Institute and Faculty of Actuaries

# A Network Theory-Based Approach To Pricing Cyber Risk

Karthik Tumuluru
Milliman
Dubai, UAE
karthik.tumuluru@milliman.com

*Any views expressed in this document are those of the author and do not represent Milliman Inc.*

09 November 2021

# Agenda

**Introduction**

**Constructing a Model**

- Network Theory – The ABC's
- Organization Network Infrastructure
- Determining Spread of Attacks
- Impact of Corporate Social Networks
- Risk Scenarios

**Using the Model for Pricing**

- Data Vulnerability and Value
- Business Interruption
- Insuring Specific Nodes and Sub-Networks
- Other Uses

**Takeaways and Conclusions**

**Q&A**

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

# Introduction

09 November 2021

# Cyber Risk – What, How and Why?

## What?

Damaging a company's operations and/or reputation through its data and/or its IT infrastructure

Broad categories:
- Data breaches
- Business interruption
- System hijacking

## How?

- Social Engineering (like Phishing)
- Ransomware
- Password Theft
- Malware (like Trojan viruses)
- Eavesdropping
- DDOS
- SQL Injections
- Man-In-The-Middle
- Accidental Node Failure

## Why?

**Money** – Kaseya 2021 (Amateurs, Criminals, Many)

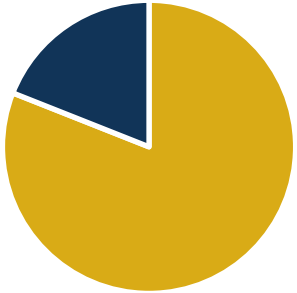
**Espionage** – Sony 2014 (Competitors, Governments)

**Political/Personal** (Hacktivists, ex-employees)

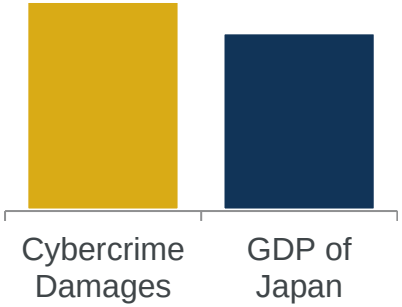
**Accidental** – AWS 2017 (carelessness, mistakes)

Institute and Faculty of Actuaries

# Cyber Risk and the Insurance Market Today



2021 Munich Re Global Cyber Risk survey: only 19% C-level respondents feel adequately protected




Estimated 2021 cybercrime damages: $6 trillion

- Network security makes a growing portion of cyber losses, rising from <5% of incidents in 2017 to ~20% in 2021
  - Attacks originating through phishing account for 4 out of 5 security incidents, with 94% of malware delivered by email
  - Data privacy still makes up over 50% of incidents
- Market concentration increases vulnerability and repeat attacks (Geer et al, 2020)
- Global cyber insurance market size as of 2020 estimated at $7.8B, with expected 21% CAGR through 2025

Institute and Faculty of Actuaries

# Current Cyber Insurance Pricing

- Risk factor-based underwriting with focus on industry revenue, employee and record count (Gallagher, 2021)
- Pricing strategies include: (FTC (USA), 2019)
  - Flat rate based on frequency-severity for different types of coverage
  - Base rate depending on company revenues
  - Qualitative/survey-based
- Qualitative cyber risk evaluation usually affected by misrepresentations (UNIVPM, 2019)
- Limited data availability among key challenges (AAA, 2019)
- Not understanding cyber exposure → customers see less value in cyber insurance (Geneva Association, 2018)
- The more quantifiable the exposure and loss, the better

Institute and Faculty of Actuaries

# Scope of Presentation

- Spread of risk based on IT network structure
- Broad risks – data access, business interruption
- Binary approach – risk either propagates or does not
  - Not considering partial impacts
  - Not considering specific attack types due to variety and complexity
- Not tackling reputational/legal risk
  - Definitions and ramifications may vary greatly by industry and company

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

# Constructing a Model

09 November 2021

# Review of Existing Research

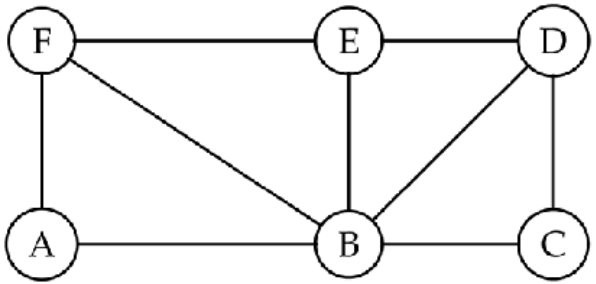
- Network theory has previously been applied in analyses of cyber-physical system vulnerability
  - Zhu, Milanović and Mihić (2019) identified node degree, node importance, betweenness and closeness centrality as key importance measures in vulnerability analysis
  - Zhu and Milanović (2017) used weighted adjacency matrices to analyse system interdependency and vulnerability
  - Guo, Yu et al (2019) constructed a stochastic cyber-physical power system model to investigate cascading failure
  - Fan et al (2020) defined 3 categories of damages: destruction of availability, integrity, and confidentiality of data
- Böhme and Schwartz (2010) presented an early framework on cyber-insurance
  - Five key components: supply side, demand side, info structure, organizational and network environments
  - Defines risk arrival and propagation
- Gil, Kott and Barabási (2014) applied a framework of genetic mutation impact on diseases, to ascertain associations between network services and cyber threats
- Shetty et al (2009) observed that the presence of competitive cyber-insurers may weaken incentives for users to improve their security

Institute and Faculty of Actuaries

# Network Theory – The ABC's

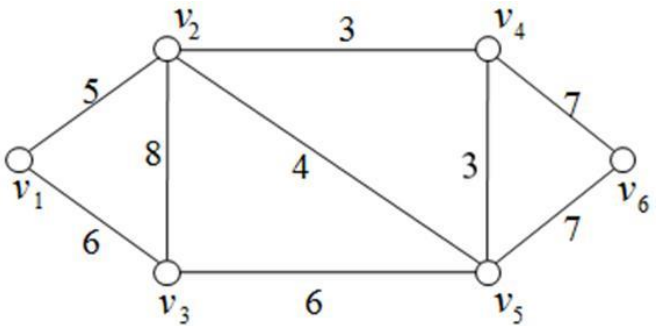
- Study of how objects in a system are related

Unweighted graph




Source

Weighted graph

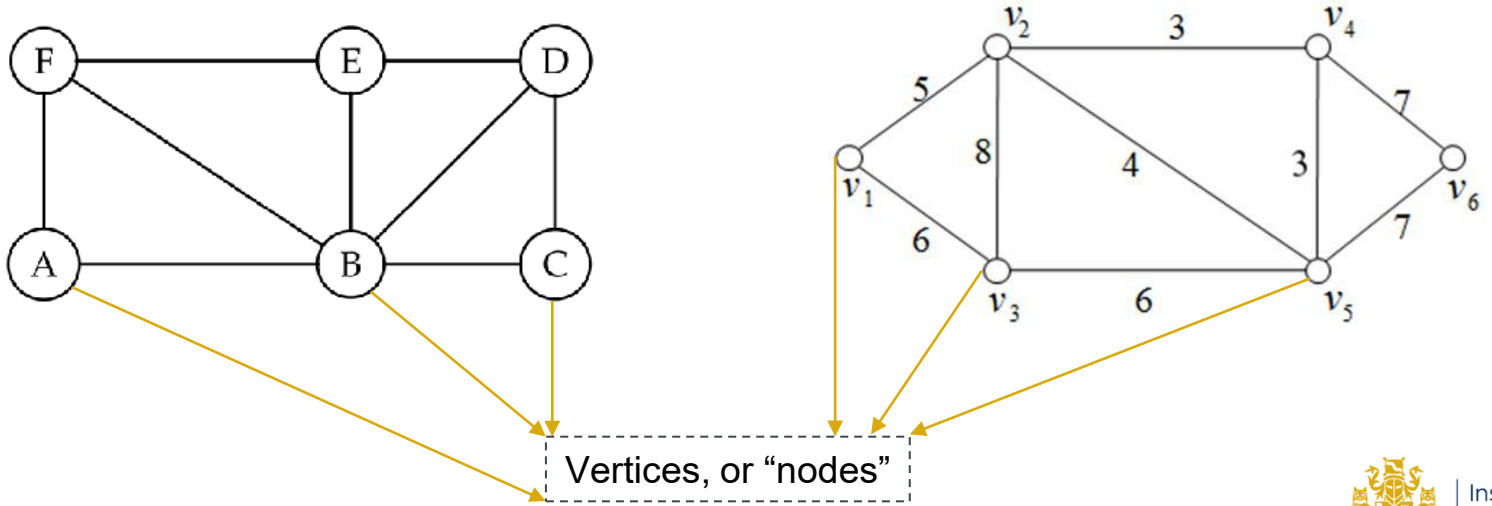



Institute and Faculty of Actuaries

# Network Theory – The ABC's

Unweighted graph

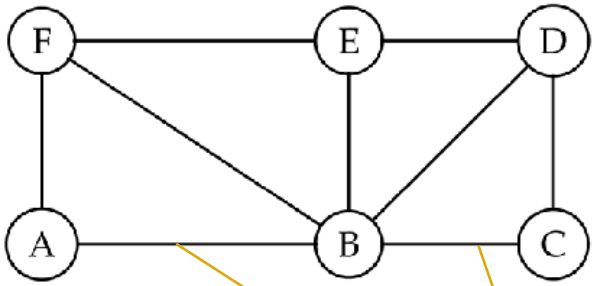
Weighted graph



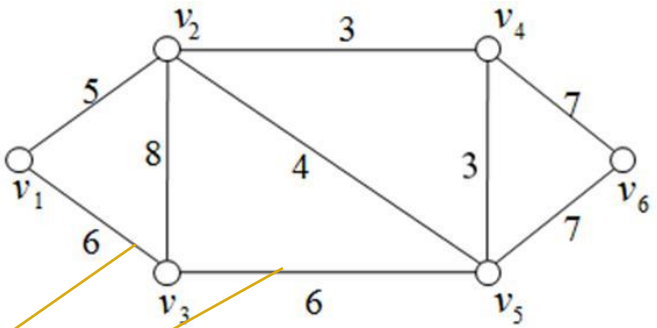

Institute and Faculty of Actuaries

# Network Theory – The ABC's

Unweighted graph




Weighted graph

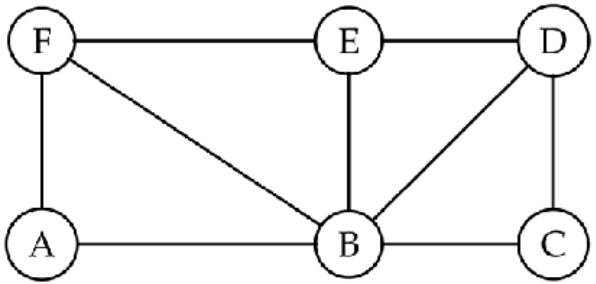



Edges

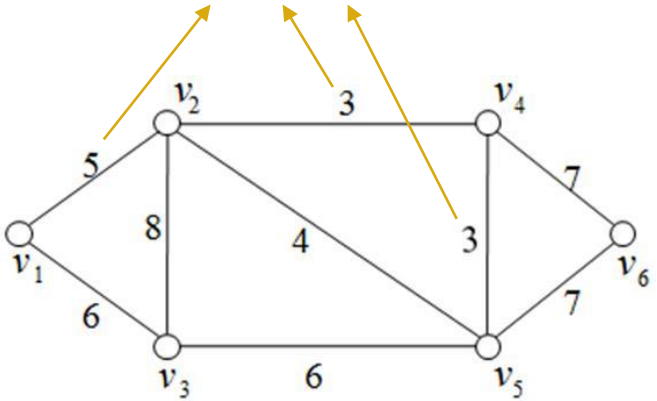
Institute and Faculty of Actuaries

# Network Theory – The ABC's

Unweighted graph




**Weighted** graph

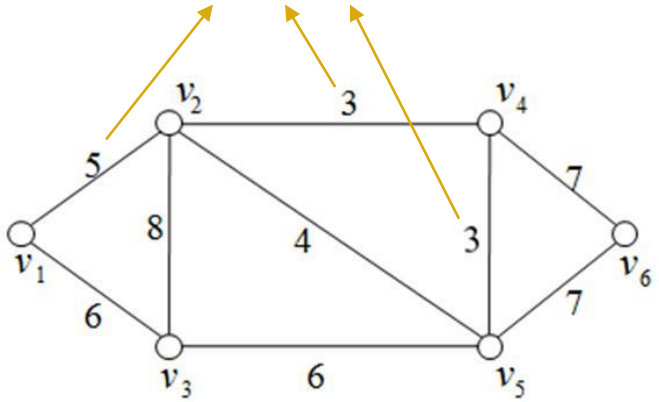



e.g. traveling salesman problem

Institute and Faculty of Actuaries

# Network Theory – The ABC's

**Weighted** graph




Adjacency matrix

| $v_1$ | $v_2$ | $v_3$ | $v_4$ | $v_5$ | $v_6$ |
|---|---|---|---|---|---|
| 0 | 5 | 6 | 0 | 0 | 0 |
| 5 | 0 | 8 | 3 | 4 | 0 |
| 6 | 8 | 0 | 0 | 6 | 0 |
| 0 | 3 | 0 | 0 | 3 | 7 |
| 0 | 4 | 6 | 3 | 0 | 7 |
| 0 | 0 | 0 | 7 | 7 | 0 |

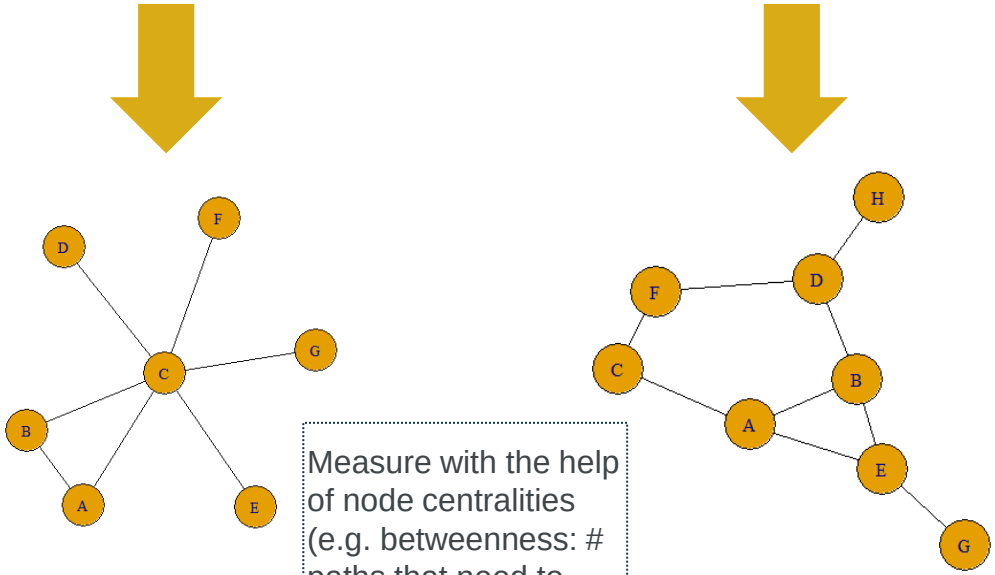
*e.g. $v_1$ is connected to $v_2$ with an edge weight of 5, so in the adjacency matrix, we populate elements [2nd row,1st column] and [1st row,2nd column] with 5*

Institute and Faculty of Actuaries

# Network Theory – The ABC's

- Concentration of a network

This network is **more concentrated** than this network

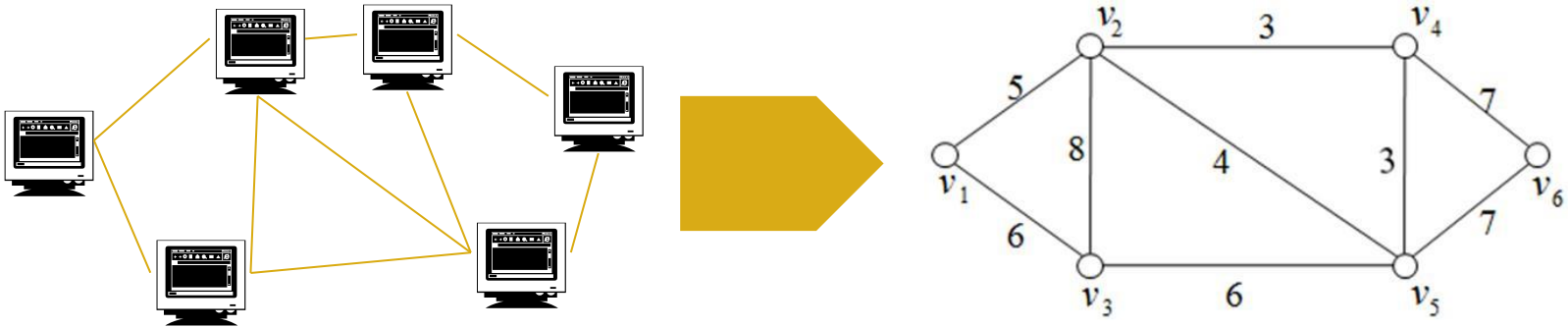



Measure with the help of node centralities (e.g. betweenness: # paths that need to pass through a node)

Institute and Faculty of Actuaries

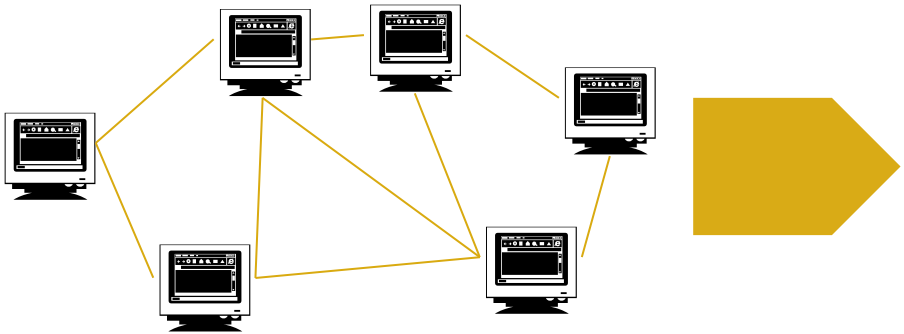
# Organization Network Infrastructure

- A set of interconnected workstations
  - Represented through weighted graph
  - Security protocol and strength



# Organization Network Infrastructure

- Basis to understand movement of risk
  - Transition steps
  - Effect of network centrality on severity

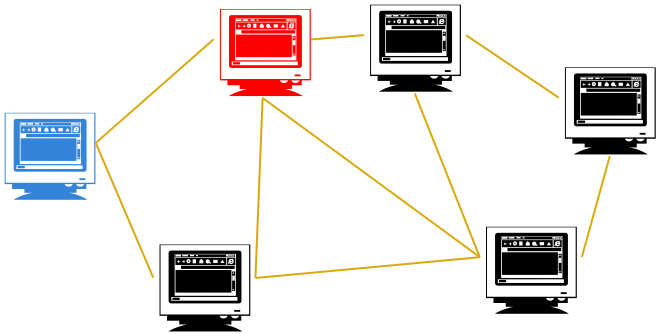


$$\begin{pmatrix} 1 & p_{12} & p_{13} & p_{14} & p_{15} & p_{16} \\ p_{21} & 1 & p_{23} & p_{24} & p_{25} & p_{26} \\ p_{31} & p_{32} & 1 & p_{34} & p_{35} & p_{36} \\ p_{41} & p_{42} & p_{43} & 1 & p_{45} & p_{46} \\ p_{51} & p_{52} & p_{53} & p_{54} & 1 & p_{56} \\ p_{61} & p_{62} & p_{63} & p_{64} & p_{65} & 1 \end{pmatrix}$$

Institute and Faculty of Actuaries

# Probability Calculation

- Measuring the probability that the attack transfers from node 1 (blue) to node 2 (red) would need to consider the nodes' connectivity
  - Mean-field approximation on very large networks in epidemic models (e.g. ε-SIS, Pastor-Satorras and Vespignani, n-Intertwined)



$p_{12}$, or P(1 infects 2 | 1 is infected)

= P(1 infects 2) / P(1 infects adjacent node)

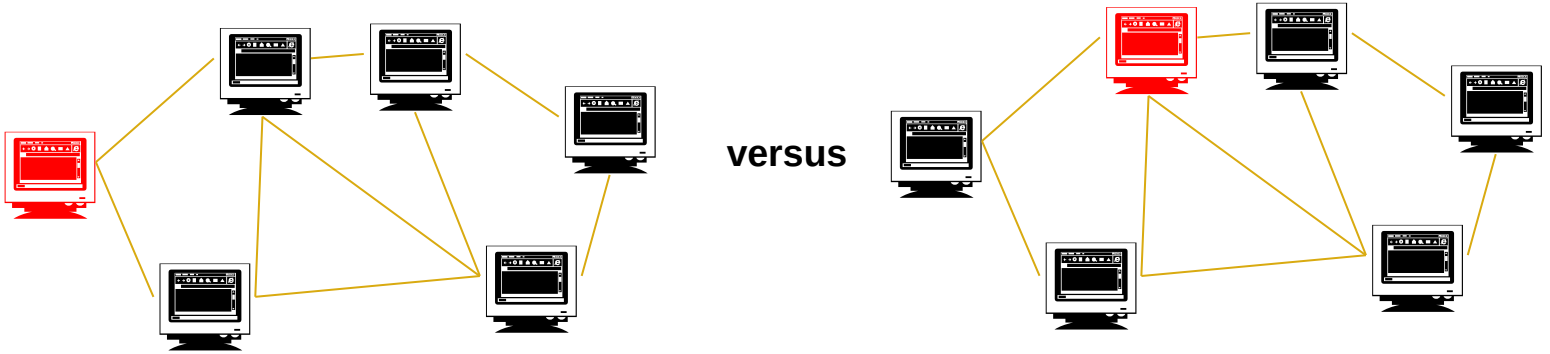
= $F(Closeness_{1,2}, Importance_2)$ / $F(Degree_1, Importance_1)$

- Akin to SIS model
  - Still possible to get infected again

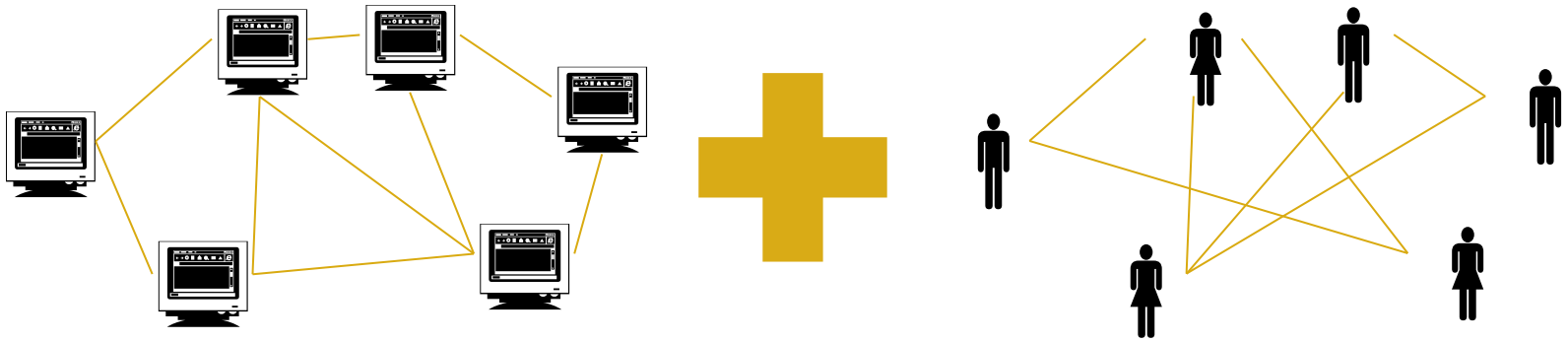
Institute and Faculty of Actuaries

# Determining Spread of Attacks

- Patient zero
  - Internal vs external (how would behaviour change?)
- Path of least resistance?



# Impact of Corporate Social Networks



# Impact of Corporate Social Networks

- Social network analysis
  - Organisational structure
  - Social engineering
  - Privacy concerns
- Internal attacks
  - Modelling behavioural element
- Using a “fire drill” to gauge susceptibility
  - Needs familiarity and expertise, but pros outweigh cons

Institute and Faculty of Actuaries

# Risk Scenarios

- Define objective
  - Motivation in internal attack scenarios
- Select various origins of breach for each scenario
- Consider different network cyberattack strategies
  - Attack sophistication (online presence of company?)
  - How would people respond to the attack?
  - How would the firm as a whole respond? How fast can it respond?
  - Complexity of existing security protocols
- Monitor risk levels using defined metrics
  - Zhu (2019) defines 2 methods to measure cyberattack success on firewall:
    - Rejected Attempts/Total Traffic
    - Malicious Packets/Total Packets bypassing firewall for a given rule

Institute and Faculty of Actuaries

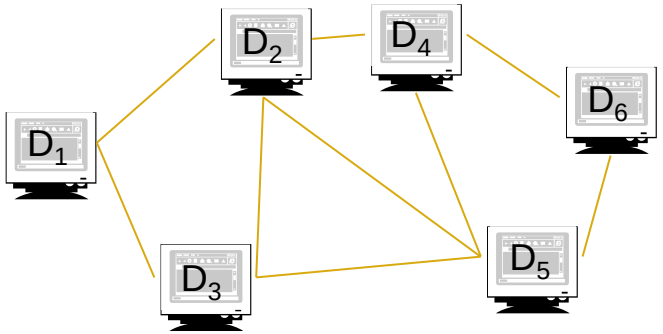
# Using the Model for Pricing

09 November 2021

# Data Vulnerability and Value

- Metric: Total data-at-risk (based on probability of risk transfer, $p_{ij}$)
- For a single-step transition, if each workstation *i* has volume of data $D_i$, then

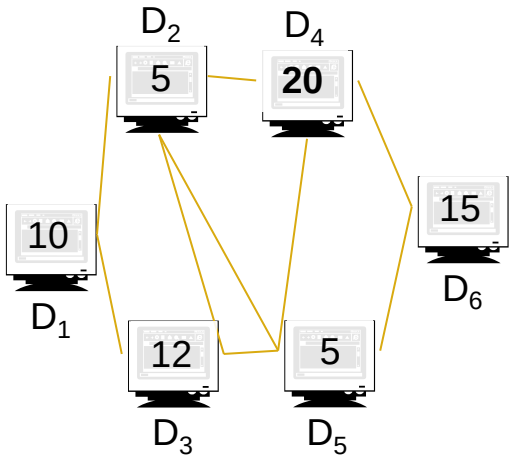
$$\begin{pmatrix} D_1 \\ D_2 \\ D_3 \\ D_4 \\ D_5 \\ D_6 \end{pmatrix}^{T} \begin{pmatrix} 1 & p_{12} & p_{13} & p_{14} & p_{15} & p_{16} \\ p_{21} & 1 & p_{23} & p_{24} & p_{25} & p_{26} \\ p_{31} & p_{32} & 1 & p_{34} & p_{35} & p_{36} \\ p_{41} & p_{42} & p_{43} & 1 & p_{45} & p_{46} \\ p_{51} & p_{52} & p_{53} & p_{54} & 1 & p_{56} \\ p_{61} & p_{62} & p_{63} & p_{64} & p_{65} & 1 \end{pmatrix} = \begin{pmatrix} DaR_1 \\ DaR_2 \\ DaR_3 \\ DaR_4 \\ DaR_5 \\ DaR_6 \end{pmatrix}$$



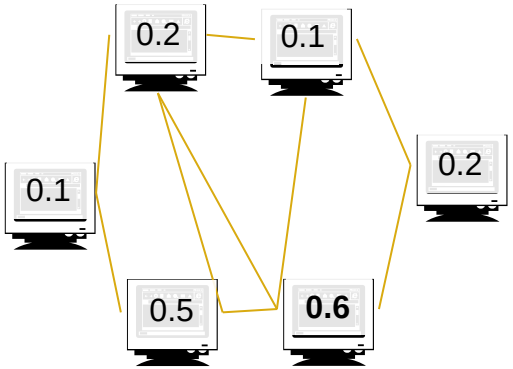

- How does total risk evolve over policy duration?
  - Contingent on centrality of network
- Price based on threshold? Data point?

Institute and Faculty of Actuaries

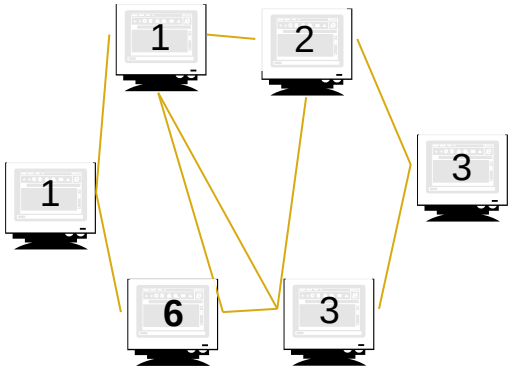
# **Data Vulnerability** – Example




Data present



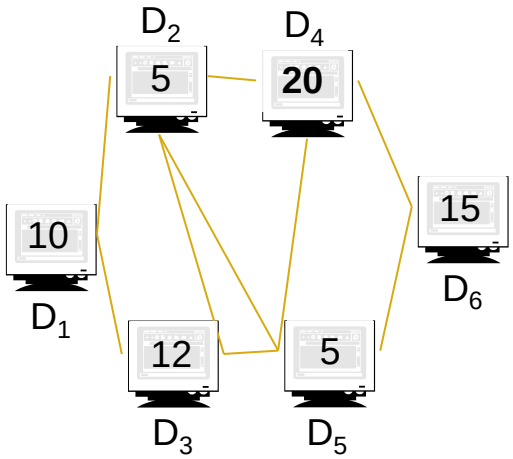

Probability of access



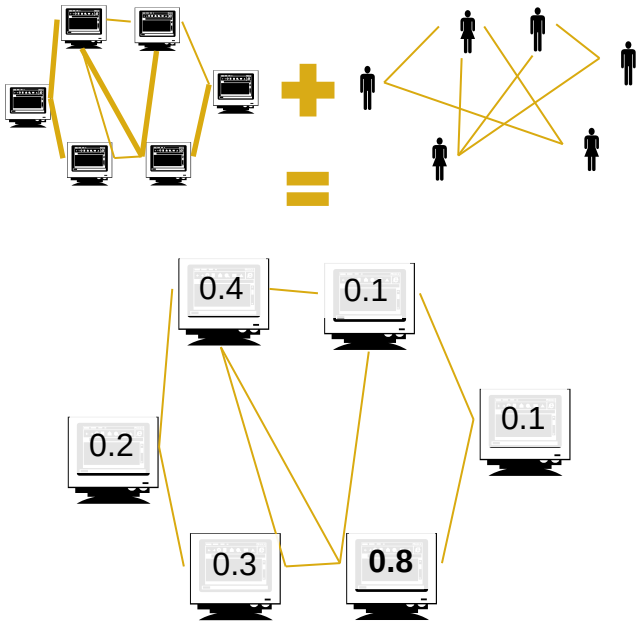

Data at risk

Institute and Faculty of Actuaries

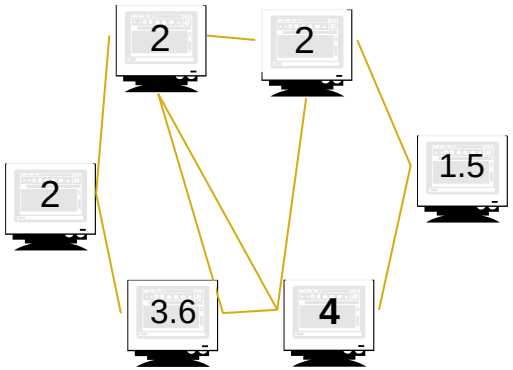
# **Data Vulnerability** – Example 2




Data present




Probability of access



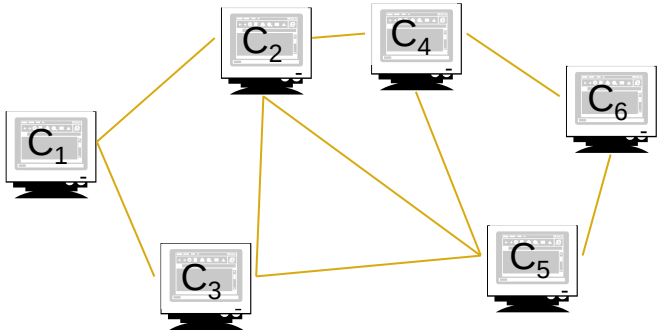

Data at risk

Institute and Faculty of Actuaries

# Business Interruption

- Metric: Expected downtime (**c**apacity below threshold & **r**ecoverability)
- Capacity of workstation or center (how fast can each workstation recover?)

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5 \\ C_6 \end{pmatrix}^T \begin{pmatrix} r_1 & p_{12} & p_{13} & p_{14} & p_{15} & p_{16} \\ p_{21} & r_2 & p_{23} & p_{24} & p_{25} & p_{26} \\ p_{31} & p_{32} & r_3 & p_{34} & p_{35} & p_{36} \\ p_{41} & p_{42} & p_{43} & r_4 & p_{45} & p_{46} \\ p_{51} & p_{52} & p_{53} & p_{54} & r_5 & p_{56} \\ p_{61} & p_{62} & p_{63} & p_{64} & p_{65} & r_6 \end{pmatrix} = \begin{pmatrix} C'_1 \\ C'_2 \\ C'_3 \\ C'_4 \\ C'_5 \\ C'_6 \end{pmatrix}$$

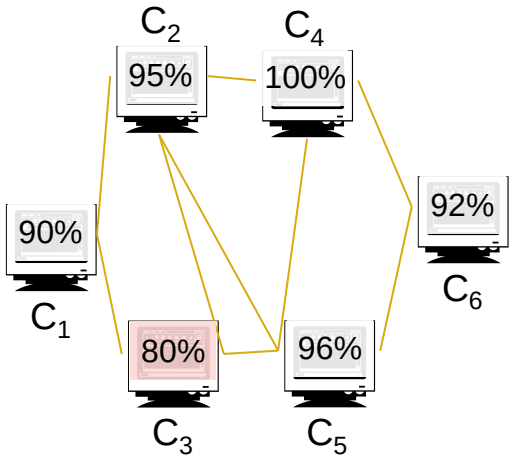



- Set thresholds to determine proper functioning, e.g. C > 90%
- Number of workstations overloaded → use to determine downtime
  - E.g. DDOS

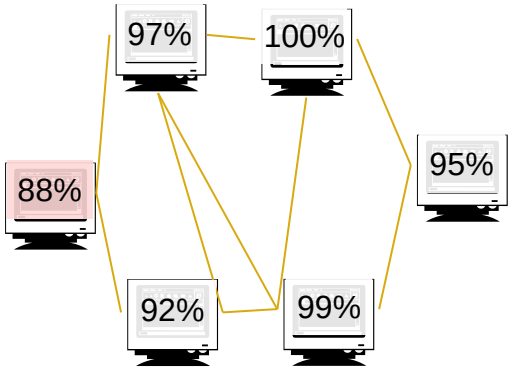
Institute and Faculty of Actuaries

# Business Interruption - Example

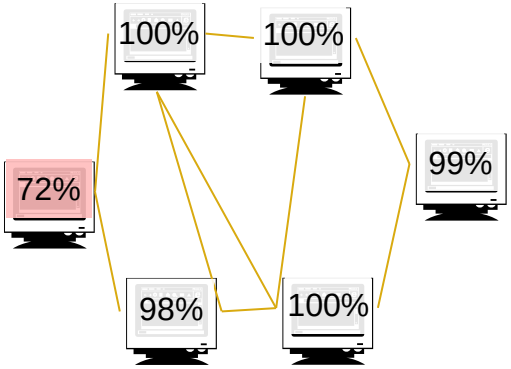
- Threshold of 90%




Network at t = 5




Network at t = 6



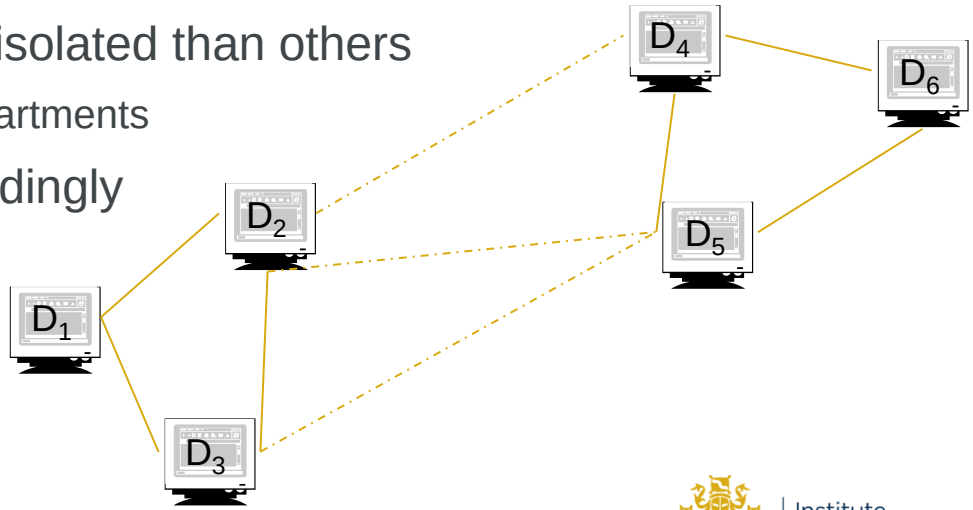

Network at t = 7

- Between t = 5 and t = 7, station 3 has an expected downtime of 1 while station 1 has an expected downtime of 2

Institute and Faculty of Actuaries

# Insuring Specific Nodes and Sub-Networks

- Certain nodes may be more important, so more targeted
  - E.g. data centres, workstations of members with public exposure
- Some sub-networks may be more isolated than others
  - Geographic dispersion, specific departments
- Need to adjust edge weights accordingly
- Determine risk entry points
  - Origin from obscure network node




Institute and Faculty of Actuaries

# Other Uses

- Cyber risk capital allocation based on attack scenario results
  - Determine VaR/CTE based on worst impacts
- Identification of own weak points
  - Turning descriptive into prescriptive analysis
  - Costs vs benefits of different network architecture (ASTIN, 2018)
  - Addressing silent cyber as a result
  - Antifragility e.g. Chaos Monkey

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

# Takeaways and Conclusions

09 November 2021

# Takeaways and Conclusions

- Network theory presents a way to look at cyber risk on a highly granular level
- Subcategories of risks modelled through same framework
  - Data
  - Interruption
- Propagation of risk across a system can be modeled with dynamic scenarios

Institute and Faculty of Actuaries

# Considerations

- Evolution of risk with work-from-home environments
- A → B may not be same as B → A
  - Directed graphs?
  - Workstations with and without certain permissions?
- Moral hazard
- Continuous time modelling
- Blockchain
- Benchmarks for smaller companies (SMEs)
  - Insurability based on size
  - Third-party/IT service usage

Institute and Faculty of Actuaries

# Further Information for Interest

- Literature
  - Network attack detection (MIT, 2019)
  - Cybersecurity incident prediction through mandatory disclosure regulation (Berkeley, 2020)
  - Understanding human decisions in cybersecurity (Carnegie Mellon, 2014)
- Data
  - USB-IDS – Public intrusion detection dataset for more complex analysis of cybersecurity attacks
  - VizSec – Comprehensive list of open-source datasets pertaining to cybersecurity
  - TowerStreet – Data containing 37,500 unique breach incidents
  - Privacy Rights Clearinghouse – Chronology of recent data breaches with details

Institute and Faculty of Actuaries

# Questions

# Comments



Institute and Faculty of Actuaries