

Georgia State University

## ScholarWorks @ Georgia State University

---

EBCS Presentations

Evidence-Based Cybersecurity Research Group

---

2019

### An Evidence Based Cybersecurity Approach to Risk Management: Risk Management and "Market for Lemons"

David Maimon  
*Georgia State University*

Follow this and additional works at: [https://scholarworks.gsu.edu/ebcs\\_presentations](https://scholarworks.gsu.edu/ebcs_presentations)



Part of the [Criminology Commons](#), [Criminology and Criminal Justice Commons](#), and the [Information Security Commons](#)

---

#### Recommended Citation

Maimon, David, "An Evidence Based Cybersecurity Approach to Risk Management: Risk Management and "Market for Lemons"" (2019). *EBCS Presentations*. 1.  
[https://scholarworks.gsu.edu/ebcs\\_presentations/1](https://scholarworks.gsu.edu/ebcs_presentations/1)

This Article is brought to you for free and open access by the Evidence-Based Cybersecurity Research Group at ScholarWorks @ Georgia State University. It has been accepted for inclusion in EBCS Presentations by an authorized administrator of ScholarWorks @ Georgia State University. For more information, please contact [scholarworks@gsu.edu](mailto:scholarworks@gsu.edu).

# An Evidence Based Cybersecurity Approach to Risk Management





# Agenda

- 9:00 -10:30 Keynotes
- 10:30 Break
- 10:45 Group discussions
- 12:00 Lunch
- 1:00 Group discussions
- 2:15 Group discussions summaries
- 2:45 Conclusions

# Risk Management and “Market for Lemons”

Dr. David Maimon



Andrew Young School of Policy  
Criminology and Criminal Justice  
Center for Evidence Based Cybersecurity





# Risk

- The extent to which an entity is threatened by a potential circumstance or event.
- Risk is typically a function of:
  - The adverse impacts that would arise if the circumstance or event occurs;
  - The likelihood of occurrence.



# Information Security Risks

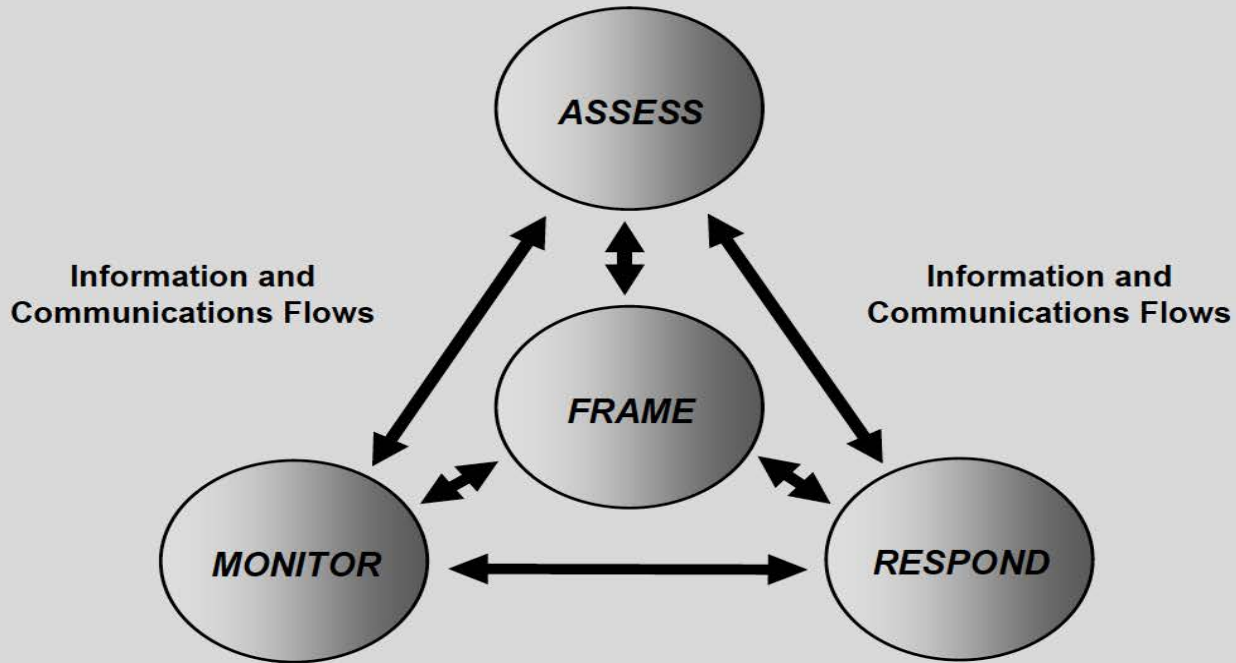
- Those risks that arise from loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations, organizational assets, and individuals.



# Risk Management

- The process of Identifying , assessing and evaluating the level of risk facing the organization, and then deciding what countermeasures to take in reducing risk to an acceptable level

# Risk Management Process (NIST)







# Assess

- Identify
  - Threats to organizations (i.e., operations, assets, or individuals)
  - Vulnerabilities internal and external to organizations;
  - The harm (i.e., adverse impact) that may occur
  - The likelihood that harm will occur.
- The end result is a determination of risk



## Respond

- Developing alternative courses of action for responding to risk
- Evaluating the alternative courses of action
- Determining appropriate courses of action consistent with organizational risk tolerance;
- Implementing risk responses based on selected courses of action



## Monitor

- Determine the ongoing effectiveness of risk responses



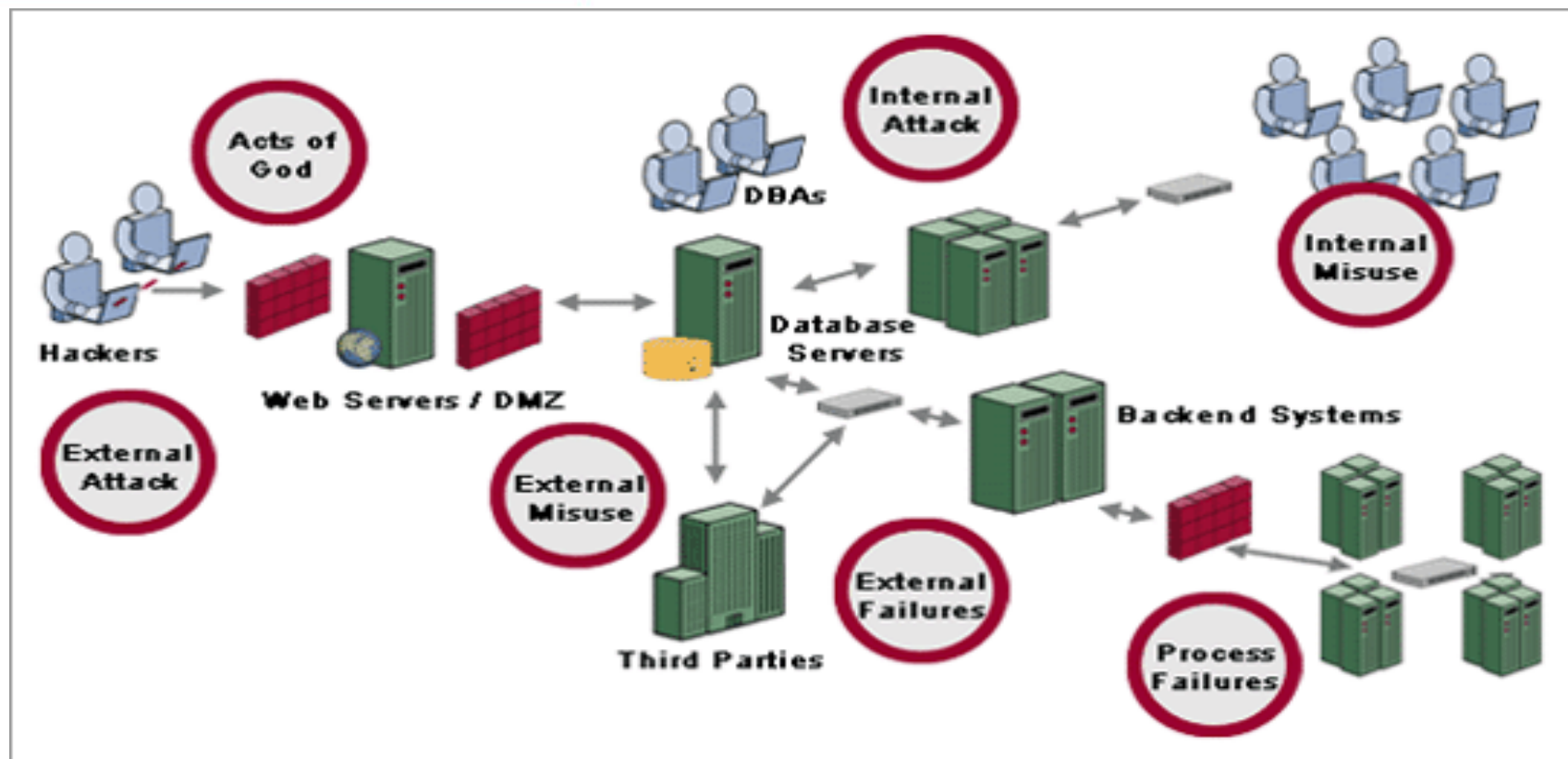
## Problem

- The current common approaches for risk assessment (likelihood and impact) and the implementation of response are problematic at best



## Likelihood of Occurrence

The *likelihood of occurrence* is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).





## Determine the Likelihood a Harm will Occur

	Definition
Low	0-25% chance of successful exercise of threat during a one-year period
Moderate	26-75% chance of successful exercise of threat during a one-year period
High	76-100% chance of successful exercise of threat during a one-year period



## Potential Impact

- The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.





# Israel Cybersecurity Landscape

- 150 active companies -

**Cloud Security** \$100M

AVANAN, Vaultive, CATO, FIRELAYERS, Dome, Sookasa, CloudLock, SKYFORMATION, hexatier

**Software Development Life Cycle** \$45M

snyk, SafeDK, CHECKMARK, PureSec

**Containers Security**

Twistlock, STABLEWAVE, aqua

**Identity and Fraud** \$120M

**Authentication**

SILVERFORT, plainID, SECURE PUSH, TRANSPARENT SECURITY, SecuredTouch, BIO CATCH, TokenID, DYADIC

**Fraud Detection**

FORTER, riskified, PROTECTED MEDIA, I AM REAL, REVENUESTREAM, pagilant, CymCompliant, IS IT YOU

**Network Security** \$230M

portnox, Metasploit, Securi, LIGHT CYBER, Dimpera Security, ForeScout, tufin, algosec

**Industrial Control Systems** \$150M

CLAROTY, NextNine, ThetaRay, Indegy, HISCADA fence, BEPIO, ICS, WATERFALL, CRITENCE, FIRMITAS, NATION, HALO ANALYTICS, radii, APERIO, Sigo, BISEC, CyberX

**Endpoint Protection** \$80M

SentinelOne, PERCEPTION POINT, HYDRON, MORPHISSEC, promisc, BUFFERZONE, MINERVA, DW

**Detection & Prevention** \$150M

deepinstinct, IRONSCALES, VOTIRO, FENIX, 3E-SEC, odi, fireglass, SOLEBIT, Cybellum, UBA, FORTSCALE, exabeam, preempt, SecuPi

**Mobile Security** \$150M

cellrox, eMune, wandera, ZIMPERIUM, CoroNet, KAYMERA, NUBO, helixOS, AppDomain, VAULTO, INPEIDIO, Skycure

**Deception** \$100M

GuardiCore, Cymmetria, TRAPX SECURITY, JAVELIN, illusive

**Incident Response & Forensics** \$150M

wirex, DEMISTO, SIMPLIFY, HEXADITE, nightingale, EDR, Cynet, SECDO, cyberreason

**Web Security** \$25M

perimeterx, IPVTEC, namogoo, MAZEBOUL, HYBRID SECURITY, Reblaze, FIBERBLADE, Armeron, 6scan

**Cyber Intelligence** \$30M

KELA, Cyberint, SPARK, QCE, comilion, CYFORT, SamsaraCy, IntSights

**Internet of Things** \$5M

SECURITHINGS, Perytons, Regulus, CyberRed, Protectix, ddyolabs

**Data Leakage Prevention** \$35M

COVERTIX, nuro, EUC AUTHORITY, D.DAY LABS

**Automotive** \$35M

ENSILIO, safend, Minereye, CYMOTIVE, Guard Knox, ARGUS, Karamba Security, CARSDOME

**Cyber Posture** \$100M

SafeBreach, IMVISION TECHNOLOGIES, empow, cyteleg, CRONUS, infoSec, SKYBOX, CYMULATE, cyberOBSERVER

\* Acquired in 2016  
Amount raised by active companies in this category

**BESSEMER VENTURE PARTNERS**  
Email: israel@bvp.com

January 2017



## Market for Lemons (Akerlof 1970)

- A market with asymmetric information



\$2000



\$1000



## Cybersecurity Market

- Vendors may make claims about the security of their products, but in the absence of evidence regarding the effectiveness of the products, buyers have no reason to trust them.



## Solutions for Lemon Markets

- Warranties
- More information regarding the product





## The Million Dollar Question

- What should be done in effort to support CISOs' and General Counsels' decision making regarding the assessment of risks as well as the adoption of security policies and tools within their organizations?



## Evidence-Based Cybersecurity (EBCS)

- Stresses moving beyond decision makers' political, financial, social background and personal experience to a model in which tools' adoption and policy enforcements decisions are made based on scientific studies findings.





# Cybercrime Ecosystem



Offenders



Enablers

The Deep Web and Darknet



Guardians



Targets

The Surface Web



# Rigorous Scientific Research Designs





Georgia State Home

STUDENTS

FACULTY & STAFF



## Evidence-Based Cybersecurity Research Group

About

People

Academics

Advisory Board

Research

Resources

Events

News

# Resources

The resources below are available for free download. Please enter your email address and a download link will be sent to you.



### Prompt Patching

257.88 KB 2 downloads

A description about how Prompt vulnerability helps in providing cyber security. ...

DOWNLOAD



### Passwords

196.18 KB 0 downloads

How Passwords can help in authentication and help in preventing the development...

DOWNLOAD



### Intrusion Detection System (IDS)

193.08 KB 0 downloads

A device or software application that monitors a network or systems for malicious...

DOWNLOAD



### Honeypots

191.29 KB 0 downloads

Tools which permits the collection of information on hackers and real system trespassing...

DOWNLOAD



### Firewalls

194.16 KB 2 downloads



## Key Principals of the Approach

Generate and employ empirical evidence to:

- Identify online threats and vulnerabilities and educate targets of cybercrime
- Guide policy development and guardians' efforts to secure cyberspace
- Guide the design and configuration of computing environments that can mitigate effectively the consequences cybercrime events

# Evidence Based Cybersecurity and Threat Assessments (Examples)





## A Threat-Oriented Approach

- A threat-oriented approach starts with the identification of threat sources and threat events, and focuses on the development of threat scenarios; vulnerabilities are identified in the context of threats, and for adversarial threats, impacts are identified based on adversary intent.

# The Origin and Time of Attacks Against a Network (Maimon et al 2013)



# Data

- Intrusion Prevention System (IPS) data from a large university computer network
  - Potential attack attempts (unlike for incidents, false alarms might exist)
    - Collected between September 2007 and until 2009





## Hourly Distribution of Computer-Focused Crimes

Time of day	2007 (N = 2,168, 478)	2008 (N = 3,270,895)	2009 ( N = 645,554)
9:00am – 4:59pm	59.04%	38.25%	50.06%
5:00pm- 12:59am	16.19%	27.36%	21.44%
1:00am-8:59am	24.8%	34.39%	28.5%





## Foreign Network Users and Computer-Focused Crimes Against the Network

	2007		2008		2009	
	IRR	95% CI	IRR	95% CI	IRR	95% CI
Population between 15-64 years	1.13***	1.06, 1.20	1.15***	1.09, 1.22	1.18** *	1.10, 1.25
% Urban	1.04***	1.02, 1.06	1.01*	1.00, 1.03	1.03**	1.01, 1.05
Internet users	1.03***	1.01, 1.05	1.03***	1.02, 1.05	1.02*	1.00, 1.03
Foreign network users per 1000 users	1.64*	1.00, 2.98	1.58*	1.05, 2.38	1.43*	1.05, 1.95

\*p<0.05   \*\*p<0.01   \*\*\*p<0.001



## An Asset/Impact-Oriented Approach

- An asset/impact-oriented approach starts with the identification of impacts or consequences of concern and critical assets, possibly using the results of a mission or business impact analyses and identifying threat events that could lead to and/or threat sources that could seek those impacts or consequences.



## Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

**REF CODE:2550CGE**

You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.

[Amazon.com](#)

Email ID: 

Your computer files have been encrypted. Your photos, videos, documents, etc.... But, don't worry! I have not deleted them, yet.  
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.  
Every hour files will be deleted. Increasing in amount every time.  
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.  
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.  
Send to the Bitcoins address specified.  
Within two minutes of receiving your payment your computer will receive the decryption key and return.  
Try anything funny and the computer has several safety measures to delete your files.  
As soon as the payment is received the crypted files will be returned to normal.

Thank you

58:59

1 file will be deleted.

[View encrypted files](#)

Please, send \$150 worth of Bitcoin here:

1Bitcoin1com:1Pz9yY83Sg8P11F4Z

I made a payment, now give me back my files!



----- Forwarded message -----

From: **Richard Hoption** <[richard.hoption@huji.ac.il](mailto:richard.hoption@huji.ac.il)>

Date: Mon, May 18, 2015 at 6:05 PM

Subject: Richard Hoption has shared the following PDF:

To: [Tamar.Berenblum@mail.huji.ac.il](mailto:Tamar.Berenblum@mail.huji.ac.il)

- 545 logins (20 per 1000 users)
- 178 phishing (6.87 per 1000 users)
- 21% of the logins and 25% of the phishing occurred from university network

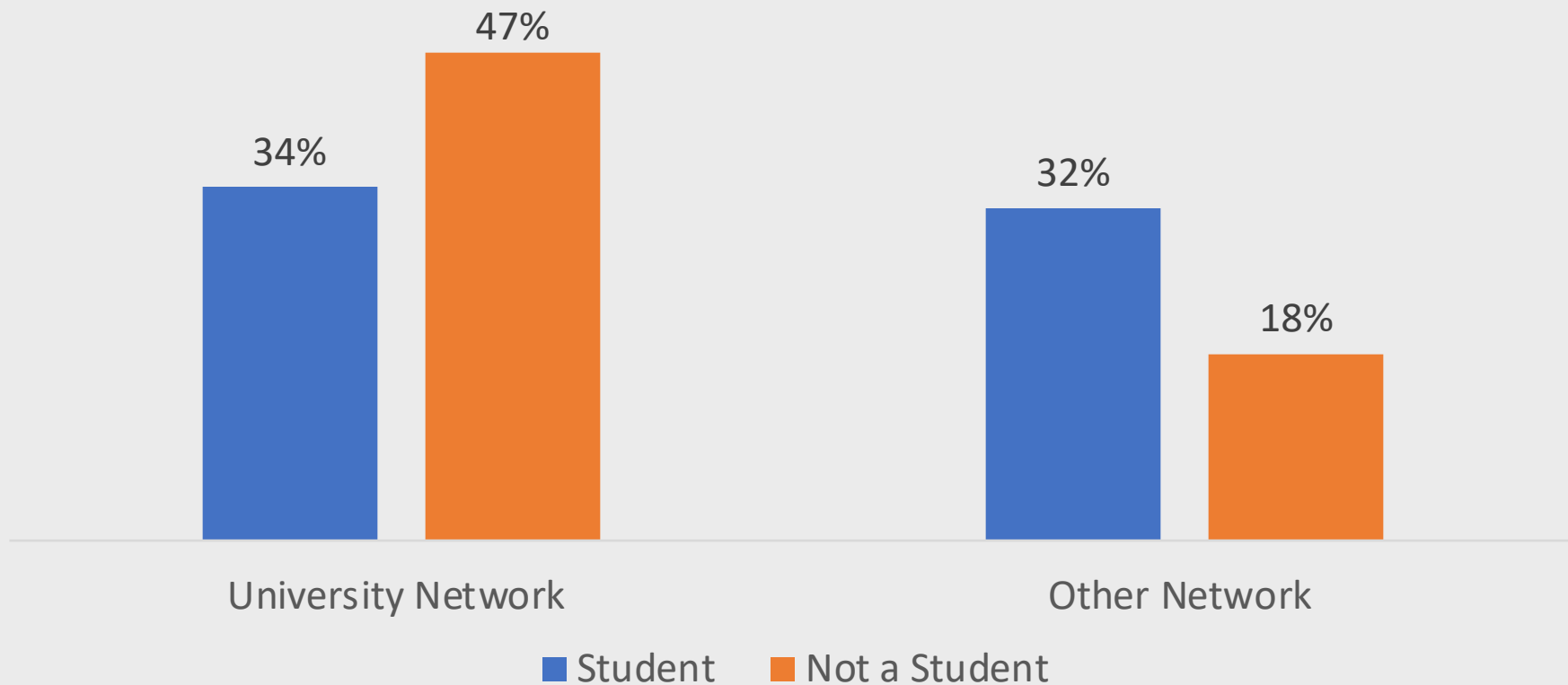
Richard Hoption has shared the following PDF:



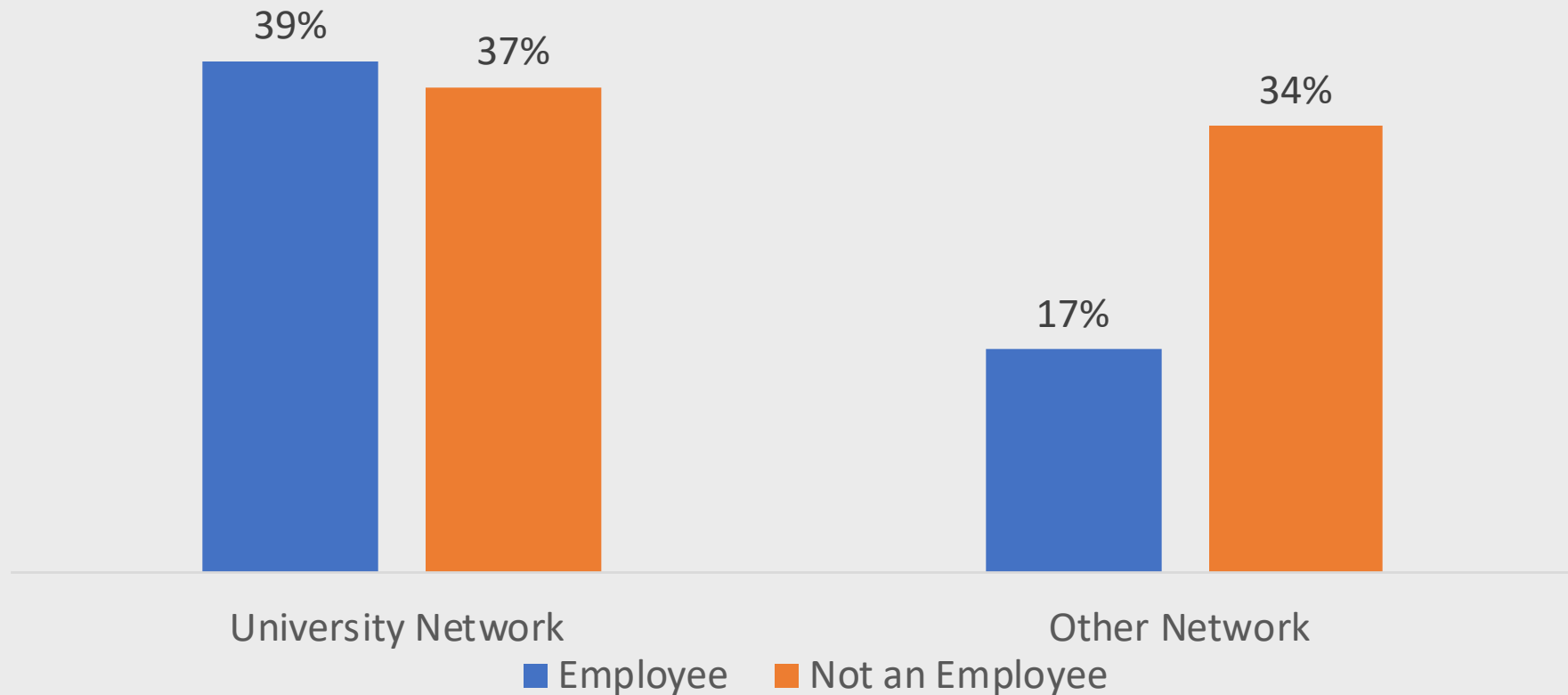
Secured File Via Google Drive

Open

# Predicted Probability of Students and Non-Students to Click on Links Embedded in Suspicious Emails while Using University and Non-University Networks



# Predicted Probability of Employees and Non-Employees to Click on Links Embedded in Suspicious Emails while Using University and Non-University Networks

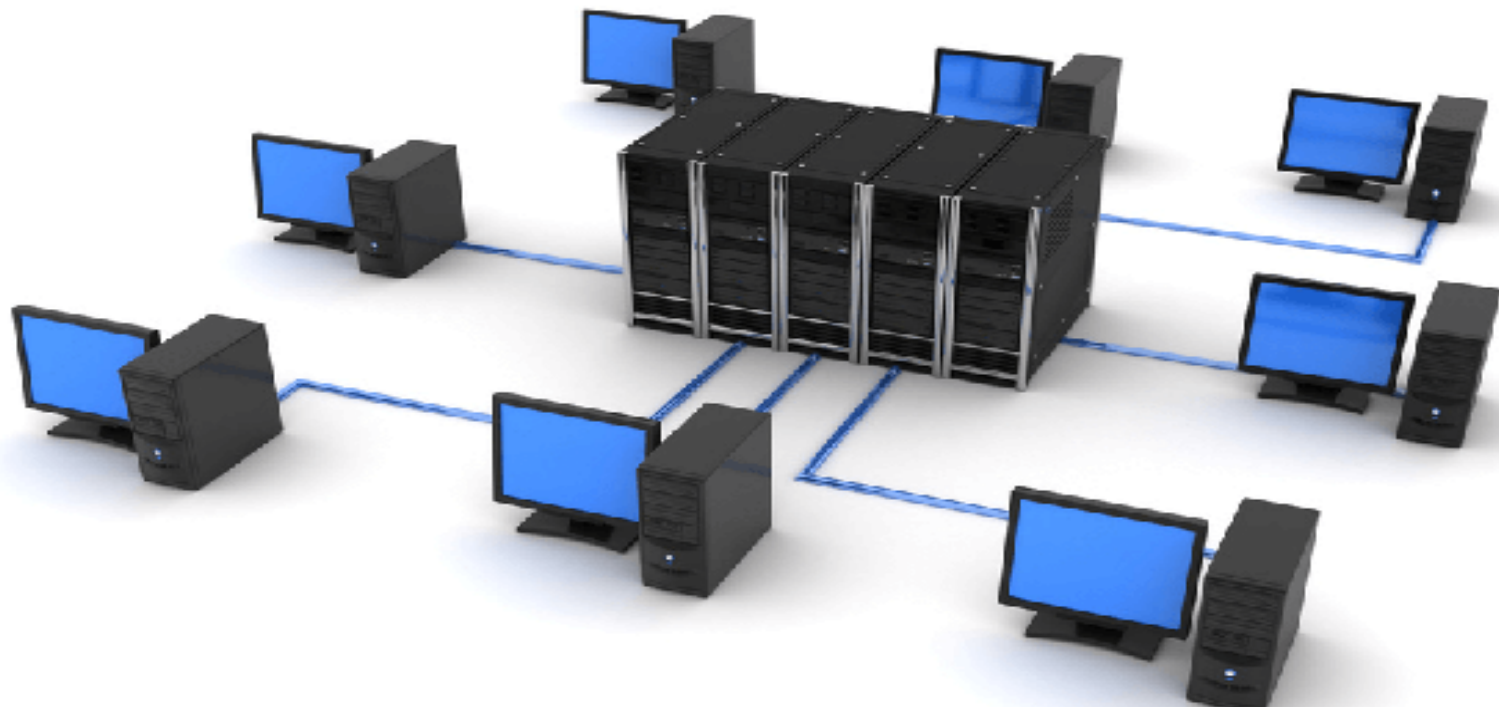




## A Vulnerability-Oriented Approach

- A vulnerability-oriented approach starts with a set of predisposing conditions or exploitable weaknesses/deficiencies in organizational information systems or the environments in which the systems operate, and identifies threat events that could exercise those vulnerabilities together with possible consequences of vulnerabilities being exercised.

# Diffusion of Viruses, Worms and Trojans





# Evidence Based Cybersecurity and Response Effectiveness (Example)





## Antivirus Programs and Companies



Microsoft®  
Security Essentials

<http://www.computerhope.com>





## Lévesque et al (2013)



38% of the study participants  
were exposed to malware

20% of the computers were  
infected by some form of malicious  
software that was not detected by  
the antivirus



## In conclusion,

- Risk assessments should be guided by the design of rigorous scientific studies and the collection of evidence which will provide more accurate probabilities of threats to develop
- Rigorous evaluations of the effectiveness of cybersecurity tools and policies could improve the security posture of organizations and individuals, and in turn, reduce the occurrence of successful cybercrime events
- To guide CISOs and GC decision making regarding security related issues, such information should be publicly available and accessible



David Maimon

Email: [dmaimon@gsu.edu](mailto:dmaimon@gsu.edu)

Website: [www.davidmaimon.net](http://www.davidmaimon.net)

Twitter: [@david\\_maimon](https://twitter.com/david_maimon)



Georgia State  
University