Global DFIR In a Fractured World

Challenges in Managing International Incidents
Law Talking

- **Who am I?**
  - Former Litigator
  - Chief Privacy Officer
  - Leader of a Cybersecurity Business
  - Not a fan of being detained at borders
• Moving data across borders is easy .... TOO easy.
• Laws restricting cross-border data transfers are poorly understood, inconsistently enforced and routinely violated unwittingly
• Practical challenges are often overlooked . . . Until it’s too late
• You need to understand the laws and the risks if you are going to engage in international DFIR
Laws n’ Stuff
Many foreign jurisdictions view US data protection model as “inadequate” to protect personal data

Transferring personal data to the US is therefore complicated

US rules around preservation, collection and production of data for litigation and regulatory matters increasingly in conflict with global data privacy regulations
Companies looking to send data to the U.S. from the EU for any reason, including incident response or litigation must ensure there is a transfer mechanism in place:

- Standard Contract Clauses
- Binding Corporate Rules
- Consent
- Privacy Shield (replaced Safe Harbor, which was invalidated in 2016)
China

- New Cyber Security Law took effect June 2017
- Two main pillars
  - 1. privacy and protection of personal information
  - 2. standards for collection and use of personal information
- Data localization (need to get approval from National Cyberspace Administration and State Council to send data out of country)
Russia

- 2014 – Russia adopted personal data localization laws
- Employers cannot disclose personal data to a 3rd party (including affiliates) without specific written consent and “wet” signature.
- Must obtain specific consent to transfer data to US or other countries that do not provide “adequate protection” of PII
- No specific prohibition of cybersecurity measures such as packet inspection, traffic monitoring, malicious signature detection. But watch out for privacy issues.
Tales from the Field
Carribbean (in)Competence
Carribbean (in)Competence
South American Suckers
South American Suckers
Italian Inconvenience
Italian Inconvenience
Lessons Learned . . . The Hard Way
Preparation and Planning

• Go onsite only as last resort
• Make sure you have the most accurate inventory of devices/evidence as you can get – FROM AN IT PERSON
• Choose your team wisely
• Choose your gear wisely
• Assess your risk soberly
• Establish clear rules of engagement
• Assume EVERYTHING will go wrong
Logistics and Travel

• Have a letter of invitation from local contact explaining purpose of visiting
• Be prepared for language challenges
• NEVER travel alone
• Pre-arrange all transportation
• Choose a hotel for security first, convenience second
• Establish regular check-ins with team at home
Legal Risk Mitigation

• Consult with counsel before you plan your trip – understand the local laws
• Pre-register with local embassy/consulate
• Identify a local resource to call if you have law enforcement trouble
• Ensure data transfers are lawful and examine data localization laws
• Confirm visa requirements
• Minimize collection of personal data
(not so) Common Sense Issues

• Absolutely avoid situations presenting physical risk (not as easy as it sounds)
• Only stay for minimum amount of time necessary to complete mission
• Assume at least one person will be unavailable each day onsite
• Assume all gear will be confiscated on the way home (back-up!)
Operational Security
Take-Aways

• Only travel internationally for IR when absolutely necessary
• Plan, plan and plan some more
• Consult with counsel and make sure you know the applicable laws
• Be prepared for everything to go wrong
• Do everything you can to ensure you won’t have to go back.
THANK YOU!

R Jason Straight
SVP, Cyber Risk Solutions/CPO
UnitedLex Corp.
jason.straight@unitedlex.com