Mapping information, conducting threat modelling and managing risk

Introduction

Providing effective information security is often a delicate balance. Threats can often be varied and information about them can be confusing or incomplete. Resources are also limited, so organisations need to concentrate on dealing with risk in the most effective way that they can.

This module provides a starting point for the course and to create a framework for thinking and addressing choices made in other modules.

Learning Goals

- Understand what information (both digital and physical) that they use in their work, where it is stored, who has access to it, who might want to access it and how to map it out
- Have a clear understanding of the differences between likelihood, impact, risk and mitigation
- Have located and utilised resources for understanding and accessing their own threat environment
- Understand the challenge of creating an effective information security policy within an organisation

Assessment Goals

- Have created an information map for their organisation
- Add generic and localised threat resources (where available) to their threat assessment
- Have divided their information into easily understandable traffic light map with corresponding mitigation measures

Recommend Preparations

- Mapping is best done physically using flipcharts and/or post-it notes
- Participants should have access to secure wifi
- It may be useful for have a shared hackpad or other document that will allow participants to ensure any new resources that they may find.
- It is helpful for the trainer to have already have an understanding of any localised threats already faced within the countries and/or organisations that the participants are from. In the "Deepening" section, a number of case studies should be selected. Ideally these will have public information already known about them (e.g media reports), so that the participants will be able to research the topics and make recommendations themselves. It is suggested to use some of the locations in the "Resources" section for this.

Suggested Time

75 Minutes

Notes

- Occassionally the participants in this module may end up driving the conversation into being completely being about digital information. It is important to ensure that participants also consider physical information - including things such as the storage of paper files, secure diposal of sensitive waste, the importance of caution in physical conversations etc.

Activity

Break participants into groups, provide them with a flipchart and/or post-it notes and ask them to ask answer the following questions.

Where possible, each answer should be scaled from most to least sensitive etc.

- What information does their organisation store?
- Where do they store that information?
- Who has access to that information?
- Why do they have access to that information?
- What adversaries may wish to access that information?
- How might an adversary access that information?
- What mitigation measures can we take to protect that information?

The participant should then record the information into their own assessment sheet or document.

Discussion

- What information security breaches or threats have we experienced or heard about?
- How did we react to those informations security breachs?
- How do we think we would react to those information security breachs?
- What security policies do we have in place already?
- What problems have we seen with the implementation of security policies?
- How might we overcome these implementation policies?
- What soures of information do we use for keeping up-to-date on security threats?

Inputs

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very likely	Medium	Medium	High	High	High

The trainer should demonstrate a simplified version of how to access risk.

Risk is the liklihood that something will happen multiplied by the impact if that it does happen. This concept can often be confusing to be people addressing it for the first time, especially if a trainer attempts to immediately attach numbers to each part. One way to make it easier to understand initially is by drawing a horizontal and then vertical line at a 90 degree angle, like a two sided triangle. Name one line "likelihood" and the other "impact."

Participants should then each be given a post-it note, asked to think of an information security risk and then place it on the chart depending on where they think the risk should fit before any mitigation measures are taken. They should then be asked to name some mitigation measures and then move the post-it note to where they think it should be after implementing them.

The objective for this activity is to ensure a participant realises that risk by reduce by either or both reducing likelihood or reducing impact. Often people tasked with managing risk tend to concentrate on only one of these two factors.

If the participants feel comfortable with the concept the trainer can then introduce more formalised ways of measuring risk, such as a simplified "risk register." The trainer should demostrate how to fill out a register using a couple of examples. If they are using numbers (1 to 5) or levels ("Low, Medium or High") to measure likelihood etc, it is useful to ask the participants to provide their opinion and then select the average. This technique helps ensure that risk registers suffer less from individual biases.

Individuals can now start to add topics they feel are specific risks to them into the risk register but we will wait until the "Deepening" to start looking at measuring the risks through threat modelling.

Deepening

Threat Modelling Reseach

This section focuses on participants on researching information security threats that already have occurred in countries or within organisations similar to their own. From this they will have to make assessments of the mitigations that they would need to take to reduce any potential similar risks.

- On a flipchart, ask participants what resources they use for keeping up-to-date on information security issues. An example would be reports by Citizen Lab.
- Ask them to provide an opinion on the usefulness of each of the resources that they mention. Including topics such as:
    - How up-to-date they are
    - How easy they are to read, understand and draw information from
    - How applicable they are to the context of the participants
    - What languages they are in
    - Other useful information

- Ask participants what well known information threats they are aware of that have affected organisations similar to their own.

The group will be broken down into teams and asked to use the suggested (or other) resources they have collected to go out and research an information security threat that is relevant to their work. They will be asked to report back on the threat addressing such issues as:

- What was the threat?
- Who did it effect?
- Why were they targetted?
- How did it effect the individuals or organisations?
- How could the likelihood be mitigated?
- How could the impact be mitigated?
- What residual risk would the participants face if they were targetted by this method?

For example:

In July 2017 Citizen Lab reported that a group of investigators into mass disapperances in Mexico were targeted with spyware developed by the NSO Group. Participants could be asked to research this case study with available resources and then propose mitigation measures.

Source: "Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware" https://citizenlab.ca/2017/07/mexico-disappearances-nso/

Trainer Note:

- It may not be possible to find case studies that closely match the profile of the participants in the room. In that case it can often make sense to open the research to include regional threats, as often trends are likely to spread.
- If a participant was involved in one of the cases being research, it may make sense to have them not involved in the research on it, instead have another group research on it, provide their recommended solutions and then use the knowledge of the individual to add to the debrief.

Synthesis

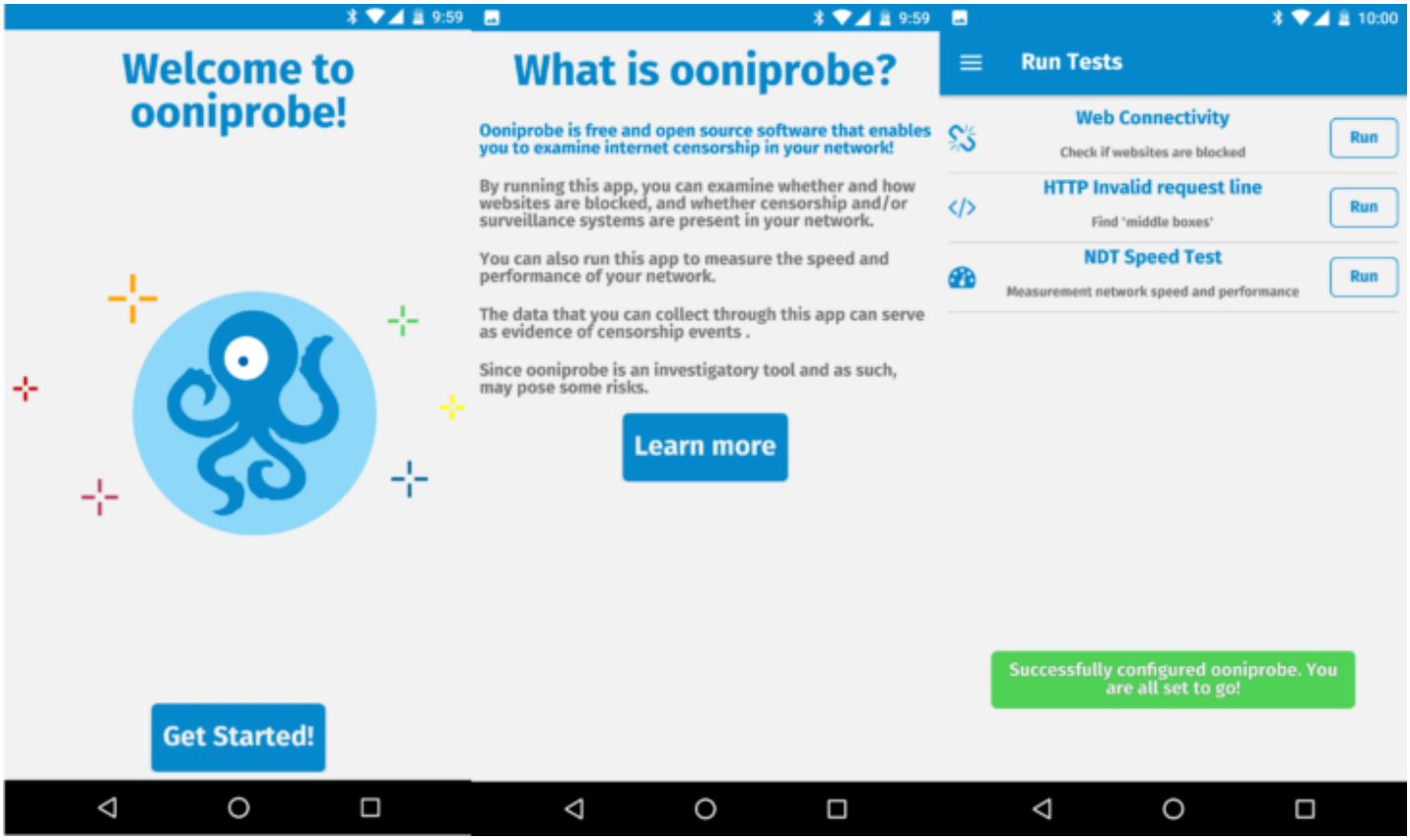
Participants should turn to their assessment documentation and consider how their organisation deals with the subject matter covered in this module. Where necessary they should ask questions and work with other participants to identify any:

- Issues they have found that effect their organisations
- Possible solutions they have learned
- Possible difficulties they may face in implementation (ideally using the time ad experience of trainers and other participants)
- Things would need to overcome these difficulties
- Connections to other organisations or individuals that would help them
- Timeline, resources and costs for implementation

This should be noted in their assessment, for future use.

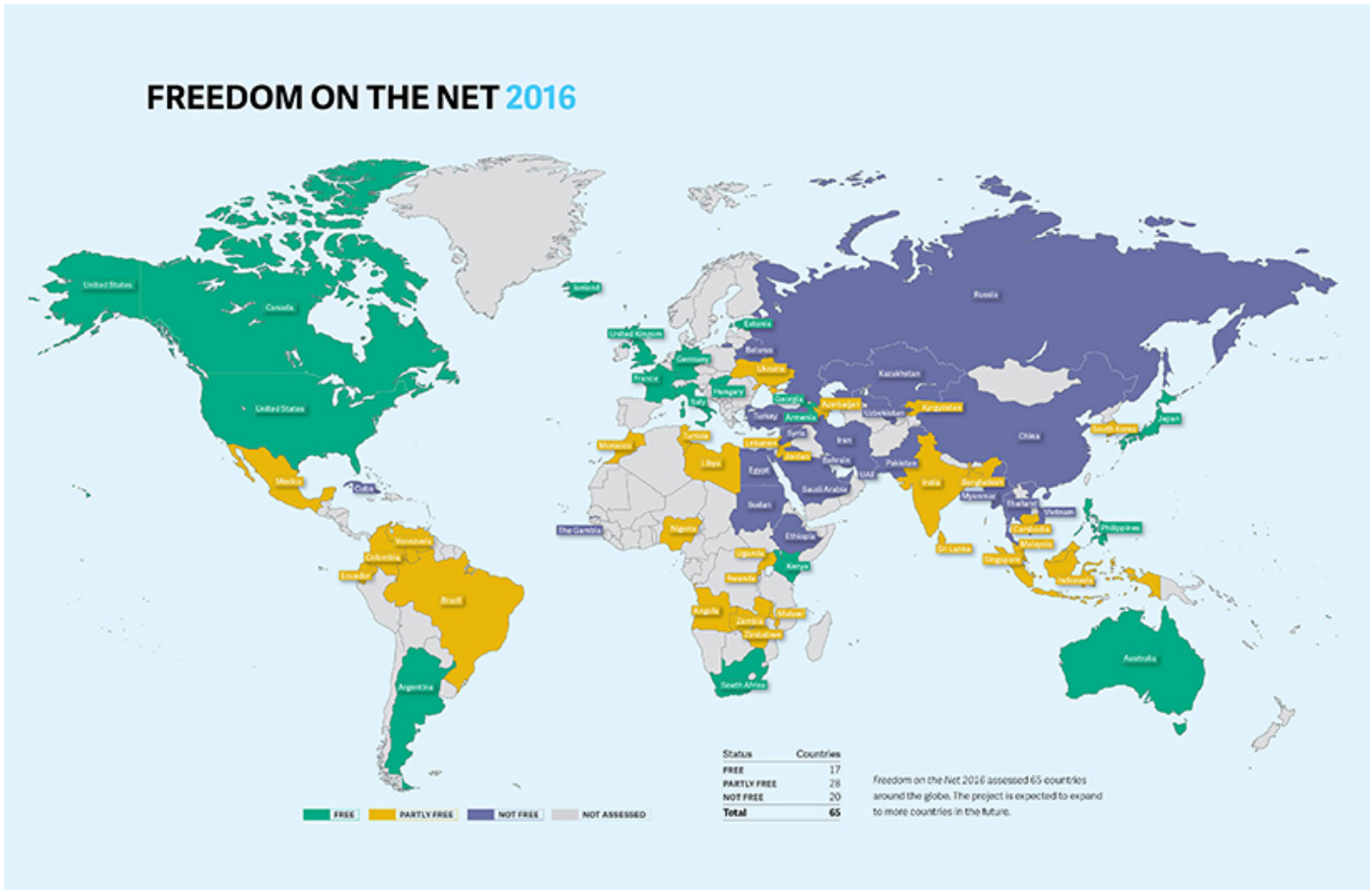
In line with keeping this curriculum as an updated community tool, we would also ask that participants provide comments, feedback and new ideas for this module on the project website and/or Github!

TODO: - add




THE CITIZEN LAB


DLA PIPER
DATA PROTECTION LAWS OF THE WORLD


FREEDOM ON THE NET 2016
FREE
PARTLY FREE
NOT FREE
NOT ASSESSED
Status Countries
FREE 17
PARTLY FREE 28
NOT FREE 20
Total 65
Freedom on the Net 2016 assessed 65 countries around the globe. The project is expected to expand to more countries in the future.

PRIVACY INTERNATIONAL

Menu

Reports

Privacy International has been producing world-class research reports for over a decade, in collaboration with academic institutions across the globe. We work on a huge range of topics and produce in-depth reports, from topics like communications surveillance, to country specific reports and submissions to the United Nations using local research and experience.

TEAM CYMRU

Our Insight | Our Initiatives | Dragon News | Who We Are

Information about country :

China

Population:	**1,330 million**
IPv4 assigned:	339 million
IPv4 advertised:	**89%**
IPv6 assigned:	7,656 nonillion[1]
IPv6 advertised:	**3%**
Overall malicious activity	15% (out of 100%)
Malicious activity increase	↑1% (compared 30 days ago)

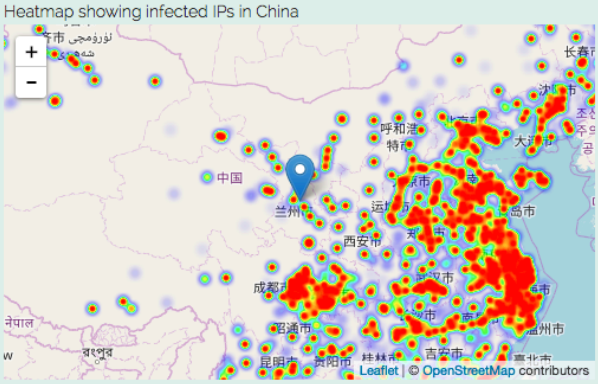
Ranking[2] in the last 24 hours

Rank	Country	Rank change since 30 days
0		→0
1	**China**	→0
2	**Brazil**	↑3

Ranking of neighboring countries in the last 24 hours

Rank	Country	Rank change since 30 days
117	**Lao**	↑7
171	**Bhutan**	↓10
124	**Tajikistan**	↑47
43	**Kazakhstan**	↑12
85	**Mongolia**	↑19
69	**Afghanistan**	↑3
98	**Nepal**	↓41
119	**Myanmar**	↓31
111	**Kyrgyz Republic**	↑37
27	**Pakistan**	↑8
227	**Korea**	↓16
4	**Russian Federation**	↓2
11	**Vietnam**	↓4
3	**India**	↑1

Heatmap showing infected IPs in China



Compare:

Please Select	Please Select
Country: China	Country:
Population: **1,330 million**	Population: **0**
IPv4 assigned: 339 million	IPv4 assigned: 0
IPv4 advertised : **89%**	IPv4 advertised : **0%**
IPv6 assigned: 7,656 nonillion	IPv6 assigned: 0
IPv6 advertised: **3%**	IPv6 advertised: **0%**
Overall malicious: **14%** of total	Overall malicious: **0%** of total
Ranking in last 24 hours: **1** →0	Ranking in last 24 hours:
Number of countries: **1**	Number of countries: **0**
China	

Resources

- Botherder’s list of reports detailing digital attacks on Civil Society
- Citizen Lab
- Open Observatory of Network Interference
- OpenNet Initiative
- "Fredom on the Net" Annual Reports by Freedom House
- SAFETAG Full Guide: "Risk Assessment and Analysis," Page 10
- SAFETAG Full Guide: "Context Research," Page 27