OCIO ES

YOU are the Alpha and Omega of a secure future: *Explore, understand and practice your role in advancing a positive cybersecurity.* ***2019***

BRITISH COLUMBIA

Ministry of Citizens' Services

Welcome to the workshop

an opportunity to explore together the weakest link of cybersecurity

- PEOPLE

Alena Kottova, M.A., M.Sc., Ph.D.

- *Sessional Professor*
- Faculty of Engineering, University of Victoria
- Faculty of Social Sciences, Department of Philosophy
- akottova@uvic.ca

- *Sessional Professor*
- Faculty of Computing Science,
- Vancouver Island University
- alena.kottova@viu.ca

Kimberley Dray B.Ed. CISM CISSP GSEC

- Sr. Information Security Analyst /Cybersecurity Professional
- 20 years in the information technology and education sectors
- Multiple information security certifications
    - Recent: CISSP (ISC2), CCSP (ISC2), CISM (ISACA). GIAC-GSEC (SANS)
    - Old: MSCA, MCP, SCNP (SCP) and Linux +
- Bachelors of Education, Diploma in Information Technology, Diploma in Certified Network Security Analyst, Criminology Certificate
- ISACA Victoria Chapter Communications Director

Workshop overview

- Introductions & expectations
- The Landscape: what it is & what do we want it to be?
- Help from Ethics: How do we find out what decision is good in particular situation?
- Practical decision making: simple tool to explore
- Ethics vs law: understanding Privacy vs. Anonymity

- BREAK

Workshop Overview

- White, Black and Grey Hats
- Social Engineering 101 – in the shoes of a hacker
- Organizational view: Blue, Purple and Red teams
- Cybersecurity professional
- Closing discussion
- Feedback

- Good Byes

Working together

- We want to target situations relevant to YOU
- Explore & discuss openly and honestly
- Take a positive view of cybersecurity in our lives
- Create new micro-habits that we do not need to think about – like playing with juggling balls - try and practice

Work and PLAY

- **Play is an extremely important part of learning and adaptation**
- Helps to explore, create and learn new meanings (Vygotsky)
- creates a unique space that feels safe and encourages risk taking
- elements of playfulness: fun, spontaneity, relationship and connection, silliness or goofiness, creativity and imagination.
- proven to help to gain the self-confidence required to engage in new experiences and environments.
- positive affect such as fun, enjoyment, and laughter

Playfulness in Cybersecurity

- cybersecurity landscape shifts every year
- booming, immature industry
- serious shortfall of skilled graduates
- focus on developing individuals’ cybersecurity knowledge
- talent is put on the front line as quickly as possible
- WITH CARE and SUPPORT
- “Fake it till you make it” attitude forces you to “play” the role and therefore adopt the meanings and attitudes required by the field

Lets test our playfulness

- Turn to your partner, say hi, tell them your name
- Take a sheet of paper and pencil and get ready:

- You have 60 sec to draw/sketch a portrait of your colleague

- START

- FININSH

Introductions

- Answer the questions on your worksheet (cc 3 min)
- Fold the plane
- Get ready to fly …

- Collect one random plane
- Read the answers
- Discuss in group - combine results into 3 concerns (5 min)
- present to the class

Landscape

- Every company is a software company … technology company
- Every person is connected, often using a variety of computerized tools
- Every household is full of computerized tools

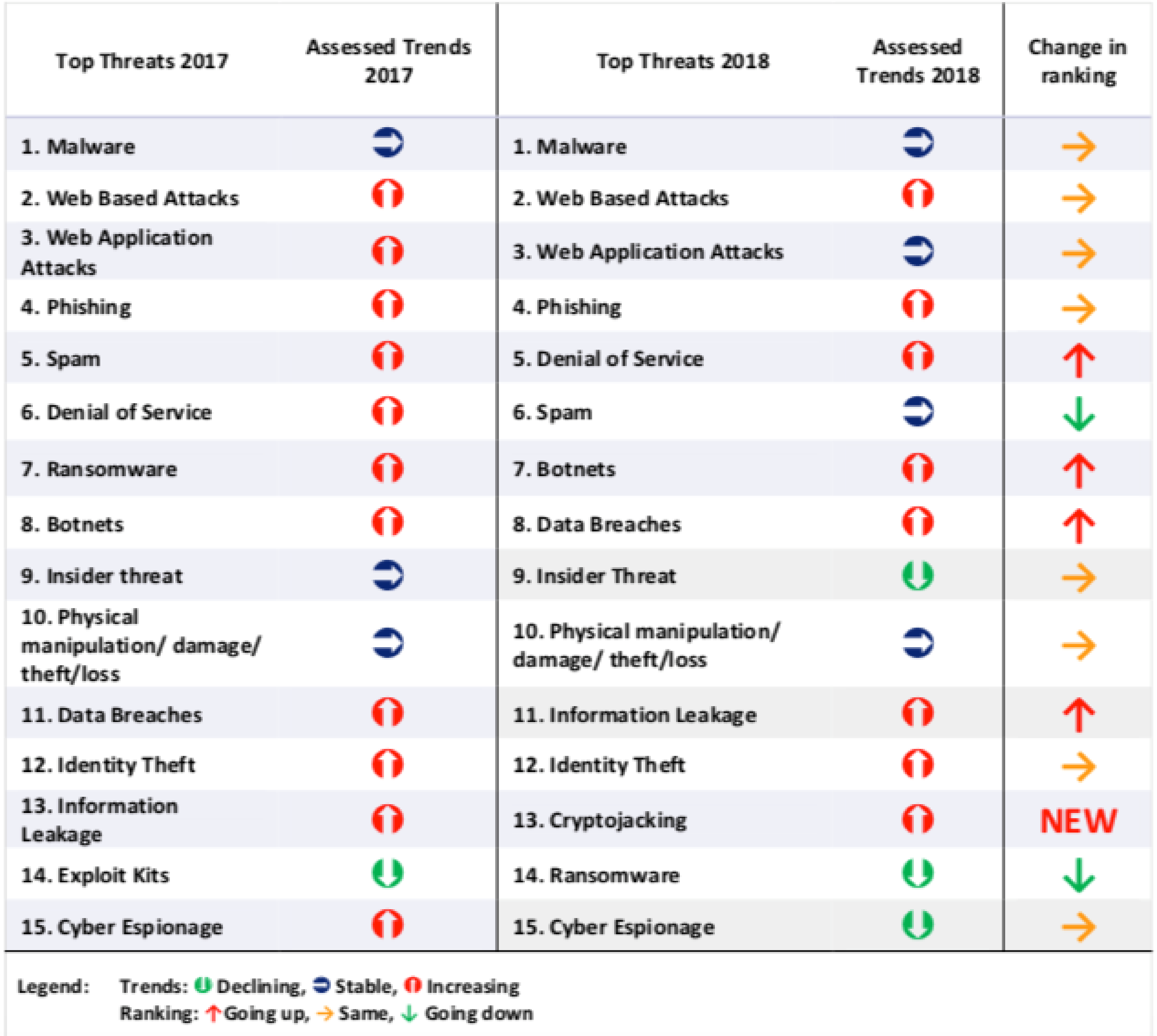
- And all is changing constantly and with increased speed!

- **CYBERSECURITY IS A PROCESS NOT A PRODUCT (**Bruce Schneier)

- Most software is poorly written and insecure
- Internet was never designed with security in mind
- Extensibility of computers means everything can be used against us
- The complexity of computerized systems means attack is easier than defense
- There are new vulnerabilities in the interconnections
- Computers tend to fail in many different ways
- Attacks always get better, easier, and faster **(**Bruce Schneier, Click here to kill Everybody)

ENISA 2018

- Mail & Phishing Messages became the primary malware infection vector
- Spear phishing & whaling is on the rise
- Trends in malicious attachments
- 80-98% of attacks could be prevented



Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⟳	1. Malware	⟳	→
2. Web Based Attacks	⇧	2. Web Based Attacks	⇧	→
3. Web Application Attacks	⇧	3. Web Application Attacks	⟳	→
4. Phishing	⇧	4. Phishing	⇧	→
5. Spam	⇧	5. Denial of Service	⇧	↑
6. Denial of Service	⇧	6. Spam	⟳	↓
7. Ransomware	⇧	7. Botnets	⇧	↑
8. Botnets	⇧	8. Data Breaches	⇧	↑
9. Insider threat	⟳	9. Insider Threat	⇩	→
10. Physical manipulation/ damage/ theft/loss	⟳	10. Physical manipulation/ damage/ theft/loss	⟳	→
11. Data Breaches	⇧	11. Information Leakage	⇧	↑
12. Identity Theft	⇧	12. Identity Theft	⇧	→
13. Information Leakage	⇧	13. Cryptojacking	⇧	NEW
14. Exploit Kits	⇩	14. Ransomware	⇩	↓
15. Cyber Espionage	⇧	15. Cyber Espionage	⇩	→

Legend: Trends: ⇩ Declining, ⟳ Stable, ⇧ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

ENISA 2018 - trends

- **Mail and phishing** messages have become the primary malware infection vector.
- **Web based** attacks continue to be observed as one of the most important threats due to their wide spread surface across the threat landscape
- **Cryptominers** have become an important monetization vector for cyber-criminals.
- **State-sponsored agents** increasingly target banks by using attack-vectors utilised in cyber-crime.
- Exploit Kits have lost their importance in the cyberthreat landscape.

ENISA 2018

- **Skill and capability building** are the main focus of defenders.
- Public organizations **struggle with staff retention** due to strong competition with industry in attracting cybersecurity talents.
- The **technical** orientation of most cyberthreat intelligence produced is considered an **obstacle towards awareness raising** at the level of security and executive management.
- Cyberthreat intelligence needs to respond to increasingly **automated** attacks.
- The emergence of **IoT environments** will remain a concern due to missing protection mechanisms.
- The **absence of cyberthreat intelligence solutions for low-capability organisations/end-user**s needs to be addressed by vendors and governments.

- These trends are influenced the way we build and use the technological tools.
- Need for user awareness – **“cybersecurity with human face”**
- Companies have tendency to limit use or track behavior – craze for data & data driven decisions
- **BUT**
- Careful review and in-depth though about the implications of these decisions are needed
- How do we know what is good or evil in particular situation?

Help from Ethics

- Ethics is not about **making a list** of good and bad acts,
- …. it’s about **creating a method**
- to evaluate each decision and each act from an ethical perspective.
- It needs to become a part of thinking, part of system design

Ethical thinking

- Every digital use decision is a decision **made on behalf of the users**.
- our **decisions impact the person** on the other end of the conversation.
- With every decision, we have the shared opportunity and **responsibility** to think about the ethics of the decisions,
- not just as a high flying ideal of "doing no harm" or doing the right thing, but **as a fundamental part** of our everyday process.
- allows understanding of the benefits & therefore the value to "customers" as well as to "adversaries"

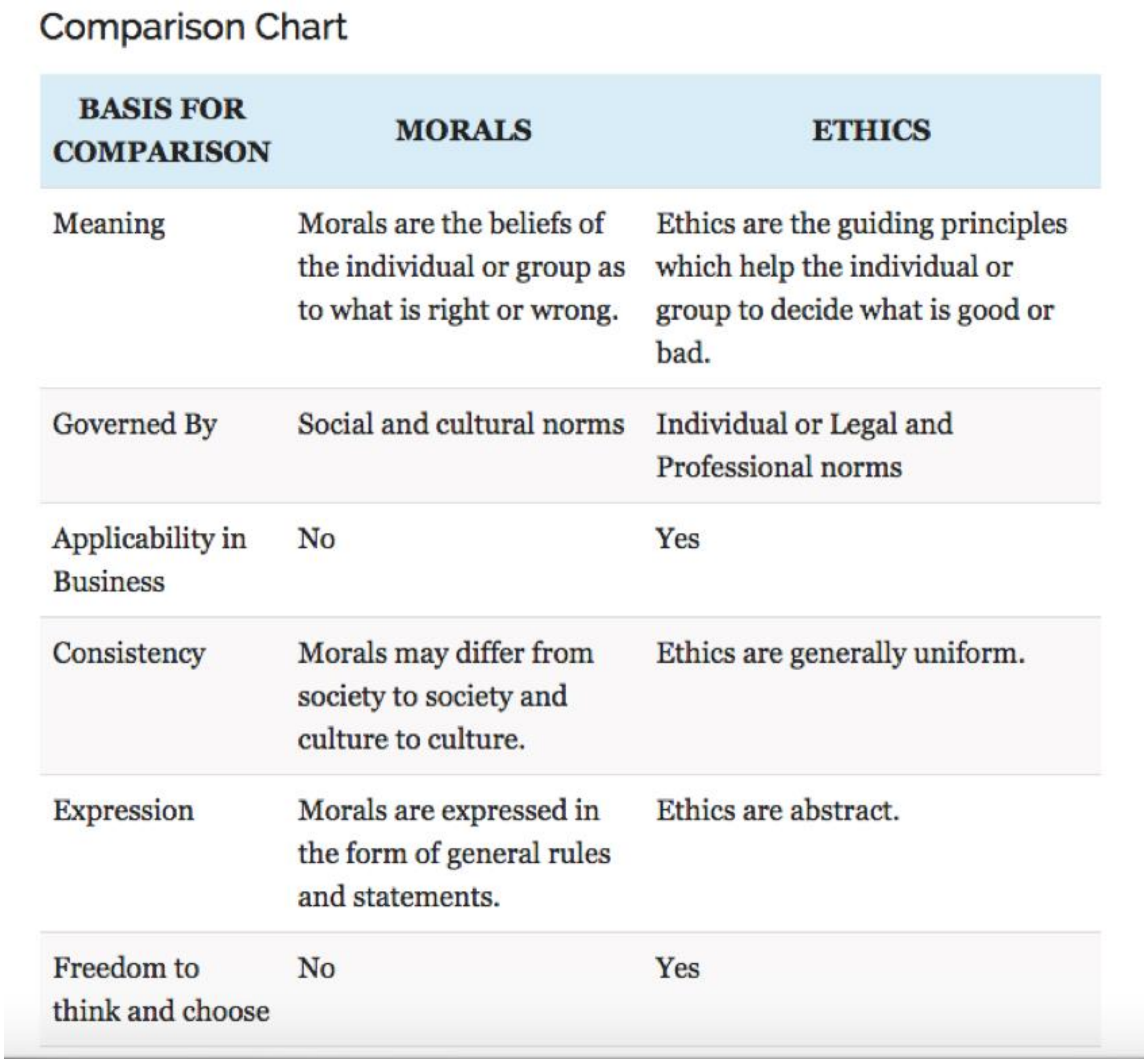
Ethics vs Morals

- **Morals** are the **social, cultural and religious** beliefs or values of an individual or group
- tells us what is **right or wrong,** what is acceptable behaviour and what is considered deviant behaviour.
- These are **rules** and standards made by the **society or culture** which is to be followed by us to be accepted by the society.

Ethics vs Morals

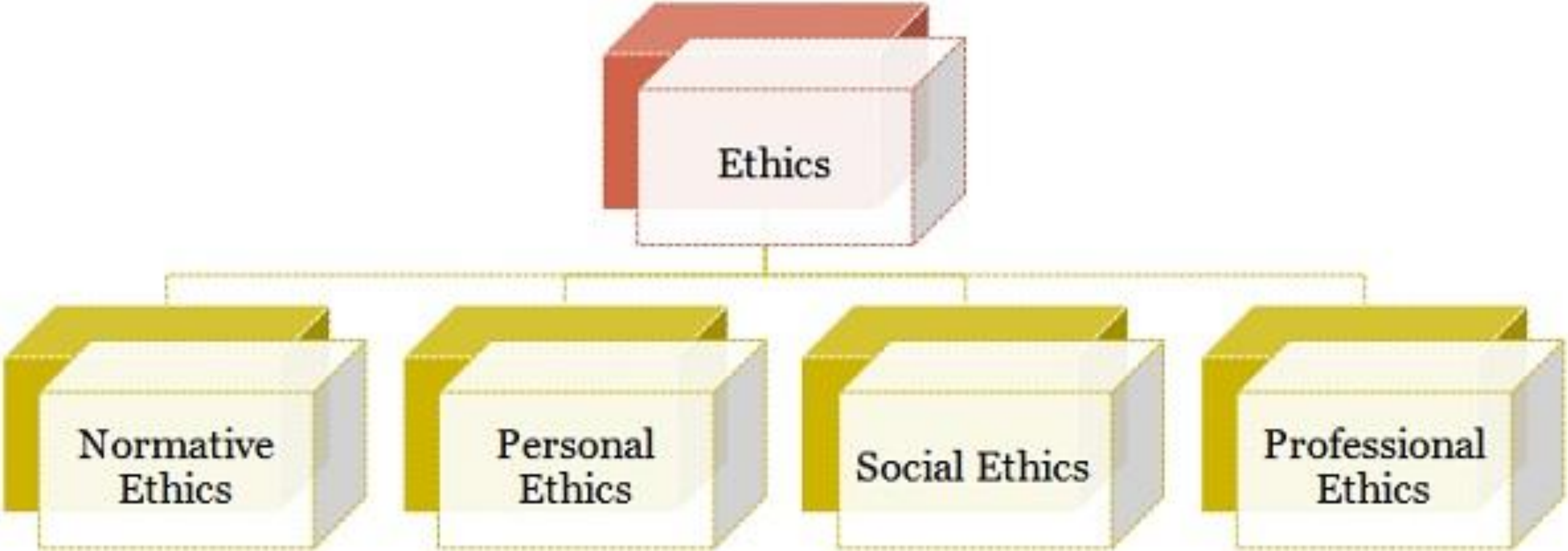
- **Ethics** is a **branch of philosophy**, a theoretical subject
- it deals with the **principles** of conduct of an individual or group.
- works as a guiding principle as to decide what is **good or bad**.
- They are the standards which govern the life of a person (regardless of society).
- these **standards** are explored in depth by philosophy; Ethics as moral philosophy.

Ethics vs Morals



Comparison Chart

BASIS FOR COMPARISON	MORALS	ETHICS
Meaning	Morals are the beliefs of the individual or group as to what is right or wrong.	Ethics are the guiding principles which help the individual or group to decide what is good or bad.
Governed By	Social and cultural norms	Individual or Legal and Professional norms
Applicability in Business	No	Yes
Consistency	Morals may differ from society to society and culture to culture.	Ethics are generally uniform.
Expression	Morals are expressed in the form of general rules and statements.	Ethics are abstract.
Freedom to think and choose	No	Yes



Ethics

Normative Ethics

Personal Ethics

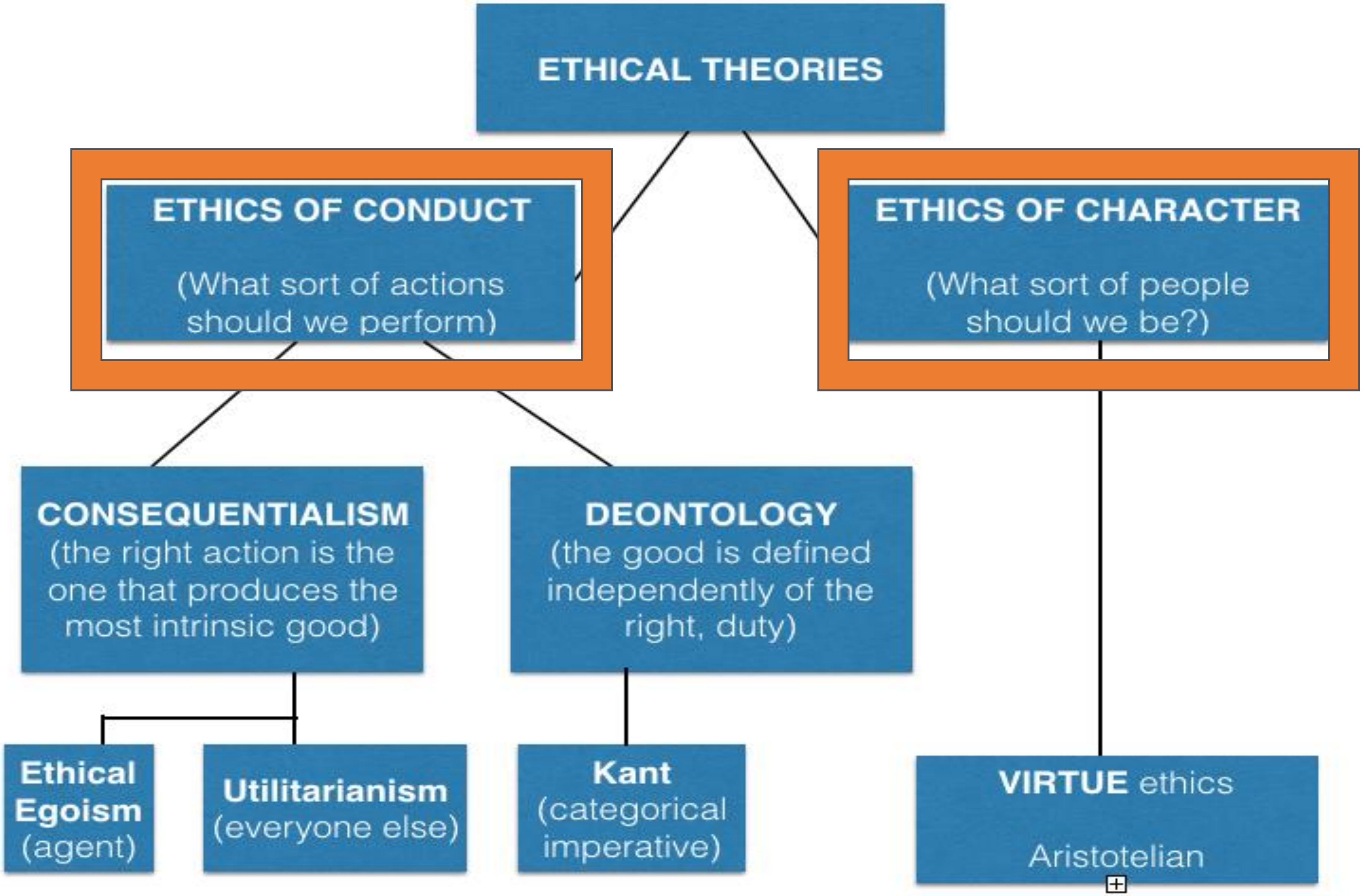
Social Ethics

Professional Ethics

Normative Ethics

- Examines **standards** for the rightness and wrongness of actions

- Three main approaches:
- **Consequentialism**
- **Deontology**
- **Virtue** ethics (ethics of character)



ETHICAL THEORIES

ETHICS OF CONDUCT

(What sort of actions should we perform)

ETHICS OF CHARACTER

(What sort of people should we be?)

CONSEQUENTIALISM (the right action is the one that produces the most intrinsic good)

DEONTOLOGY (the good is defined independently of the right, duty)

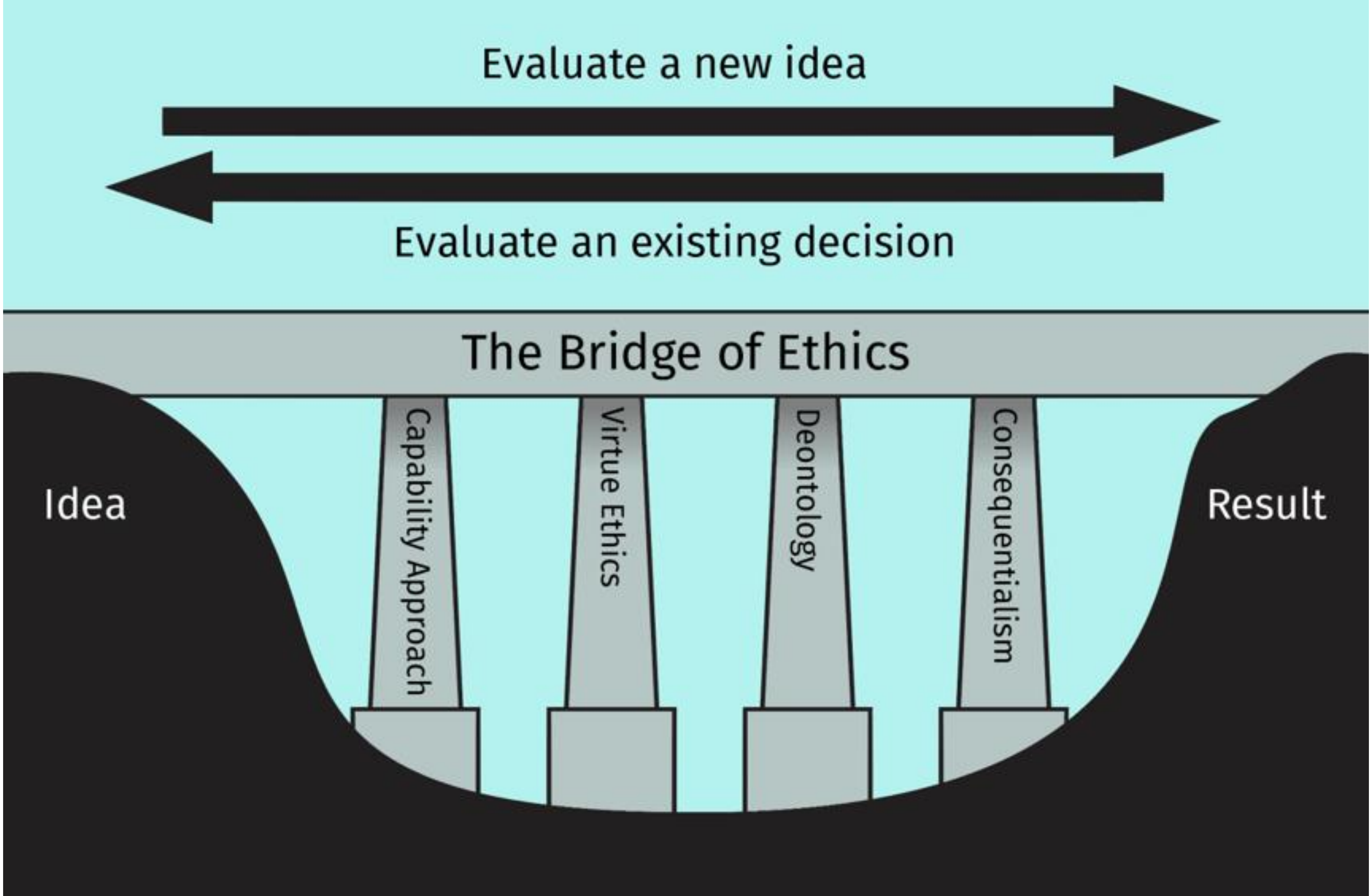
Ethical Egoism (agent)

Utilitarianism (everyone else)

Kant (categorical imperative)

VIRTUE ethics

Aristotelian



Evaluate a new idea

Evaluate an existing decision

The Bridge of Ethics

Idea

Capability Approach

Virtue Ethics

Deontology

Consequentialism

Result

Capability

- **Capability Approach:**

- What world are you building for the end-user?
- What capabilities are you granting or enabling?
- What limitations are you imposing?
- What dangers you mitigate and/or enliven

Virtue

- **Virtue Ethics:**

- What type of person do you become in the process?
- What type of person you force the customer/user to become?
- What virtue (good thing) you protect/establish?
- Whose virtue you protect/establish?

Deontology

- **Deontology:**

- What norms and expectations are you establishing?
- What duties you are upholding?
- How are you implementing your duties of care?

Consequentialism

- **Consequentialism:**

- What are the consequences of your decision?
- Do they improve the common good of those affected?
- Who (or how many) will benefit from the consequences?
- Who (or how many) might suffer by the consequences?

Lets try this

- Use the worksheet

- Select a question & imagine a scenario around that question.
- In groups discuss the four pillars, note FOR & AGAINST
- Come to decision

- Note the support to the decision within your team

Privacy versus Anonymity

What is the difference between having privacy and being anonymous?

What does it mean to have privacy?

What does it mean to be anonymous?

General personal safety and best practices with respect to our digital use and footprint

VPNs: Are they secure and what can they do for you?

Anonymity options: TOR , Darknet exploration, other tools & considerations

Privacy and Anonymity

- Focal Point is your IP and geo location

- Regular usage - saved passwords, links, bookmarks, recent files, Internet history details, etc. Ease of use. ☺

- Browsers in private or incognito mode
  - Local Network proxying and filtering - monitoring and logging
  - Internet Service Provider

  - Not very effective if hey have access to your laptop or your router logs and they want to check out your activities;
  - Use private mode and some clean-up plugins and possibly add a VPN client

Privacy

- Options:
  - Virtual Private Networks (VPNs)
  - Anonymizing Services i.e. TOR

Virtual Private Networks (VPNs)

- Acquire a different IP address as your destination
- Most, if secure and transparent are not free. @$10/month
- Login just like any other application with username and passwords. Few minutes to setup.
- VPN will provide you with privacy, but not necessarily anonymity
- VPN Service Provider knows your real IP
- Offers privacy, not anonymity

The layers of our cyberspace / the Internet

- Clear net /Surface Net

Regular indexed and searchable internet/web; No Login

- Deep Web /Dark Web?

Non-public internet resources requiring login or subscription only services

- Dark Web /Dark Web

Can only access via TOR

Anonymity Tools:
The TOR Browser and the Dark Net

- Comes configured with Firefox with default privacy, anti-tracking plugins (i.e. https everywhere, noscript)
- Several applications can expose your IP ie. Javascript, Torrents
- Tor Onion websites – hidden – access only from Tor network
  - Site owner and visitors cannot be traced
  - “hidden service protocol” via “onion routing”

TOR Network

Who’s Using it?

Free speech enthusiasts

Cybersecurity Professionals

Government Officials

Good law-sab ing dissident Journalists

Oppressed People

Policing and legal professionals

What can you find there?

How to obtain illegal drugs

Warez operations

Virus creation

Anonymous use of bitcoins,

Illegal pornography

Hacked PayPal accounts

How to hire contract killers

Sites to expose human rights abuse, political corruption, and government /politician scandals.

Deep Web

It is what these Deep Web resources and services are eventually used for that define their ethics.

Social Engineering 101

- YOU ARE THE TARGET!

- Based on the trends
  - Phishing attacks became more targeted.
  - Shift from consumer to enterprise targets.
  - Steady growth in mobile phishing attacks.
  - Rapid increase in phishing sites using HTTPS
  - The problem of Business Email Compromise (BEC or whaling)
  - Spearphishing is the de facto delivery method for APT groups.
  - Trends in malicious attachments.

White, grey and black hatters

- Not new terms.
- Black hats
- Grey Hats
- White Hats

- Sub type that can fall into any of the above categories:
  - Script kiddies
  - Hacktivists

Blue, purple and red teams – Corporate view

- Red Team
- Purple Team – temporary engagement?
- Blue Team

- Ideally red and blue work in harmony. No need for purple
- Goals shared between them: improve the security posture of the organization

Your Value as Target

- People often do not realize what value they have for an attacker
- We have hard time imagining the complex web of connections and interactions we participate in
- The complexity muddles our view of the possible connections points
- But the data available about you, your connections, your friends and family and their connections to friends and family and organizations et cetera … provide the opportunities for an attacker

Draft your value

- Check the worksheet
- fill in the possible connections
- How many companies do you – theoretically – provide access to?

Context

- Social context and news provide opportunities for an attacker

- Check the news worksheet
- What kind of messages you may get in your e-mail tempting you to click (and kill everybody)

Let’s see this in action

- https://phishingquiz.withgoogle.com/

The Cybersecurity Profession

- Organizational Size, Industry and Maturity Level
- Job Roles and Responsibilities
- Threats and What Keeps Us Up At Night
- How do we stay current or keep up?
- What are we/YOU doing about the so-called cybersecurity skills gap?

Certifications and Training

- Cybersecurity Certifications
  - ISC2 CISSP
  - ISACA CISM
  - ISC2 CCSP
  - GIAC-GSEC – SANS
- Websites: CodeAcademy
- Soft Skill development: Debate clubs, Toastmasters, Lunch and Learns, other public speaking opportunities

- Certification body official courseware: SANS, ISC2, ISACA,
- Cybrary.it
- Udemy
- LinkedIn Learning

- Local Meetup groups:

  Coding, Dev, Hack, etc.

What does a cyber professional do?

Types of tasks and activities

- Proactive Threat Prevention and Monitoring
- Phishing Mitigation and Response
- Data Loss Prevention Monitoring
- Anti-virus Administration, Management and Response
- Security Consults, Vulnerability and Risk Assessments and Reviews

Tools and processes

- Syslog Querying – bash / grep etc.
- Data Analysis, Aggregation and Correlation (Log Monitoring and Analysis)
- Host and Network Vulnerability Testing ie. Nessus, Wireshark
- Web Application Testing ie. Burpsuite, Acunetix, OWASP Zap Proxy
- SIEM Security Information and Event Management

Risk assessment, prevention and response

How do we stay current and keep up?

- Lifelong Learners
- Professional Mailing lists and security intelligence sharing
- Home Labs
- Local Meetups
- Online courses
- Conferences, webinars, workshops

We are our own enemies!

The So-Called Skills GAP

The so-called Skills Gap

- Imposter Syndrome
- Certifications or NOT
- Entry level options /Certs?
- Computer Science/Math backgrounds vs. Arts and Business
- Women in IT, Tech, Science and/or Cybersecurity Initiatives
- Technology, Coding and Cybersecurity Skills for K-12

- Our existing IT teams are doing security. You are doing security.
- We are all doing security and where there are gaps we seek training, knowledge sharing, and job shadowing opportunities.

Closing

- Please fill in the feedback card for us
- Feel free to contact us with questions, suggestions or stories.

- THANK YOU

Call to Action

- Consider your present digital usage and interactions:
  - Review all of your email and social media accounts, check privacy settings and clean them up. Great resource: https://www.lockdownyourlogin.org/
  - Get a Password Manager
  - Ensure there’s no Password Reuse
  - Use Two factor or Multifactor whenever it is offered
  - Don’t save passwords in your browsers or on websites
  - Only visit sites that use HTTPS but don’t assume they are safe sites. ☺
  - Use privacy plugins to prevent tracking and stop scripts from running
  - Research and consider use of a reliable virtual private network (VPN) client
  - Consider trying Tor only after you have investigated and explored safe ways to navigate

Resources and References

- Electronic Frontier Federation (EFF): https://www.eff.org/
- Tor Project: https://www.torproject.org/ (Tor Browser and the Onion Project)
- "Tor and the Deep Web: bitcoin, darknet and cryptocurrency in 2017-2018", by Lance Henderson
- "The Dark Web" – Geoff White and Bernard P. Achampong
- Dark Net – isn't what you think. Key to your privacy – Alex Winter (Bill & Ted) –https://www.youtube.com/watch?v=luvthTjC0OI
- Have I Been Pwned: https://haveibeenpwned.com
- How Secure Is Your Password: https://howsecureismypassword.net/
- Shining a Light on the Encryption Debate (L. Gill, T. Israel, C. Parsons): https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/
- VPN Comparison Chart: https://thatoneprivacysite.net/vpn-comparison-chart/

Cont.

- Bruce Schneier: Click here to kill everybody.
- Morten Rand-Hendriksen: Using Ethics In Web Design
- ENISA 2018
- Canadian Cybersecurity 2018
- A. Kottova: Course in Cybersecurity Ethics
- https://phishingquiz.withgoogle.com/