SEC_RITY IS NOT COMPLETE WITHOUT U!

Roy Campbell

Lecture 1: Motivation, Introduction, The importance of Information Assurance and the assessment of risk.

ABOUT THE INSTRUCTOR

- 43 years as Professor of Computer Science
- 3 years as Associate Dean of Engineering for IT
- 20 years as Director of NSA approved Center of Educational Excellence on Information Assurance
- 10 or more Projects in Cyber Security
- His PhD advisor was Brian Randell who discovered the existence of the Colossus machine – a British wartime effort at Bletchley Park to decode automatically German Encrypted war messages
- Now Emeritus Professor with Wife Ann and 6 grandchildren, 3 sons, 1 daughter
- Trisha Crowley, as his class moderator, will try to keep things running smoothly despite his help.


SECURITY CODE AUDITOR
my shitty code
imgflip.com

RULES OF THE ROAD

- Please ask questions but at allotted times (middle or end of lecture)
- Email rhc@Illinois.edu for more lengthy suggestions, questions, and comments.
- Many slides will have an attribution of the information source. If they don't, Google and Wikipedia can probably tell you.
- My knowledge is typical of some Professors – I know a lot about a very small amount of knowledge.
- Please don't expect me to be able to answer all your questions about Windows 11 or Apple Monterey 12.1. They were built after I retired.
- I have no idea about the inner motives of the government, industry, Russian mafia, or cyber criminals. They do all provide a good motivation for the employment of security professionals.
- There are no guarantees or safety assurances implied by anything I might say in class.

WEEK 1: INTRODUCTION

1. Motivation [9-19]:
   a) The Dark Web and Cost/Benefit of Cybercrime
2. A brief introduction to
   a) Information Assurance Principals [19-27]
   b) The Assessment of Risk [28-33]
   c) ATTACKS. An EASY EXERCISE [34-38]
3. GUIDELINES TO AVOID CYBER CRIME [39-63]
4. PASSWORDS [slide 64-69]
5. Cyber Warfare – Russia/Ukraine Cyberwar Part 1 [70-72]
6. Slaughterbots, MOVIES and references [72-]

WEEK 2: HOW CYBERSECURITY AFFECTS US ALL

- Infrastructure, Finance, Supply Chains and Denial of Service
- News, Reputation, Disinformation, Fake News
- Ransomware, Pfishing, Privacy, Property Theft
- Cloud hacks and data breaches.
- Practical Exercise in Computer Security
- Making your Home Computing Secure
- Russia/Ukraine Cyberwar maybe – Part 2

WEEK 3: IS IT POSSIBLE TO MAKE SOFTWARE, HARDWARE, AND NETWORKS SECURE?

- The fallibility of humans?
- What does theory tell us?
- The difficulties of governance, management, and maintenance.
- Encryption: its uses and abuses.
- Benefits and problems of artificial intelligence in cybersecurity
- The dark web. Cybercrimes. Mobiles. Bitcoin. The Great Firewall of China.
- Making your home network secure?
- Russia/Ukraine Cyberwar perhaps – Part 3

WEEK 4: CYBER WARFARE.

- Principles of Cyberwarfare
- War Games
- Resources
- Terrorist Networks and the Dark Web
- Trading in Weapons
- Examples taken from war games, pipeline attacks, the nuclear industry, invasions, drones, disinformation, SolarWinds, SolarStorm, Sunburst, grassroot revolution, ransomware
- Practical Exercise in Security: What you can do?
  - Democracy, Freedom of Information, Standards, Protection through Law
- Russia/Ukraine Cyberwar or maybe latest Cybercrime – Part 4

1. MOTIVATION

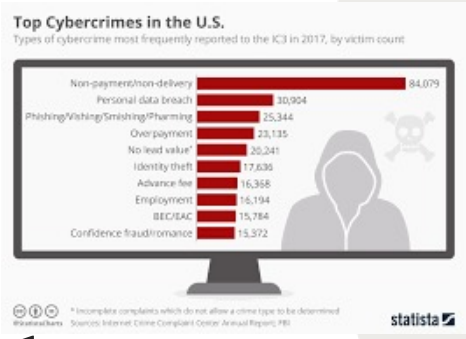
- Cyber Security essential for the technology underlying modern society
  - CyberSecurity is really about you
  - What do you want for your life?
  - What do you want for society?
  - What do you want for humanity?
- The Cost/Benefit of Privacy, CyberSecurity, Cyber Attacks, Cyber Crime, Cyber Warfare

TOTAL COST OF CYBERCRIME2021

$6 trillion USD

https://cybersecurityventures.com/cybersecurity-almanac-2022/

HOW MUCH DOES CYBERCRIME COST US?



- In general, the average cost of a cyber attack in 2020 was ***around $133,000***. That is the total average of all types of cyber attacks.
- Cyber crime costs have grown 15% per year annually over the last 5 years.

Cybersecurityventures.com

HOW MUCH DOES A CYBERCRIME TOOLKIT COST?

- spearphishing attacks between $100 and $1,000. Spear phishing is a fishing scam targeting a specific individual, organization or business.
- single ransomware kit as little as $66.
- $311 DDoS attacks against a specific website.

https://www.privacyaffairs.com/dark-web-price-index-2021/

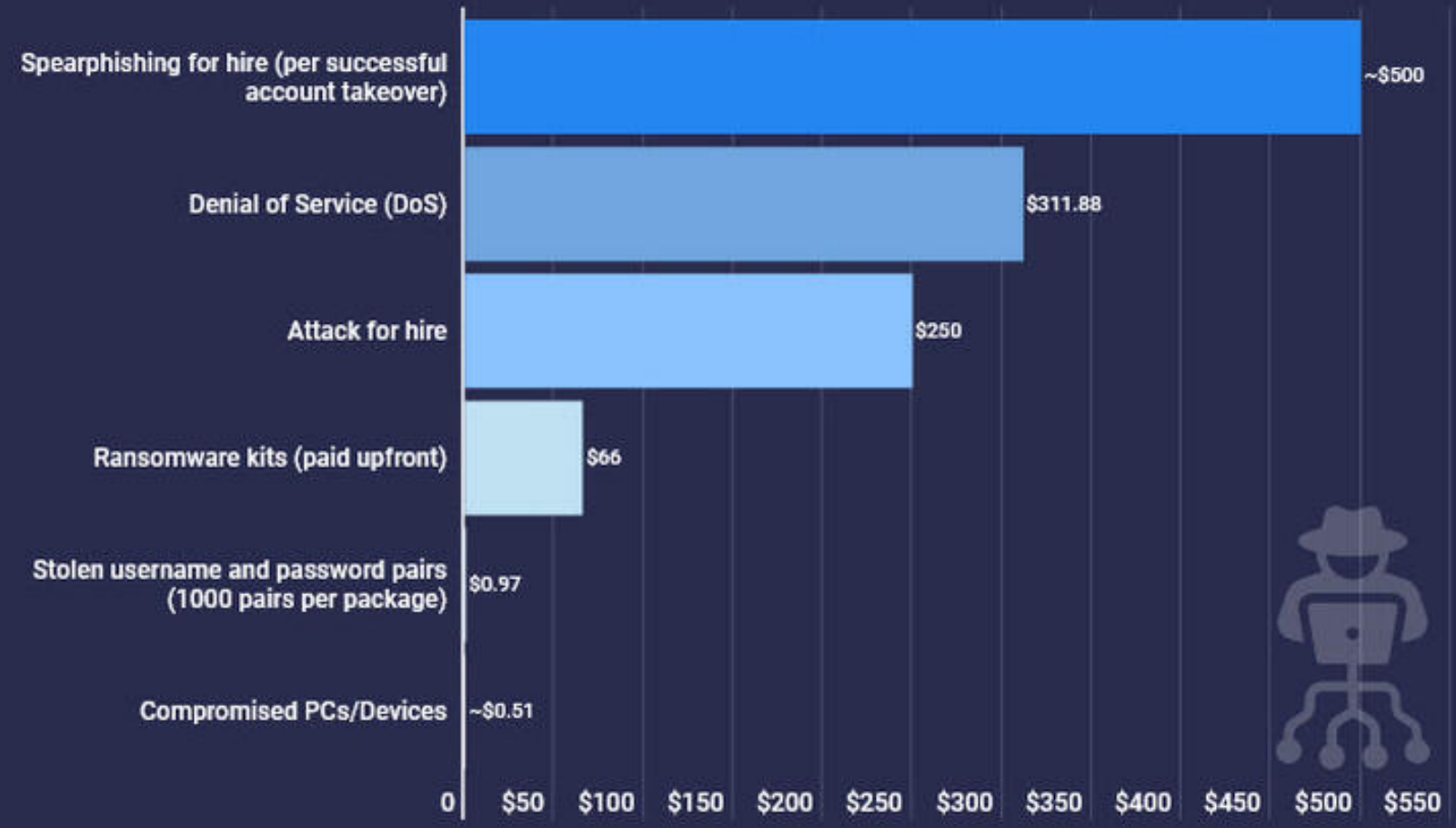
HOW MUCH DOES A CYBERCRIME TOOLKIT COST

- Stolen account credentials sell for as little as 97 cents per 1,000. (Most sellers don't guarantee that the credentials will work.)
- A single hacker job typically costs around $250

https://www.privacyaffairs.com/dark-web-price-index-2021/

Average prices of cybercrime services for sale in 2021

Information: these illicit things are sold on the dark web. The dark web is a network-encrypted area that requires special software to access. Furthermore, most marketplaces require an invitation to enter. Cybercriminals use this method to shield themselves from unwanted attention.



Source: Microsoft

atlasVPN

DARK WEB PRICE INDEX 2021

Info reflects data updated on September 9 2021.

- https://www.privacyaffairs.com/dark-web-price-index-2021/

RATE YOUR CRIMINAL SERVICE

Feedback received as vendor [1 - 20 of 53]

First 1 2 3 Last

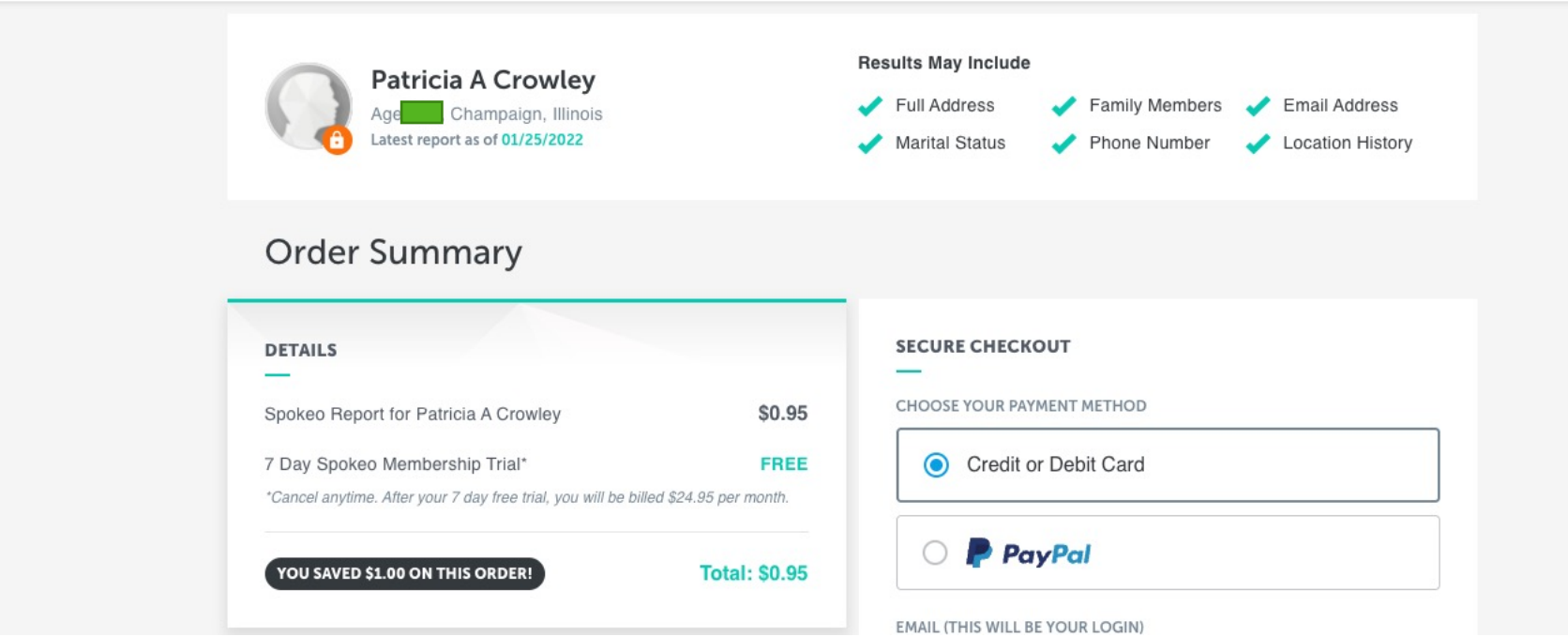
Rating	Listing Title	User Comment	Date
5 / 5	(Premium) North Carolina Fake ID/Drivers License w/ Tracking (NC)	None left	2021-02-02
5 / 5	(Quality) New Jersey Fake ID/Drivers License w/ Tracking (NJ)	great id. will be back	2021-02-01
5 / 5	(Quality) Missouri Fake ID/Drivers License w/ Tracking (MO)	ids are amazing	2021-02-01
5 / 5	(Quality) Pennsylvania Fake ID/Drivers License w/ Tracking (PA)	This is my 7th purchase with this vendor and i received the id everytime quickly and the work is actually better then qualityfakeids And the jackass that said this vendor sent a book thats impossle just another LIEING cheapskate trying to get this vendors work for free BUY WITH CONFIDENCE, BEST FAKE REAL IDS ON HERE ! Infact my first ever buy was not on here so this vendor can be trusted off here	2021-01-30
5 / 5	(Quality) Indiana Fake ID/Drivers License w/ Tracking (IN)	a1	2021-01-30
5 / 5	(Premium) Texas Fake ID/Drivers License w/ Tracking (TX)	goated	2021-01-29

PERSONAL INFORMATION AVAILABLE LEGALLY

E.g. Spokeo.com, RocketReach

beenverified.com, peoplesmart.com

SPOKEO



2020 VICTIMS BY AGE GROUP

Victims		
Age Range[7]	Total Count	Total Loss
Under 20	23,186	$70,980,763
20 - 29	70,791	$197,402,240
30 - 39	88,364	$492,176,845
40 - 49	91,568	$717,161,726
50 - 59	85,967	$847,948,101
Over 60	105,301	$966,062,236

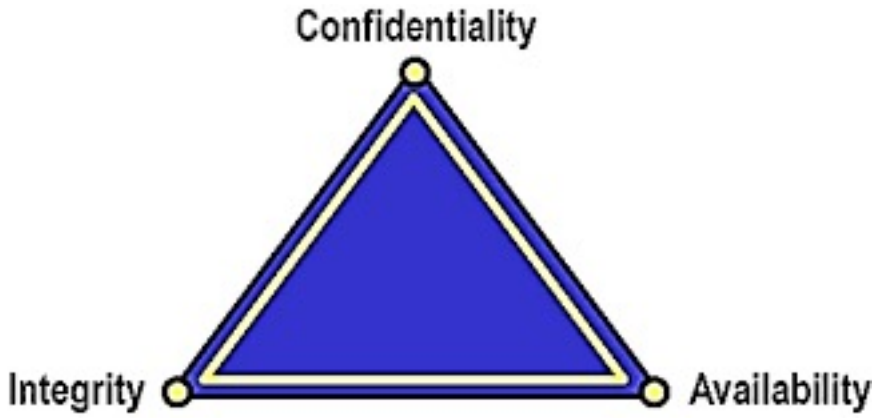
Source: FBI/IC3 - Internet Crime Report
https://www.computerweekly.com/opinion/The-shape-of-fraud-and-cyber-crime-10-things-we-learned-from-2020

2. INTRODUCTION

A brief history of the importance of Information Assurance, Computer Security Principles, and the Assessment of Risk.

2A INFORMATION ASSURANCE AND ITS PRINCIPLES

- Measures that protect and defend information and information systems or CIA
- ***Confidentiality,***
- ***Integrity, and***
- ***Availability*** along with
- Authentication and
- Non-repudiation



CONFIDENTIALITY

Information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO 27000, Common Criteria ISO/IEC 2014)

Note: Privacy ≠ Confidentiality.
Confidentiality is a component of privacy that implements to protect our data from unauthorized viewers.

INTEGRITY

Maintaining and assuring the accuracy and completeness of data over its entire lifecycle. (ISO 27000, ISO/IEC 2014)

Note: involves human/social, process, and commercial integrity, as well as data integrity. Touches on aspects such as credibility, consistency, truthfulness, completeness, accuracy, timeliness, and assurance

AVAILABILITY

Information should be consistently and readily accessible for authorized parties.

Make ***security audits routine***. Auto-update or stay abreast of system, network, and application updates.

AUTHENTICATION

- Authentication is the act of verifying a claim of identity.
- Something you know:
  PIN, password, or your mother's maiden name
- Something you have:
  driver's license or a magnetic swipe card
- Something you are:
  biometrics, including fingerprints, voice prints

AUTHORIZATION

After identification and authentication, then it must be determined what informational resources a person, program, or computer can be permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change).

ACCESS CONTROL

- Non-discretionary consolidates all access control under a centralized administration
- Need-to-know principle gives access rights to a person, program, or computer to perform their job functions
- Mandatory access control approach, access is granted or denied basing upon the security classification assigned to the information resource.
    - Role-based access control
    - File permissions
    - Group policy objects
    - Kerberos
    - Simple access lists

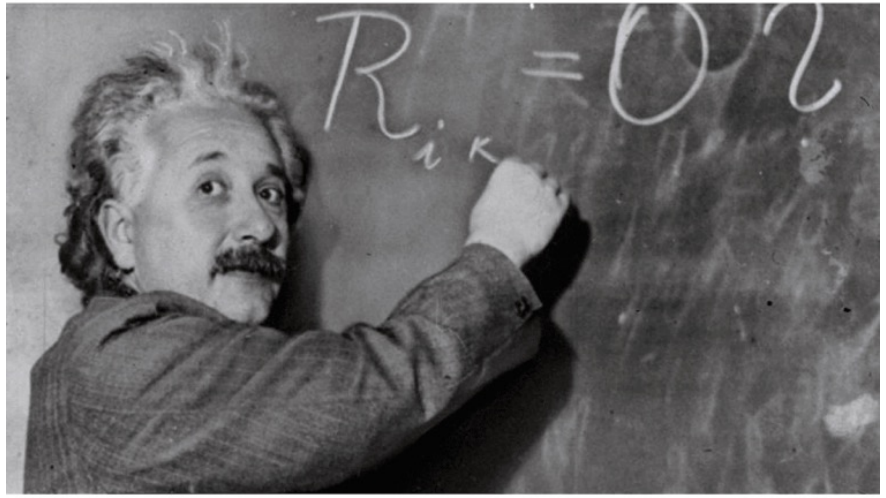
NON-REPUDIATION

- Non-repudiation implies one's intention to fulfill their obligations to a contract.

It also implies that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction.

2 A brief history of Information Assurance

How I think I look explaining cyber risk to the board



How I actually look

2b The Assessment of Risk

CYBER RISK

Cyber risk, or cybersecurity risk, is the potential exposure to loss or harm stemming from an organization's information or communications systems.

Two frequently reported examples of cyber risk:

1. Cyber attacks, or
2. Data Breaches

CYBER RISK

However, cybersecurity risk extends beyond:

a. damage and
b. destruction of data or
c. monetary loss

and encompasses:

d. theft of intellectual property
e. productivity losses, and
f. reputational harm.

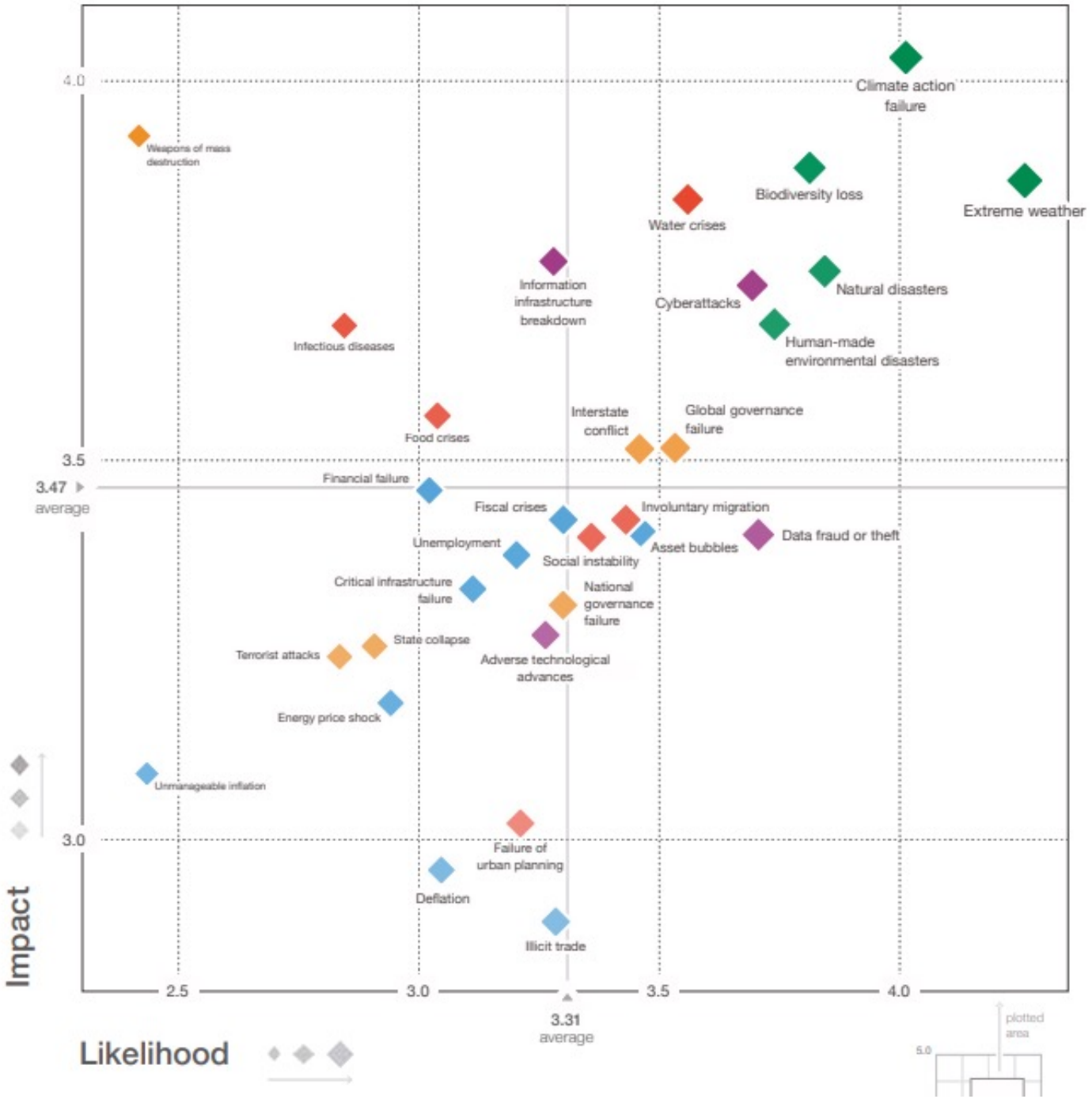
CYBER RISK

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

i) the adverse impacts that would arise if the circumstance or event occurs; and

ii) the likelihood of occurrence.

A 2020 report suggests that cyberattacks on infrastructure were the fifth top risk of the year. Not only that but it is expected that the cost of cybercrimes might reach $10.5 trillion dollars by 2025.



THE GLOBAL RISKS LANDSCAPE 2020

World Economic Forum Global Risks

PARALLEL CYBERSPACE.

- Connectivity depends on internationally established protocols.
- Historically, multilateral stakeholders have tended to favour a fairly open and loosely regulated cyberspace.
- However, current international developments point to an increased risk of divergence in protocols—old and new—that could lead to fragmentation of cyberspace and future technologies.

  (Example of DNS and Blockchain DNS in later lecture.)

2C) TOP 10 CYBER ATTACKS IN HISTORY

1999 Melissa Virus (David Lee Smith) sending users file opened by Microsoft Word. Estimated cost of repairs $80M.
1999 Nasa Cyber Attack (James Jonathan 15 years old) hacked and shutdown NASA's computers for 21 days. Cost of repairs $41,000.
2007 Estonia Cyber Attack (Konstantin Goloskokov) First cyber attack on an entire country: over 58 Estonian government, banks and media outlets websites went offline.

TOP 10 CYBER ATTACKS IN HISTORY

2011 A Cyber Attack on Sony's PlayStation Network (criminal data breach and cyber attack "We are Legion" file) A cyber attack on Sony's PlayStation Network claimed the personal information of 77M users.

2013 Adobe Cyber Attack Cyber attack/Data Breach compromised the personal data of up to 38M users! 2.9M user's passwords and credit card information compromised, and 35.1M suffered the loss of their passwords and IDs.

TOP 10 CYBER ATTACKS IN HISTORY

2014 Cyber Attack on Yahoo 500M accounts were compromised. Basic information and passwords were stolen, whereas bank information was not.

2015 Ukraine's Power Grid Attack (Sandworm, Russia) First cyberattack on a power grid left around half of the homes in the Ivano-Frankivsk region in Ukraine without power in 2015 for a few hours.

2017 WannaCry Ransomware Cyber Attack (North Korea agents) 200,000 computers were affected in more than 150 countries. Data was encrypted and ransomed. Massive impact across several industries and had a global cost of about 6B pounds!

TOP 10 CYBER ATTACKS IN HISTORY

2018 A Cyber Attack on Marriott Hotels went unnoticed for years
An estimated 339M guests have had their data compromised. This had led the UK's data privacy watchdog to fine the Marriott Hotels 18.4M pounds.
2021 Rock You widget maker for compilation of about 8.4B passwords were leaked. Rock You declared bankruptcy.

EASY EXERCISE

- https://haveibeenpwned.com/
- Have a look to see if any of your old account names or passwords have been collected by hackers.

3. GUIDELINES TO AVOID CYBER CRIME

- 15 tips on how to protect yourself.
- Be proactive, don't wait until its too late.
- Keep your possessions safe: Back them up, keep multiple copies, encrypt useful data, check up on your possessions, don't trust anything on-line, keep paper copies, avoid telling other people information about your on-line accounts.
- Contact the authorities when something goes wrong.

1) USE A FULL-SERVICE INTERNET SECURITY SUITE

Most provide real-time protection against existing and emerging malware including ransomware and viruses, and help protect your private and financial information when you go online.

Both Macs and Windows already have some security provisions, we will in future lecture.

TREND MICRO™

McAfee™

Norton

Bitdefender

2) USE STRONG PASSWORDS

- Don't repeat your passwords on different sites.
- Change your passwords regularly.
- Make them complex, no dictionary words.
- Combinations of at least 12 letters, numbers, and symbols.
- A password manager or secure browser can help you to keep your passwords locked down and remember them.

To be discussed later

3) DON'T FALL FOR POP-UPS

- Beware of fraudulent emails and text messages!
- If an email or pop-up window asks you to enter username or password, don't do it. Instead, open your browser and visit the site directly.
- If you are yet not convinced, then contact the company or entity that supposedly got to you.
- Know that established and recognized companies will never ask you for your login information through an email.

4) UPDATE SOFTWARE

- This is especially important with your operating systems and internet security software.
- Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system.
- Patching those exploits and flaws can make it less likely that you'll become a cybercrime target.


MY CYBERSECURITY PROGRAM
OUTDATED CERTIFICATES
IMPROPERLY ENCRYPTED DATA
WEAK PASSWORDS
Balbix

5) MANAGE SOCIAL MEDIA

- Keep your personal and private information locked down.
- Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better.
- For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.

6) STRENGTHEN YOUR NETWORK

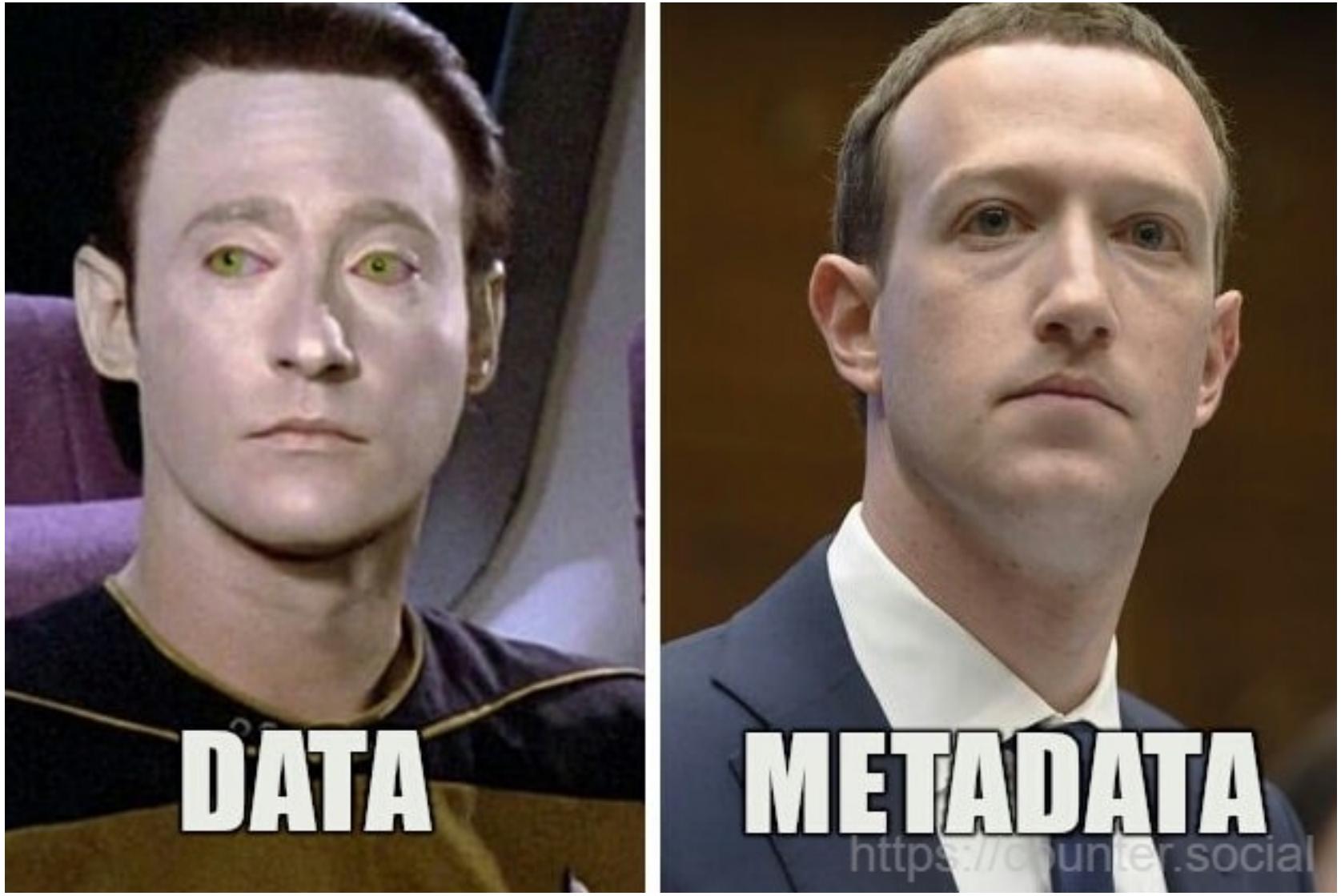
- It's a good idea to start with a strong encryption password as well as a virtual private network.
- Change the default password!
- A VPN will encrypt all traffic leaving your devices until it arrives at its destination.
- If cybercriminals do manage to hack your communication line, they won't intercept anything but encrypted data.
- It's a good idea to use a VPN whenever you use a public Wi-Fi network, whether it's in a library, café, hotel, or airport.

7) TALK TO YOUR GRAND CHILDREN ABOUT THE INTERNET

- You can teach your grand kids about acceptable use of the internet without shutting down communication channels.
- Make sure they know that they can come to you if they're experiencing any kind of online harassment, stalking, or bullying.

8) KEEP UP TO DATE ON MAJOR SECURITY BREACHES

If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately.


DATA
METADATA
https://counter.social

9) TAKE MEASURES TO HELP PROTECT YOURSELF AGAINST IDENTITY THEFT

- Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. How? You might be tricked into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. That's why it's important to guard your personal data.
- A VPN — short for virtual private network — can also help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.


SHOULD WE BE CONCERNED ABOUT CYBERSECURITY, PARTICULARLY IDENTITY THEFT?
NAH, WE'RE FINE. WHAT'S OUR NETWORK PASSWORD AGAIN?
Infosys

10) KNOW THAT IDENTITY THEFT CAN HAPPEN ANYWHERE

- It's smart to know how to protect your identity even when traveling.
- There are a lot of things you can do to help keep criminals from getting your private information on the road.
- These include keeping your travel plans off social media and using a VPN when accessing the internet over your hotel's Wi-Fi network.

WHAT'S A HACKER'S FAVORITE SEASON?

Phishing season.

11) KEEP AN EYE ON THE GRAND KIDS

- Just like you'll want to talk to your grand kids about the internet, you'll also want to help protect them against identity theft.
- Identity thieves often target grandchildren because their Social Security number and credit histories frequently represent a clean slate.
- You can help guard against identity theft by being careful when sharing your grandchild's personal information. It's also smart to know what to look for that might suggest your child's identity has been compromised.


Son, you're old enough now for THE TALK.
You know, about CYBER SECURITY.
Tell me what I need to know.
©MIT

12) KNOW WHAT TO DO IF YOU BECOME A VICTIM

If you believe that you've become a victim of a cybercrime, you need to alert the local police and, in some cases, the FBI and the Federal Trade Commission.

This is important even if the crime seems minor.

Your report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future.

13) PROTECT YOUR FINANCIAL DETAILS

- Remember this: Legitimate banks or companies will never ask for any personal details or ask you to transfer money into an account.
- People face fraudulent who are looking to steal money or personal information by asking people to fill some random online forms with their details.

.

AND WHEN YOU CANT AVOID CYBER CRIME

If you think cybercriminals have stolen your identity. These are among the steps you should consider.

1. Inform the local police.
2. Contact the companies and banks where you know fraud occurred.
3. Place fraud alerts and get your credit reports.
4. Report identity theft to the FTC.

"WELL, I *TOLD* YOU NOT TO OPEN THAT ATTACHMENT!"

14) SECURE YOUR COMPUTER AND MOBILE DEVICES

- Firewalls are the first line of cyber defence – activate it. It blocks connections to unknown or bogus sites and will keep various viruses and hackers.
- Use anti-virus/ malware software. Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.
- For mobile devices, keep certain things in mind like download applications from trusted sources, install the latest OS updates, keep your applications and operating system current with the latest system updates.


OUR DEVICES ARE NOW 100% SECURE.
I TURNED THEM ALL OFF.
HOW DID YOU DO THAT?
© D.Fletcher for CloudTweaks.com

15) PROTECT YOUR DATA

- Critical and sensitive files like tax returns and financial records need to be protected – use encryption.
- Moreover, make regular backups for your essential data and store it in another location.
- Don't just copy files to another disk.
  Read more: Date Breach and Cybersecurity: Highlighting Possible Challenges and Solutions

KEY TAKEAWAYS:

- You must be worried about your online banking, credit card or financial activities. This would make you skeptical about cyber-crime.
- Focus on what you can do to protect your device and data.
- Keep complicated passwords, and don't allow others to visit your password-protected sites in your absence.
- Avoid uncertain sites and chatrooms.
- Encrypt sensitive files.
- Keep backups of important data on isolated storage.
- Don't respond on pop-ups, texts and emails that ask your login information.
- Look for a secured VPN connection and don't share your details with strangers.

4. PASSWORDS

"Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers."

– Chris Pirillo

WHAT IS A STRONG PASSWORD?

- Is at least 12 characters long. The longer your password is - the better.
- Uses uppercase and lowercase letters, numbers and special symbols. Passwords that consist of mixed characters are harder to crack.
- Doesn't contain memorable keyboard paths.
- Is not based on your personal information.
- Password is unique for each account you have.
- Avoid past passwords

DO'S IF YOU MUST REMEMBER YOUR PASSWORD

- ***Use a password generator***
- ***Choose a passphrase rather than a password***

My friend Matt ate six doughnuts at the bakery café and it cost him £10	MfMa6d@tbc&ich£10

- ***Opt for a more secure version of dictionary method***

Jigsaw, quest, trait, fork	Jigsaw%Quest7trait/fork48

PASSWORD STRENGTH

- https://www.security.org/how-secure-is-my-password/

#Characters	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*11*	*12*	*12*	*16*
Easy to Read	e&89Z	s5Q54#	A9s3T^Y	vG3^8Epf	#99&Dmw9t	!S#Cy$n556	7562989777 4	6NxxrA#n46A	tBISyxpzxSvV	4VMA#y8qjtr#	★^mTEZy$0N4LD10c
Time to Crack	67ms	5 secs	6 min	8 hrs	3 wks	5 yrs	2 secs	400 yrs	300 yrs	34000 yrs	1 trillion years
	LNS	LNS	LNS	LNS	LNS		Numbers	Mix	Letters	LNS	LNS

PASSWORD STRENGTH

#Characters	*5*	*6*	*7*	*8*
Easy to Read	word	word5	word56	word567
Time to Crack	instant	1 ms	54 ms	1 s
	LNS	LNS	LNS	LNS

TEST YOUR OWN PASSWORDS

https://www.security.org/how-secure-is-my-password/

We will talk about how passwords are cracked and about encryption next week.

A NEW DIGITAL ARMS RACE.

- Digital dependency is changing the nature of international and national security, raising three urgent issues:
  a) how to protect critical infrastructure,
  b) uphold societal values and
  c) prevent the escalation of state-on-state conflicts.

A NEW DIGITAL ARMS RACE.

- Digital technologies increasingly feature in asymmetric warfare, enabling attacks by smaller countries and non-state actors on larger states.
- Viruses developed as cyberweapons have been re-purposed by adversaries after being released into cyberspace.
- Cyberspace has become an extension of the military domain, triggering new technological arms races.

UKRAINE UPDATE CERT-UA

From March 13 to September 14, 2022, when viewing website information resources in Koristuvachev, an image of a provocative scam appeared.
In some cases, at the final stage of the cyberattack, the attackers had encrypted or removed data.

The most likely vector for the implementation of this cyberattack is the compromise of the post-employees (supply chain), which made it possible to win over the obvious trusted links for the introduction of harmonized information-telecommunications and automation systems.

Origin: Computer Emergency Response Team of Ukraine

https://cert-gov-ua.translate.goog/article/18101?_x_tr_sl=ru&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp

DRONE ATTACKS

- A drone attack claimed by Yemen's Houthi rebels targeting a key oil facility in Abu Dhabi killed three people on Monday and sparked a fire at Abu Dhabi's international airport. NPR Jan 17, 2022
- Small drones and quadcopters have been used for strikes by the Islamic State in Iraq and Syria. LA Times 2 October 2017
- Syria War: Russian forces thwarted a drone (UAV) swarm attack on the base, the first of this kind in the history of warfare. BBC. 7 January 2018.
- Two small drones carrying explosives were detonated while President Maduro delivered an outdoor speech, possibly in attempt to attack the president and other government officials. *The Guardian*. 4 August 2018

CYBER SECURITY HORROR MOVIE OF THE WEEK – NOT FOR THE FAINT AT HEART

Introduction (Stuart Russell) – delegating life decisions to machines?

https://youtu.be/9fa9lVwHHqg?t=432

Film

https://www.youtube.com/watch?v=9fa9lVwHHqg

INFORMATION RESOURCES

- https://cybersecurityventures.com/movies-about-cybersecurity-and-hacking
- 2020 Internet Crime Report https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- 10 Biggest Cyber Attacks in History https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/
- Dark Web Price Index. https://www.privacyaffairs.com/dark-web-price-index-2021/
- 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics,https://cybersecurityventures.com/cybersecurity-almanac-2022/
- FBI/IC3 - Internet Crime Report https://www.computerweekly.com/opinion/The-shape-of-fraud-and-cyber-crime-10-things-we-learned-from-2020
- 11 ways to help protect yourself against cybercrime (contains advertising unfortunately) https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html
- Advice on passwords https://www.security.org/how-secure-is-my-password/
- Horror Movie https://www.youtube.com/watch?v=9fa9lVwHHqg


Thank
you!!