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







Communicating Security Programs to Achieve Buy-In

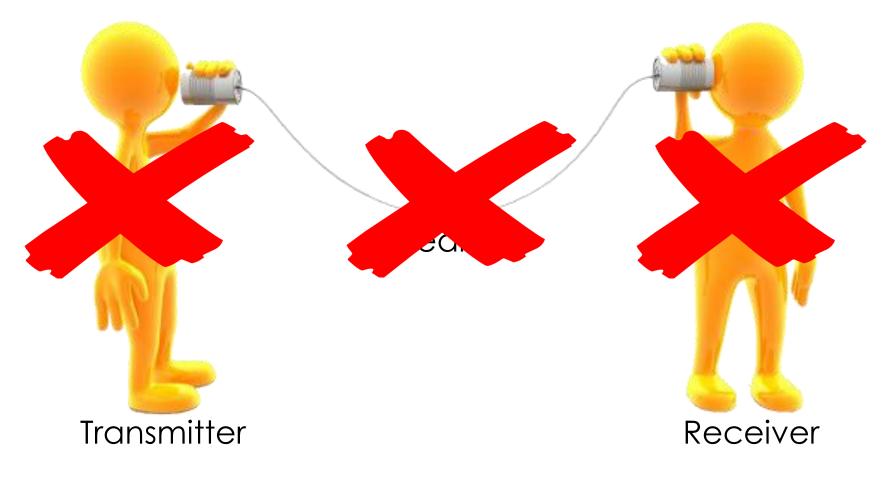
Stephen Fried CISO Peoples United Bank





September 10-11, 2012

How Communications Fail







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 Goals.

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











How do You Convey Risk Information?



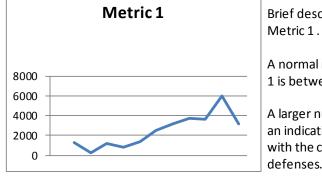
September 10-11, 2012

How to Send the Wrong Message.

IAM Metric 1 Description for IAM Metric 1 0% 0% 0% 1 Target 0% IAM Metric 2 Description for IAM Metric 2 96% 90% 91% G-90%, V 0% <	0							
Number 1 Description for NAM Metric 2 96% 90% 91% Composition Com	Identity & Access Mgmt			November		Monthly Trend	Quarterly Trend	Target
Ham Metric 2Description for IAM Metric 329%29%19%Interminant DescriptionRisk, Threat, & Vulnerability ManagementOctoberNovemberDescriptionMonthly TrendMonthly TrendNARTVM Metric 1Description for RTVM Metric 21,501,301,40InterminantG<20, V2	IAM Metric 1	Description for IAM Metric 1	0%	0%	0%			Target 0%
IAM Metric 3 Description for IAM Metric 3 29% 22% 19% Image: Comparison of C	IAM Metric 2	Description for IAM Metric 2	96%	90%	91%			G:>90%, Y:80- 90%, R:<80%
RTV. Mutric 1 Description for RTVM Metric 1 43% 63% 14% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 63% 14% 64% 64% 63% 14% 64% 64% 64% 64% 64% 64% 64% 63% 14% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 64% 63% 14% 64% 64% 64% 64% 63% 14% 64%	IAM Metric 3	Description for IAM Metric 3	29%	22%	19%			
RTVM Metric 2 Description for RTVM Metric 2 1.50 1.30 1.40 Rescale Rescale RTVM Metric 2 Description for RTVM Metric 3 4% (2) 4% (2) 4% (3) Gescale Gescale <td colspan="2">Risk, Threat, & Vulnerability Management</td> <td>October</td> <td>November</td> <td>December</td> <td>Monthly Trend</td> <td>Monthly Trend</td> <td>Target</td>	Risk, Threat, & Vulnerability Management		October	November	December	Monthly Trend	Monthly Trend	Target
RTVM Metric 2 Description for RTVM Metric 2 1.50 1.30 1.40 Image: Color	RTVM Metric 1	Description for RTVM Metric 1	43%	63%	14%			G:<20, Y:20-35,
RTVM Metric 4 Description for RTVM Metric 4 25% (10) 24% (12) 18% (13) 335% (12) 395%	RTVM Metric 2	Description for RTVM Metric 2	1.50	1.30	1.40			Target <1.0
RTVM Metric 4 Description for RTVM Metric 5 84 20 29 Image: Control of Control	RTVM Metric 3	Description for RTVM Metric 3	4% (2)	4% (2)	4% (3)			G:<16%, Y:16-
RTVM Metric 5 Description for RTVM Metric 6 84 20 29 Image: Comparison of Co	RTVM Metric 4	Description for RTVM Metric 4	25% (10)	24% (12)	18% (13)			G:<16%, Y:16-
RTVM Metric 7Description for RTVM Metric 77.234.265.79Monthly TrendMonthly TrendTarget <1.0Incident ManagementOctoberNovemberDecemberMonthly TrendMonthly TrendTarget <=1	RTVM Metric 5	Description for RTVM Metric 5	84	20	29			
RTVM Metric 7Description for RTVM Metric 77.234.265.79Monthly TrendMonthly TrendTarget <1.0Incident ManagementDescription for IM Metric 1243015Monthly TrendMonthly TrendMonthly TrendTarget <=1	RTVM Metric 6	Description for RTVM Metric 6	28:141	7:101	34:109			G:<10%, Y:10%-
IMAGENTIAL SegmentImage: Construction of the index of the	RTVM Metric 7	Description for RTVM Metric 7	7.23	4.26	5.79			35%, R:>35% Target <1.0
Infinite from the formation of the Metric 1Image: Construction of the Metric 1Image: Construction of the Metric 1Image: Construction of the Metric 2Image: Construction of the Metric 2Image: Construction of the Metric 3Image: Construction of the Metric 3 <t< td=""><td>Incident Management</td><td></td><td>October</td><td>November</td><td>December</td><td>Monthly Trend</td><td>Monthly Trend</td><td>Target</td></t<>	Incident Management		October	November	December	Monthly Trend	Monthly Trend	Target
Init Metric 2 Description for IM Metric 2 0 0 1 <td>IM Metric 1</td> <td>Description for IM Metric 1</td> <td>24</td> <td>30</td> <td>15</td> <td></td> <td></td> <td>Target <= 10</td>	IM Metric 1	Description for IM Metric 1	24	30	15			Target <= 10
IM Metric 3Description for IM Metric 3Immetric 3 <t< td=""><td>IM Metric 2</td><td>Description for IM Metric 2</td><td>0</td><td>0</td><td>1</td><td></td><td></td><td>Target <=2</td></t<>	IM Metric 2	Description for IM Metric 2	0	0	1			Target <=2
Invince 4Description for IM Metric 4Image: Figure 4 <thimage: fi<="" td=""><td>IM Metric 3</td><td>Description for IM Metric 3</td><td>0</td><td>0</td><td>3</td><td></td><td></td><td>Target <=10</td></thimage:>	IM Metric 3	Description for IM Metric 3	0	0	3			Target <=10
Invitation of the Mieric 3Solution for IN Mieric 3Solution for IM Mieric 3NovemberSolution for IM Mieric 3NovemberDescriptionMonthly TrendMonthly TrendMonth	IM Metric 4	Description for IM Metric 4	1	3	1			Target <=2
IM Metric 0 Description for IM Metric 0 \$ 1,300 \$ 4,030 \$ -1 Image: Constraint of the metric 0 Target = 0 IM Metric 7 Description for IM Metric 7 2 0 0 Image: Constraint of the metric 0 Target = 0 Infrastructure Protection October November December Monthly Trend Monthly Trend Target = 0 IP Metric 1 Description for IP Metric 1 754 1403 2450 Image: Constraint of the metric 0 N/A IP Metric 2 Description for IP Metric 2 21 29 17 Image: Constraint of the metric 0 N/A IP Metric 3 Description for IP Metric 3 18 10 6 Image: Constraint of the metric 0 Constraint of the metric 0 IP Metric 4 Description for IP Metric 5 4 0 0 Image: Constraint of the metric 0 IP Metric 5 Description for IP Metric 6 0 0 Image: Constraint of the metric 0 Constraint of the metric 0 IP Metric 6 Description for IP Metric 6 0 0 Image: Constraint of the metric 0 Constraint of the metric 0 IP Metric 7 Description for IP Metric 6 0	IM Metric 5	Description for IM Metric 5	\$ -	######	\$ -			N/A
Infrastructure Protection Description for IP Metric 1 754 1403 2450 Monthly Trend Monthly Trend N/A IP Metric 1 Description for IP Metric 2 21 29 17 G: <20, Y:2	IM Metric 6	Description for IM Metric 6	\$ 1,500	\$ 4,850	\$ -			N/A
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:2	IM Metric 7	Description for IM Metric 7	2	0	0			Target = 0
IP Metric 1Description for IP Metric 1IP Metric 2212917IPIP Metric 2Description for IP Metric 2212917 $\frac{1}{R:>50}$ IP Metric 3Description for IP Metric 318106 $\frac{1}{R:>20}$ IP Metric 4Description for IP Metric 4000 $\frac{1}{R:>20}$ IP Metric 5Description for IP Metric 54000 $\frac{1}{R:>10}$ IP Metric 6Description for IP Metric 6000 $\frac{1}{R:>15}$ IP Metric 7Description for IP Metric 7N/A91.0%100.0% $\frac{1}{R:>15}$	Infrastructure Protection		October	November	December	Monthly Trend	Monthly Trend	Target
In Metric 2Description for IP Metric 2212317IP Metric 3Description for IP Metric 318106 $\frac{R:>50}{R:>20}$ IP Metric 4Description for IP Metric 4000Target = 0IP Metric 5Description for IP Metric 54006 $\frac{G:<3, Y:4-1}{R:>10}$ IP Metric 6Description for IP Metric 6000 $\frac{G:<3, Y:4-1}{R:>10}$ IP Metric 7Description for IP Metric 7N/A91.0%100.0% $\frac{G:<98\%, Y}{G:>98\%, Y}$	IP Metric 1	Description for IP Metric 1	754	1403	2450			N/A
IP Metric 3Description for IP Metric 318106 $a = \frac{1}{R \ge 20}$ IP Metric 4Description for IP Metric 4000 $a = \frac{1}{R \ge 20}$ IP Metric 5Description for IP Metric 5400 $a = \frac{1}{R \ge 10}$ IP Metric 6Description for IP Metric 6000 $a = \frac{1}{R \ge 10}$ IP Metric 7Description for IP Metric 7N/A91.0%100.0% $a = \frac{1}{R \ge 98\%}$	IP Metric 2	Description for IP Metric 2	21	29	17			G:<20, Y:20-50,
IP Metric 4 Description for IP Metric 4 0 0 0 Target = 0 IP Metric 5 Description for IP Metric 5 4 0 0 8	IP Metric 3	Description for IP Metric 3	18	10	6			G:<10, Y:10-20,
IP Metric 6Description for IP Metric 6000 $R > 10$ IP Metric 7Description for IP Metric 7N/A91.0%100.0% $R > 10$	IP Metric 4	Description for IP Metric 4	0	0	0			
IP Metric 6 Description for IP Metric 6 0 0 0 G:<6, Y:6-7 IP Metric 7 Description for IP Metric 7 N/A 91.0% 100.0% G:<98%, Y	IP Metric 5	Description for IP Metric 5	4	0	0			G:<3, Y:4-10,
IP Metric 7 Description for IP Metric 7 N/A 91.0% 100.0%	IP Metric 6	Description for IP Metric 6	0	0	0			G:<6, Y:6-15,
98%. R:<90	IP Metric 7	Description for IP Metric 7	N/A	91.0%	100.0%			G:>98%, Y:90-
IP Metric 8 Description for IP Metric 8 4 4 1	IP Metric 8	Description for IP Metric 8	4	4	1			

September 10-11, 2012

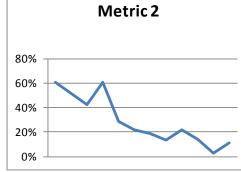
Make your point clear.



Brief description of Metric 1 .

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

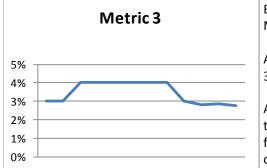
A larger number may be an indication of a problem with the company's defenses.



Brief description of Metric 2 .

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

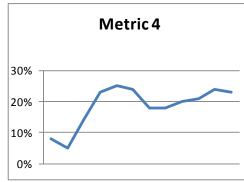
A higher number indicates a larger risk of <something> the company.



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 .

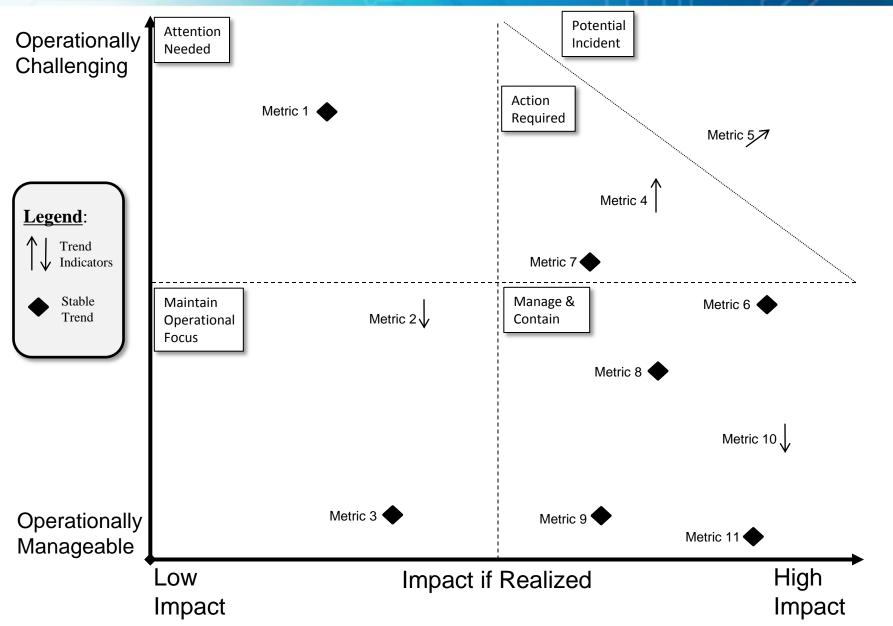
A normal range for Metric 4 is between <X> and <Y>.

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.

September 10-11, 2012







Build credibility with every interaction







September 10-11, 2012

Thanks for listening...

Stephen Fried, CISSP, CISM

FVP, Chief Information Security Officer Information Technology



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

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

