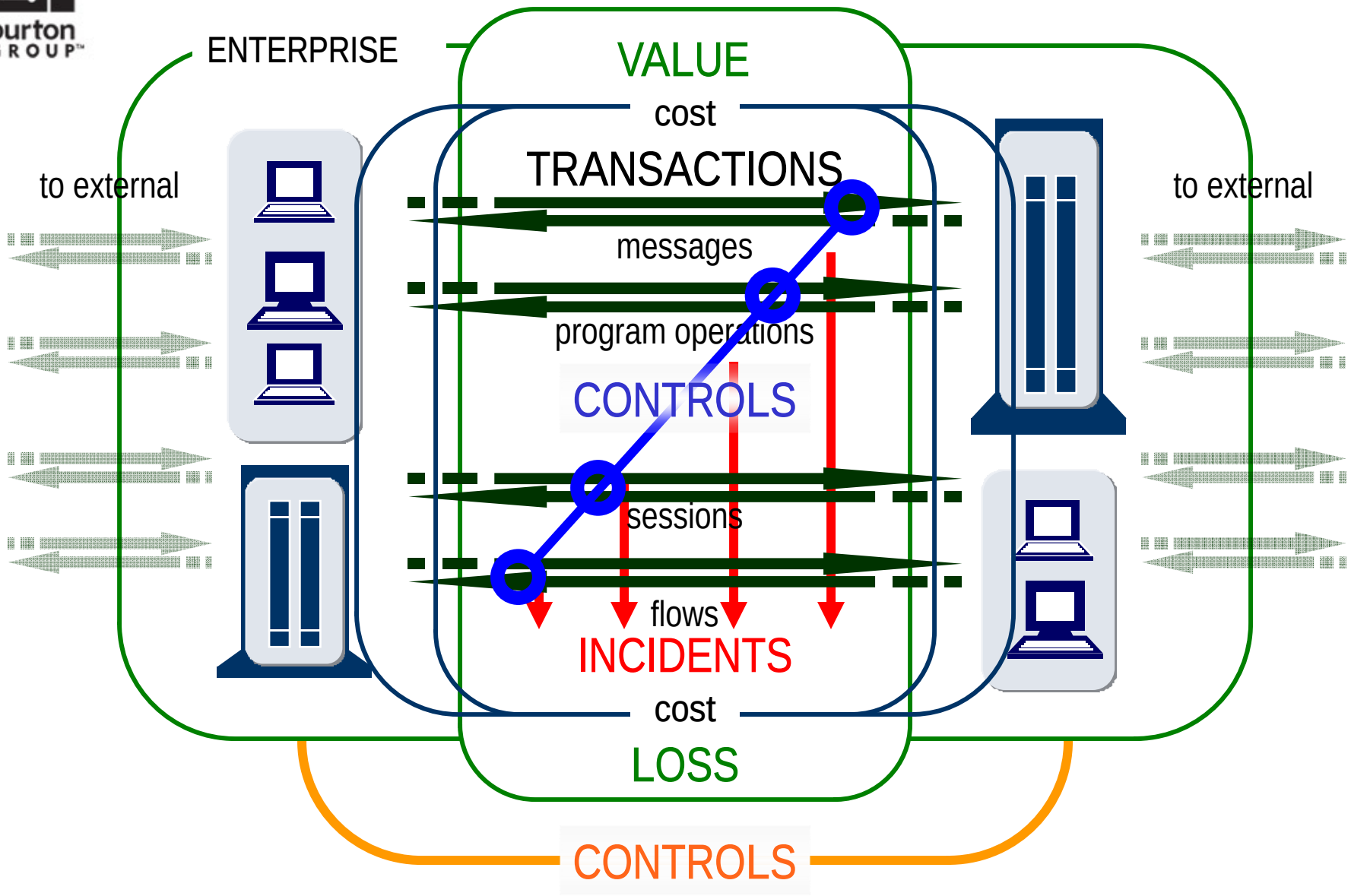
Enterprise Security Metrics

Pete Lindstrom

A Basic Model

A Basic Model



Value

First level: estimate enterprise-wide losses

	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

Value and Loss

First level: estimate enterprise-wide losses

	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

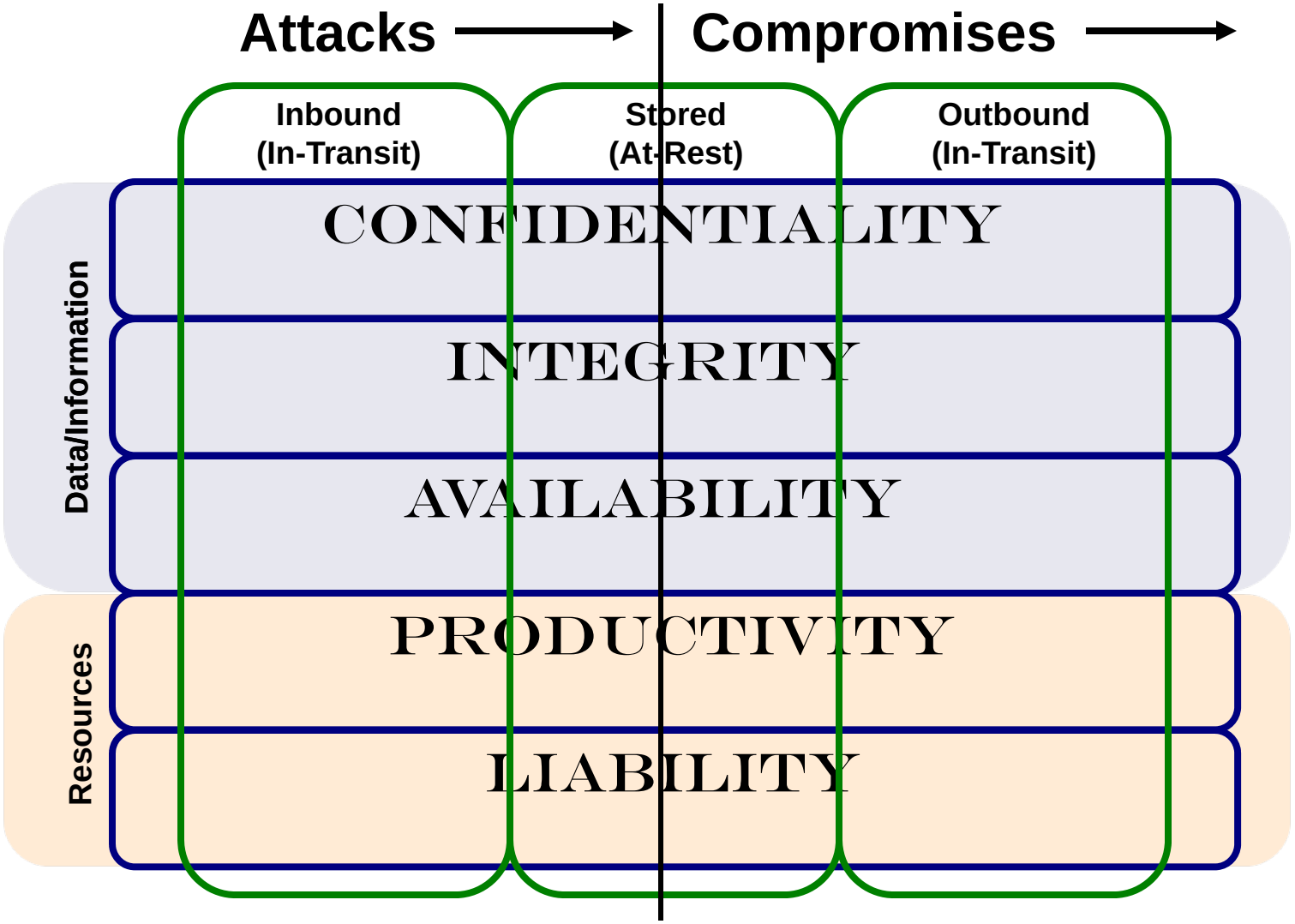
Estimating Loss

Second level: estimate losses for each type of compromise

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

Classifying Value and Losses

The Ginsu approach to Unwanted Outcomes



Risk and Control Metrics

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

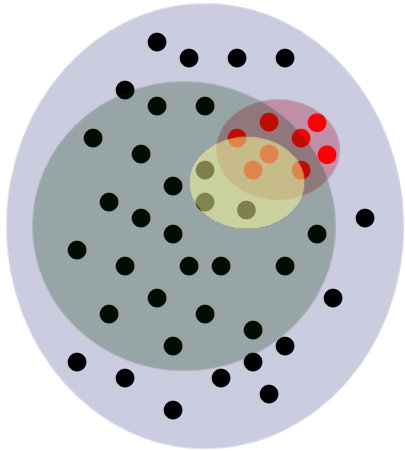
- System calls
- Application calls

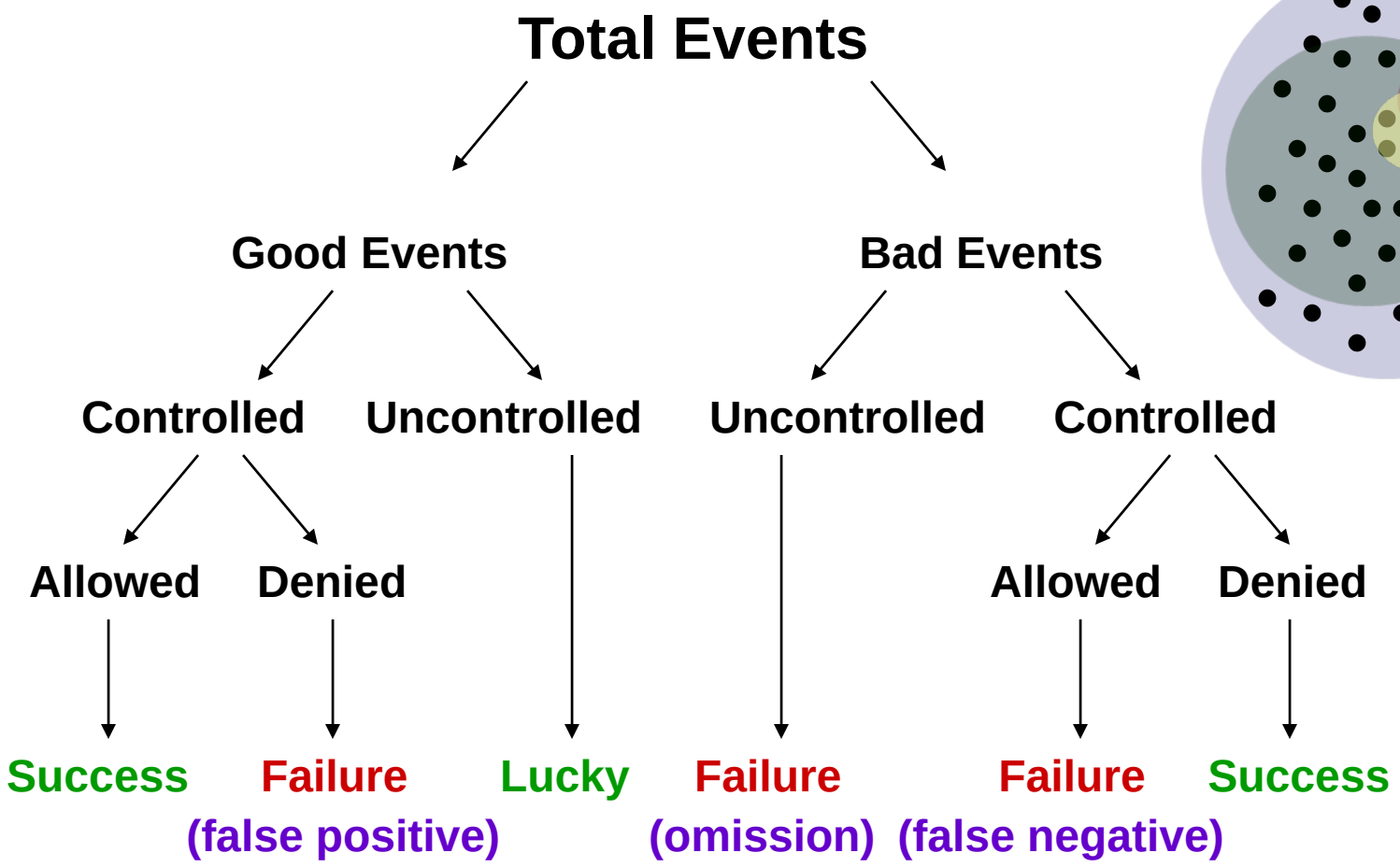
Data Layer: Transactions

- Messages
- Business Events (financial trades, purchase orders, published articles, etc.)

Risk and Control Metrics

5. Control Success / Failure





Risk and Control Metrics

Testing Outcomes

Actual

Test Result	Illegitimate (malicious)	Legitimate	
Negative (Deny)	(TP) True Positive	(FP) False Positive	Total Denies (TP + FP)
Allow	(FN) False Negative	(TN) True Negative	Total Allows (TN + FN)
	Total Malicious (TP + FN)	Total Legitimate (TN + FP)	Total Events

Positive Predictive Value
TP / (TP + FP)

Negative Predictive Value
TN / (TN + FN)

Sensitivity
TP / (TP + FN)

Specificity
TN / (TN + FP)

Prevalence
TP+FN / Total

5. Calculate Control Success Rate

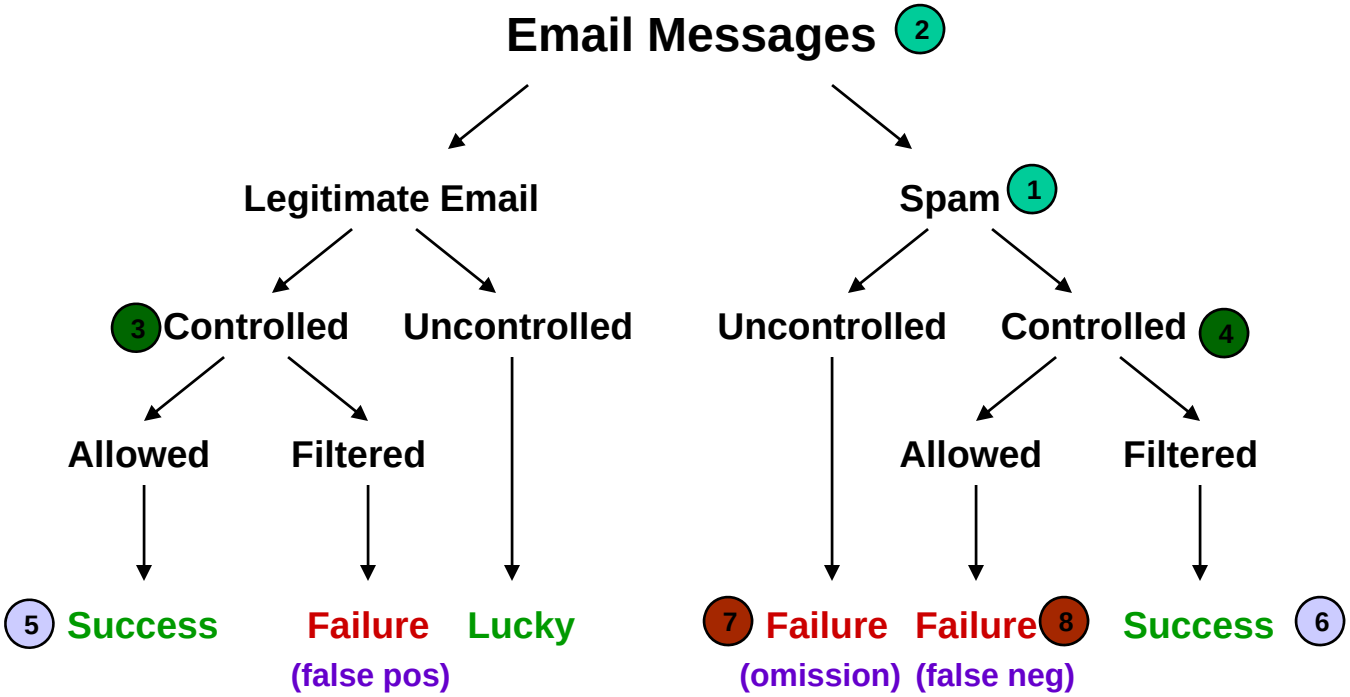
Success and failure:

$$\text{Control Success} = \frac{\text{Good/Allowed (TN)} + \text{Bad/Denied (TP)}}{\text{Total Events}}$$

$$\text{Control Failure} = \frac{\text{False Negatives} + \text{Omissions}}{\text{Total Events}}$$

(This is “residual risk”)

Example 1: Email Risk



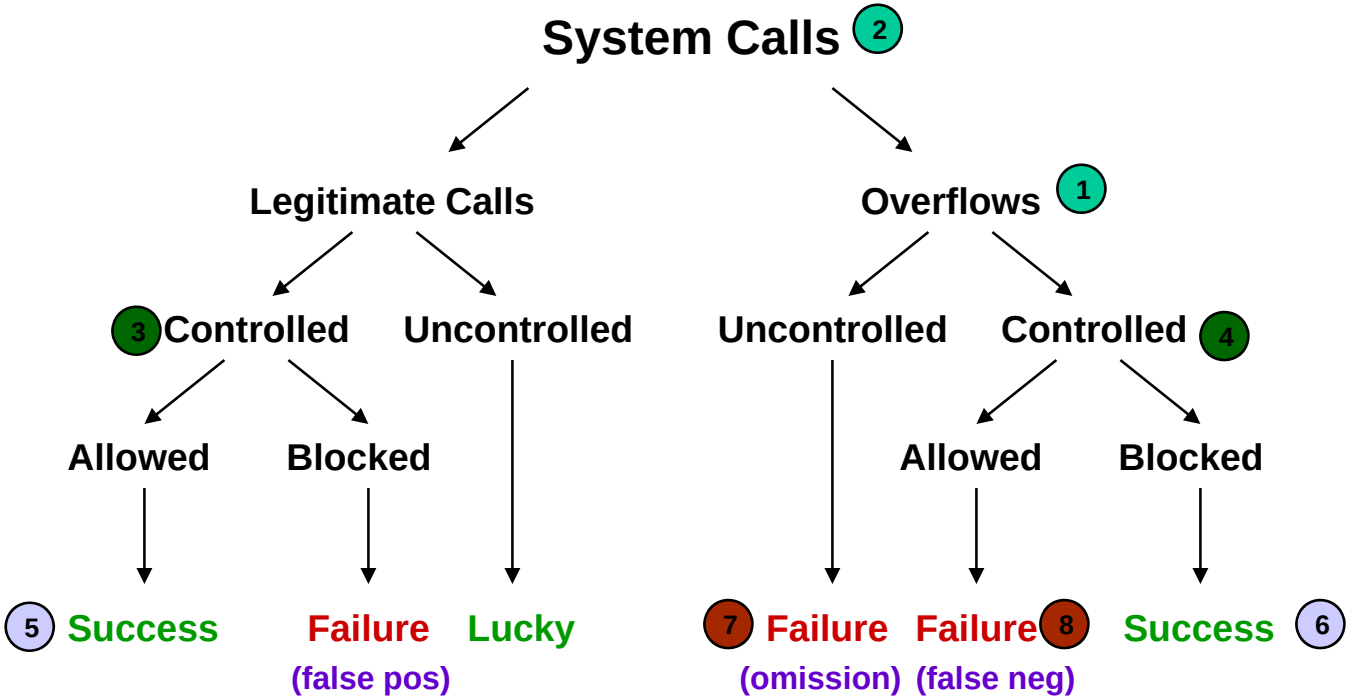
$$\text{Risk} = \frac{\text{Spam } 1}{\text{Email Msgs } 2}$$

$$\text{Coverage} = \frac{\text{Controlled } 3 + 4}{\text{Email Msgs } 2}$$

$$\text{Effectiveness} = \frac{\text{Success } 5 + 6}{\text{Email Msgs } 2}$$

$$\text{“Resid” Risk} = \frac{\text{Incidents } 7 + 8}{\text{Email Msgs } 2}$$

Example 2: Buffer Overflow Risk



$$\text{Risk} = \frac{\text{Overflow}\ 1}{\text{Sys Calls}\ 2}$$

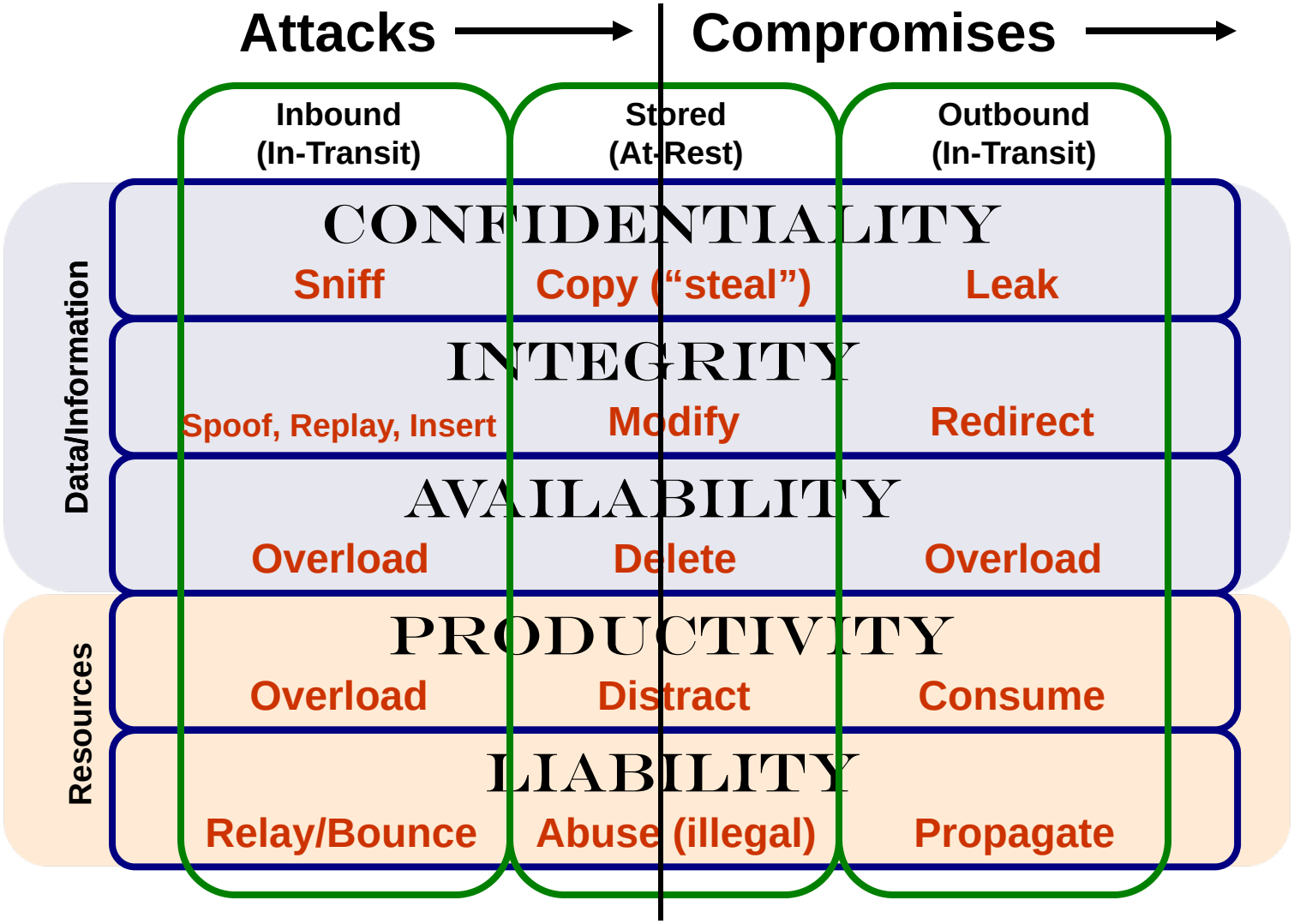
$$\text{Coverage} = \frac{\text{Controlled}\ 3 + 4}{\text{Sys Calls}\ 2}$$

$$\text{Effectiveness} = \frac{\text{Success}\ 5 + 6}{\text{Sys Calls}\ 2}$$

$$\text{“Resid” Risk} = \frac{\text{Incidents}\ 7 + 8}{\text{Sys Calls}\ 2}$$

Classifying Value and Losses

The Ginsu approach to Unwanted Outcomes



Risk and Control Metrics

Three faces of risk:

- Manifest Risk – The risk of attack or compromise associated with system events. (Activity)
- Inherent Risk – the risk associated with the "possibility" of attack due to the availability or exposure of targets. (Asset)
- Contributory Risk – the risk related to control process failure and/or incompletene. (Admin)

Elements of Controls

Manifest Risk Metrics – IT Events (activity)

A. Total Events
B. Total Addressed
C. Legitimate Allows
D. Legitimate Denies
E. False Positives
F. False Negatives
G. Time Period
H. Cost

Elements of Compliance

Target Resources (asset)

A. Total Population
B. Total Addressed
C. Total Control Points
D. Errors
E. Exceptions (approved)
F. Time Period
G. FTEs
H. Cost

Elements of Administration

Security Activities (admin)

A. Requests

B. Errors

C. Time to Complete

D. Time Period

E. FTEs

F. Cost

Process Effectiveness:	B/A
Staff Productivity:	A/E
Frequency:	A/D
Cycle Time:	D/A
Cost Effectiveness:	F/A

What's the Status Quo?

Vulnerability Management

- Total Systems
- Avg Time to Patch (days)

Identity Management

- Awareness Training
- Total Accounts
- Adds/Deletes
- Password Resets
- Time Period

Incident Metrics

- Malware incidents
- User-based incidents

Others Recommendations

A Group of CISOs

1. Failed logins
2. Blocked viruses
3. Blocked spam
4. Trained employees / total employees
5. access control owners - owners per repositories
6. monthly validation of access control by owners
7. % exceptions to OS level policy
8. total daily employee adds and subtracts - workforce
9. Badges assigned / new employees
10. Number of accounts / new employees
11. Number of accts terminated / terminated employees
12. Number of badges turned in / terminated employees
13. awareness index
14. URL blocks /total URL requests
15. Vulnerabilities found
16. % of machines patched “in time”
17. time to patch
18. time to terminate
19. reported misuse of access
20. incidents of copying large numbers of records
21. password reset - calls to help desk
22. approved policy waivers
23. servers up vs. servers not up over time
24. servers improved vs. servers degraded
25. restricted port access attempts
26. manually reviewed spam

Value-Based Metrics

- IAV (Information Asset Value): dollar amount of how much info assets are worth. Since most people appear concerned about valuing assets I have two prescriptions: 1) read Kenneth Feinberg's "What is Life Worth?" to realize that EVERYTHING can be valued, and it only has to be "right" to the people involved; and 2) use IT Spending as a placeholder and potentially change the word "value" to "cost." (This is sort of like balance sheet stuff).
- Transactions: (I count flows, sessions, program operations, and data transactions). Used to understand the volume of activity that occurs online within the context of human usage and value.
- Value (Cost) per Transaction: IAV / Transactions

Risk / Control Metrics

- **Risk (or Attack Ratio):** the number of bad events over total events, expressed as a ratio. This number would assert, for example, that 1 of every 250,000 events is an attack.
- **Control Coverage:** a metric that addresses the breadth of a control. For example, 95% control coverage means that 5% of the activity in an environment associated with that control is not evaluated.
- **Control Success Rate:** (Total controlled events minus (false positives plus false negatives)) all over total controlled events.
- **CPTs (Controls per transaction):** the average number of control events being applied to any single transaction. This applies to inline "gateway" controls like authentication, user access control, system access control, nips, hips that evaluate activity and either allow it or deny it.
- **Exposure Index:** the total number of attackable items for any given resource. This may be as simple as open ports or as complex as some derivative of Howard/Wing's RASQ. It also relates to control coverage, sort of like potential vs. kinetic energy.
- **CPC (Cost per control):** a dollar measure that divides the total security spend by the total CPTs above.

Thanks!

Pete Lindstrom
Senior Analyst
Burton Group
plindstrom@burtongroup.com