SearchFinancialSecurity.com INFORMATION SECURITY

FINANCIAL INFORMATION SECURITY DECISIONS

# Your Strategic Security Metrics Program

**Pete Lindstrom**

*Senior Analyst, SRMS*

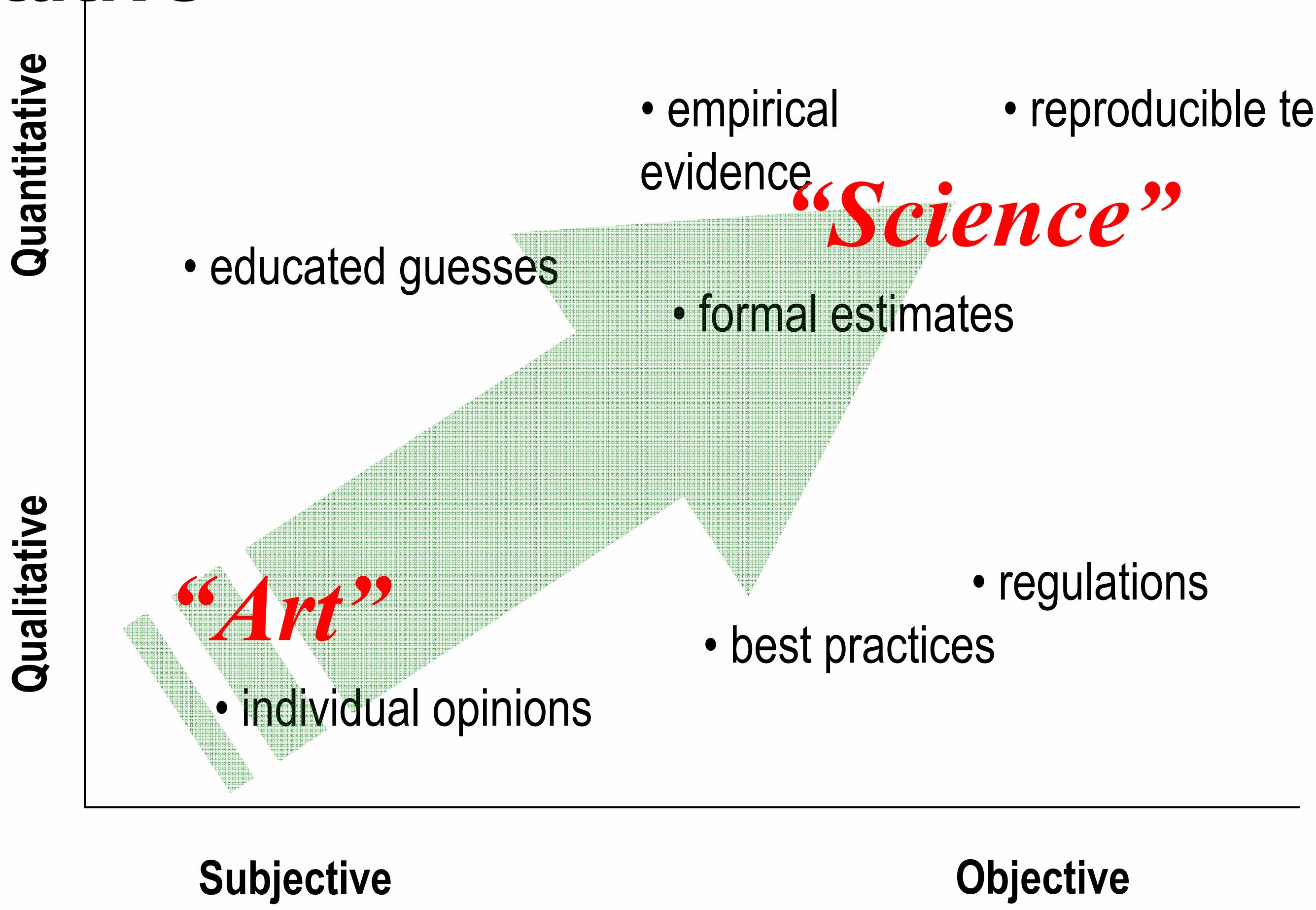
plindstrom@burtongroup.com

www.burtongroup.com

burton GROUP

# Strategic security approach

- **From subjective, qualitative to objective, quantitative**



# Strategic security approach

- **Why objective, quantitative information is better**
  - Clinical Versus Statistical Prediction: A Theoretical Analysis and Review of the Evidence (Meehl, 1954/1996)

*“Empirical comparisons of the accuracy of the two methods (136 studies over a wide range of predictands) show that the mechanical method is almost invariably equal to or superior to the clinical method…”*

  - Timid Choices and Bold Forecasts: A Cognitive Perspective on Risk Taking (Lovallo, Kahnemann, 1993)

*“…decision makers are excessively prone to treat problems as unique, neglecting both the statistics of the past and the multiple opportunities of the future.”*

# Strategic security approach - Just how human are we?

### Decision Making and Behavioral Biases

Bandwagon effect
Base rate fallacy
Bias blind spot
Choice-supportive bias
Confirmation bias
Contrast effect
Endowment effect
Extreme aversion
Focusing effect
Framing
Hyperbolic discounting
Illusion of control
Impact bias
Information bias
Irrational escalation
Loss aversion
Mere exposure effect
Moral credential effect
Omission bias
Outcome bias
Planning fallacy
Post-purchase rationalization
Pseudocertainty effect
Reactance
Selective perception
Status quo bias
Unit bias
Von Restorff effect
Zero-risk bias

### Biases in probability and belief

Ambiguity effect
Anchoring
Attentional bias
Availability heuristic
Clustering illusion
Capability bias
Conjunction fallacy
Gambler's fallacy
Hawthorne effect
Hindsight bias
Illusory correlation
Ludic fallacy
Neglect of prior base rates effect
Observer-expectancy effect
Optimism bias
Overconfidence effect
Positive outcome bias
Primacy effect
Recency effect
Regression toward the mean disregarded
Reminiscence bump
Rosy retrospection
Selection bias
Stereotyping
Subadditivity effect
Subjective validation
Telescoping effect
Texas sharpshooter fallacy

### Social biases

Actor-observer bias
Dunning-Kruger effect
Egocentric bias
Forer effect (aka Barnum Effect)
False consensus effect
Fundamental attribution error
Halo effect
Herd instinct
Illusion of asymmetric insight
Illusion of transparency
Ingroup bias
Just-world phenomenon
Lake Wobegon effect
Notational bias
Outgroup homogeneity bias
Projection bias
Self-serving bias
Self-fulfilling prophecy
System justification
Trait ascription bias
Memory errors
Beneffectance
Consistency bias
Cryptomnesia
Egocentric bias
False memory
Hindsight bias
Suggestibility

# Strategic security approach

- **Bottom line**
  - Risk is impossible to eliminate
  - Subjective approaches are full of bias and ambiguity
  - Decisions are being made based on assumptions and guesses
  - We must move toward objective approaches to be taken seriously
  - In the end, we can demonstrate what a strong security program looks like

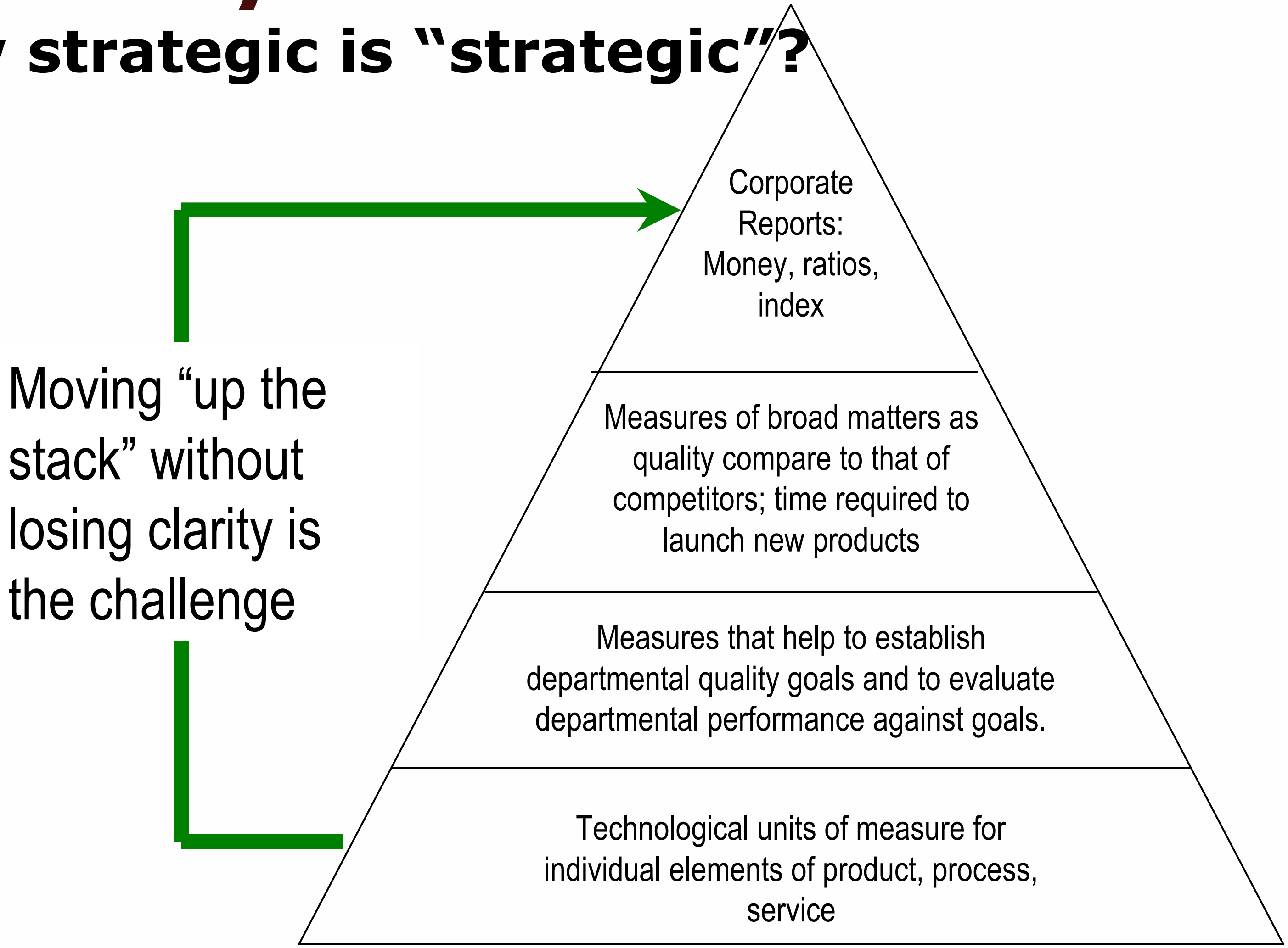
# A security metrics model

- **What does executive management want to know?**
  - What is our risk level?
  - How strong is our security program?
  - Are we maintaining appropriate cost control?
- **What they don't want to know…**
  - How many security FTEs it takes to change a lightbulb?
  - The risk difference between SSL VPNs and IPsec VPNs
  - A smirky, self-righteous "nobody knows for sure"
- **What we give them**
  - Red, Yellow, Green based on guesses
  - Thumbs up, thumbs down

burton GROUP

# A security metrics model

- **How strategic is "strategic"?**



Moving "up the stack" without losing clarity is the challenge

Corporate Reports: Money, ratios, index

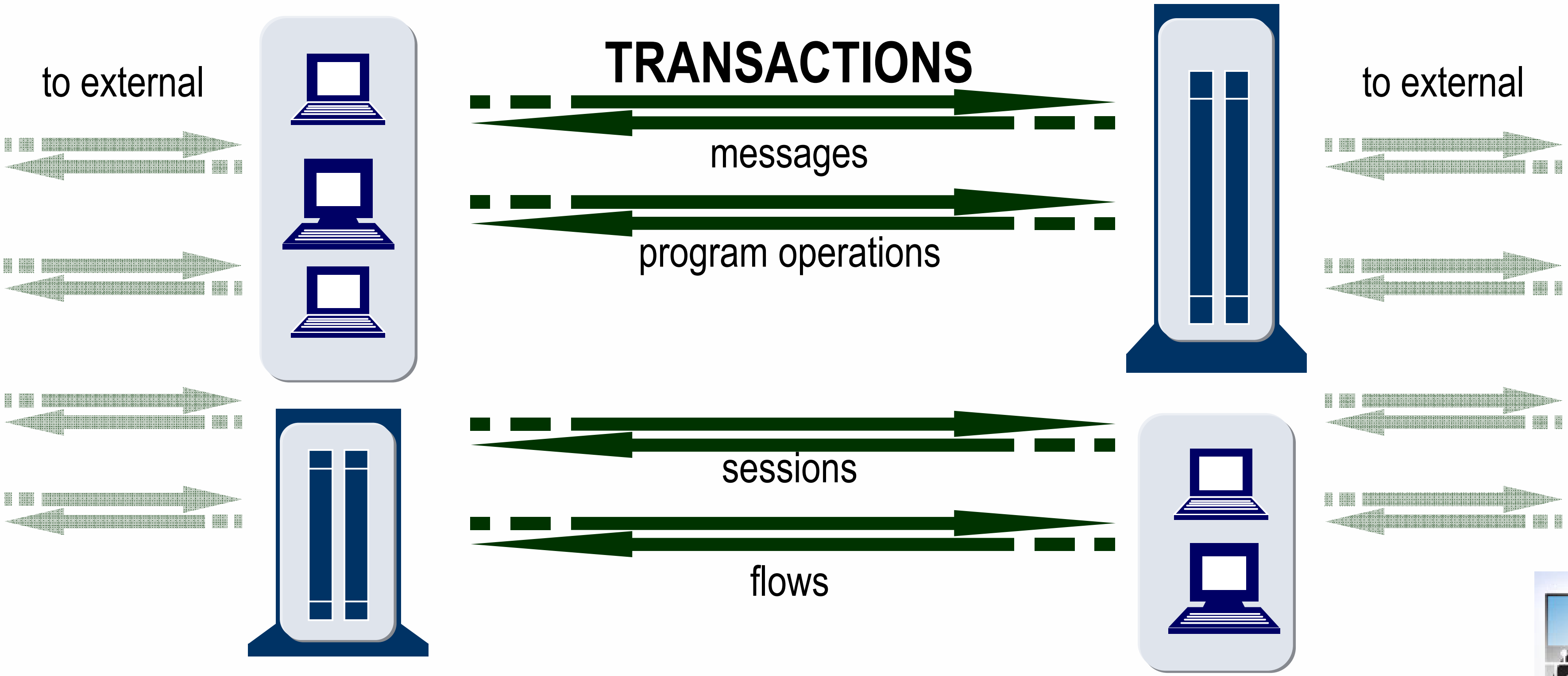
Measures of broad matters as quality compare to that of competitors; time required to launch new products

Measures that help to establish departmental quality goals and to evaluate departmental performance against goals.

Technological units of measure for individual elements of product, process, service

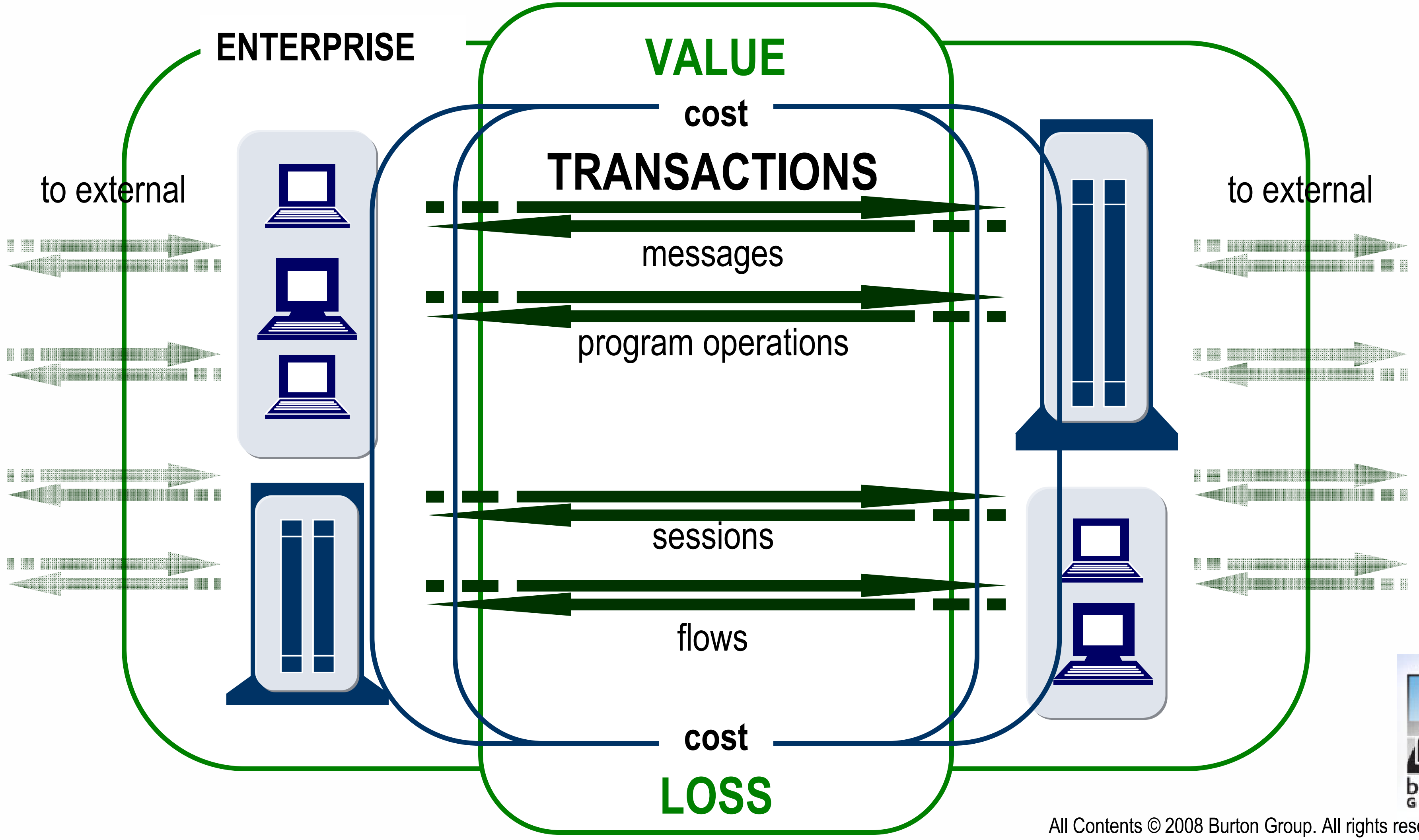
# A security metrics model

- **The lowest layer: the technology**



# A security metrics model

- **Adding value and loss**



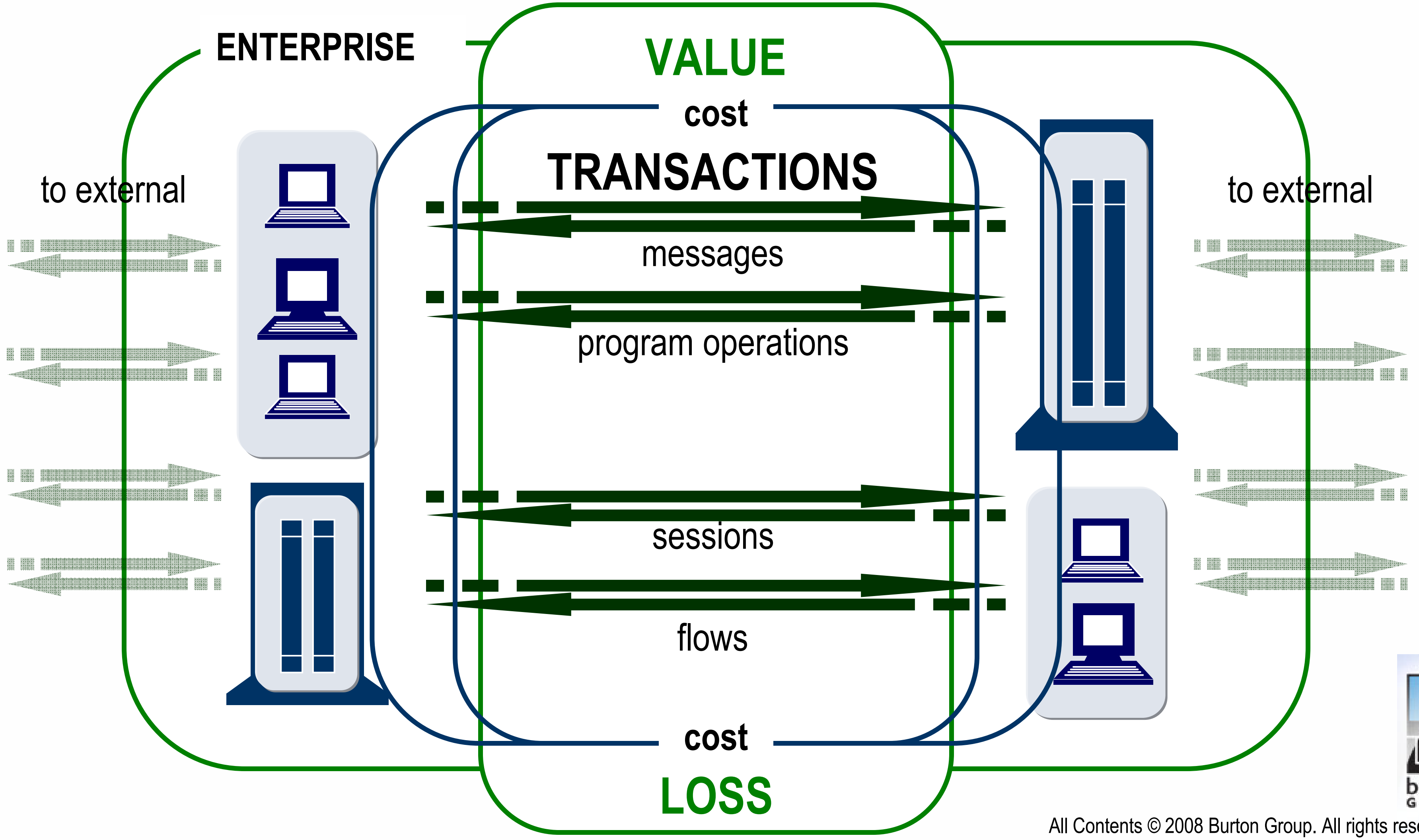
# A security metrics model

- **Estimating value and loss at an aggregate level**

| | **Threshold** | **Loss Potential** |
|---|---|---|
| **User Productivity** | Unpaid overtime; alternative options | Hours x Rate x Downtime |
| **Revenue** | Three-way-match; accounts receivable | Rev/Hr x Downtime; Shrinkage |
| **Liquid Assets** | Manual reviews | Allowances |
| **Intellectual Property** | Legal costs | Competitive revenue; market share |
| **IT Productivity** | Direct costs | Hours x Rate x Work |
| **Legal/ Fines** | Legal dept fees | Legal dept fees |

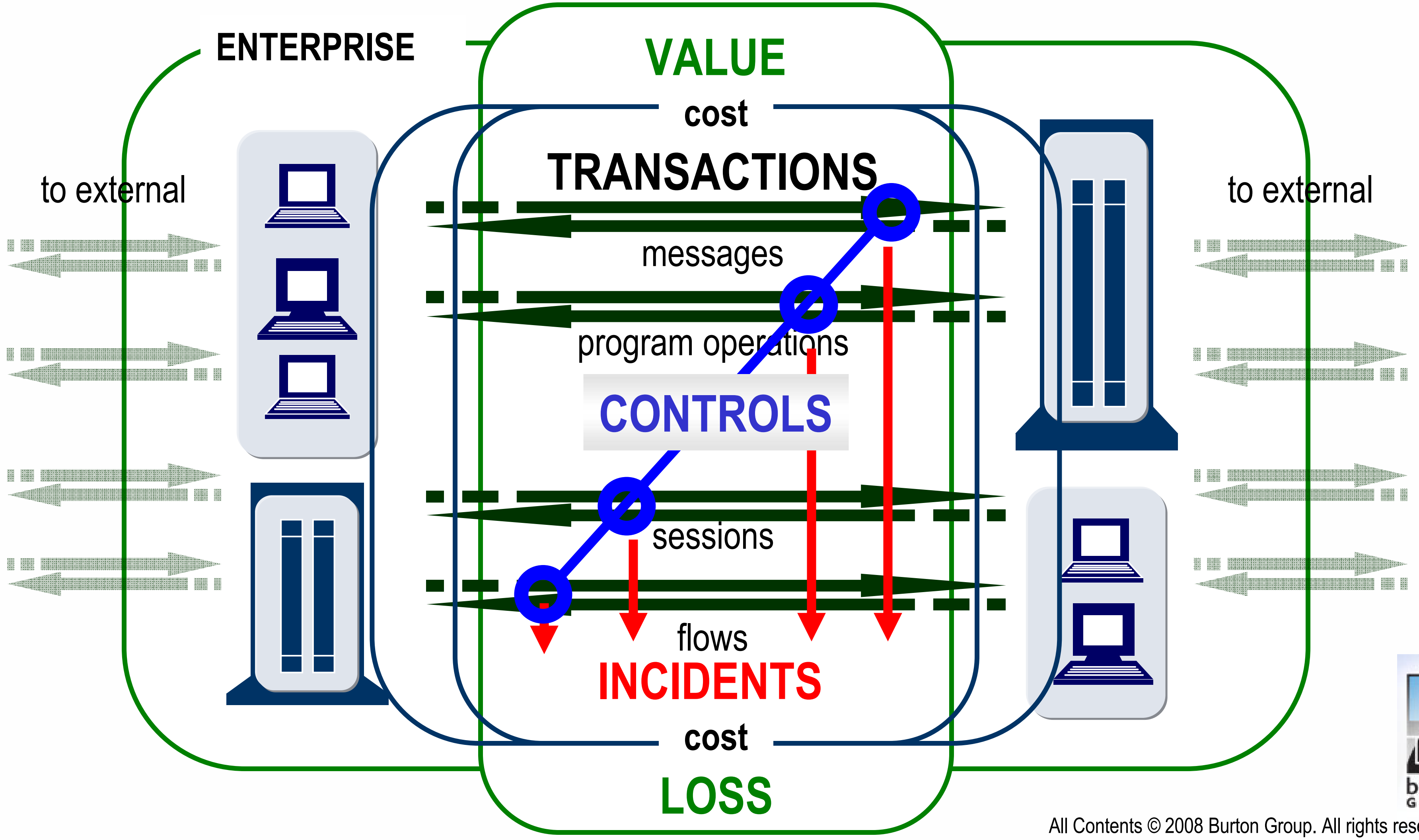
# A security metrics model

- **Adding value and loss**



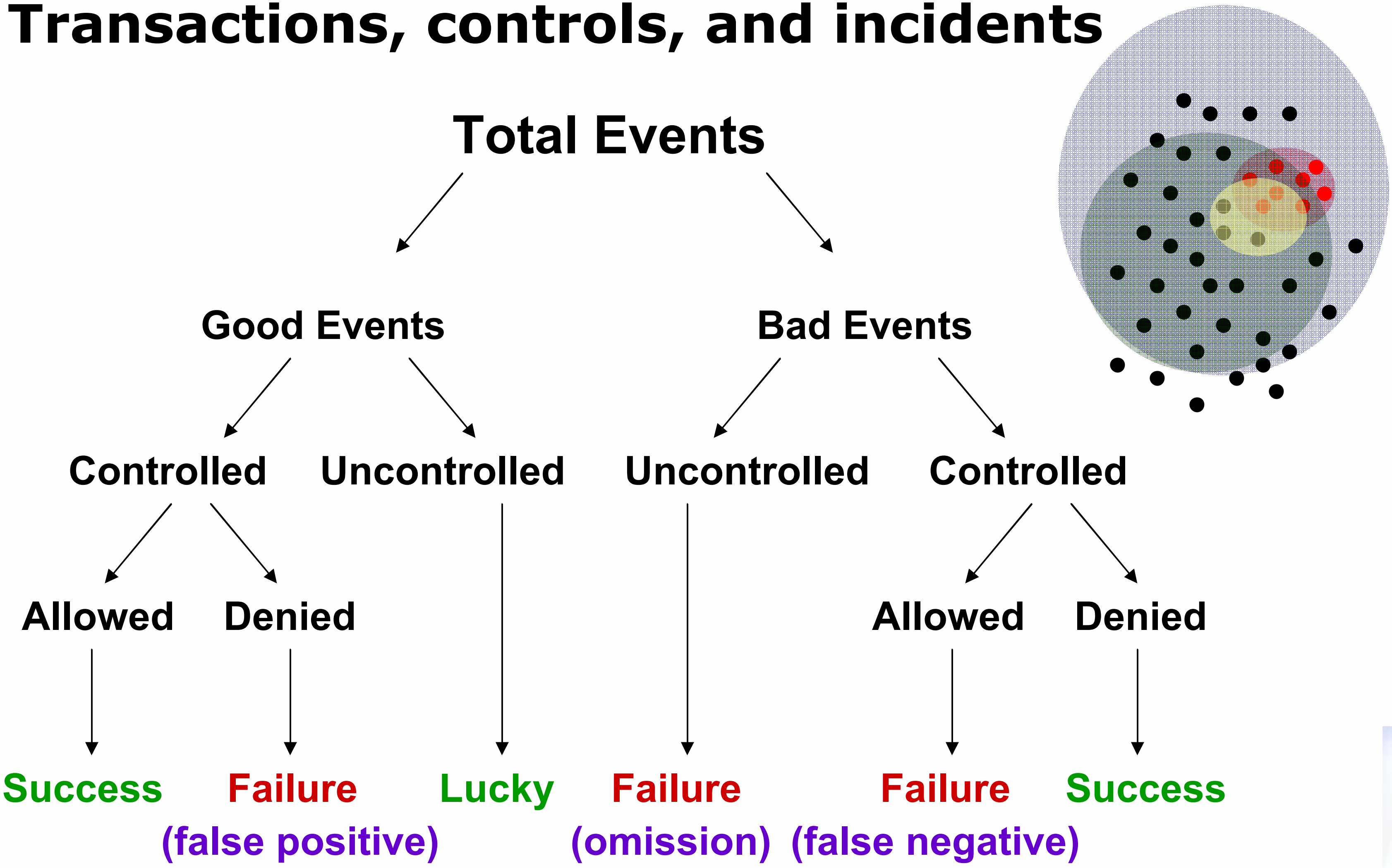
# A security metrics model

- **Controls and incidents**



# A security metrics model

- Transactions, controls, and incidents



Total Events

Good Events

Bad Events

Controlled

Uncontrolled

Uncontrolled

Controlled

Allowed

Denied

Allowed

Denied

Success

Failure (false positive)

Lucky

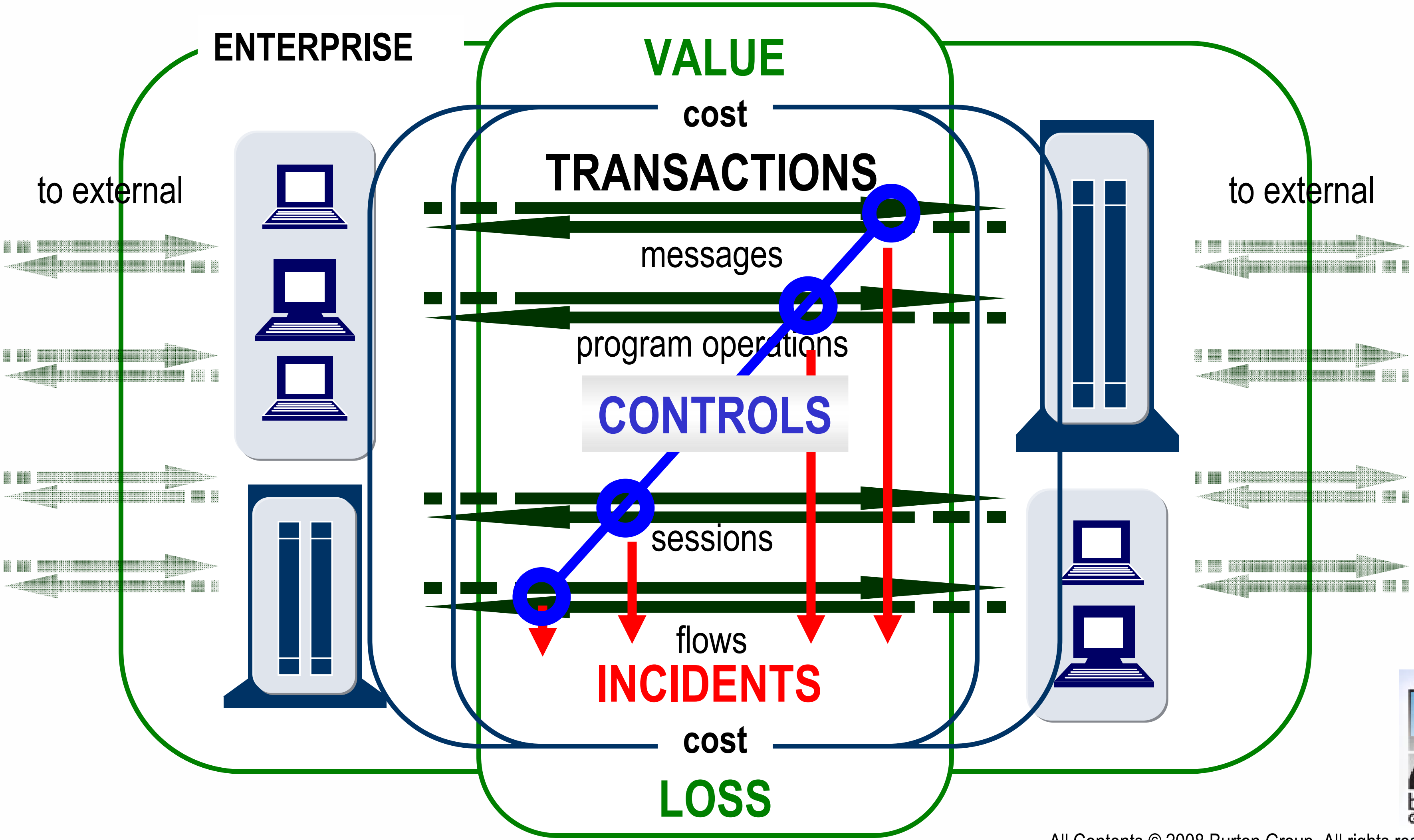
Failure (omission)

Failure (false negative)

Success

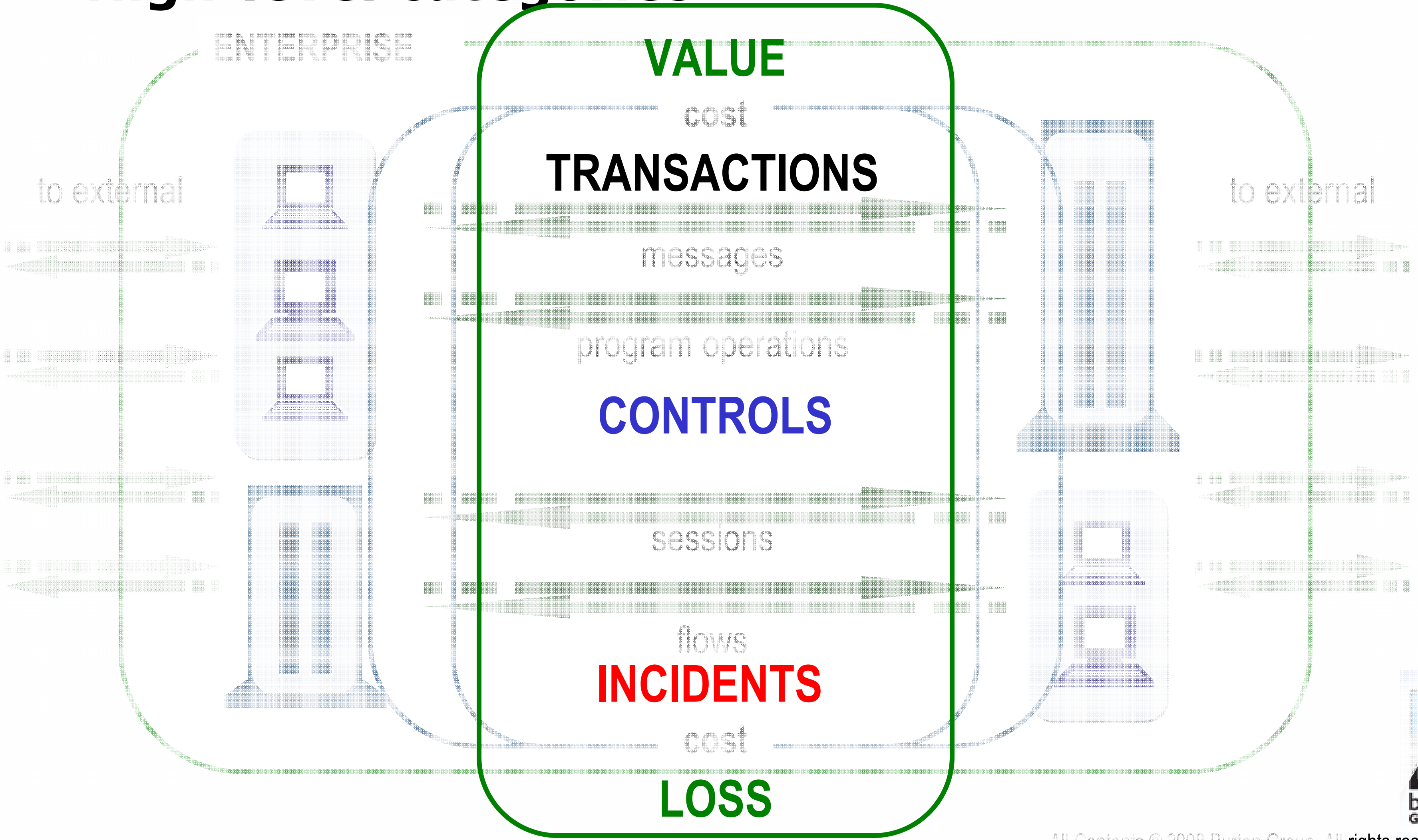
# A security metrics model

- **The complete model**



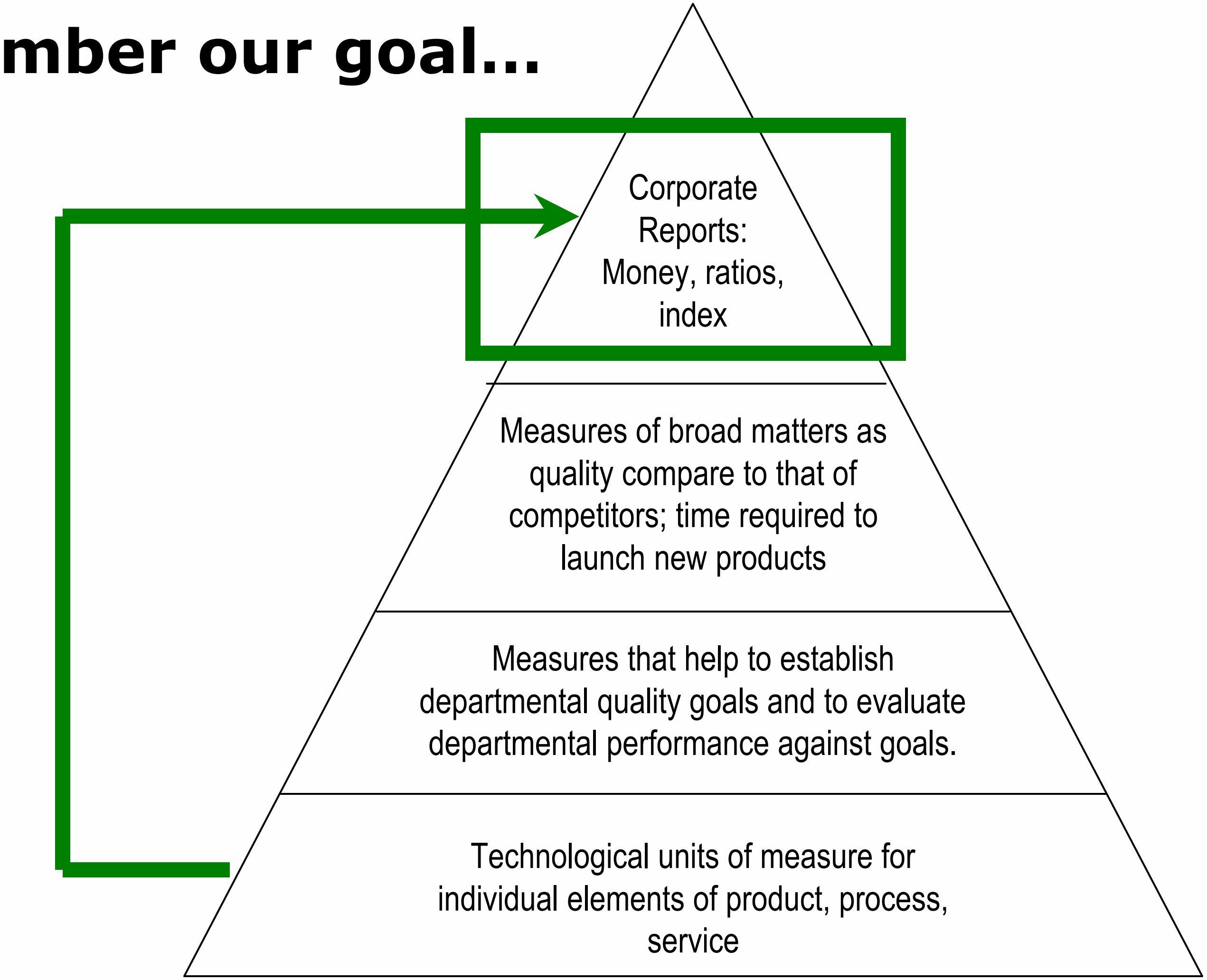
# A security metrics model

- **High-level categories**



# Top ten strategic metrics

- **Remember our goal…**



Corporate Reports: Money, ratios, index

Measures of broad matters as quality compare to that of competitors; time required to launch new products

Measures that help to establish departmental quality goals and to evaluate departmental performance against goals.

Technological units of measure for individual elements of product, process, service

# Top ten strategic metrics

- **The Top Ten (1-5)**
  - Transaction Value (TV)

    (Total Value of IT and Information Assets $ / Total Transactions)
  - Transaction Cost (TC)

    (Total Cost of IT and Information Assets $ / Total Transactions)
  - Controls per Transaction (CPT)

    (Total Number of Inline Control Events / Total Transactions)
  - Cost per Control (CPC)

    (Total Cost of Control $ / Total Number of Inline Control Events)
  - Security to Value Ratio (STV)

    (Total Security Costs $ / Total Value of IT and Information Assets $)

# Top ten strategic metrics

- **The Top Ten (6-10)**
  - Loss to Value Ratio (LTV)
    (Total Losses $ / Total Value of IT and Information Assets $)
  - Control Effectiveness Ratio (CE)
    ((Good Allowed Control Events + Bad Denied Control Events) / Total Number of Inline Control Events)
  - Incidents per Million (IPM); Incidents per Billion (IPB)
    ((Total Number of Incidents / Total Transactions) x One Million or Billion)
  - Incident Prevention Rate (IPR)
    (1 – (Total Incidents / (Good Denied + Total Incidents)))
  - Risk Aversion Ratio (RAR)
    (Good Denied / Total Incidents)

# Top ten strategic metrics

- **An example: Email**

## Assumptions and Data

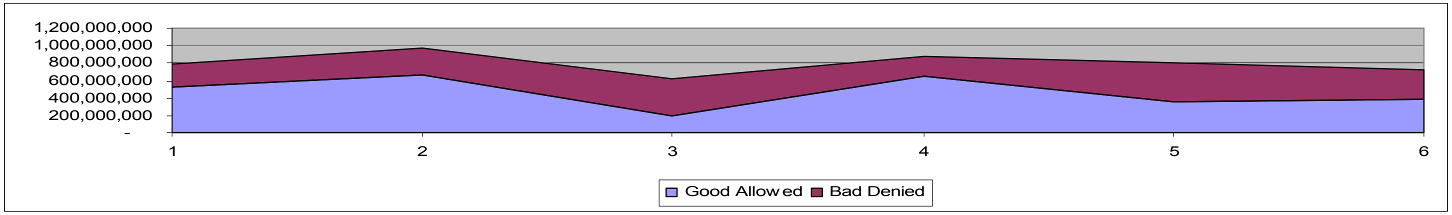
| | | |
|---|---|---|
| Value | $ | 1,000,000 |
| Cost | $ | 250,000 |
| Security Cost | $ | 20,000 |
| Loss per Incident | | $ 300 |
| Transactions | | 400,000,000 |
| Validate IP | | 300,000,000 |
| Antispam | | 400,000,000 |
| Antivirus | | 150,000,000 |
| Good Allowed | | 80,000,000 |
| Bad Denied | | 300,000,000 |
| Good Denied | | 200,000 |
| Bad Allowed | | 500 |

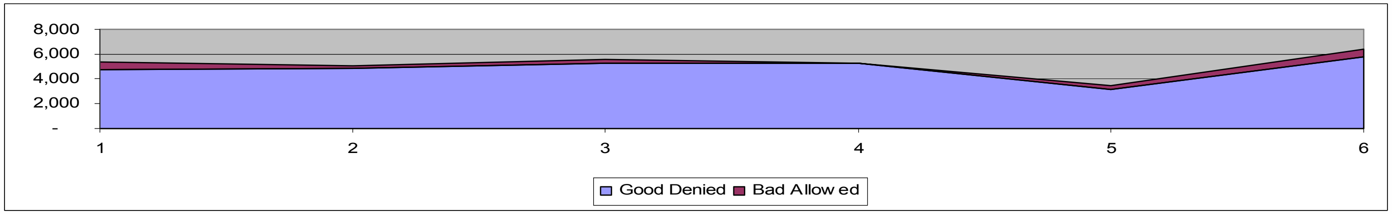
## Calculated Metrics

| | | |
|---|---|---|
| Transaction Value (TV): | $ | 0.0025 |
| Transaction Cost (TC): | $ | 0.000625 |
| Cost per Control (CPC): | $ | 0.000023529 |
| Controls per Transaction (CPT): | | 2.13 |
| Security to Value Ratio (STV): | | 2% |
| Loss to Value Ratio (LTV): | | 15% |
| Control Effectiveness (CE): | | 95% |
| Incidents per Million (IPM): | | 1.25 |
| Incident Prevention Rate (IPR): | | 99.9998% |
| Risk Aversion Ratio (RAR): | | 400 |

# Top ten strategic metrics

- **What will it look like?**





| | | | | | | |
|---|---|---|---|---|---|---|
| Transaction Value (TV): | $ 0.00126 | $ 0.00103 | $ 0.00162 | $ 0.00114 | $ 0.00124 | $ 0.00138 |
| Transaction Cost (TC): | $ 0.00032 | $ 0.00026 | $ 0.00041 | $ 0.00029 | $ 0.00031 | $ 0.00035 |
| Cost per Control (CPC): | $ 0.0000132 | $ 0.0000092 | $ 0.0000132 | $ 0.0000117 | $ 0.0000115 | $ 0.0000129 |
| Controls per Transaction (CPT): | 1.911 | 2.241 | 2.467 | 1.954 | 2.153 | 2.150 |
| Security to Value Ratio (STV): | 2.00% | 2.00% | 2.00% | 2.00% | 2.00% | 2.00% |
| Loss to Value Ratio (LTV): | 18.73% | 7.76% | 10.48% | 0.60% | 8.32% | 19.32% |
| Control Effectiveness Ratio (CE): | 0.999993 | 0.999995 | 0.999991 | 0.999994 | 0.999996 | 0.999991 |
| Incidents per Million (IPM): | 0.787692 | 0.266218 | 0.567262 | 0.022708 | 0.344143 | 0.891477 |
| Incident Prevention Rate (IPR): | 0.999998 | 0.999999 | 0.999999 | 1.000000 | 0.999999 | 0.999998 |
| Risk Aversion Ratio (RAR): | 7.630747 | 18.674157 | 15.012644 | 264.806976 | 11.438912 | 8.969902 |

# Top ten strategic metrics

- **Putting a plan into action**
  - Identify logical starting points
    - Where data is readily available
    - Closed or otherwise contained environments
    - Control-specific data
  - Define the baseline
    - 3-6 months of data to evaluate variance
    - Average, weighted average, cycles, other trends
  - Normalize the data
  - Incorporate other data
    - From other controls, business units, geographic locations, etc.
  - Compare to peers
    - Benchmark for same-size, same-industry peers

# Recommendations

- **Moving forward…**
  - Be consistent, but adapt
  - Understand first, act second
  - Think of data as inputs, not outputs
  - Manage expectations
  - Consider opportunities for benchmarking
  - Get started