SAN JOSÉ STATE UNIVERSITY

THE Open GROUP

Innovative Collaboration at the Open Group Security Forum: Fruit from the Open Group Academic Program

January 31, 2017

Mike Jerbic, Lecturer, Department of Economics, SJSU
Sushmitha Kasturi, BS Economics Student, SJSU
Eva Kuiper, Tech Lead, GRC Enterprise Security Services, HP Enterprise
John Linford, Lecturer, Department of Economics, SJSU

SJSU SAN JOSÉ STATE UNIVERSITY

The Open Group Academic Program

- Objective: Get more Open Group work done in less time
- Problem: How can members be more productive on Open Group projects?
- Observation: Member projects don't always need all the expertise members bring
- Solution: Specialization
  - Members guide and direct the project
  - University students "do the work" under faculty and industry member mentorship

First (Interrelated) Projects

- Open FAIR Process Guide
  - John Linford, principal author
  - Eva Kuiper, member guide, director, and contributor
- Norwegian Regional Health Authority Risk Analysis
  - Sushmitha Kasturi, student researcher on the opportunity costs of present privacy and security policy
  - Biljana Stangeland, PhD, Managing Solution Architect at Capgemini in Norway has played a principal role as member guide, director, and advisor
  - Stig Hagestande, Enterprise Architect at Sykehuspartner HF, Shared Services Provider for the South East Regional Health Authority in Norway and member of the Health Care Forum provided the risk analysis problem statement

The Kingdom of Norway

Some facts and figures[1]:

- Constitutional monarchy and parliamentary democracy
- Population: 5,165,802 (January 2015)
- Capital: Oslo (population 647,676, January 2015)
- Area: 385,170 km^2
- Currency: Norwegian Krone, NOK, about $0.12/NOK
- GDP in 2014: NOK 3,151,483 million ($378,200M)

From data.worldbank.org[2]

- Norway GDP per capita: $74,734
- US GDP per capita: $55,837

[1]http://www.eu-norway.org/eu/Facts-about-Norway/#.WES46XdJk-U accessed 12.4.2016
[2]http://data.worldbank.org/indicator/NY.GDP.PCAP.CD accessed 12.4.2016

End Stage Renal Disease (ESRD) in Norway

- About 11 percent of the Norwegian population suffers from chronic kidney disease.
  - 1240 people on dialysis in 2012, and of those about 16.4 percent received dialysis at home.
- Patient prevalence grows at about 5 percent per year.
- Once diagnosed, total costs associated with a new patient are estimated between 1.23M to 2.63M NOK ($148,000 to $316,000).
- Home treatments are the lowest cost methods to treat ESRD. Home treatment saves between $30,000-$50,000 per year per patient.
- The Regional Health Authority would like to expand home dialysis.

Home Dialysis (HD): A Problem Statement

- Patients today on HD transport data to / from the physician's site to communicate treatment information and to update their treatment plan.
- Why are these patients doing this? Why not connect the home dialysis machine online to the hospital/physician's office?
- Information security and privacy policy, of course!

Example Dialogue – As Presented to Us

A typical dialogue between that architect and the service provider's compliance and security team might look like this:

Architect: Why can't we read and update treatment data and plans online? This would give us the following benefits:

- Patient quality of life improves
- Patient security with home treatment rises
- More precise treatment can be administered
- Doctor and other medical service provider productivity rises
- The population of patients willing to accept home dialysis treatment rises

Example Dialogue – As Presented to Us

The ensuing conversation with information security (Sec) and the architect (Arc) goes something like this:

Sec: No, the network transport is not secure.
Arc: And a memory stick is? Besides we already have a VPN solution in place. We can use that.
Sec: No, the VPN solution cannot be used to connect to patient sensitive solutions.
Arc: Okay, then le's put crypto equipment in both ends and secure it that way.
Sec: No, we don't have a policy for that, besides we don't have control over the end computer at the patient's home.
Arc: Then let's give the patient a secure computer we can control.
Sec: No, we don't have a policy for that.
Arc: (unintelligible…)

In Other Words…

- Fear of the risks associated with privacy and security prevents even the discussion of whether HD machines will be allowed to connect to hospital data systems.
- Perceived costs keeping this policy are high. Allowing online connections improves medical services productivity, reduces costs associated with travel.
- When pressed, these risks dominated the fear
  - The risk to the hospitals associated with malware
  - The risk to the hospital associated with ransomware
  - The risk to patient privacy associated with transferring treatment information between the home and hospital.

How Would an Economist Look at This?

- Estimate the forgone opportunity of the cost savings not achieved through the status quo policy.
- Estimate the benefits of the risk avoided through the status quo policy.
- Determine whether the social costs exceed the social benefit.

- And maybe, critically think whether the architect and security/ compliance team are asking the right questions. Challenge assumptions, develop rationales, etc.

Foregone Benefits – Cost of Status Quo

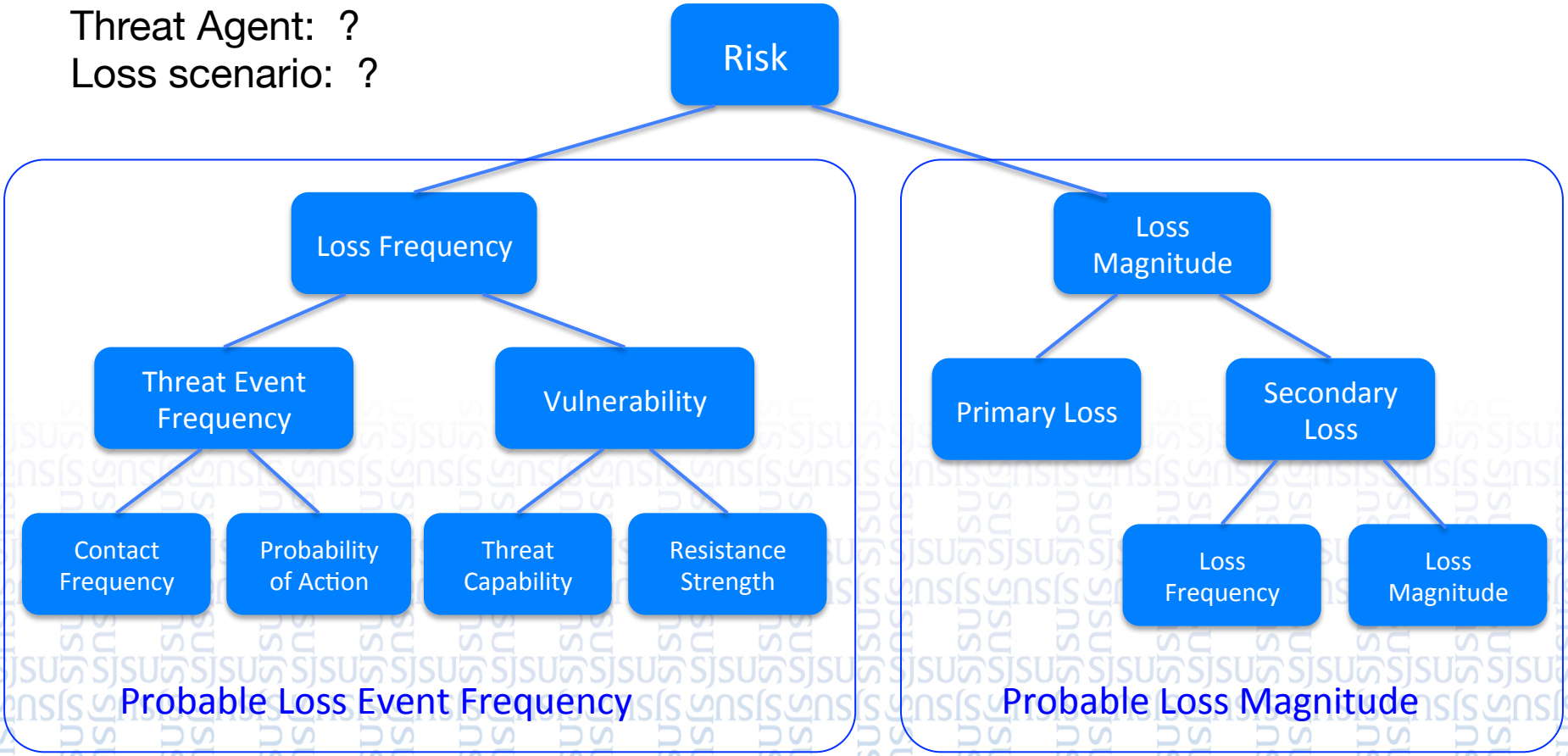
- What is Norway giving up by adhering to this policy?
  - Patients' travel and wait time, 2-3 times per week
  - Patients' time valued at national average hourly wage NOK 245 by 4-8 hours. If transporting data 3x / week or 156 times per year, about 229,000NOK. (p. 79, Table 33 and author's estimates/calculations).
  - Travel costs estimated at 156,000-227,000NOK (Table 33)
  - Total travel avoided about 430,000NOK per year per patient, or about $50,000 USD per patient per year.
  - At about 203 patients on home dialysis, that's about $10M per year in leisure and travel costs avoided
- And will rise with increasing home dialysis adoption

Risk Avoided: Benefits of the Status Quo

- Two perspectives
  - Patient as stakeholder in privacy
  - Hospital as stakeholder in information security
- Two separate FAIR discussions required!

Patient Privacy Analysis

Stakeholder: Patient
Asset: Control over dialysis data
Threat Agent: ?
Loss scenario: ?

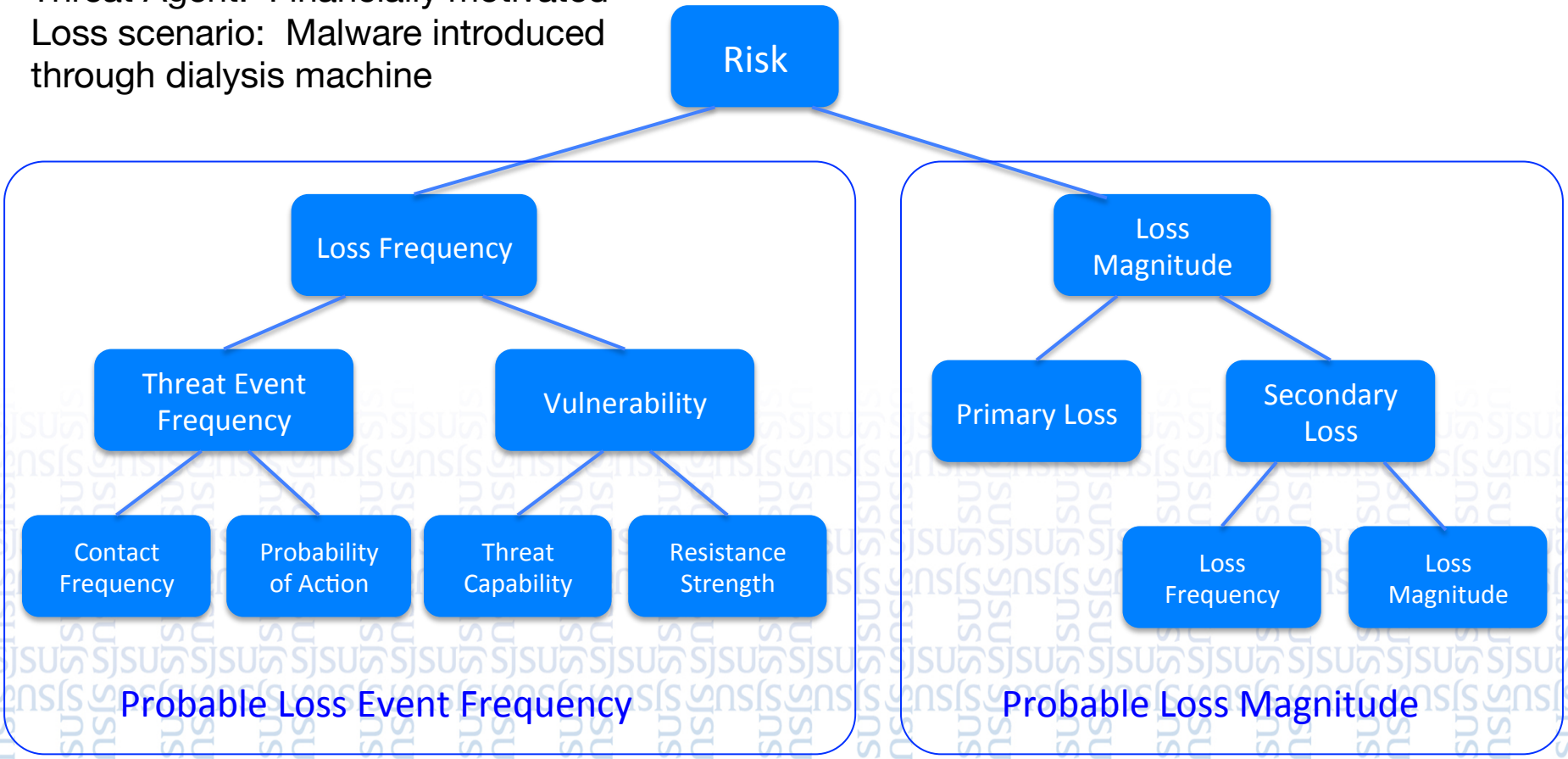


Patient Privacy Analysis

- Unlike the US, Norway has a “single payer” system. The incentive for threat agents to invade patient privacy in Norway is very different than in the US.
- What would a threat agent gain? How would he benefit?
  - From getting access to the information?
  - From changing the information?
- For a motivated threat agent, are there easier ways to accomplish the objective?

Risk Associated with Malware/Ransomware

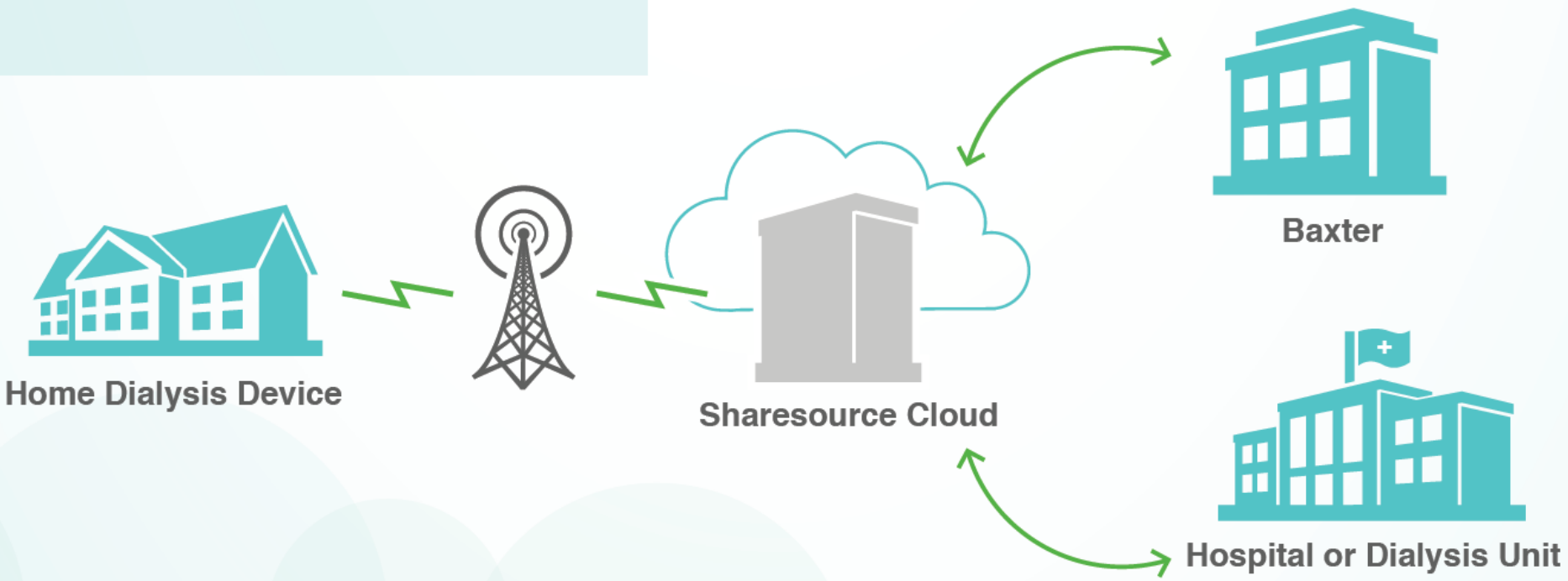
Stakeholder: Hospital
Asset: CIA of Information assets
Threat Agent: Financially motivated
Loss scenario: Malware introduced through dialysis machine



Risk of Malware/Ransomware

- No data in Norway – hospitals isolated from internet
- Fully depends upon information system architecture connecting the home dialysis machine to the hospital
- Can be arbitrarily reduced to any desired level
  - But at what cost?
- Refine the question to an engineering challenge
  - Build an interconnection system whose risk of loss is less than the benefits received – or something like that.

Likely Feasible: Technologists Working on Solutions



1. Baxter International Inc.; Sharesource Connectivity Platform; Accessed on April 1, 2014 from http://viviahomehd.com/sharesource.html
2. Data on file, Baxter International Inc., Jan. 16, 2014
3. Data on file, Baxter International Inc., Aug. 20, 2013

Baxter

Critically Thinking About the Problem

- Recall the the number of trips patients go to the hospital each year
  - Patients actually visit about 15 times per year, not 156, and they would visit in-person anyway
  - The privacy and security controls have minimal opportunity costs as originally stated.
  - However, other research suggests benefits of home dialysis that have not been included here. Improved QALY.
- Patient home dialysis adoption may rise with better monitoring and telemedicine.
  - A more meaningful margin is around the relationship between telemedicine and home dialysis adoption.

Areas for Further Research

- Better questions might be
  - How can we safely and securely implement a broader telemedicine solution?
  - What is the social value of broader adoption of home dialysis, the entire savings per patient: Longer lives, improved quality of life, and lower costs?
  - How do patients value privacy, and who should decide questions of privacy?
  - How do risks associated with broader telemedicine solutions change over the specific risks discussed here?

SJSU SAN JOSÉ STATE UNIVERSITY

To Discuss More About the Academic Program, Our Panelists

- John Linford, former SJSU graduate student and lecturer
- Sushmitha Kasturi, SJSU BS Economics, December 2016
- Eva Kuiper, GRC Consultant Enterprise Security Services, HP Enterprise
- Steve Nunn, CEO, The Open Group
- Dr. Lydia Ortega, SJSU Economics Professor

SAN JOSÉ STATE UNIVERSITY *powering* SILICON VALLEY

Mike Jerbic
stephen.jerbic@sjsu.edu