THE UNIVERSITY OF BRITISH COLUMBIA

# Analysis of Interdependencies between CITI and other Critical Infrastructures using RISKS Forum data

**Hafiz Abdur Rahman and Konstantin Beznosov**

{rahmanha, beznosov}@ece.ubc.ca

Laboratory for Education and Research in Secure Systems Engineering

lersse.ece.ubc.ca

# Outline

- Objectives
- Information Requirement for CITI Failure Analysis
- Use of Public Domain Failure Reports
- Existing Classification Methods
- Our Method of Classification and Analysis
- Results of our Analysis
- Conclusions

# Objectives

- To get understanding of the CITI failure pattern and how it affects other Infrastructures
- To classify failure related data in a systematic way
- To test usefulness of the proposed classification for modeling and simulation

# Information Sources for CITI Fault Analysis

- Data from Infrastructure Service Providers
  - Could give detail information of systems' states and control parameters, input/output specification, operating assumptions, environmental constraints, etc.
  - Government and corporations reluctant to share
- Reports from newspapers and private individuals
  - Public access
  - Patterns can be detected by studying large number of cases.
  - No progressive picture(s) of fault sequences
  - RISKS forum
    - ACM's forum on Risks to the public in computers and related systems
    - Online version of RISKS is: http://catless.ncl.ac.uk/Risks

# Related Work

- Neumann: RISKS forum (from 1985), “Computer Related Risks” (1994)
  - Publicly known accidents due to computers
  - No analysis or taxonomy
- Howard (1997): taxonomy and frequency analysis on vulnerability reports of Computer Emergency Readiness Team Coordination Center (CERT/CC) data
- Chakrabarti and Manimaran (2002): another taxonomy to classify Internet infrastructure security attacks/faults
  - Network level only
- Rinaldi et al. (2001): taxonomy for Infrastructure interdependencies based on six functional dimensions.
- Limitations:
  - (Howard 1997) and (Chakrabarti and Manimaran, 2002) developed taxonomies for attacks (intentional). No accidental (unintentional) failures.
  - (Rinaldi et al 2001) have no specific focus for CITI and other infrastructure interdependencies.

# Our Method of Failure Classification and Analysis

- Failure reports are classified into three groups based on Infrastructure Interdependencies:
  - **Class A:** Physical Layer
  - **Class B:** Network Layer
  - **Class C:** IT Service Layer
- Following attributes are captured from each failure report
  - Date
  - Locality: Organization/City/Region/Country/Continent/World
  - Fault Type: Intentional/Unintentional/Unknown
  - Degree of Impact: High/Medium/Low
  - Duration: “x” hours
  - Public Safety: Yes /No/Unknown
  - Financial Impact: Million USD
  - Simulation: Yes/No/Unsure
  - Origin of Fault: e.g., “Electrical device failure”
  - Source Infrastructure: e.g., “IT Infrastructure”
  - Affected Infrastructures: e.g., “Telecommunication Infrastructure”
  - Affected Industry Sectors: e.g., “Financial”
  - Description

# Important Report Attributes

- Degree of Impact: High/Medium/Low
- Public Safety: Yes /No/Unknown
- Locality: Organization/City/Region/Country/
  Continent/World
- Source and Affected Infrastructures:
  - IT Infrastructure
  - Telecommunication Infrastructure
  - Water Supply
  - Electrical Power System
  - Oil and Gas
  - Road Transportation
  - Railway Transportation
  - Air Transportation
  - Banking and Financial Services
  - Public Safety Services
  - Healthcare System
  - Administration and Public Services
  - Multiple Infrastructures

# Sample Reports

- Degree of Impact – High (A.1) - On November 19, 1994, Iowa City's US West telephone system shut down at about 3:30 p.m., local time, and service was gradually restored between 7:30 and 9:30 p.m, affecting about 60,000 people. Analysis showed that a new switching system had been installed in July 1994. In removing the old system, an electrical grounding cable had been inadvertently removed.
- Degree of Impact – Medium (B.1) - MCI's inbound Internet gateways were saturated during July 1994, resulting in days of delay in delivering e-mail to MCI customers. A fix was considered to be months in the offing

# Sample Reports (Cont.)

- Degree of Impact – Low (C.3) - A software glitch on March 10, 1995, caused Prodigy's e-mail system to send 473 e-mail messages to incorrect recipients and to lose 4,901 other messages. The system had to be shut down for five hours
- Example of a report that is not selected – I suppose I shouldn't be surprised, but the power went out for 17,000 here in our small town (38,000) last week. The local newspaper first reported that the power company didn't know why it went out, but that it "may be related to someone digging in their back yard". A week later they fixed the blame. A phone call (by the power company), supposedly to one substation, (completely automated judging by the tone of the article) went instead to a different substation (for unexplained reasons) and shut that substation down. It was down for 1.5 hours. – "Make a Call, Turn Off the Power, RISKS (17, 4)"
  - Relation to CITI is not clear
  - No clear reference to town name, location etc
  - Undefined term 17000

# A Sample Report

| A.1 | Ground-cable removal blows Iowa City phone system upgrade | | | |
|---|---|---|---|---|
| **Date** | **Country** | **Locality** | **Degree of Impact** | **Simulation** |
| 11/19/1994 | USA | City | High | Unsure |
| **Fault Type** | **Duration** | **Financial Impact** | **Public Safety** | **Affected Sites** |
| Unintentional | 6 hours | Unknown | Yes | Unknown |

On November 19, 1994, Iowa City's US West telephone system shut down at about 3:30 *p.m.,* local time, and service was gradually restored between 7:30 and 9:30 *p.m,* affecting about 60,000 people. Analysis showed that a new switching system had been installed in July 1994. In removing the old system, an electrical grounding cable had been inadvertently removed.

| | |
|---|---|
| **Report Source** | *Iowa City Press Citizen,* November 22, 1994; see discussion by Douglas W. Jones, *RISKS (16, 58)* |
| **Report Accuracy** | 6 |
| **Fault Origin** | Fault in electrical system due to human error. |
| **Source Infrastructure** | Electrical Power System |
| **Affected Infrastructures** | Telecommunication Infrastructure |
| **Affected Industry Sectors** | All kinds of industries of Iowa City |
| **Comment** | Lack of detailed planning |

# Collected Data

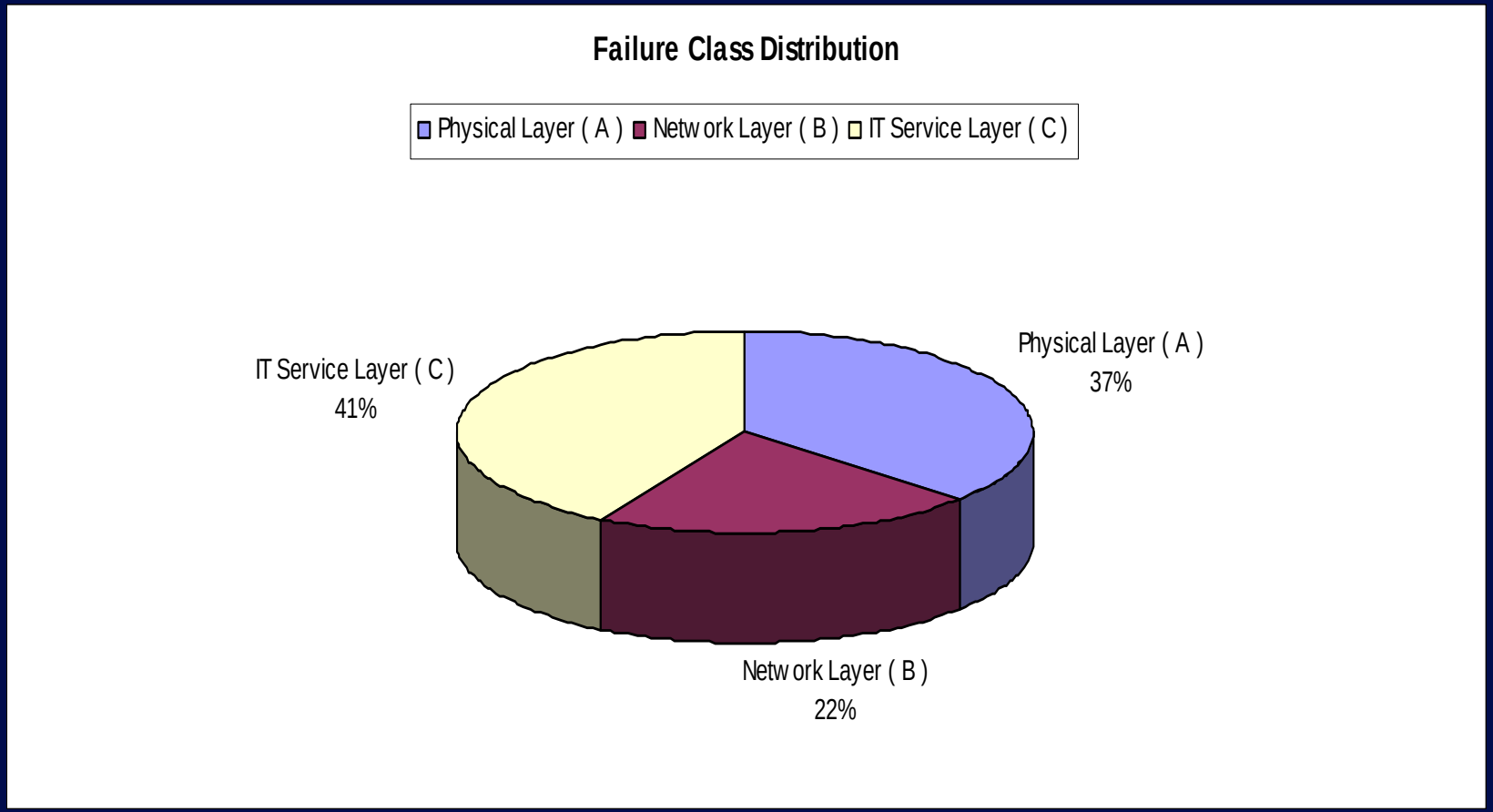
- 125 cases for 8 years (1994 – 2001)

| Year | Incidents # |
|---|---|
| 1994 | 5 |
| 1995 | 7 |
| 1996 | 8 |
| 1997 | 13 |
| 1998 | 16 |
| 1999 | 20 |
| 2000 | 24 |
| 2001 | 31 |

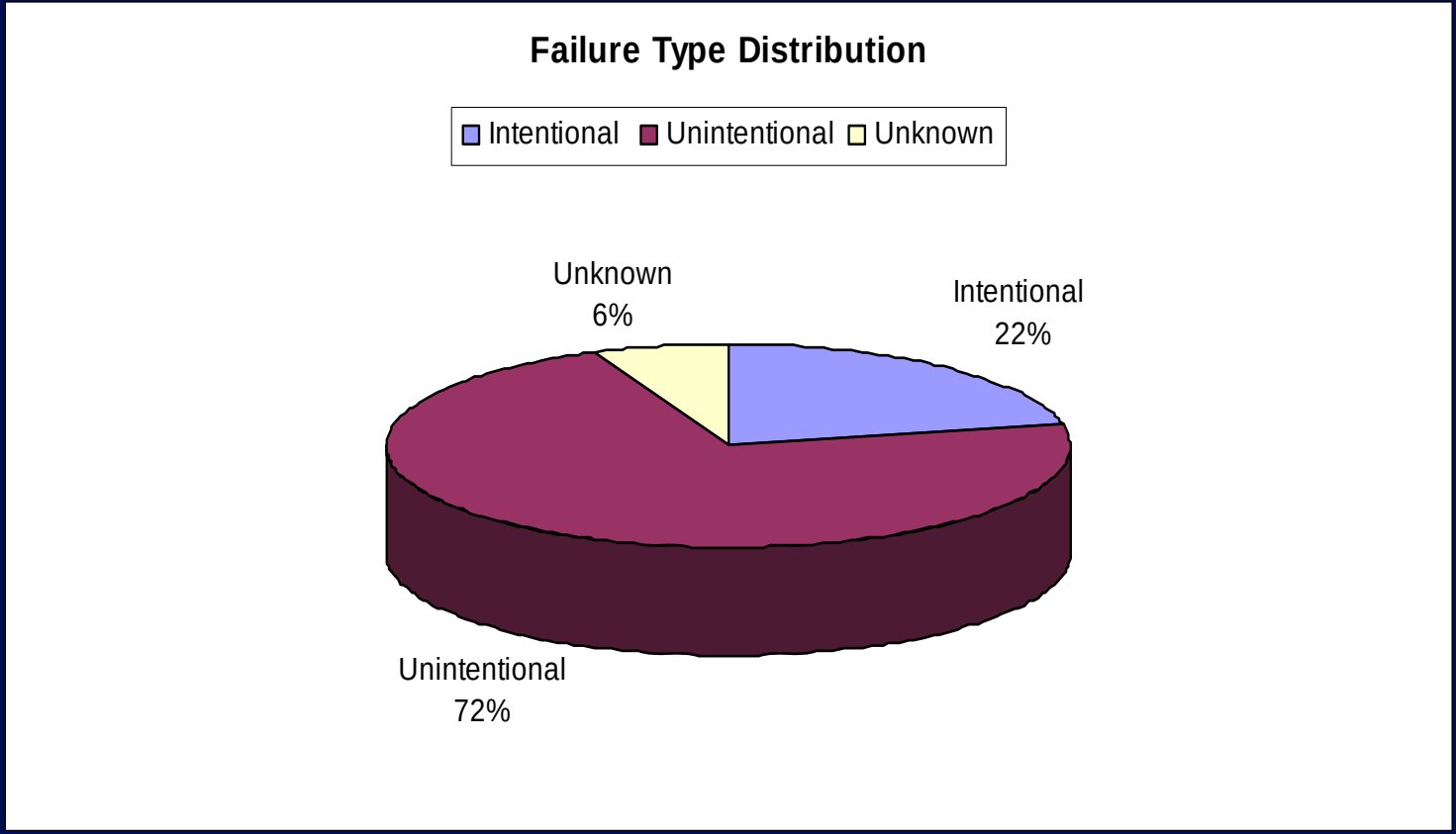
# Preliminary Stats/Results

| | Physical Layer ( A ) | | Network Layer ( B ) | | IT Service Layer ( C ) | | Total | |
|---|---|---|---|---|---|---|---|---|
| Total/category | 46 | 37% | 27 | 22% | 52 | 42% | 125 | 100% |
| **Type** | | | | | | | | |
| Intentional | 2 | 4% | 18 | 67% | 7 | 13% | 27 | 22% |
| Unintentional | 39 | 85% | 9 | 33% | 42 | 81% | 90 | 72% |
| Unknown | 5 | 11% | 0 | 0% | 3 | 6% | 8 | 6% |
| **Impact Scale** | | | | | | | | |
| High | 37 | 80% | 20 | 74% | 31 | 60% | 88 | 70% |
| Medium | 8 | 17% | 6 | 22% | 12 | 23% | 26 | 21% |
| Low | 1 | 2% | 1 | 4% | 9 | 17% | 11 | 9% |
| **Location** | | | | | | | | |
| US/Canada | 26 | 57% | 15 | 56% | 34 | 65% | **75** | 60% |
| Other | 20 | 43% | 12 | 44% | 18 | 35% | 50 | 40% |
| World | 2 | 4% | 6 | 22% | 0 | 0% | 8 | 6% |
| **Public Safety** | | | | | | | | |
| Concern | 15 | 33% | 7 | 26% | 10 | 19% | 32 | 26% |
| No Concern | 20 | 43% | 16 | 59% | 34 | 65% | 70 | 56% |
| Unknown | 11 | 24% | 4 | 15% | 8 | 15% | 23 | 18% |

# Failure Class Distribution

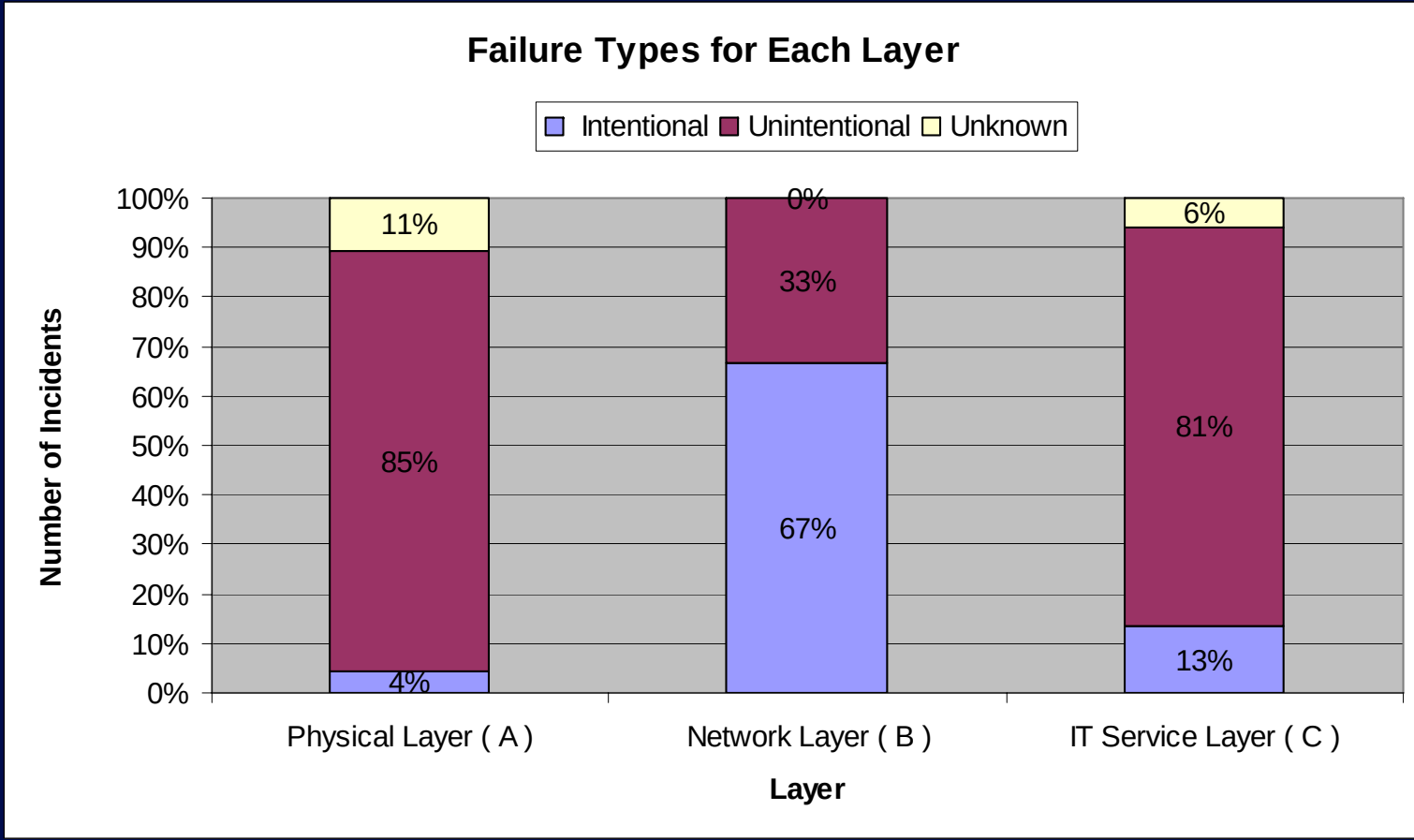


# Failure Type Distribution



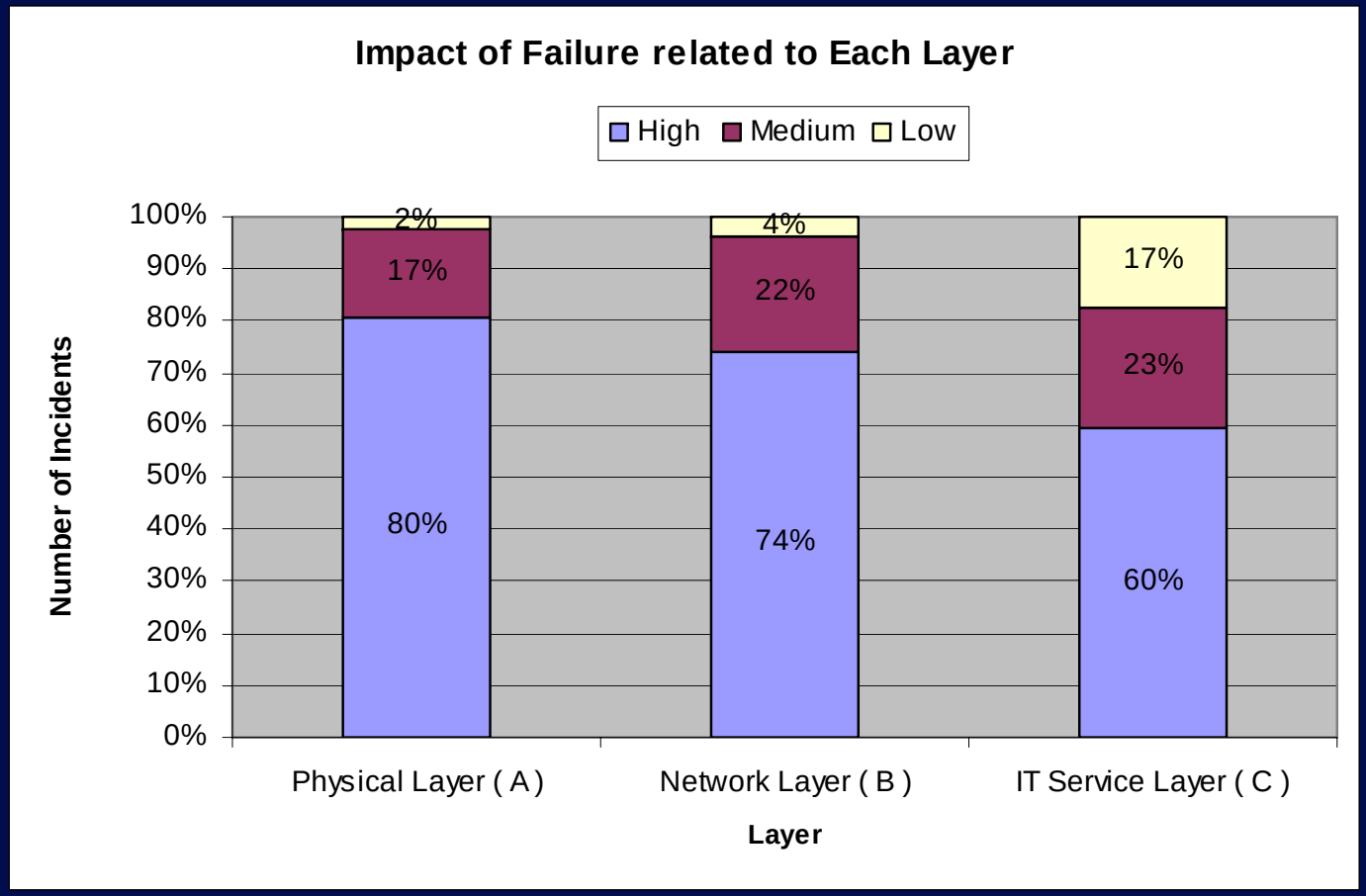

- Remark 1: Origins of most of the CITI failures are unintentional.

# Failure Type for Each Layer



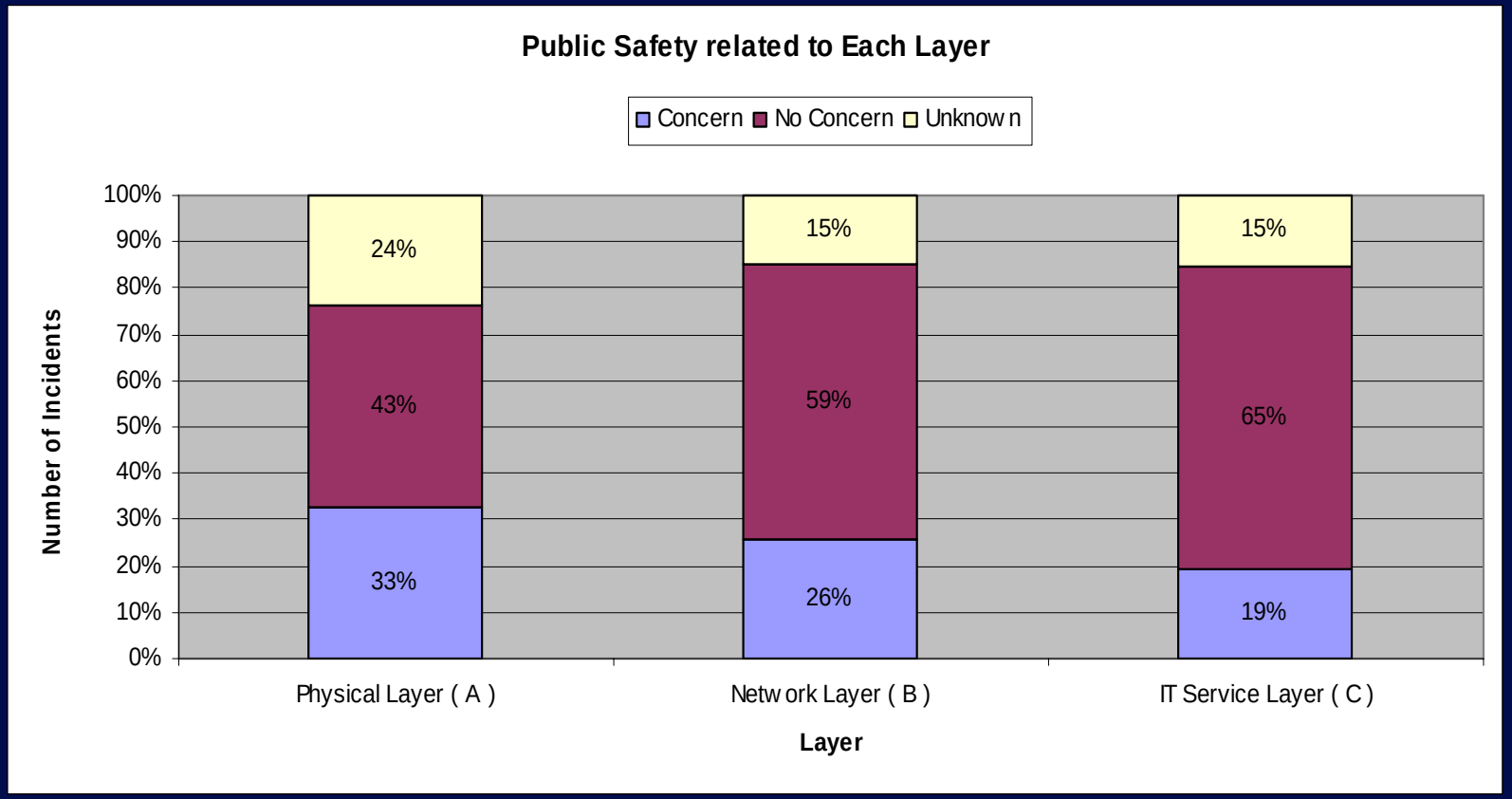

- Remark 2: Intentional failures are mostly concerned with network layer.

# Impact of Failure related to Each Layer




- Remark 3: Failure in the lower layer has higher impact than upper layer

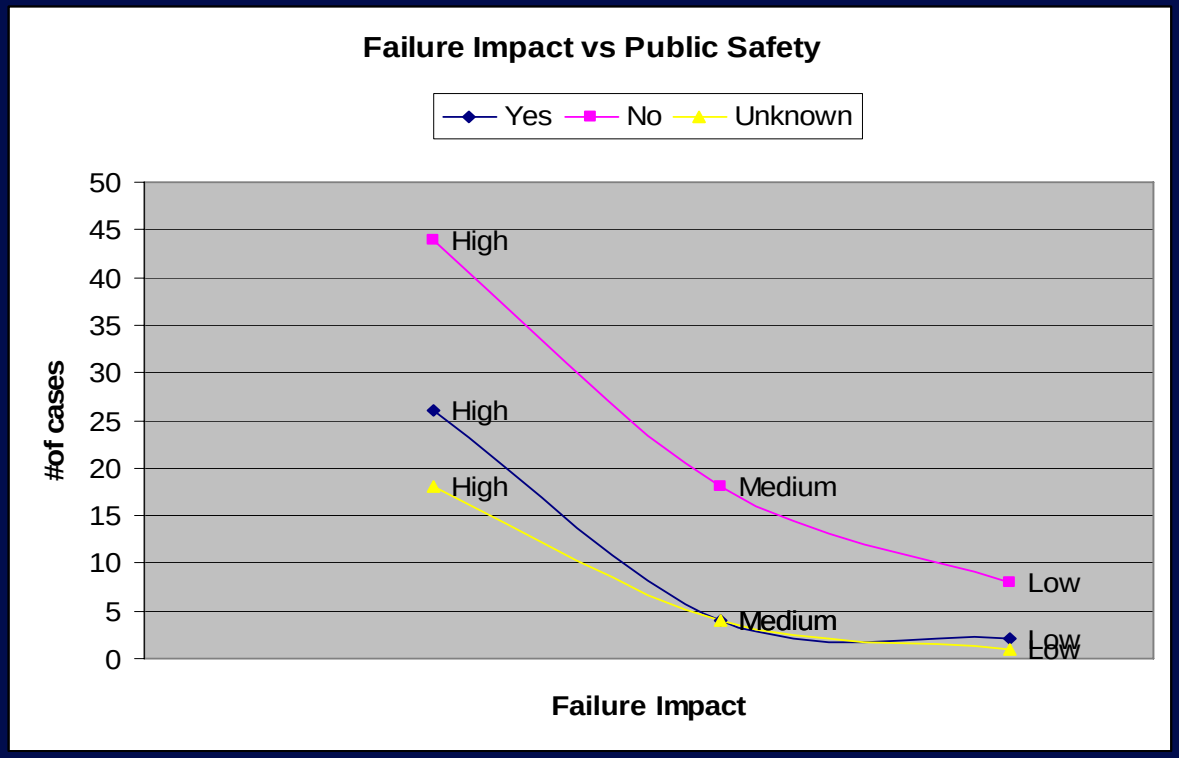
# Public Safety related to Each Layer




- Remark 4: Public safety concern is more for lower layer failures.

# Public Safety vs Failure Impact

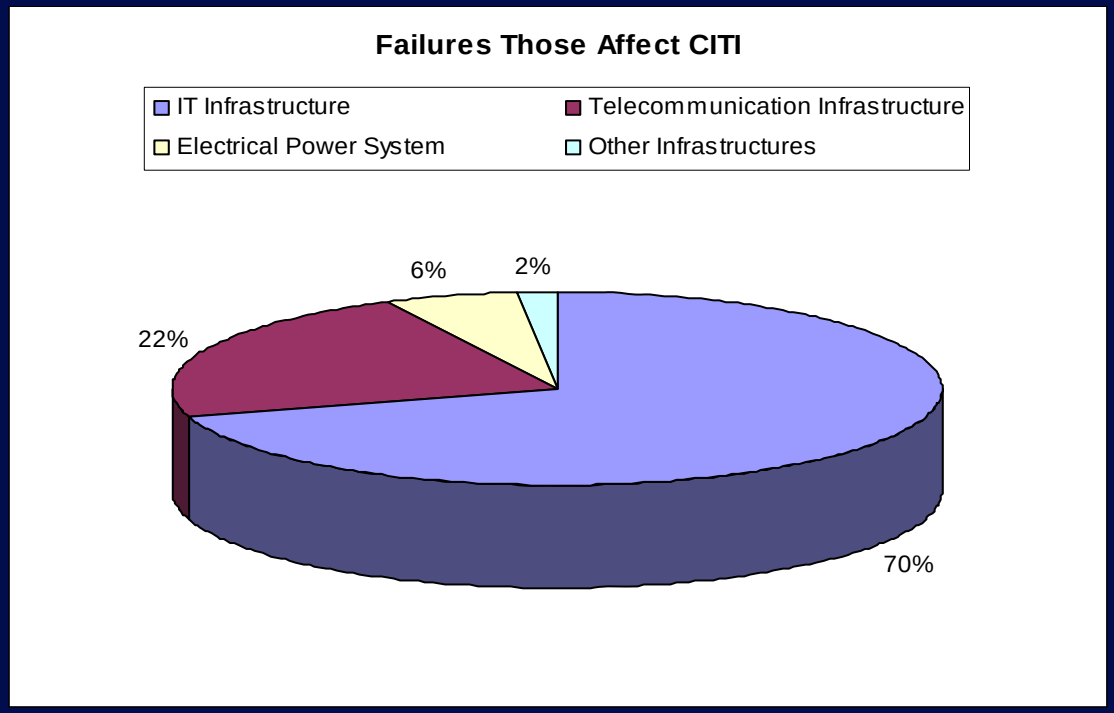
| | High | Medium | Low |
|---|---|---|---|
| Yes | 26 | 4 | 2 |
| No | 44 | 18 | 8 |
| Unknown | 18 | 4 | 1 |




- Remark 5: Public safety is not directly related to the degree of impact.

# CITI Failure Sources

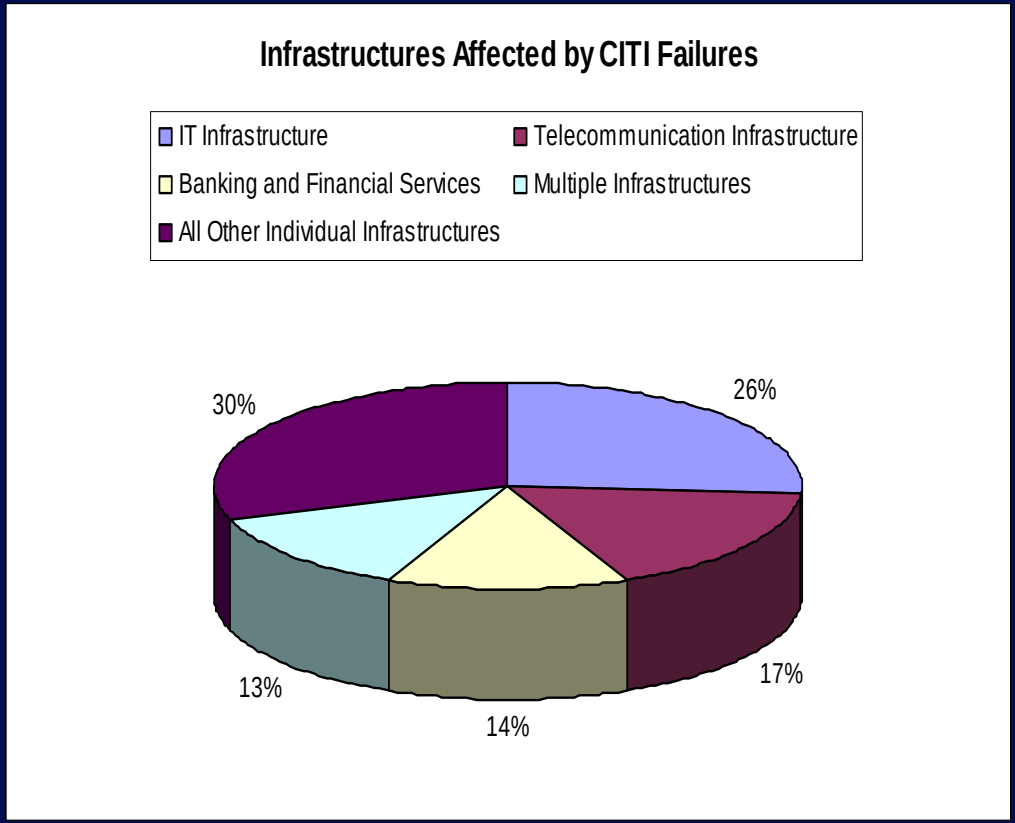
| | |
|---|---|
| IT Infrastructure | 88 |
| Telecommunication Infrastructure | 28 |
| Electrical Power System | 7 |
| Public Safety Services | 2 |




- Remark 6: CITI failures are mostly originated from within CITI infrastructure.

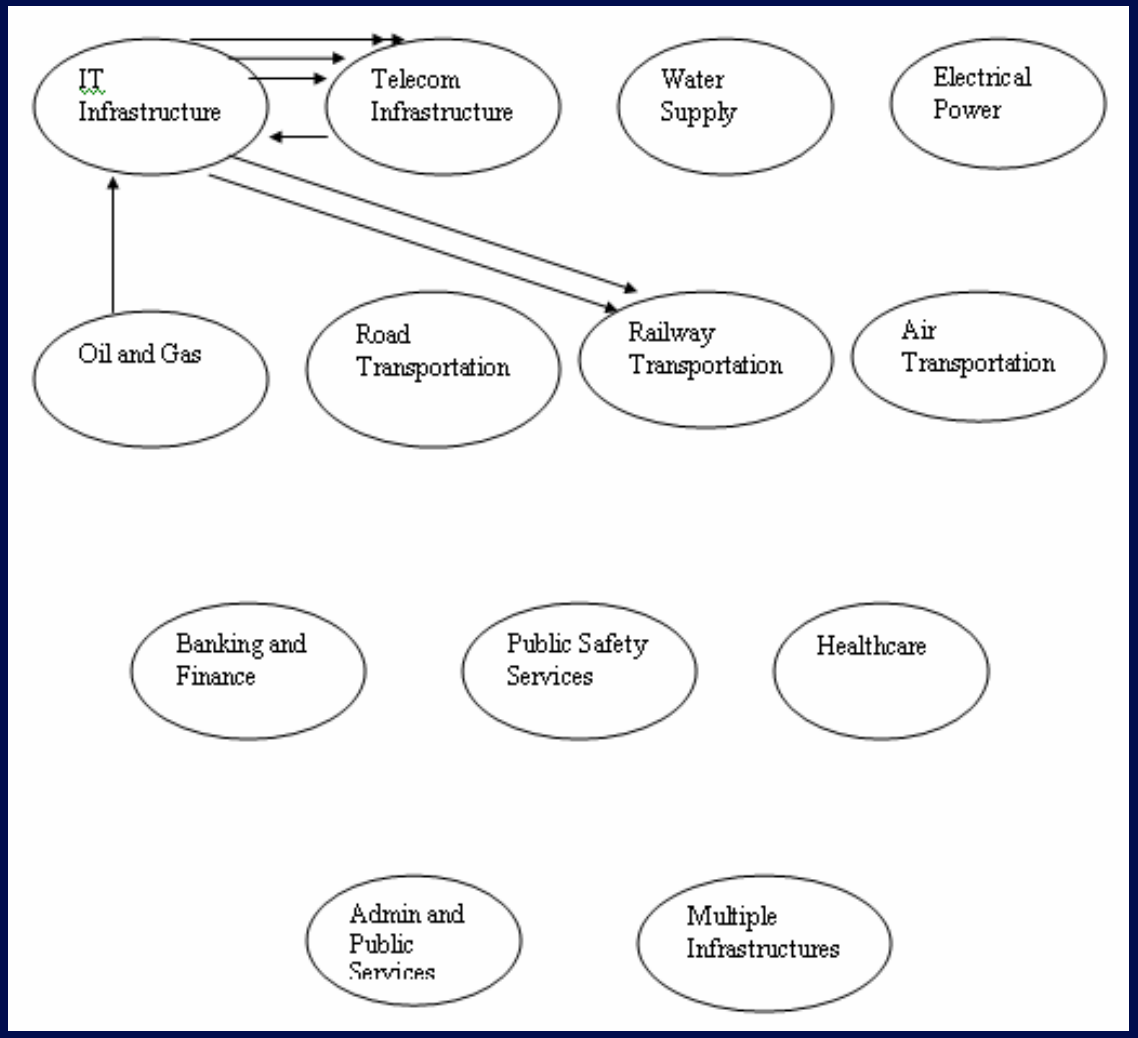
# Infrastructures Affected by CITI Failures

| | |
|---|---|
| IT Infrastructure | 33 |
| Telecommunication Infrastructure | 21 |
| Banking and Financial Services | 17 |
| Multiple Infrastructures | 16 |
| Air Transportation | 11 |
| Administration and Public Services | 8 |
| Railway Transportation | 7 |
| Public Safety Services | 5 |
| Water Supply | 1 |
| Electrical Power System | 2 |
| Oil and Gas | 1 |
| Road Transportation | 1 |
| Healthcare System | 2 |

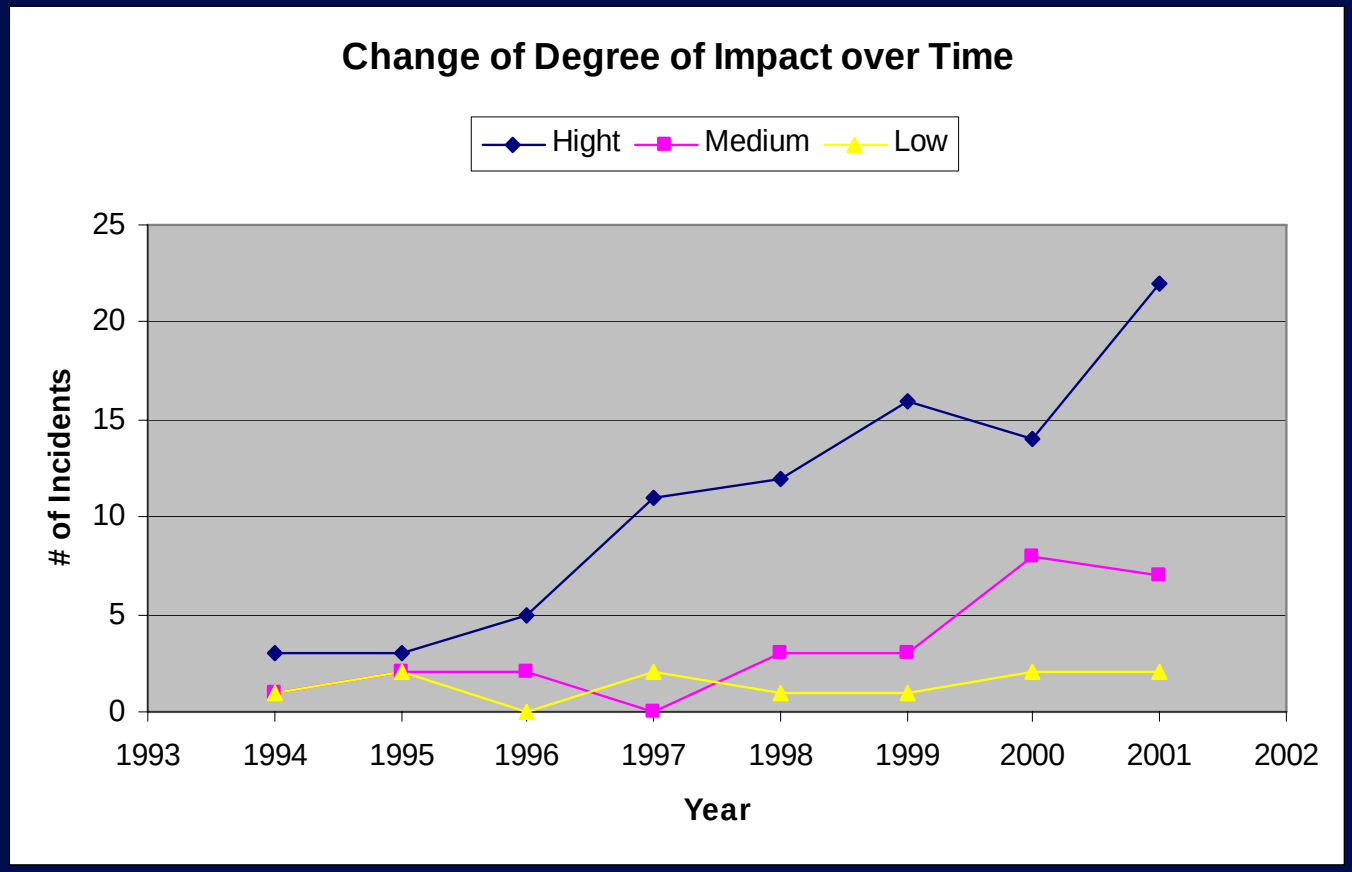



- Remark 7: Most of the CITI failures affect CITI, Banking and Finance and/or Multiple (more than one) Infrastructures.

# Interdependency Graph (Under Construction)

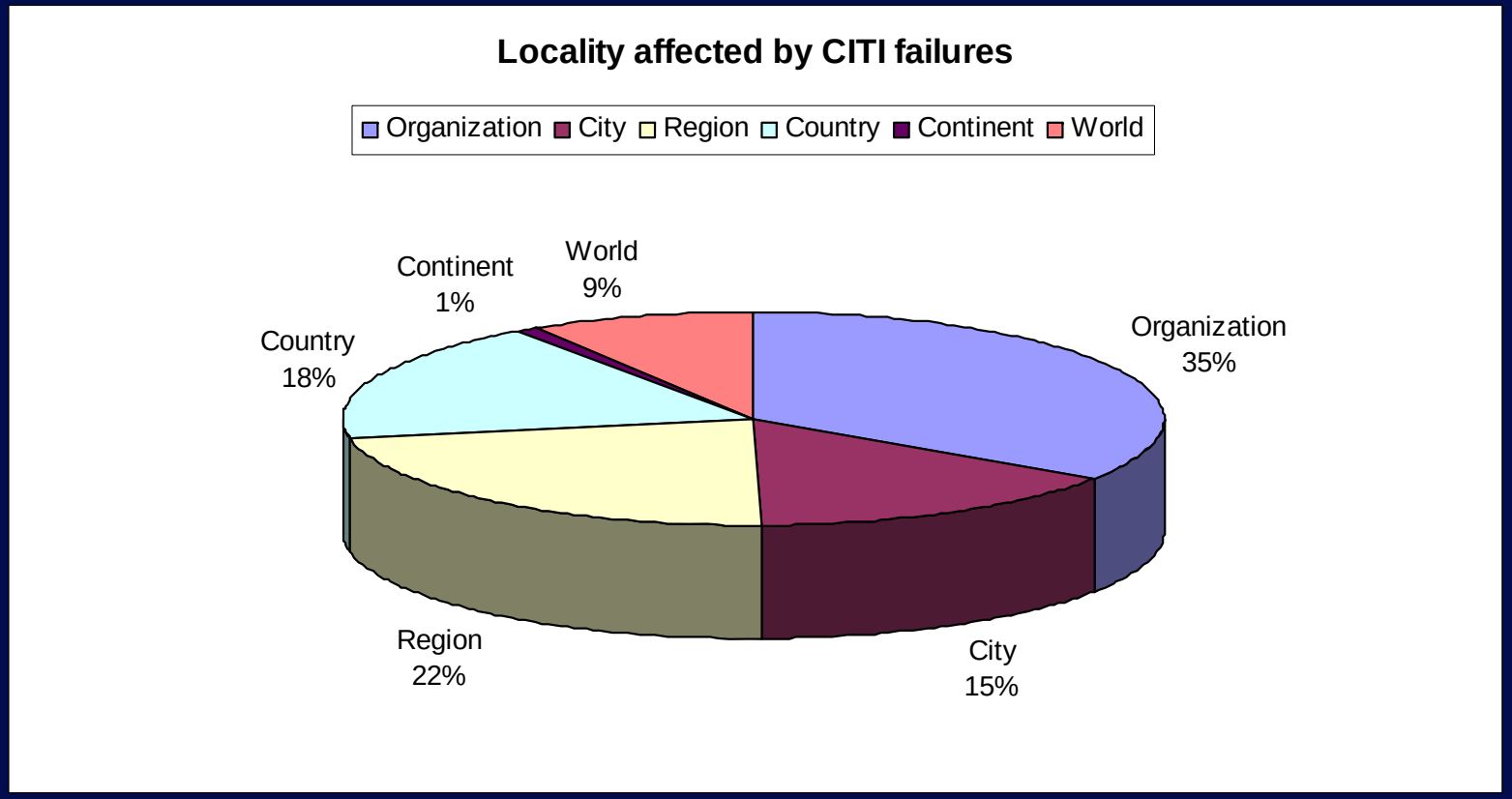


# Change of Degree of Impact over Time



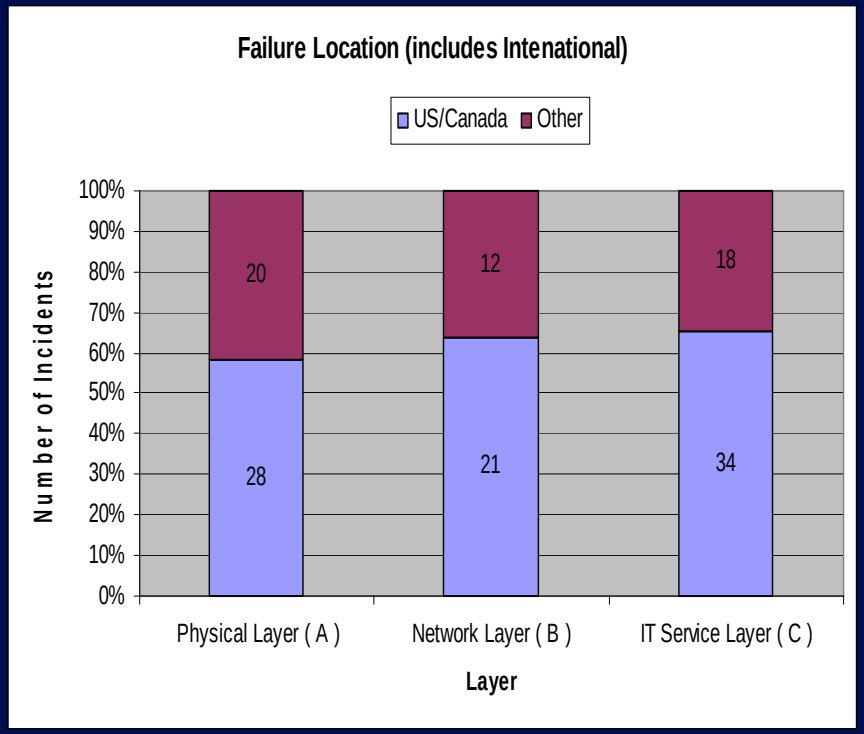

- Remark 8: Degree of impact (severity) of CITI failures are on the rise.

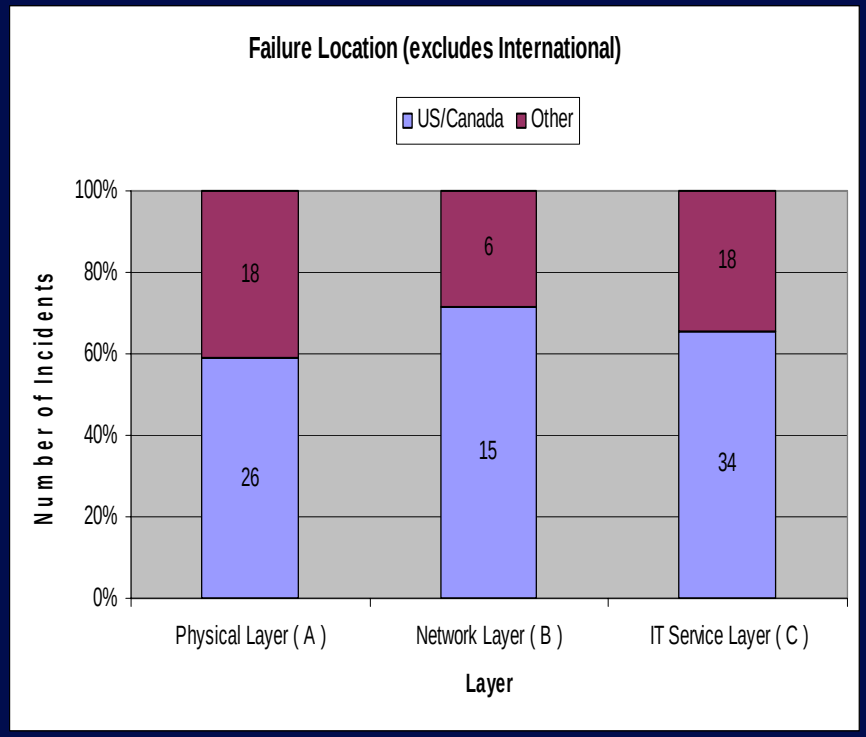
# Locality affected by CITI Failures




- Remark 9: Most of the time CITI failures affect individual setup or organization. However, affects of many of the failures cross organization boundary and may affect the whole country. Crossing the national boundary is very unlikely, unless a failure is targeted internationally.

# Failure Locations in the World




- Remark 10: Most the reported failures (above 60%) are related to North America (US/Canada)

# Conclusions

- Identifying CITI and other infrastructures' interdependency from public domain data is an unexplored proposition.
- In this research, we have proposed a method to extract meaningful information from these public domain data.
- Using this method we have analyzed 8 years of public domain data from ACM RISKS forum and identified some patterns related to CITI and other infrastructures' interdependencies.
- Our immediate goal is to collect and analyze data up to 2005
- We will also look into the work of Stephanie Chang et al. and examine usefulness of some of their ideas in our work.

# Any Question ?