Mitigating Risk in International Operations: IT, Communication, Financial, Legal, and Physical Security

Brad McIlwain, Theresa Lynn Sidebotham, & Scott Brawner

International operations are arguably as risky as ever. These risks, however, are evolving rapidly. The panel is composed of experts in the areas of Information Security, Communication Security, Financial and Legal International Structure, Crisis Management, and Physical Security. They will identify common risks, future risks, and provide best practices and top tips to improve your international security.

Time: September 20, 3:30 - 4:45 PM

Location: Curacao 8

Learning Objectives

- Increase awareness of international risks.
- Understand the risk trends for your future operations.
- Learn best practices for mitigating your international risk profile

Outline

I. Pre-Presentation (Poll Everywhere)

II. Introduction by Nick Morgan

III. Impact Stories

A. Legal/Financial

1. An aid worker went to a North African country with a large organization, thinking that it had enough clout and information to keep her safe. Unbeknownst to her, unrest in the area was growing. One day, while driving to a remote village, her vehicle was ambushed, and she was taken prisoner. She was imprisoned for three months before her safe release was secured. After returning to the U.S., she sued the ministry. She alleged the following: her training was insufficient; the security personnel provided by

the organization were not trained; the organization's security protocols were inadequate; the organization did not track current intelligence; the organization prevented the FBI and her family from being involved, and would not pay ransom.

2. A missionary family with five children moved to an area of Asia where violence was common. A few months after arrival, while out driving to a remote area, the father was shot by a militant organization. The sending church took responsibility for caring for the widow and children. It raised the following questions: Was the family sufficiently warned about violence in the area? Were they trained in safety protocols? Did they have access to sufficient information about new developments? Was there consideration of whether certain placements were safe or appropriate for families with young children? Who would be responsible for ongoing PTSD or trauma issues for the survivors?

B. Physical

C. IT & Communication

1. Impact of data-driven technology and ability to move about anonymously. (https://www.youtube.com/watch?v=lH2gMNrUuEY).
   Are we ready? It's the data you do not know about that could harm you the most.

IV. Transition

A. This is a sobering reality. While this level of tracking and methodology is not commonplace around the world, it is becoming increasingly more plausible as our collective desire for new technology overshadows our understanding of the risk. In the context of this video, the collective is all of us as consumers; however, in our context here today, it represents a growing and present risk for our global workers. Anonymity as a component of physical security is no longer viable. Mitigating risk in international operations requires a keen focus on data privacy, mobile security, and management of online identity.

V. IT and Communication

A. Data: The Key to Kingdom Impact

1. Our IT systems exist to receive data from people that we can then transform strategically into our operations around the world. This includes data from donors who are supporting our organizations financially. It also

includes data from our prospective, active, and former workers who have entrusted even more data to our care. The risk of data leaks for either constituency is scary but very different. If we lose the trust of donors, our financial status is at risk. Even worse, if data on our sensitive workers is leaked, workers can be endangered.

B. Data Privacy

1. Cyber Crime → Vulnerability scans and Homeland Security alerts
2. Network Security → Edge device and network hardware configuration and management
3. Access Control → Multi-factor authentication
4. Internal Controls → Application layer security
5. GDPR and Corporate Responsibility
    a) Intrusion detection, authentication management, and network configurations
    b) Application layer security
    c) Data transmission between systems
    d) Data footprint

C. Mobile Security

1. Android and iOS updates and version deprecation
2. Metadata and your digital footprint
3. Mobile Apps
4. Cross device synchronization
5. Internet of Things
6. Managing device updates in the wild
7. A stolen device is a practical and even larger risk - these devices are small and can be easy to misplace, especially while traveling. What do the devices of your more high-risk workers say about them?
8. GDPR and Corporate Responsibility
    a) BYOD management
    b) Data leaks
    c) Triangulating data

D. Managing Online Identity

1. Being completely anonymous online is impractical, but know where and how you are contributing to the information available about you.
2. Ruthlessly segregate your hardware, software, and service by purpose.

3. Your social media private group may not be as private as you think.

E. Final Thought

1. Being mindful of such risks is not new to most of us, or is simply the result of technology; but the reality that anonymity is conceivable has passed. They know who you and your workers are. How much they know is up to your organization's controls, policies, and training. Your physical security is a function of data diligence.

VI. Legal

A. How Legal Liability Works

1. Negligence
2. Duty of care
3. Breach of duty of care
4. Harm caused by breach
5. Damages
6. Intentional torts or fraud claims
7. Defamation claims

B. How Is the Risk Allocated?

1. Should there be a limitation on risk for families with young children based on how dangerous the location is?
2. Do missionary families formally assume the risk by some kind of waiver or statement?
3. Are they prepared for suffering?
4. Does the mission have trained personnel and a crisis management team in place?
5. Is there awareness and agreement about a ransom policy?

C. Does the Mission Train Adequately?

1. Are people prepared for risks like being taken hostage?
2. Have they had physical crisis training?
3. What about psychological/mental training?
4. Are they prepared for the concept of suffering?

D. Is Legal Documentation in Place?

1. Do missionaries have an estate plan?
2. Have guardians been assigned for children?
3. Are there finances to care of for children?
4. Have arrangements been made to care for children in case of kidnapping?
5. Is there a crisis plan in place for evacuation (medical or other), a hostage situation, death, sexual assault, arrest, or mental breakdowns?

E. Is There Adequate Information Accessible?

1. Are families signed up for State Department updates?
2. Are other available systems being used to keep people informed (like apps)?
3. Is there a good communication plan in place for a crisis?
4. Do you have K&R insurance to help resolve a crisis?

F. Personal Data

1. Is personal data adequately protected according to worldwide standards such as GDPR?
2. Have families been trained on not putting themselves (or the mission) at risk by revealing too much on social media?

G. Aftercare and Dispute Resolution

1. Will the mission provide trauma care?
2. Is health insurance in place?
3. Is workers compensation in place?
4. Are volunteers covered?
5. Is there a good dispute resolution clause in place that will provide for Christian mediation or arbitration to resolve problems?

VII. Physical

A. Security in the Context of Ministry (SICM)
B. The Battle: Spiritual and Physical
C. Ezekiel 33: 1-6: A Model for Biblical Risk Management Practice
D. Principles and Application of Ezekiel 33:1-5
E. Principles and Application of Ezekiel 33:6
F. Traditional Security Model vs. Great Commission Model

G. Setting Values, Priorities, and Precedent
H. Application of Principles for Personal and Physical Security

VIII. Q&A