin**
  - **Password resets per admin**
- **Vulnerability Management**
  - **Vulnerabilities resolved per administrator**
- **Threat Management**
  - **Incidents per person**
- **Trust Management**
  - **Policy changes per person**

Cycle time metrics

avg "time to perform activity x"

Elements:
- **Time**
- **Activities**



Examples:
- **Accts per month**
- **Vulns fixed per month**
- **Patches per month**

Cycle time

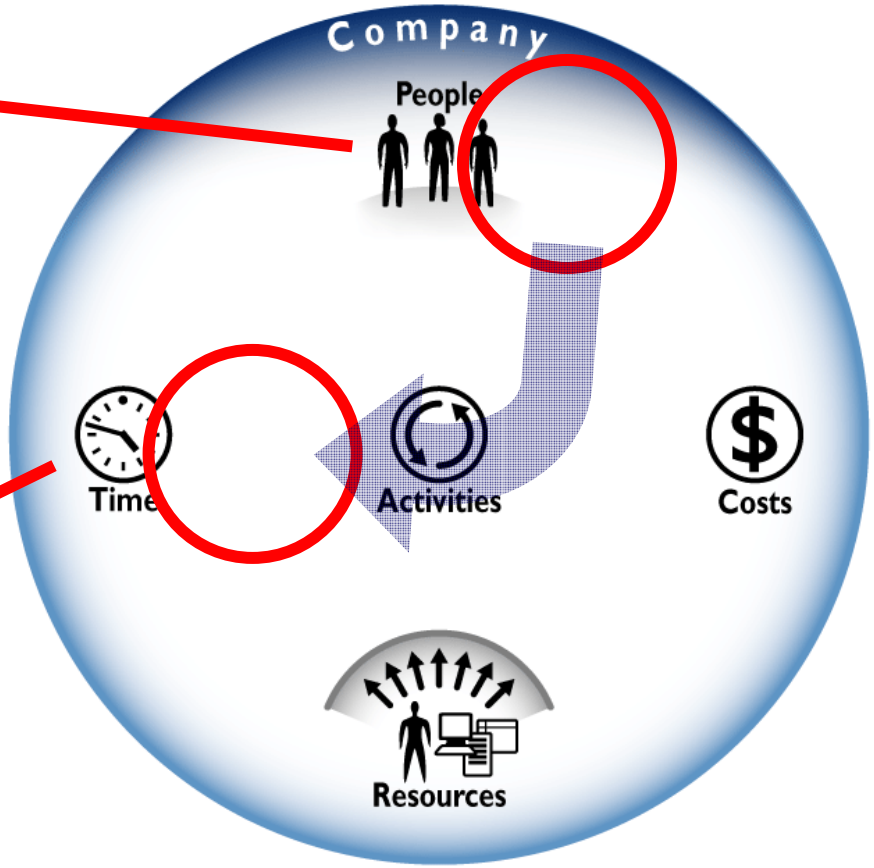
- **Process efficiency**
- **Identity Management**
  - **User account request time to complete**
- **Vulnerability Management**
  - **Remediation time to complete**
- **Threat Management**
  - **Incident response time to complete**
- **Trust Management**
  - **Policy creation time to complete**

Staff efficiency metrics

"people doing things" quicker

Admins by Department

2000 Hours per FTE



Elements:
- **People**
- **Activities**
- **Time**

Examples:
- **Accts per person/hr**
- **Vulns per person/hr**
- **Patches per person/hr**

Staff efficiency

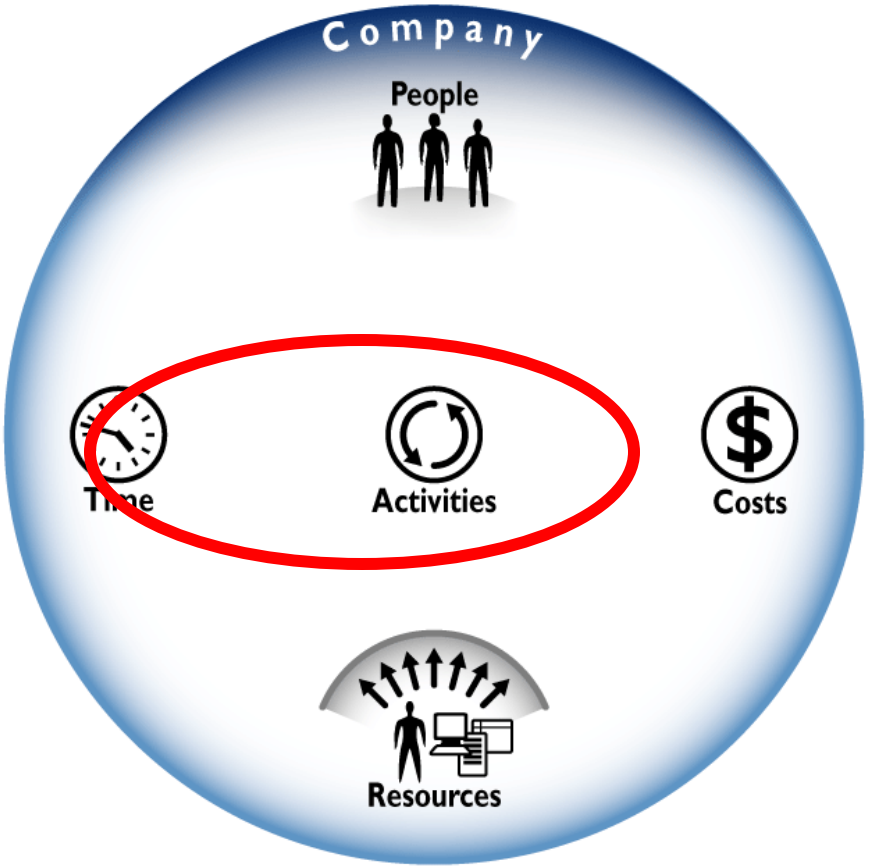
- **Combines staff productivity and cycle time metrics.**
- **Identity Management**
  - **User account requests completed per person per day/week/month**
- **Vulnerability Management**
  - **Vulnerabilities remediated per person per day/week/month**
- **Threat Management**
  - **Incidents closed per person per day/week/month**
- **Trust Management**
  - **Policies reviewed per person per day/week/month**

Cost effectiveness metrics

Cheaper transactions

Elements:
- **Activities**
- **Costs**

Examples:
- **Cost per acct**
- **Cost per vuln fixed**
- **Cost per patch**



Cost effectiveness

- **Dollars/activities; dollars/resources; dollars/demographics**
- **Identity management**
  - **Cost per request**
  - **Cost per password reset**
- **Vulnerability management**
  - **Cost per vulnerability**
  - **Cost per system setting**
- **Threat management**
  - **Cost per incident**
- **Trust management**
  - **Cost per policy**
  - **Cost per project**

Conclusions

- **Security functions are spread throughout organizations.**
- **You can't improve security until you measure it.**
- **Ultimately, security is a business operation that should be run like a business operation.**

Agree? Disagree?

Pete Lindstrom
petelind@spiresecurity.com
www.spiresecurity.com