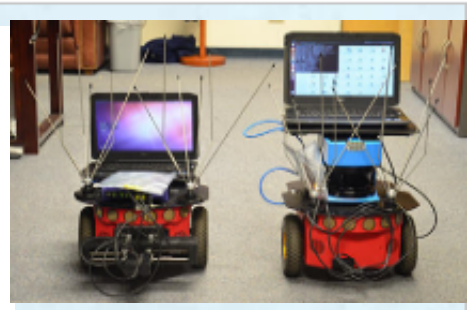
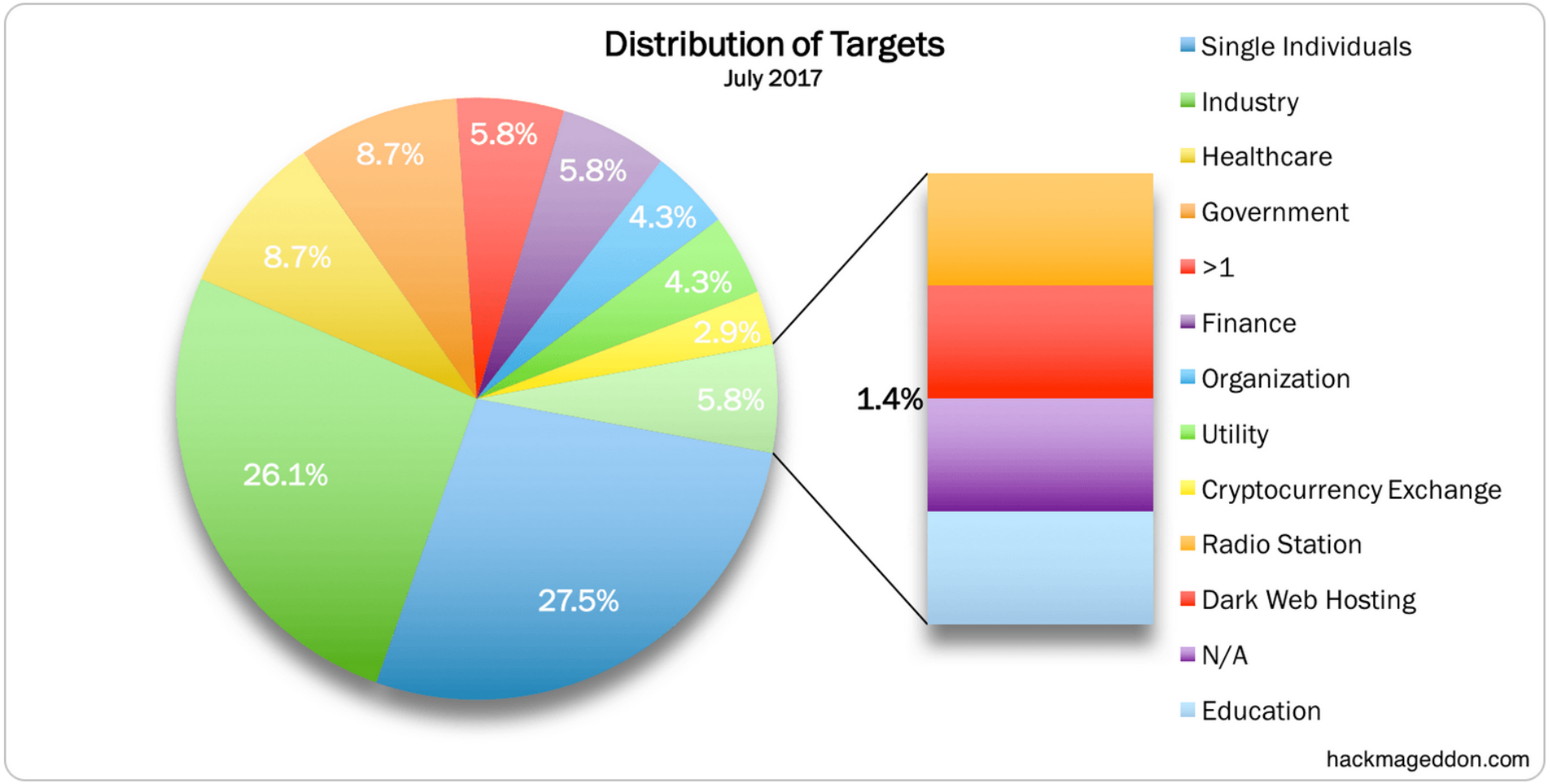


Establishing market based mechanisms for CYBer security information EXchange (CYBEX)

Contact: Dr. Shamik Sengupta (ssengupta@unr.edu)

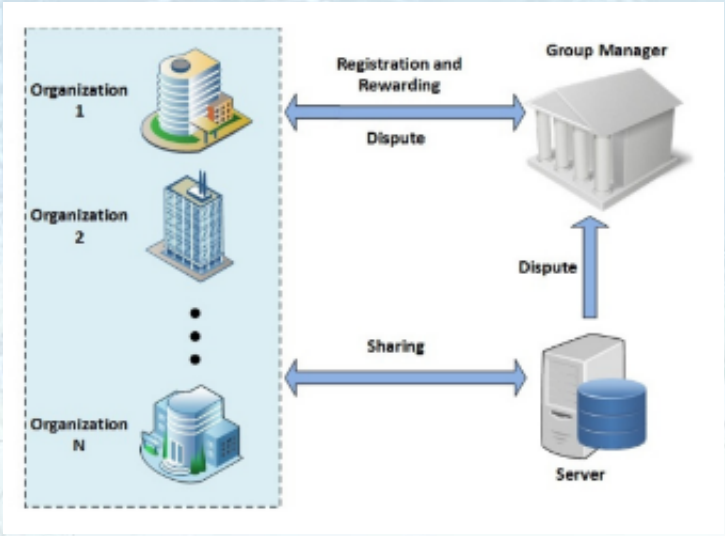


Source: http://www.hackmageddon.com/2017/08/24/july-2017-cyber-attacks-statistics/

CYBEX

- A framework to provide a service of structured information exchange about measurable security states of systems together with incidents stemming from cyber attacks.
- Benefits:
  - (1) fostering cyber situational awareness,
  - (2) developing proactive defense mechanisms,
  - (3) clarity in understanding the threat landscape, malicious actors, security loopholes etc.
- Challenges:
  - (1) the possibility of information exploitation through such exchange as the sharing organizations may not trust on the other participants,
  - (2) organizations' market reputation might get negatively affected,
  - (3) lack of incentivization with respect to a organization's sharing contribution.

CYBEX



Game Formulation

	Participate & Share	Not Participate
Participate & Share	$Sa\log(1+I)-x-c,$ $Sa\log(1+I)-x-c$	$a\log(1+I)-x-c,$ $a\log(1+I)$
Not Participate	$a\log(1+I),$ $a\log(1+I)-x-c$	$a\log(1+I),$ $a\log(1+I)$

I – amount of investment made by the firms
a - simple scaling parameter that maps user satisfaction/benefit to a dimension equitable to the price/monitory value
c - cost of participation in the CYBEX framework
S – Scaling benefits of sharing

Cyber-Insurance

•Cyber-insurance as a CYBEX model incentive:

•Insurance incentives can be used to motivate socially optimal sharing behavior and deter harmful behaviors. If cyber-insurance is added as an incentive in exchange for information sharing, firms benefit due to efficient and reliable risk management using cyber-insurance. On the other hand, supply side gets benefited by obtaining information they need.

•Modelling Cyber-Insurance with information sharing framework:

•Cyber-insurance can be modelled in such a way that the coverage and premium for the insurance will depend on the sharing level, frequency of attacks and attack severity level. As the frequency of attack increases the premium for the insurance gets incremented compared to previous, however periodically the premium amount decreases on how successfully the network strives against cyber attacks for long with the help of cooperation.

•Challenges in modelling Cyber-Insurance:

•**1)Information Asymmetry:** Insurers not being able to classify the nodes due to the lack of information such as security levels opted by the firm, attack frequencies. Often, firms do not wish to share the data due to privacy issues and also due to the concern of reputation loss.

•**2)Non-Linearity:** Risk domain for cyber security can be said as non-linear, meaning, that same attack can cause either small or big losses in different occasions.

•**3)Correlated risks:** Due to the interdependent nature of the networks, security compromises can arise from the failure of security of independently owned systems to contribute to overall prevention

Questions?

Dr. Shamik Sengupta (ssengupta@unr.edu)

Website: https://www.cse.unr.edu/~shamik/

University of Nevada, Reno

A National Tier 1 University