

Observations on the (Mostly) Inadvertent Effect of Data Management on International Cybercrime Investigations

Don Allison

Director Forensics and Incident Response

KoreLogic

RVASec 2013

DISCLAIMER

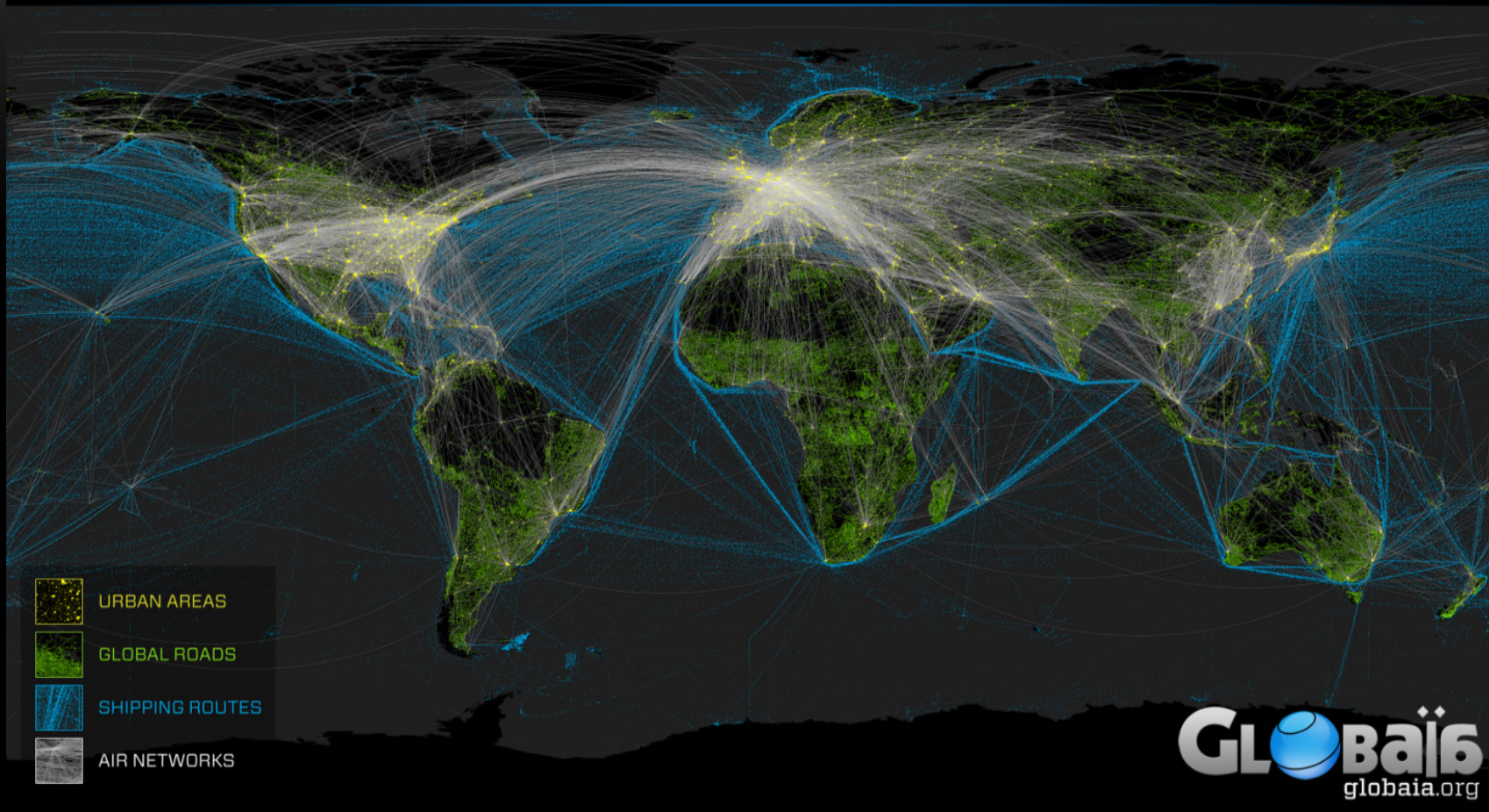
- The presentation contents express the viewpoints of the author and are not reviewed for correctness or accuracy by his employer. Any opinions, comments, solutions or other commentary expressed by the presenter are not endorsed or recommended by his employer or any other entity.

- Any resemblance to real persons, living or dead is purely coincidental. Void where prohibited. Some assembly required. Batteries not included. Contents may settle during shipment. Use only as directed. No other warranty expressed or implied. Do not use while operating a motor vehicle or heavy equipment. May be too intense for some viewers. If condition persists, consult your physician. Subject to change without notice. Edited for television. Not responsible for direct, indirect, incidental or consequential damages resulting from any defect, error or failure to perform. Sanitized for your protection. Sign here without admitting guilt.
Driver does not carry cash.

- Decision of the judges is final.

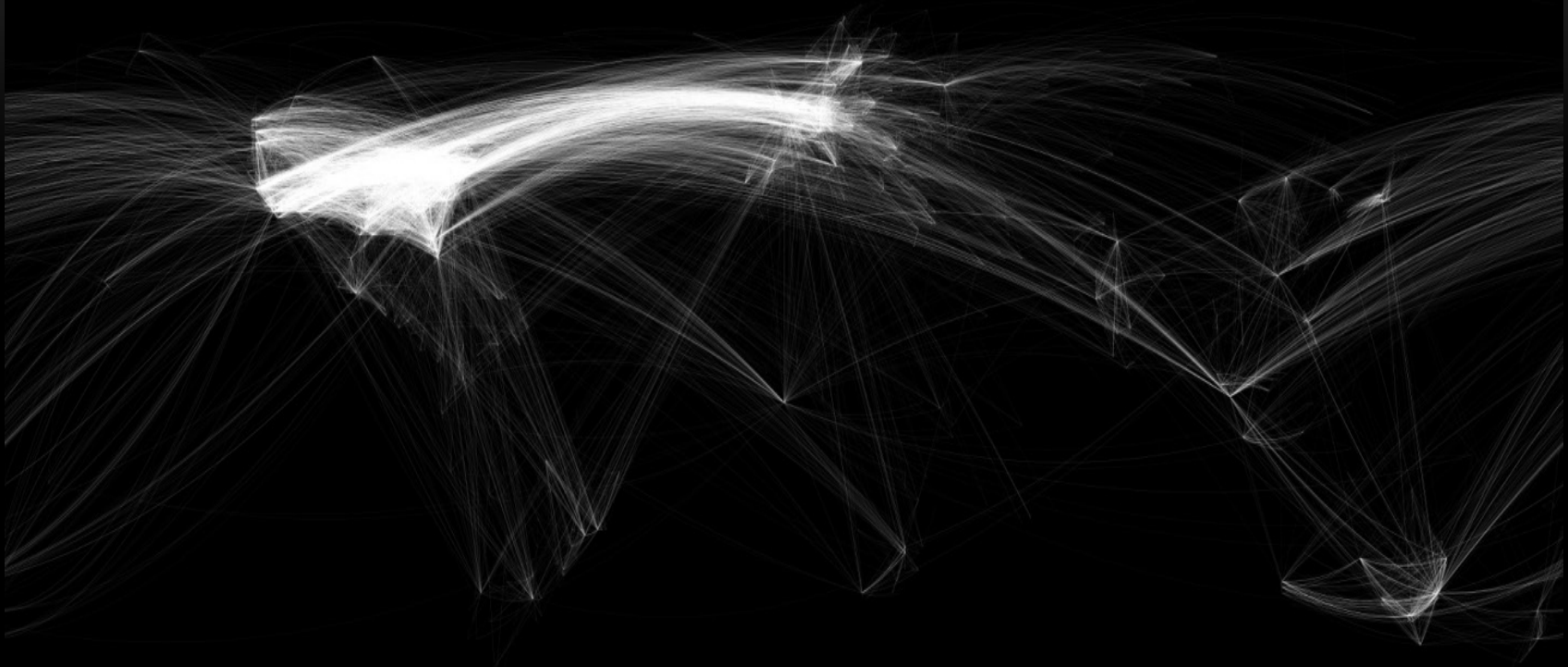
- This supersedes all previous notices.

THE GLOBAL TRANSPORTATION SYSTEM



<http://globaia.org/en/anthropocene/gts.jpg>

Internet Map
city-to-city connections



ChrisHarrison.net

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.



To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through

To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address fine@fbi.gov.



Canadian Police Association Association canadienne des policiers



ALL ACTIVITY OF THIS COMPUTER
HAS BEEN RECORDED



IF YOU USE A WEBCAM,
VIDEOS AND PICTURES
WERE SAVED FOR IDENTIFICATION

You computer is locked!

Your computer has been locked.

This could be due to one of the following reasons:

1. You computer has been used to view banned web sites.
2. You computer has been used to view web sites containing child pornography.
3. You computer has been used to illegal information, software.
4. You computer has been used for storing or viewing pirated content.

What should I do?

According to „Information Security and Control Act 2012“, you are required to pay a fine of 100 canadian dollars. For the convenience of paying the fine we provide a secure payment gateway for Ukash or PaySafeCard vouchers. You need to buy voucher for sum of 100 canadian dollars and enter the 19 or 16 digit code written on the voucher the secure payment form, then press „OK“ button to send the code.

What will happen after I submit the code?

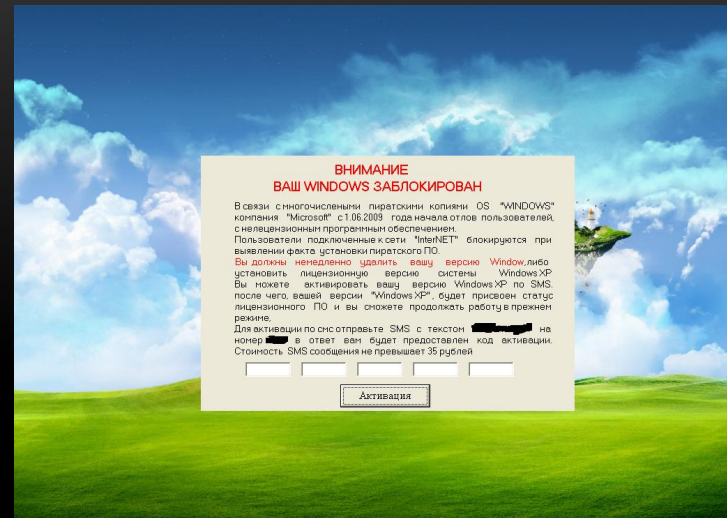
Once voucher code is verified by our system your computer will be unlocked after 24 hours.

Where can I buy PaySafeCard?

PaySafeCard is available from sales outlets from gas station and newsagents, in the Canada, exclusively from all Ezilpin outlets.

Where can I buy Ukash?

You could buy Ukash in many places, for example: shops, malls, terminals, online or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your country.



BUNDESPOLIZEI

Es ist die ungesetzliche Tätigkeit enthüllt!

Achtung!!!
Ein Vorgang illegaler Aktivitäten wurde erkannt.
Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verstoß festgestellt: Ihre IP-Adresse lautet: "212.93.0.154" mit dieser IP wurden Seiten mit pornografischen Inhalten/kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen. Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten/Elementen von Gewalt und Kinderpornografie festgestellt! Es wurden auch Emails in Form von Spam mit terroristischen Hintergründen verschickt. Diese Sperre des Computers dient dazu, Ihre legalen Aktivitäten zu unterbinden.

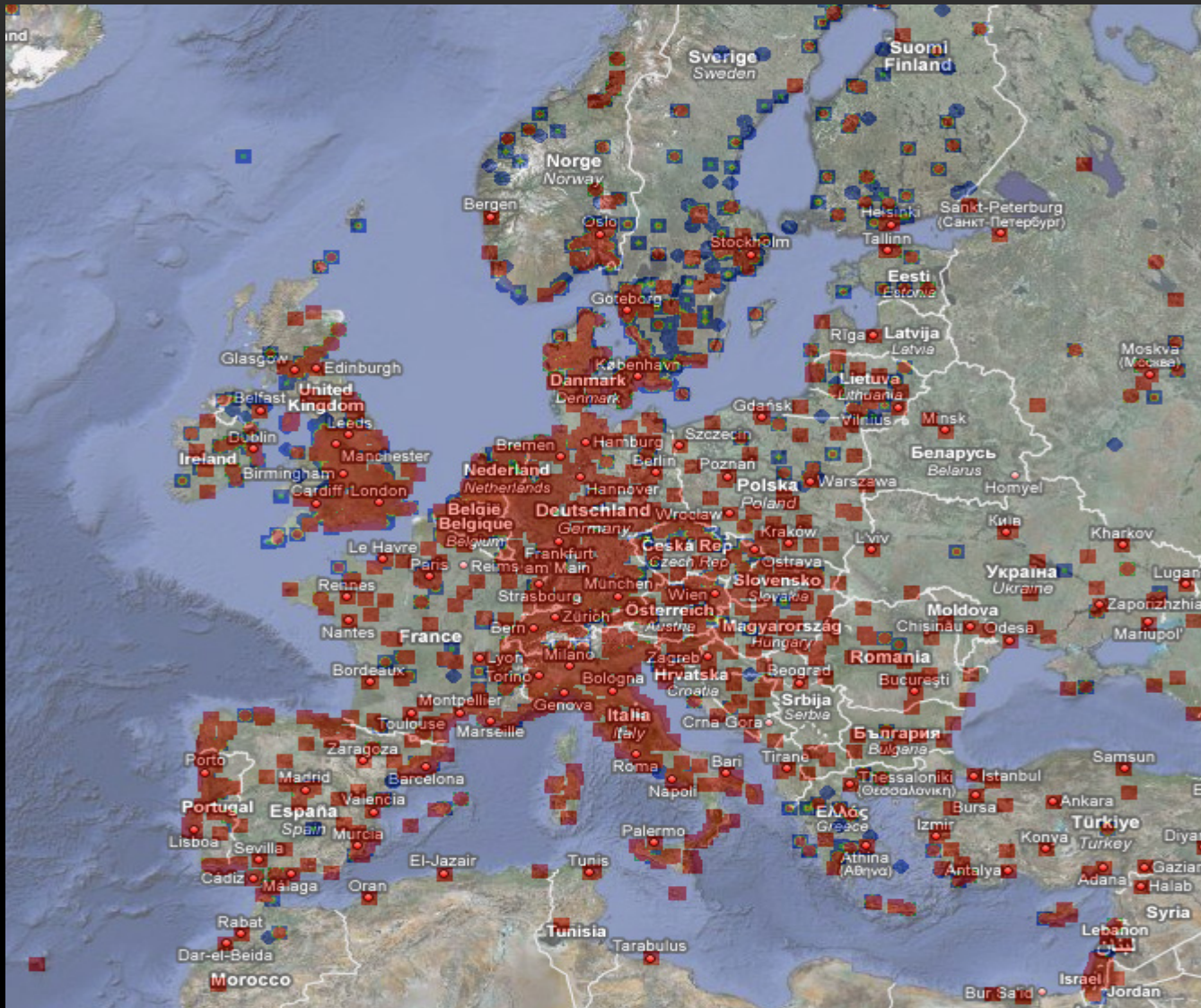
Ihre Angaben: IP: 212.93.0.154 Browser: Internet Explorer 6.0 OS: Windows XP Country: GERMANY City: BERLIN ISP: VERSATEL WEST GMBH

Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen. Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.
1) Die Zahlung per Ukash begleichen:
Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie diese einfach nacheinander ein und drücken Sie anschließend auf OK).
Sollte das System Fehler melden, so müssen Sie den Code per Email (einzahlung@bundespolizei.net) versenden.
2) Die Zahlung per Paysafecard begleichen:
Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie diese einfach nacheinander ein und drücken Sie anschließend auf OK). Sollte das System Fehler melden, so müssen Sie den Code per Email (einzahlung@bundespolizei.net) versenden.

Wo kann ich Ukash kaufen?
Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse). Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.
Tankstellen - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Aral, Esso, OMV, Q1 und Westfalen.
epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

paysafecard
pay cash, pay safe.







If it ends in .com, .net, .cc, .tv and .name
it's seizable

<http://www.ntia.doc.gov/legacy/ntiahome/domainname/agreements/summary-factsheet.htm>

Identify the geographic location of the systems that support, process, store, and backup your data

Use of subcontractors and their management of your data (including cloud providers)

Encryption transmission standards (Import - export requirements)

Data breach liability including notification procedures, data security standards, and other technical security measures for each jurisdiction

Litigation hold procedures for each jurisdiction

E-discovery procedures for each jurisdiction

Business continuity/disaster recovery procedures

Provisions in case of dispute (data held hostage)

Onward transfer agreements if 3rd party/cloud providers are
changed

Data destruction agreements

Points of contact - including jurisdictional aware counsel

Privacy laws

Blocking statutes

Native language speakers

rackspace 2004 indymedia



https://commons.wikimedia.org/wiki/File%3AContainerschiff_Hanjin_Chicago.jpg, By Oliver Ohm (Photovision at de.wikipedia) (Own work) [CC-BY-SA-2.0 (www.creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons

The geographical locations of the cloud provider's servers

The cloud provider's use of subcontractors

Encryption and transmission standards

Data breach liability, including notification procedures

Data security standards, and other technical security
measures

Backups, confidentiality provisions, auditing rights, logs,
and other related responsibilities

Procedures in the event of a litigation hold and/or discovery request

The cloud company's business continuity plan/disaster recovery procedures

Provisions in the event of a dispute with the cloud company (so that data cannot be held hostage)

Onward transfer agreements (in the event that the business migrates cloud providers)

If the topic of APTs gets information security to be addressed at the highest levels of an organization it may still be a useful topic.

There are many other threats that are out there and the APT is not the only threat that spends a fair amount of time in your computer systems and takes your data.

You are more likely to encounter losses from internal and legal problems than to lose significant data to an APT.

What you call hacking may be a legitimate business in its jurisdiction

Despite some wonderful minds and great products, there still is no promise of data security on the Internet.

The OFF button is the only technology answer to date; however, it seems to have a few unwanted limitations

One solution is available to help protect a company's data and impact an investigation

Data Management

Change your mindset and change your culture

Security is a process - not a technology

You are in an all out business war for your data - accept it

Must identify the truly important data - everything else is cat videos

Get help with legal requirements for retention and other concerns

Plan storage and backup space accordingly

Make non-essential data and systems resilient - be willing to lose
non-essential data

Get control of your data – it is not where you think it is

Classify it

Plan and map out where each level of classified data should reside – use jurisdictions to your advantage

Define who should have access to each level of data - monitor those people (especially C-level and domain admin)

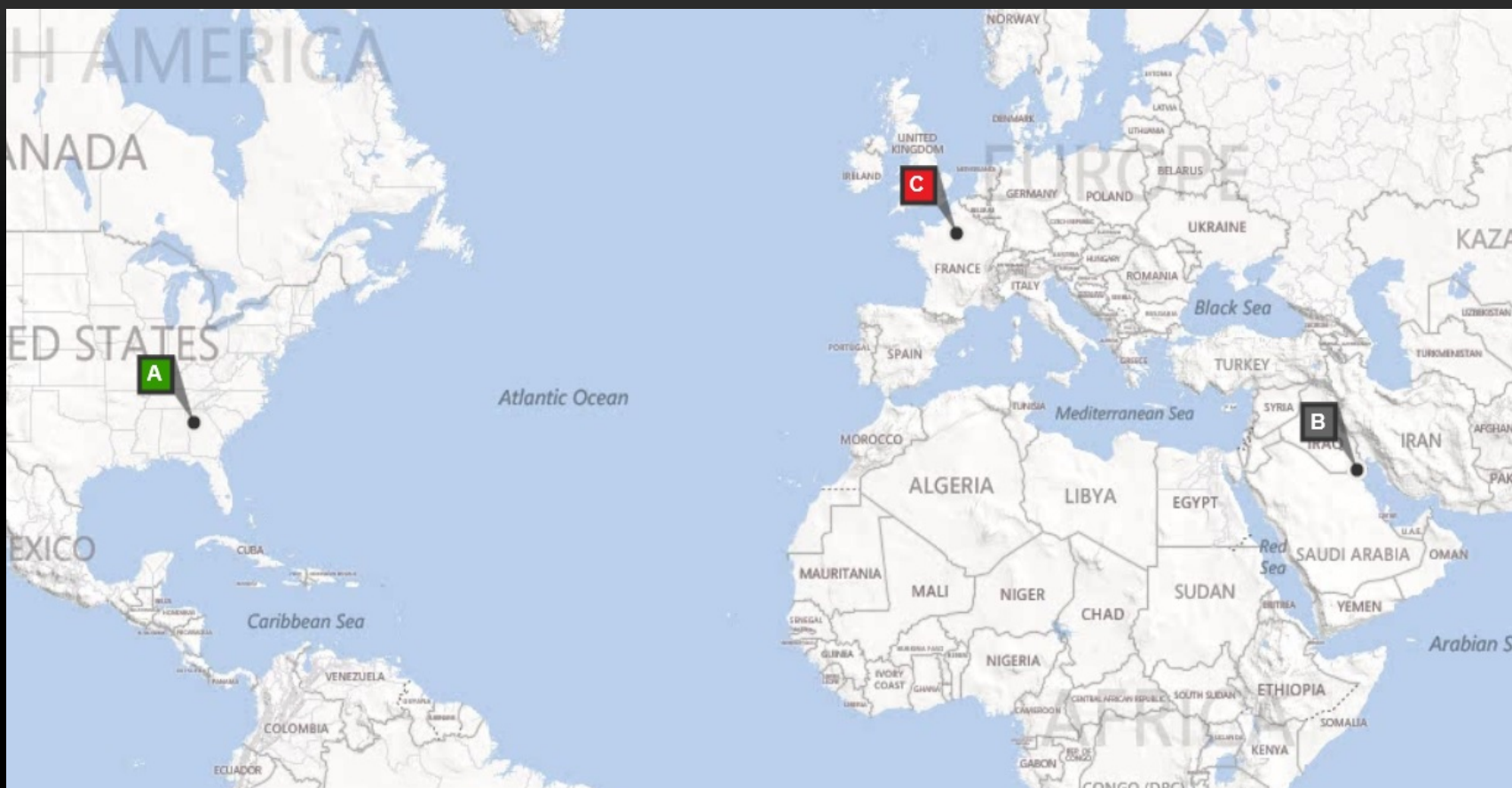
Tie security to individual responsibility - have consequences for incidents

CLASSIFICATION

OWNERSHIP

Attribution

Critical Data



- Questions?
- Comments?
- Tell the Geek to go home?
- You may cross examine the witness...