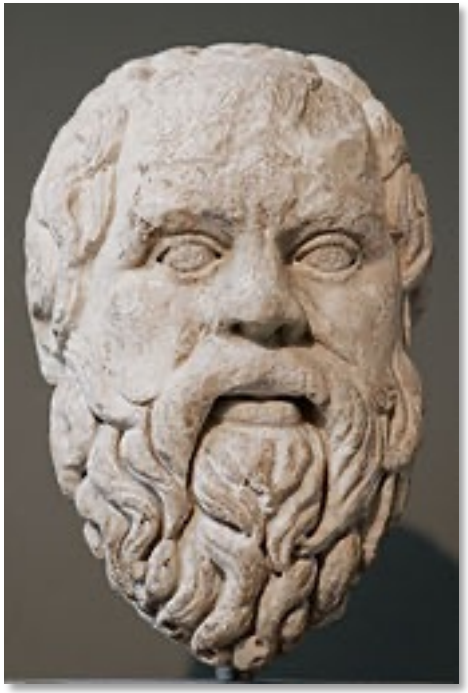
Law and Ethics

Fredrik Blix, 20211123

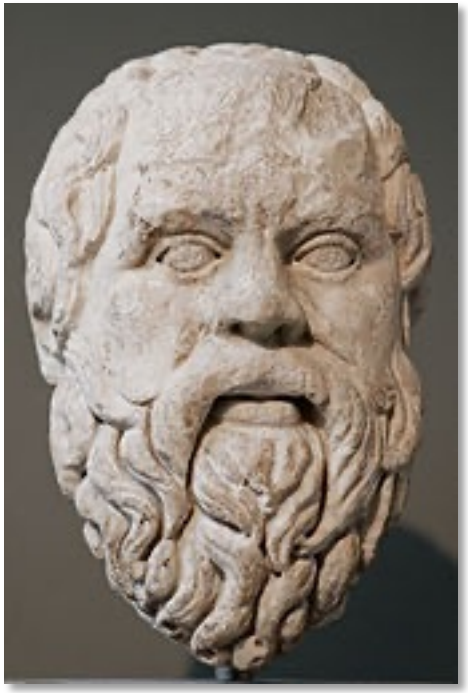


Agenda

- Part 1: 1500-1545
- Part 2: 1600-1645

Socrates

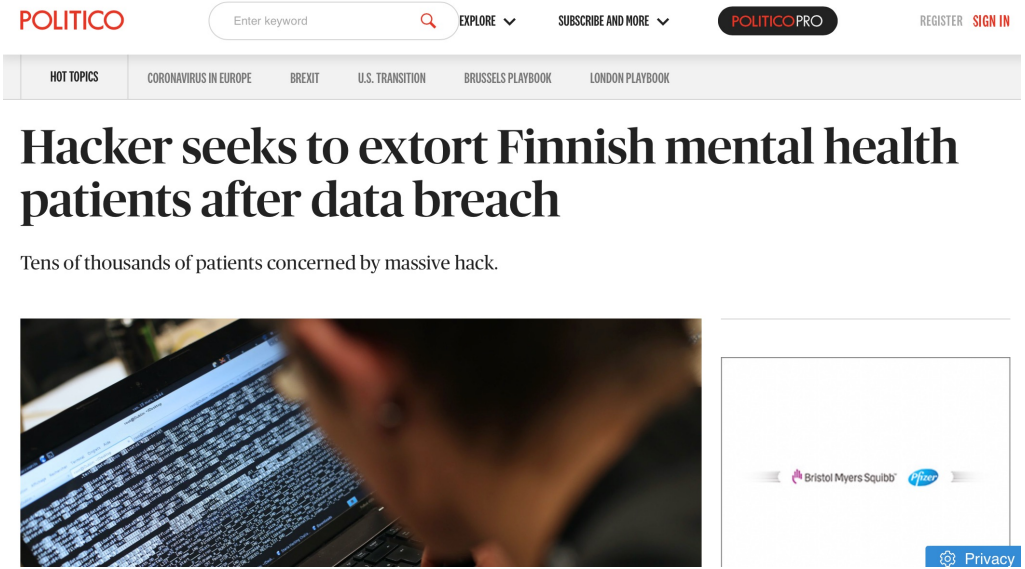
- Self-knowledge was considered necessary for success and inherently an essential good.
- A self-aware person will act completely within his capabilities to his pinnacle, while an ignorant person will flounder and encounter difficulty.
- To Socrates, a person must become aware of every fact (and its context) relevant to his existence, if he wishes to attain self-knowledge.
- He posited that people will naturally do what is good if they know what is right.
- Evil or bad actions are the results of ignorance.
- If a criminal was truly aware of the intellectual and spiritual consequences of his or her actions, he or she would neither commit nor even consider committing those actions.
- Any person who knows what is truly right will automatically do it, according to Socrates.
- While he correlated knowledge with virtue, he similarly equated virtue with joy.



What is the difference between law and ethics?

Why is ethics important in cybersecurity?

CASE 1: Ransomware



- 40000 patients
- Extorsion
- Data leak online
- Pay to not pay?

CASE 2: Bad procurement of system

Datainspektionen

OM OSS KONTAKTA OSS PRESS A-Ö IN ENGLISH

Sök frågor och svar, vägledning och regler...

AKTUELLT FRÅGOR OCH SVAR VÄGLEDNINGAR LAGAR OCH REGLER UTBILDNINGAR OCH KONFERENSER

Start → Nyheter → Allvarliga brister i Skolplattformen i Stockholm

Publicerad 2020-11-24

Allvarliga brister i Skolplattformen i Stockholm

Datainspektionen har granskat Skolplattformen, det it-system som används för bland annat elevadministration av skolor i Stockholm stad. Granskningen visar på brister i säkerheten som är så allvarliga att myndigheten utfärdar en administrativ sanktionsavgift på fyra miljoner kronor mot utbildningsnämnden i Stockholm stad.

Lyssna

Datainspektionen har tagit emot ett antal anmälningar om personuppgiftsincidenter från

- 4 MILLION SEK for you!
- Serious trouble in project.
- Leave or not leave?

CASE 3: You found something

DAGENS NYHETER. Nyheter Ekonomi Kultur Sthlm Gbg Sport Klimatet Leda Prenumer

Ekonomi

Idéer oskyddade hos myndighet

PUBLICERAD 2002-12-04

När statliga Vinnova och Nutek delade ut pengar till bästa affärsidéerna var det fritt fram för datakunniga att tjuvkika på konkurrenternas bidrag. Flera tävlande utnyttjade chansen, och riskerar nu polisanmälan.

- Found a HOLE!
- Should I tell them?

CASE 4: You found the virus author

melissaSent.htm
Press Release: Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison (May 1, 2002)

May 1, 2002

U.S. Department of Justice
United States Attorney for the
District of New Jersey
Christopher J. Christie, U.S. Attorney
Defense counsel:Ê Edward F. Borden
Jr., Princeton
970 Broad Street, Seventh Floor,
Newark, New Jersey 07102
Main Office: (973)645-2700
Public Affairs Office:Ê (973)645-2888

Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison

NEWARK - The New Jersey man accused of unleashing the "Melissa" computer virus in 1999, causing millions of dollars in damage and infecting untold numbers of computers and computer networks, was sentenced today to 20 months in federal prison, U.S. Attorney Christopher J. Christie and state Attorney General David Samson announced. David L. Smith, 34, of Aberdeen Township in Monmouth County, was ordered to serve three years of supervised release after completion of his prison sentence and was fined $5,000. U.S. District Judge Joseph A. Greenaway Jr. further ordered that, upon release, Smith not be involved with computer networks, the Internet or Internet bulletin boards unless authorized by the Court. Finally, Judge Greenaway said Smith must serve 100 hours of community service upon release. Judge Greenaway said the supervised community service would somehow put to use Smith's technology experience. Smith will be allowed to voluntarily surrender in the coming weeks, after the U.S. Bureau of Prisons designates a prison facility for him. On Friday, May 3 at 9 a.m., Smith also faces sentencing before state Superior Court Judge Lawrence M. Lawson in Freehold, Monmouth County. The state sentence is to run concurrently and co-terminously to the federal sentence. Smith pleaded guilty on Dec. 9, 1999, in state and federal court to computer-related crimes. The two prosecutions are the result of cooperative state and federal investigations of Smith, who, at his guilty pleas, admitted spreading the computer virus across North America from his home computer in Aberdeen Township.

His virus shut down the world!

Turn him in? Help the FBI to get him?

He may be put in jail

What to do?

Definitions

Moral : personal belief about right or wrong

Ethics : standard of expected behaviour by an individual or by a group

Laws: rules

Ethical Priciples

Consequence-based Principles

Egoism

The most personal good with the least consequence. Effects on others not relevant

Utilitarianism

The greatest collective good for all people with the least negative for all.

Rule-based principles

Individual rules

- Religion
- Experience
- Analysis

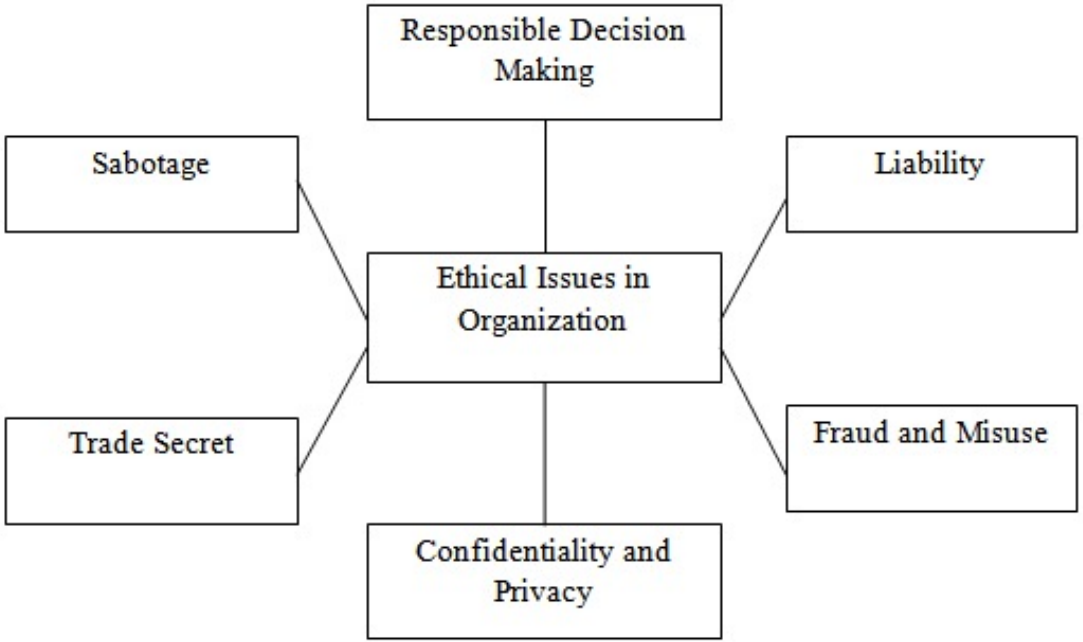
Universal rules

- The right to know
- The right to privacy
- The right to fair compensation

Code of professional ethics – ISACA members

- Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including audit, control, security and risk management.
- Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.
- Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.
- Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
- Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.
- Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
- Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

Ethical issues in organizations



Ethical analysis

- Understand situation
- Know theories of ethical reasoning
- List the ethical principles involved
- Determine which principles outweigh others
- Make and defend ethical choice

Legal aspects of information security?

- Is this important?
- How much of your work as a CISO or infosec consultant will be in the dealing with law?

Legal aspects

- Network and Information Security
- Data Protection
- Computer intrusion
- Trade secrets
- Record keeping (financial)
- Etc.

Stockholm University

How to handle legal requirements

1. Identify them
2. Interpret them
3. Implement solution
4. Check for compliance
5. GOTO 1

Law

- Criminal law
  - Statues, by government, jail and fines

- Civil Law
  - Contracts/common law, by government/ individuals/companies, damages (money)

Protecting intellectual property

- Copyrights (arts, literature, written text, movies)
- Patents (inventions, objects, processes)
- Trade secrets (secret information)
- DNS ENS names etc.
- Other new rights (in AR/VR)

Eu General Data Protection Regulation GDPR

- Controller, Processor, Data subject, Supervisory Auth.
- Management system for data protection
- Register of Processing Activities ROPA
- Data Subject Rights
- Data Protection Impact Assessment DPIA
- Risk assessment and selection of controls

Stockholm University

Discussion