THE SECURITY STANDARD

Adapting Enterprise Security to New Realities, Threats and Endpoints

September 10-11, 2012 | New York Marriott at the Brooklyn Bridge | New York City

Produced by

CSO

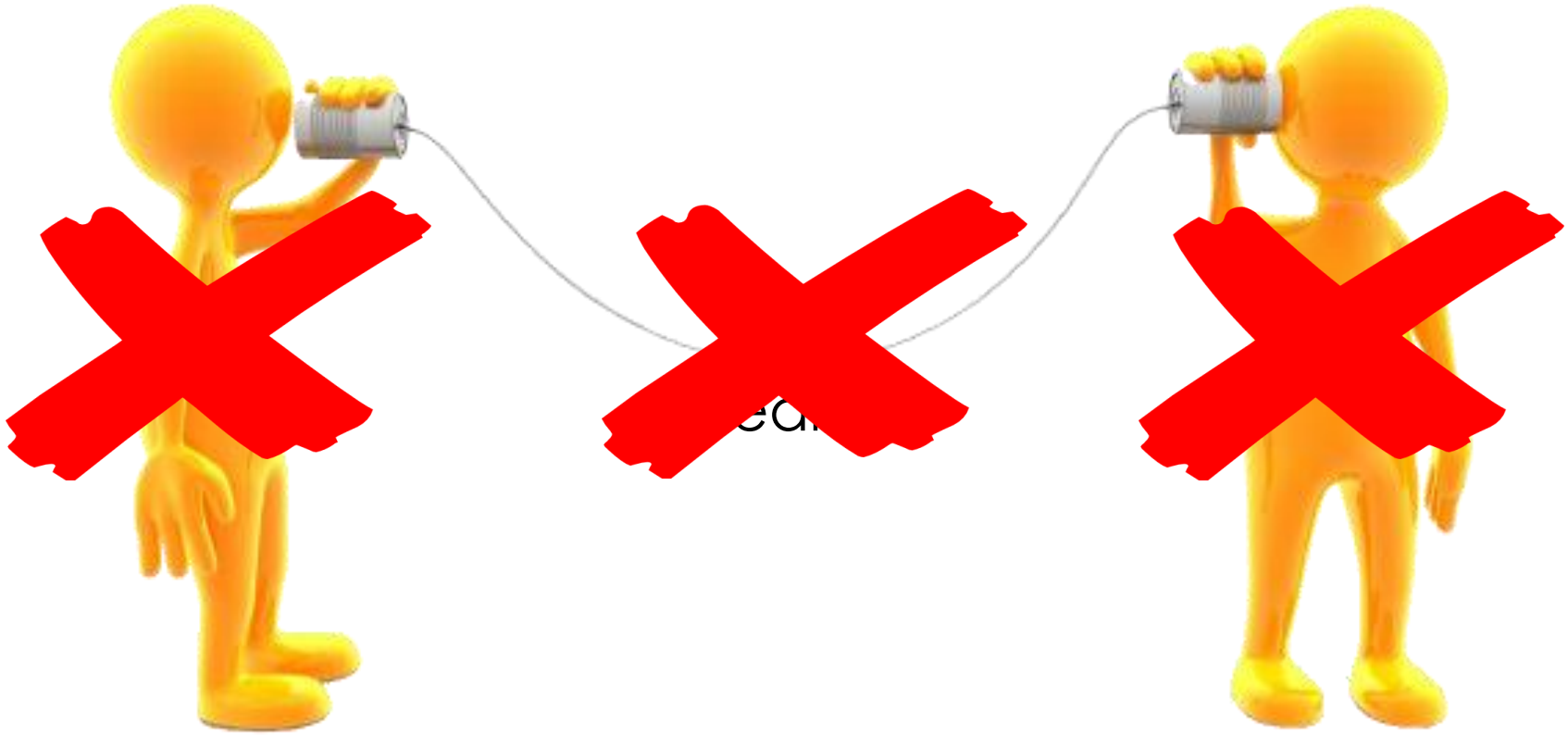
Communicating Security Programs to Achieve Buy-In

Stephen Fried

CISO

Peoples United Bank

How Communications Fail



Transmitter

Receiver

Different audiences, different information.

- Board of Directors
- Executives
- Line Management
- Technical staff
- Customers
- Consumers
- Auditors or Regulators

Situational Awareness is Critical!

- BoD Update
- Project proposal/update
- Risk analysis
- Awareness presentation
- Customer interaction
- Incident

Be Clear About ~~Your~~ Everyone's Goals.

- ☑ Information or Action?
- ☑ Increase or Reduce Concern?
- ☑ Appropriate "altitude"?
- ☑ Appropriate level of risk analysis?
- ☑ Appropriate organization impact?

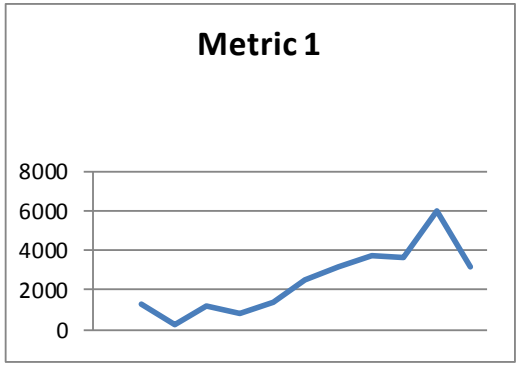


How do You Convey Risk Information?

How to Send the Wrong Message.

Identity & Access Mgmt	Description	October	November	December	Monthly Trend	Quarterly Trend	Target
IAM Metric 1	Description for IAM Metric 1	0%	0%	0%			Target 0%
IAM Metric 2	Description for IAM Metric 2	96%	90%	91%			G:>90%, Y:80-90%, R:<80%
IAM Metric 3	Description for IAM Metric 3	29%	22%	19%			N/A
Risk, Threat, & Vulnerability Management		**October**	**November**	**December**	**Monthly Trend**	**Monthly Trend**	**Target**
RTVM Metric 1	Description for RTVM Metric 1	43%	63%	14%			G:<20, Y:20-35, R:>35
RTVM Metric 2	Description for RTVM Metric 2	1.50	1.30	1.40			Target <1.0
RTVM Metric 3	Description for RTVM Metric 3	4% (2)	4% (2)	4% (3)			G:<16%, Y:16-35%, R:>35%
RTVM Metric 4	Description for RTVM Metric 4	25% (10)	24% (12)	18% (13)			G:<16%, Y:16-35%, R:>35%
RTVM Metric 5	Description for RTVM Metric 5	84	20	29			N/A
RTVM Metric 6	Description for RTVM Metric 6	28:141	7:101	34:109			G:<10%, Y:10%-35%, R:>35%
RTVM Metric 7	Description for RTVM Metric 7	7.23	4.26	5.79			Target <1.0
Incident Management		**October**	**November**	**December**	**Monthly Trend**	**Monthly Trend**	**Target**
IM Metric 1	Description for IM Metric 1	24	30	15			Target <= 10
IM Metric 2	Description for IM Metric 2	0	0	1			Target <=2
IM Metric 3	Description for IM Metric 3	0	0	3			Target <=10
IM Metric 4	Description for IM Metric 4	1	3	1			Target <=2
IM Metric 5	Description for IM Metric 5	$ -	######	$ -			N/A
IM Metric 6	Description for IM Metric 6	$ 1,500	$ 4,850	$ -			N/A
IM Metric 7	Description for IM Metric 7	2	0	0			Target = 0
Infrastructure Protection		**October**	**November**	**December**	**Monthly Trend**	**Monthly Trend**	**Target**
IP Metric 1	Description for IP Metric 1	754	1403	2450			N/A
IP Metric 2	Description for IP Metric 2	21	29	17			G:<20, Y:20-50, R:>50
IP Metric 3	Description for IP Metric 3	18	10	6			G:<10, Y:10-20, R:>20
IP Metric 4	Description for IP Metric 4	0	0	0			Target = 0
IP Metric 5	Description for IP Metric 5	4	0	0			G:<3, Y:4-10, R:>10
IP Metric 6	Description for IP Metric 6	0	0	0			G:<6, Y:6-15, R:>15
IP Metric 7	Description for IP Metric 7	N/A	91.0%	100.0%			G:>98%, Y:90-98%, R:<90%
IP Metric 8	Description for IP Metric 8	4	4	1			N/A

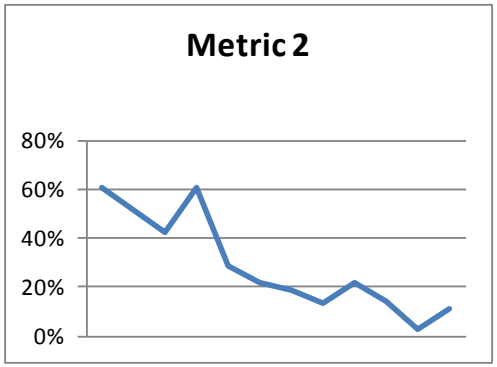
Make your point clear.



Brief description of Metric 1 .

A normal range for Metric 1 is between <X> and <Y>.

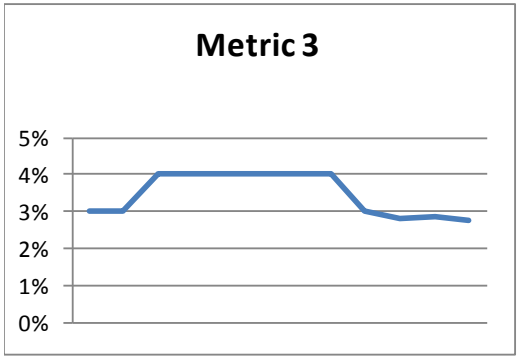
A larger number may be an indication of a problem with the company's defenses.



Brief description of Metric 2 .

A normal range for Metric 2 is between <X> and <Y>.

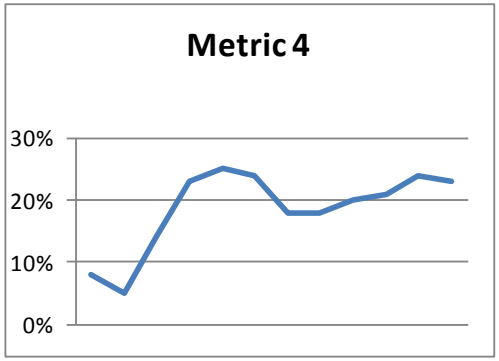
A higher number indicates a larger risk of <something> the company.



Brief description of Metric 3 .

A normal range for Metric 3 is between <X> and <Y>.

A lower value indicates that operational processes for <something> are operating well.



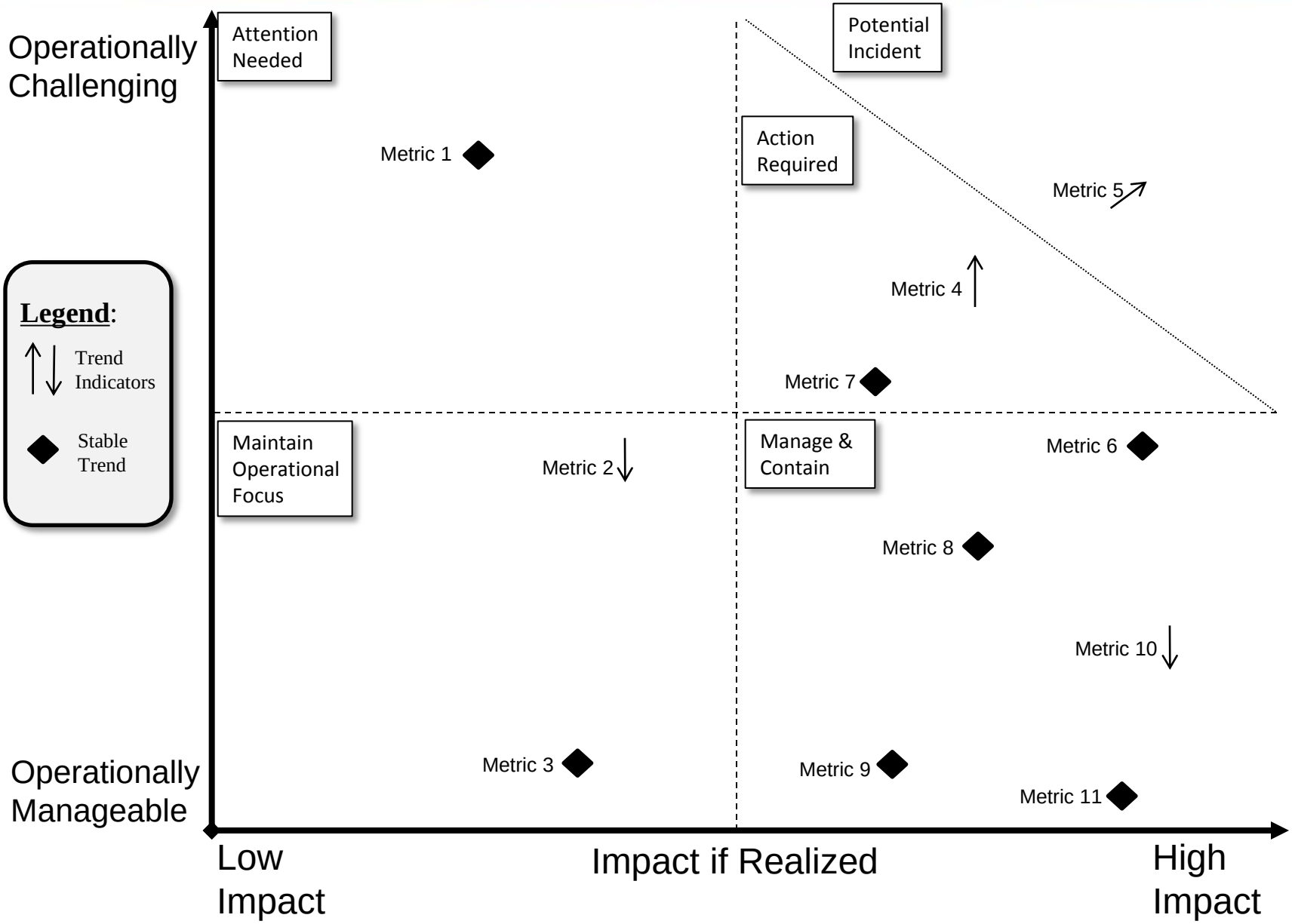
Brief description of Metric 4 .

A normal range for Metric 4 is between <X> and <Y>.

A higher value indicates that more resources may be required to address <an operational issue>.

Additional Information:

Metric 1 *This number has risen over the past few months due to <some external force>.*
Metric 2 *Increased attention in this area has reduced this problem dramatically.*
Metric 3 *Indicators in this area are operating within expected norms.*
Metric 4 *The increase in this number is the result of a full review of this area, which has not occurred for 18 months.*


Operationally Challenging
Attention Needed
Potential Incident
Action Required
Maintain Operational Focus
Manage & Contain
Legend:
Trend Indicators
Stable Trend
Metric 1
Metric 2
Metric 3
Metric 4
Metric 5
Metric 6
Metric 7
Metric 8
Metric 9
Metric 10
Metric 11
Operationally Manageable
Low Impact
Impact if Realized
High Impact

Build credibility with every interaction

Thanks for listening…

Stephen Fried, CISSP, CISM
FVP, Chief Information Security Officer
Information Technology

People's United Bank
What know-how can do SM

850 Main Street
4th Floor
Bridgeport, Connecticut 06604-4913

T: 203.338.4166
E: Steve.Fried@peoples.com

http://friedsecurity.friedfamily.net

THE SECURITY STANDARD

Adapting Enterprise Security to New Realities, Threats and Endpoints

September 10-11, 2012 | New York Marriott at the Brooklyn Bridge | New York City

Produced by

CSO