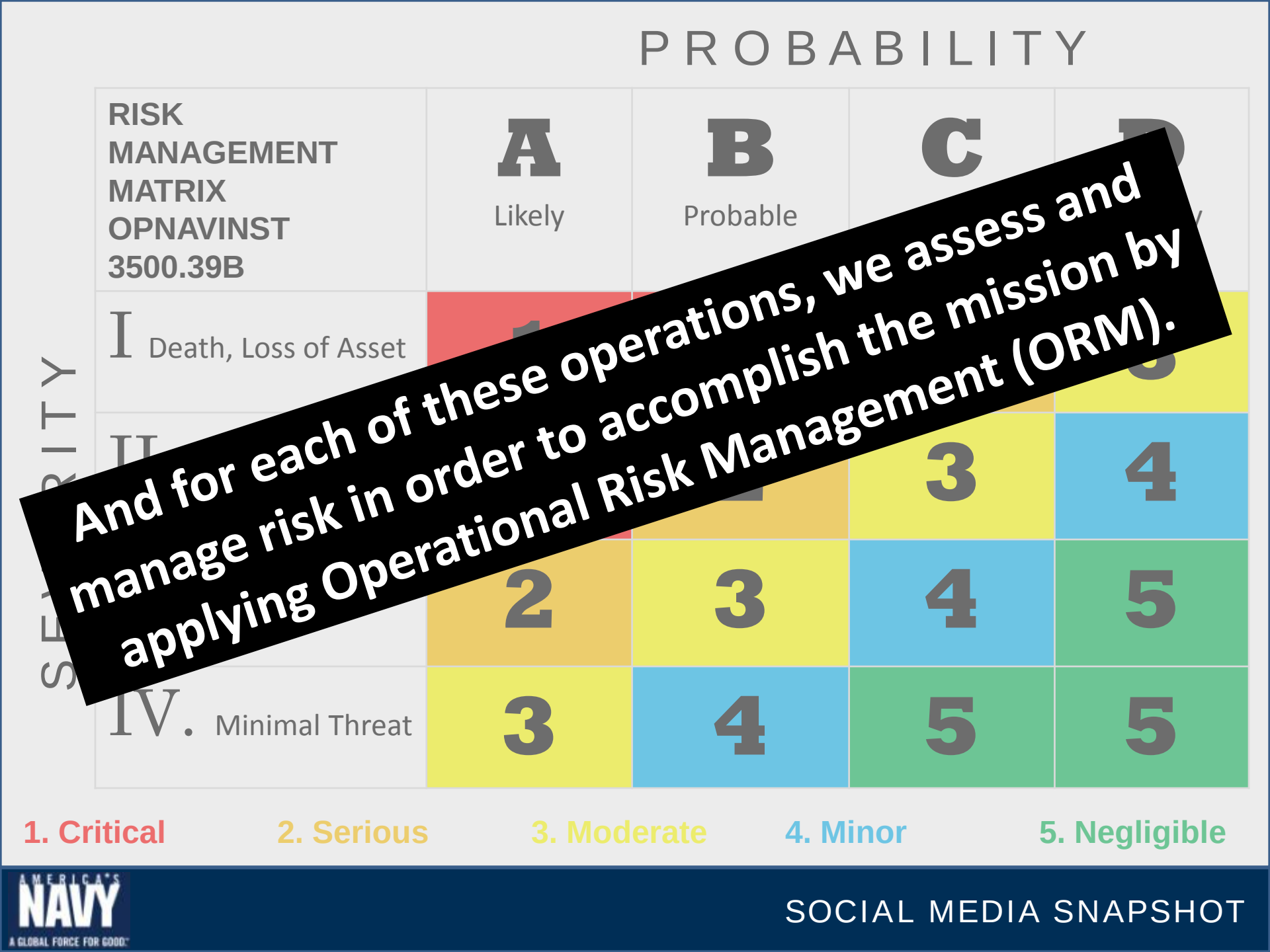
SOCIAL MEDIA SNAPSHOT

APPLYING OPERATIONAL RISK MANAGEMENT (ORM) PRINCIPLES TO SOCIAL MEDIA

Every day, Sailors perform operations that have a considerable amount of risk


PROBABILITY
RISK MANAGEMENT MATRIX OPNAVINST 3500.39B
A
Likely
B
Probable
C
D
I Death, Loss of Asset
II
IV. Minimal Threat
3
4
2
3
4
5
3
4
5
5
1. Critical
2. Serious
3. Moderate
4. Minor
5. Negligible
And for each of these operations, we assess and manage risk in order to accomplish the mission by applying Operational Risk Management (ORM).

Operational and Off-Duty Risk management is, in reality, a **tool for making smart decisions**, used by people at all levels. (Naval Safety Center)

By applying ORM principles to Social Media we can use it safer and more effectively.

The goal of Risk Management is not to eliminate risk, but to manage risk so the mission can be accomplished with minimum impact. We manage risk to operate, not avoid risk as a means to prevent loss. (Naval Safety Center)

Just like in ORM, our objective in using social media is not to eliminate risk (impossible), but to **manage risks so that we effectively communicate with minimum impact to safety and security**.

The five-step ORM process

Applying the five-step ORM process to using Social Media gives us a framework to look out how we can mitigate risks.

1. Identify hazards
2. Assess the hazards
3. Make risk decisions
4. Implement controls
5. Supervise and watch for change

Let's apply these 5 steps to some situations…

SCENARIO 1:
ANGRY COMMENTS ON BLOG

1. Identify hazards

- My command has a blog and other social media sites and we are talking about potentially controversial topics. We are concerned about negative or even threatening comments on the blog and on our other sites.

2. Assess the hazards

The threat of angry comments on our blog is probable due to the nature of our topics, but only a level IV in severity—The risk of physical injury is very low, but damage to our command/leader's reputation is possible. We assess this threat at a ***level 4= MINOR***

PROBABILITY

RISK MANAGEMENT MATRIX OPNAVINST 3500.39B	A Likely	B Probable	C May	D Unlikely
I Death, Loss of Asset	1	1	2	3
II Severe Injury, Damage	1	2	3	4
III Minor Injury, Damage	2	3	4	5
IV. Minimal Threat	3	4	5	5

SEVERITY

1. Critical
2. Serious
3. Moderate
4. Minor
5. Negligible

3. Make risk decisions

- There is minor risk that we will receive negative or threatening comments associated with controversial topics
- People are already having conversations on these topics
- There is risk if we don't discuss these issues with our audiences. We may receive negative feedback unsolicited or lose credibility if we won't talk about these issues
- We lose the opportunity to learn from the feedback (including negative comments) and perhaps mitigate it with accurate information
- By applying some controls, we can mitigate this minor risk. Communicating with the public and providing opportunities for them to communicate with us is a better option than not communicating because of the risk of angry comments and responses

4. Implement controls

- Prior to the launch of the blog, we developed a comment policy that clearly outlined what would and would not be permitted in the comment section
- The policy clearly states why and how comments will be removed
- We developed key response messaging based on several anticipated negative comments on the topics we are blogging about so we are prepared to respond as necessary
- Blog authors and administrators check the page regularly to monitor for violations of our comment policy

5. Supervise and watch for change

- The blog is regularly monitored and email alerts are sent to the blog administrators as comments are made so that the administrator can review, approve and post the comment before it goes public
- Furthermore, searches and RSS feeds on the topic have been set up to monitor the web (outside of the blog page) for mentions of the blog, our command, the topic itself, and our leadership

SCENARIO 2:
INFORMATION LEAKS THROUGH SOCIAL NETWORK

1. Identify hazards

- Personnel within my command are using Facebook, MySpace and other social networks
- They could post information or photos that could put other personnel, their families or themselves at risk
- Information shared could violate OPSEC

2. Assess the hazards

We know that too many Sailors are not using the strictest privacy settings, so this threat may presents risks (Level C probability). If enough information was obtained by an enemy it could effect the mission or at the extreme result in casualties. (Level I severity). We assess this threat to be a ***Level 2 = Serious.***

PROBABILITY

RISK MANAGEMENT MATRIX OPNAVINST 3500.39B	A Likely	B Probable	C May	D Unlikely
SEVERITY I Death, Loss of Asset	1	1	2	3
II Severe Injury, Damage	1	2	3	4
III Minor Injury, Damage	2	3	4	5
IV. Minimal Threat	3	4	5	5

1. Critical
2. Serious
3. Moderate
4. Minor
5. Negligible

3. Make risk decisions

- There are potential risks if enough of the right kind of information gets out
- Social networks such as Facebook are used by 75% of Sailors, increase morale & readiness, and are a primary means of communicating with family members while deployed
- The Navy encourages Sailors and their families to use Social Media as a means of connecting and telling the Navy story
- It would be impracticable to forbid or prohibit the use of Facebook by Sailors and their friends & family
- By applying some controls we can mitigate a significant amount of the risk and still enjoy the benefits of social media

4. Implement controls

- We already provide OPSEC training to our Sailors. We should emphasize the importance of OPSEC in Social Media as well
- Provide privacy setting recommendations to all personnel and encourage them to share with their families and friends
- Provide OPSEC and privacy setting information to our ombudsmen and encourage them to spread the word about staying safe and protecting information online
- At the next all-hands call, address social media and stress protecting information and checking privacy settings
- Developed a SOP to follow when information that should not be public is identified

5. Supervise and watch for change

- Periodically and randomly monitor the use of Social Media on command computers for potential OPSEC violations.
- Periodically monitor the web for information, photos, videos, etc. on the command or command topics. Identify any potential OPSEC violations and address with the author, and your information security manager if necessary.

REAL WORLD SCENARIO:

(THIS ACTUALLY HAPPENED)

ISRAELI MISSION CANCELED

1. The Hazards

*Background: The Israeli military had to cancel a planned operation after a soldier posted the details of the upcoming mission on Facebook. "The soldier also disclosed the name of the combat unit, the place of the operation and the time it will take place," Haaretz reports. The soldier actually wrote, "**On Wednesday we clean up Qatanah [a village near Ramallah], and on Thursday, god willing, we come home**."*

--ForeignPolicy.com

So in retrospect, if we apply ORM to this situation, what might we do the mitigate the risk in social media?

2. Assess the hazards

Publically communicating operations detail is a very severe risk that is probably without the proper education. This is a ***Level 1 = CRITICAL*** *risk.*

PROBABILITY

RISK MANAGEMENT MATRIX OPNAVINST 3500.39B	A Likely	B Probable	C May	D Unlikely
SEVERITY I Death, Loss of Asset	1	1	2	3
II Severe Injury, Damage	1	2	3	4
III Minor Injury, Damage	2	3	4	5
IV. Minimal Threat	3	4	5	5

1. Critical
2. Serious
3. Moderate
4. Minor
5. Negligible

3. Make risk decisions	•There are potentially critical risks if enough information gets out •Social networks such as Facebook are used by millions of people around the world, increase morale & readiness, and are a primary means of communicating with family members while deployed •It would be impracticable to forbid or prohibit the use of Facebook by personnel and their friends & family •By applying some controls we can mitigate a significant amount of the risk and still enjoy the benefits of social media
4. Implement Controls	•Provide OPSEC training to our personnel emphasizing the importance of OPSEC in Social Media as well •At the next all-hands call, address social media and stress protecting information and checking privacy settings •Developed a SOP to follow when information that should not be public is identified •Make it clear that violators will be punished accordingly
5. Supervise for Change	• Periodically and randomly monitor the use of Social Media on command computers for potential OPSEC violations •Periodically monitor the web for information, photos, videos, etc. on the command or command topics. Identify any potential OPSEC violations and address with the author, and with the information security manager when necessary •Publicly discipline those that violate OPSEC on Social Media

REAL WORLD SCENARIO:

(THIS ACTUALLY HAPPENED)

SAILORS KILLED IN AFGHANISTAN – PERSONAL INFORMATION AVAILABLE TO *EVERYONE*

1. The Hazards

Background: Two Sailors were feared captured in Afghanistan, but they were later found dead.

Their personal information including photos of training; equipment and family members; family members' full names and information; personal interests; and recent "wall posts" were all available to the public.

This information could have been used against them

As the risk of having a Sailor's personal information available online becomes more critical (non-permissive environment), the measures to mitigate its availability/release should increase commensurately.

So in retrospect, if we apply ORM to this situation, what might we do the mitigate the risk in social media?

2. Assess the hazards

75% of Sailors use social networking sites—mostly to stay in touch with family and friends and want to share photos. Privacy settings change regularly. Our enemies ARE using the internet to collect personal information about Sailors to use against us. This is a ***Level 1 = CRITICAL*** *risk.*

PROBABILITY

RISK MANAGEMENT MATRIX OPNAVINST 3500.39B	A Likely	B Probable	C May	D Unlikely
SEVERITY I Death, Loss of Asset	1	1	2	3
II Severe Injury, Damage	1	2	3	4
III Minor Injury, Damage	2	3	4	5
IV. Minimal Threat	3	4	5	5

1. Critical
2. Serious
3. Moderate
4. Minor
5. Negligible

3. Make risk decisions	•There are potentially critical risks if a Sailor's personal information is public in Social Media •Social networks such as Facebook are used by 75% of Sailors, increase morale & readiness, and are a primary means of communicating with family members while deployed •It would be impracticable to forbid or prohibit the use of Facebook by personnel and their friends & family
4. Implement Controls	• Provide OPSEC training to our personnel emphasizing the importance of OPSEC in Social Media as well. •At the next all-hands call, address social media and stress protecting information and checking privacy settings •Developed a SOP to follow when information that should not be public is identified •Require the Sailor to sign a Page 2 in their service record to document that they have been advised to set proper privacy settings on their social media accounts.
5. Supervise for Change	• Periodically and randomly monitor the use of Social Media on command computers for potential OPSEC violations •Periodically monitor the web for information, photos, videos, etc. on the command or command topics. Identify any potential OPSEC violations and address with the author, and when necessary with the information security manager

By applying ORM principles to using Social Media we can mitigate the majority of risks while receiving all of the benefits.

For more training resources see
http://www.slideshare.net/USNavySocialMedia