TEMPLE UNIVERSITY

Digital Systems

8.1 Cybersecurity & AI

FOX MIS

ROADMAP

START

Week 1:
Introduction & Systems Analysis
- Course Description
- Systems Thinking

Assignments #01 & 02

Week 2:
Digital Product Management
- Max Labs 1a & 1b
- Systems & Processes

Assignment #03

Week 3:
Introduction to Process Mapping
- Swim Lane Diagrams

Assignment #04

Week 4:
Data Modeling with Entity Relationship Diagrams
- ERD Diagrams

Assignment #05

Week 5:
Exam #1,
Digital Systems & Information Systems: Part I & II
- Learn IT #1
- ERP & CRM

*Exam: check course site

Assignment #06

Week 6:
Information Systems: Parts II & III
- CRM
- Data Analytics

Assignment #07

Week 7:
Information Systems: Part IV
Platforms & Digital Business Models
- SCM
- Platforms & Digital Models

Assignment #08

Week 8:
Cybersecurity & AI
- Cybersecurity
- Protection Protocols
- Artificial Intelligence

Week 9:
Exam #2 &
JavaScript Unit #1
- Parts I & II
- Hello World, Variables

*Exam: check course site

Week 10:
JavaScript Unit #2
Functions
- Values & Variables
- Operator types
- Strings

Assignment #9

Week 11:
JavaScript Unit #3
Logical Operators & Conditional Logic
- Logical Operators
- Conditional Types

Week 12:
JavaScript Unit #4
Loops
- Intro to Loops
- While and Do

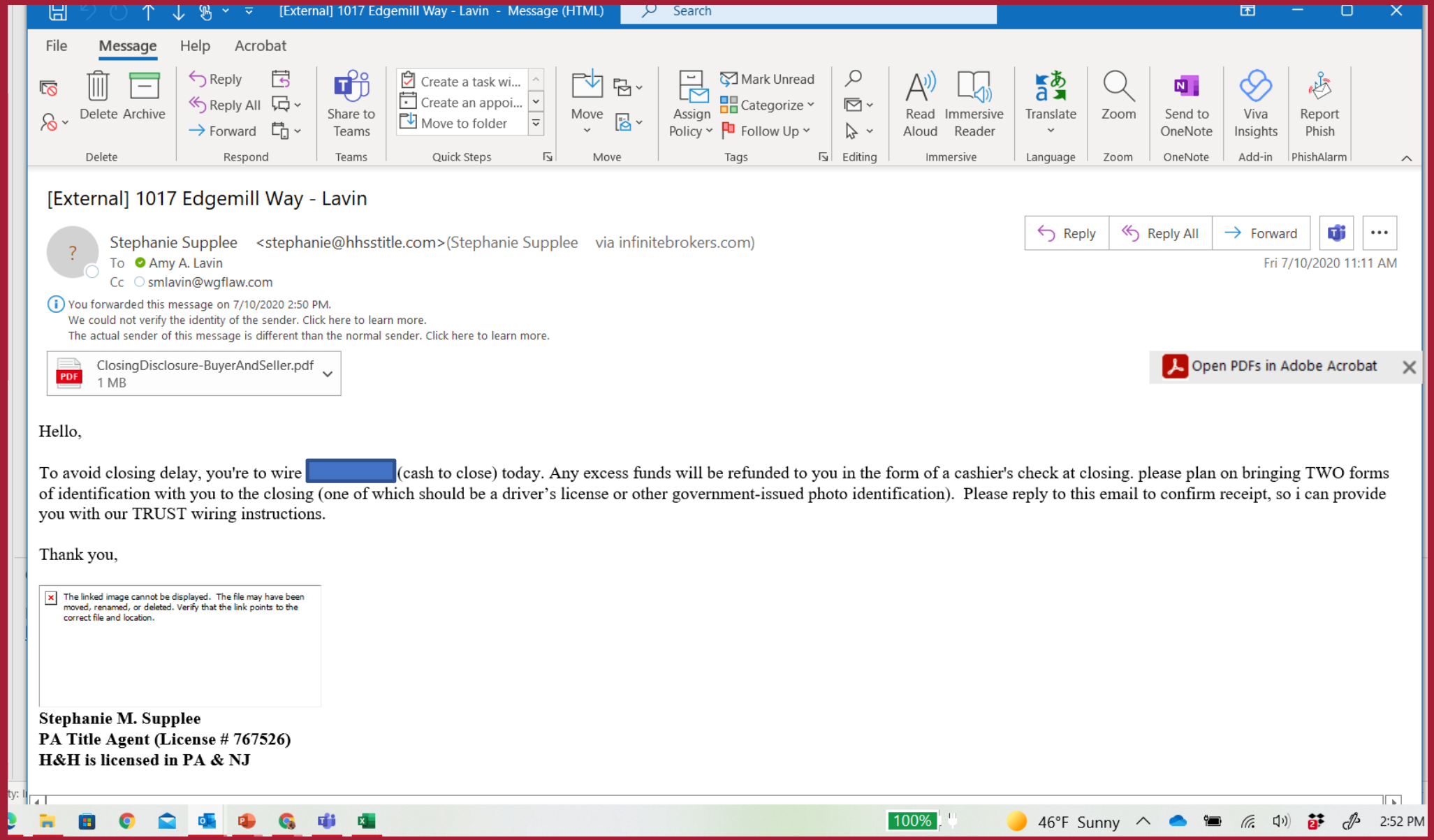
Assignment #10

Week 13:
JavaScript Unit #4
Working with Loops &
HTML & CSS Unit
- Writing the code
- HTML & CSS Basics

Week 14 + 1:
HTML & CSS Unit
(continued)
- HTML & CSS Basics
- Course Reflection

Assignments #11
*Final Exam: check course site

FINISH


[External] 1017 Edgemill Way - Lavin - Message (HTML)
Search
File
Message
Help
Acrobat
Delete
Archive
Reply
Reply All
Forward
Share to Teams
Create a task wi...
Create an appoi...
Move to folder
Move
Assign Policy
Mark Unread
Categorize
Follow Up
Read Aloud
Immersive Reader
Translate
Zoom
Send to OneNote
Viva Insights
Report Phish
Delete
Respond
Teams
Quick Steps
Move
Tags
Editing
Immersive
Language
Zoom
OneNote
Add-in
PhishAlarm
[External] 1017 Edgemill Way - Lavin
Stephanie Supplee <stephanie@hhsstitle.com>(Stephanie Supplee via infinitebrokers.com)
To Amy A. Lavin
Cc smlavin@wgflaw.com
Reply
Reply All
Forward
Fri 7/10/2020 11:11 AM
You forwarded this message on 7/10/2020 2:50 PM.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.
ClosingDisclosure-BuyerAndSeller.pdf
1 MB
Open PDFs in Adobe Acrobat
Hello,
To avoid closing delay, you're to wire [redacted] (cash to close) today. Any excess funds will be refunded to you in the form of a cashier's check at closing. please plan on bringing TWO forms of identification with you to the closing (one of which should be a driver's license or other government-issued photo identification). Please reply to this email to confirm receipt, so i can provide you with our TRUST wiring instructions.
Thank you,
The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.
Stephanie M. Supplee
PA Title Agent (License # 767526)
H&H is licensed in PA & NJ
100%
46°F Sunny
2:52 PM

Cybersecurity Threat Statistics

Number	Stat	Source
$4.24 M	Average cost of a data breach	IBM/Ponemon Cost of a Data Breach Report 2021
287	Average number of days to identify and contain a data breach	IBM/Ponemon Cost of a Data Breach Report 2021
350,000	Number of new malware programs found per day	AV-TEST Institute
18,000	Number of Solarwinds customers affected by supply chain breach	U.S. SEC filing, 12/14/20
$1.85 M	Average cost of remediating ransomware attack	Sophos State of Ransomware 2021 report
74%	U.S. companies experiencing successful phishing attack in 2020	Proofpoint 2021 State of the Phish Report

CompTIA

Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

TOP CYBER THREATS

Ransomware

10 terabytes and more of data stolen monthly.

More than 60% of affected organisations may have paid ransom demands

Malware

Malware infections are increasing due to crypto-jacking and Internet of Things malware.

Widespread cloud adoption provides attack opportunities for cybercriminals. In 2021, we observed 66 disclosures of zero-day vulnerabilities

Social Engineering threats

Social engineering and especially phishing remain a popular technique for attackers to conduct their malicious activities with new lures focusing on the Russia's invasion of Ukraine

Threats against data

They form a collection of threats that aim at gaining unauthorised access and disclosure, as well as manipulating data to interfere with the system behaviour.

Year on year increases as due to the increase in the amount of data produced

Threats against availability: Denial of Service

The DDoS landscape was affected by the Russia's invasion of Ukraine.

The numbers have risen and July 2022 was a peak with the largest ever recorded attack launched in Europe

Threats against availability: Internet threats

Destruction of internet infrastructure, outages and rerouting of internet traffic impact internet usage and free flow of information.

Disinformation – misinformation

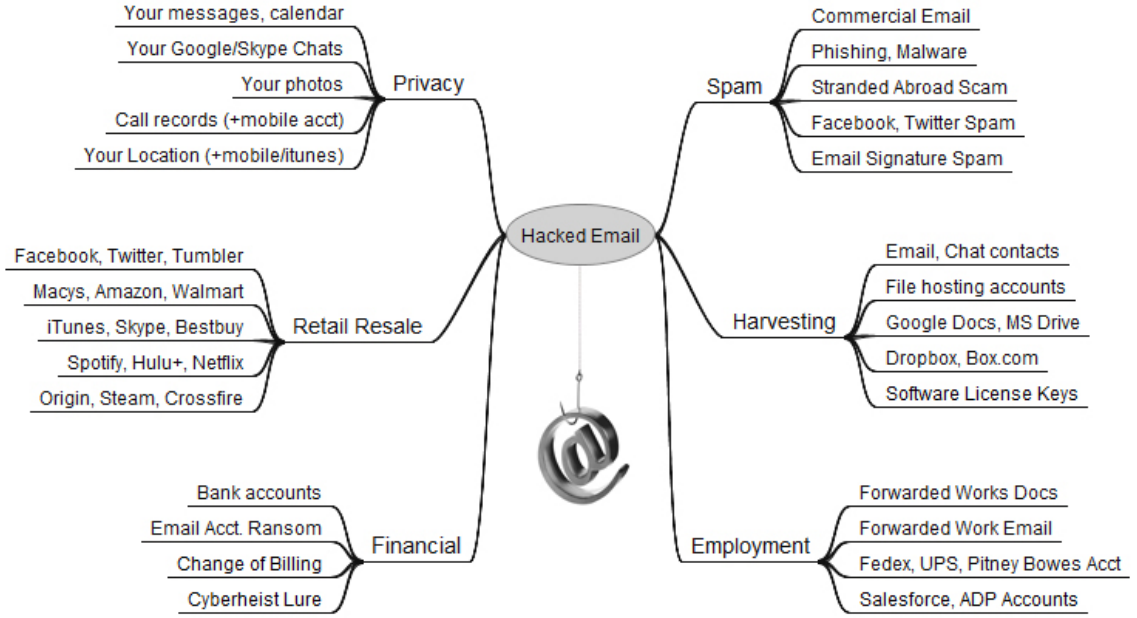
AI-enabled disinformation, deepfakes and disinformation-as-a-service are escalating with targets including elections, the green transition, covid-19 and the Russia's invasion of Ukraine

Supply-chain attacks

Cybercriminals exhibit increasing capability and interest in supply chain attacks.

Third-party incidents account for 17% of the intrusions in 2021 compared to less than 1% in 2020

Source: ENISA Threat Landscape 2022 (July 2021 to July 2022)

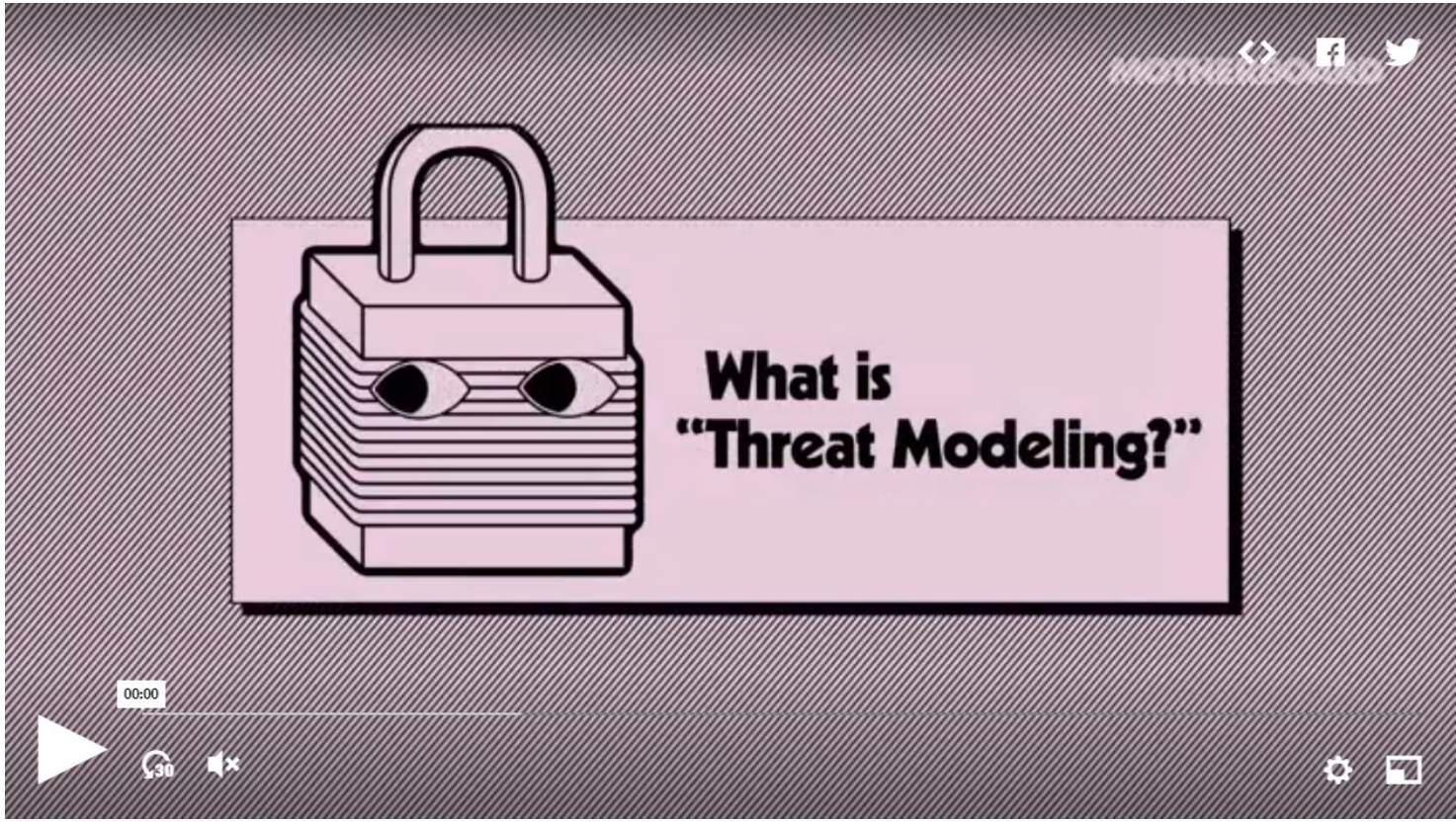


THE VALUE OF YOUR EMAIL ACCOUNT

Cybersecurity - Core Fundamentals

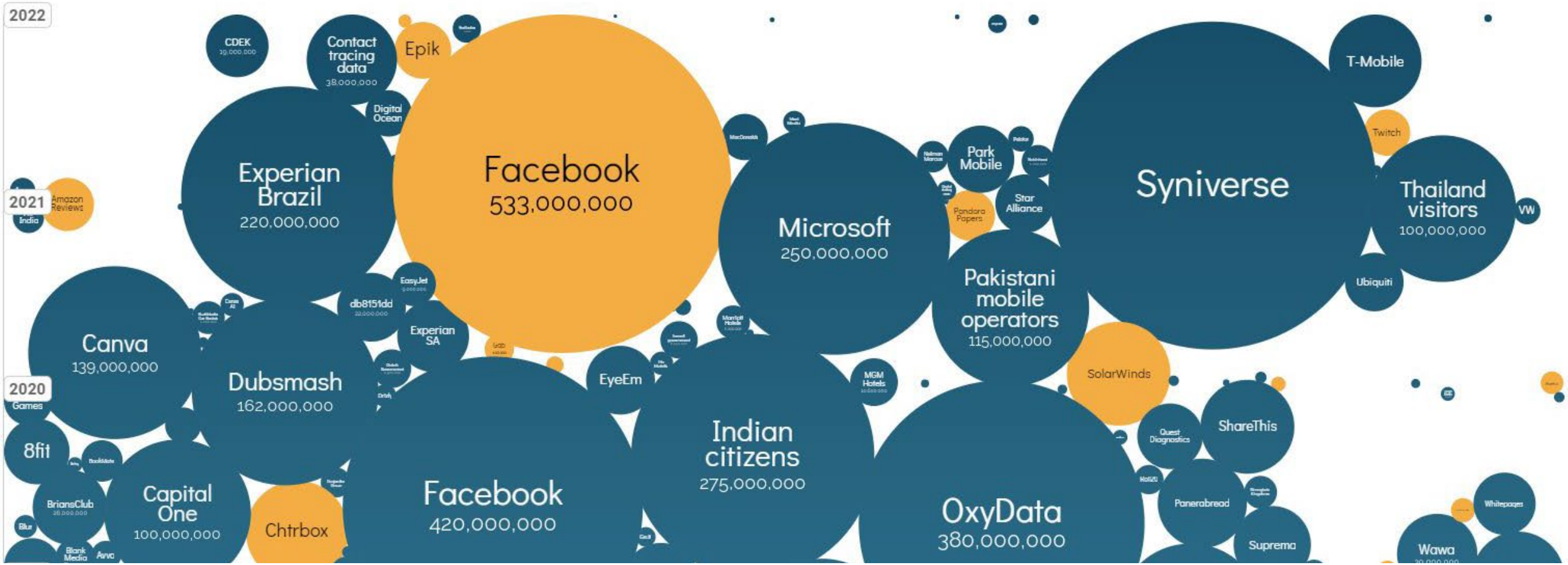
Consider these five questions:

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those consequences?



Source: https://www.vice.com/en_us/article/a37p94/what-is-threat-modeling

World's Biggest Data Breaches & Hacks



Source: https://www.oyster-ims.com/news/worlds-biggest-data-breaches-hacks

Corporate Hacks

Who was Hacked?

Why should you care?

- SSN
- Credit Cards
- Loans
- Identity

Source: https://grandmutual.com/blog/tips-for-protecting-your-business-from-a-data-breach/

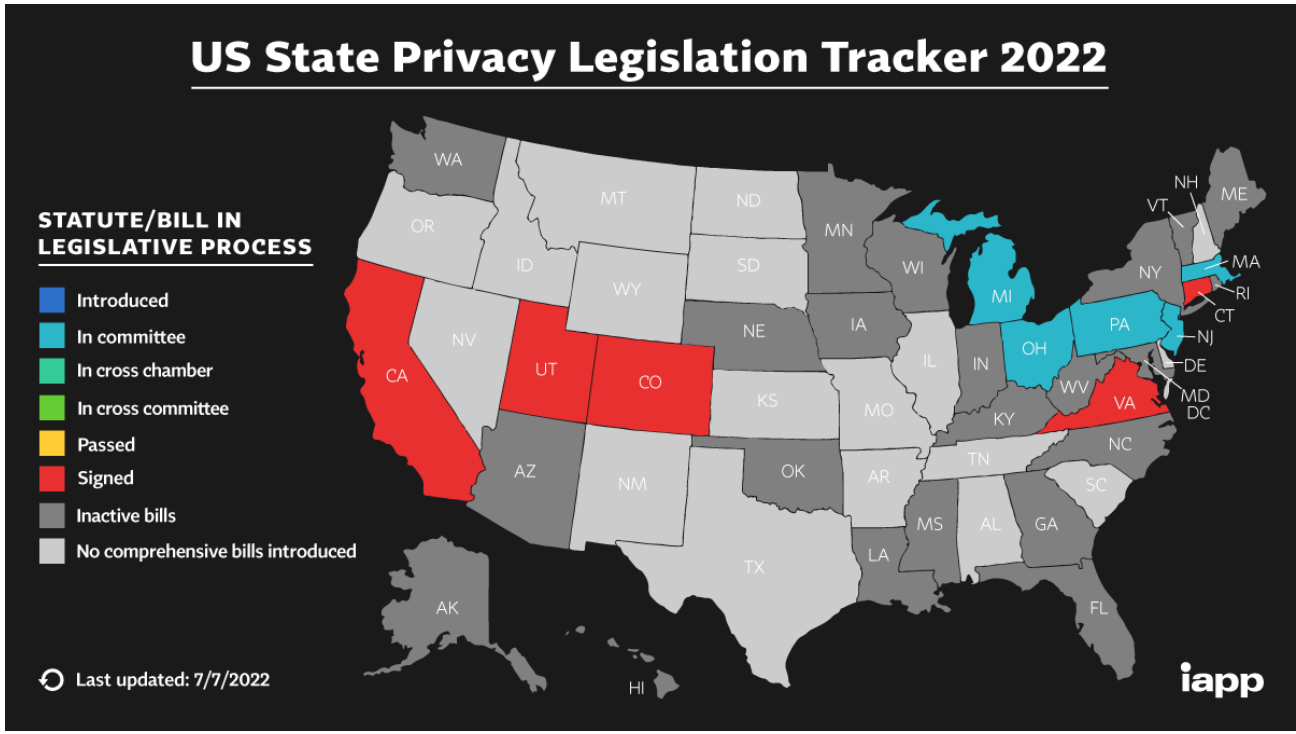
Regulations

Privacy and Personal Data Protection

- California Consumer Privacy Act (CCPA)
- General Data Protection Regulation (GDPR).

Few Federal cybersecurity regulations

- 1996-Health Insurance Portability and Accountability Act (HIPAA)
- 1999-Gramm-Leach-Bliley Act
- 2002 Homeland Security Act, includes
  - Federal Information Security Management Act
- State-level momentum for comprehensive privacy bills

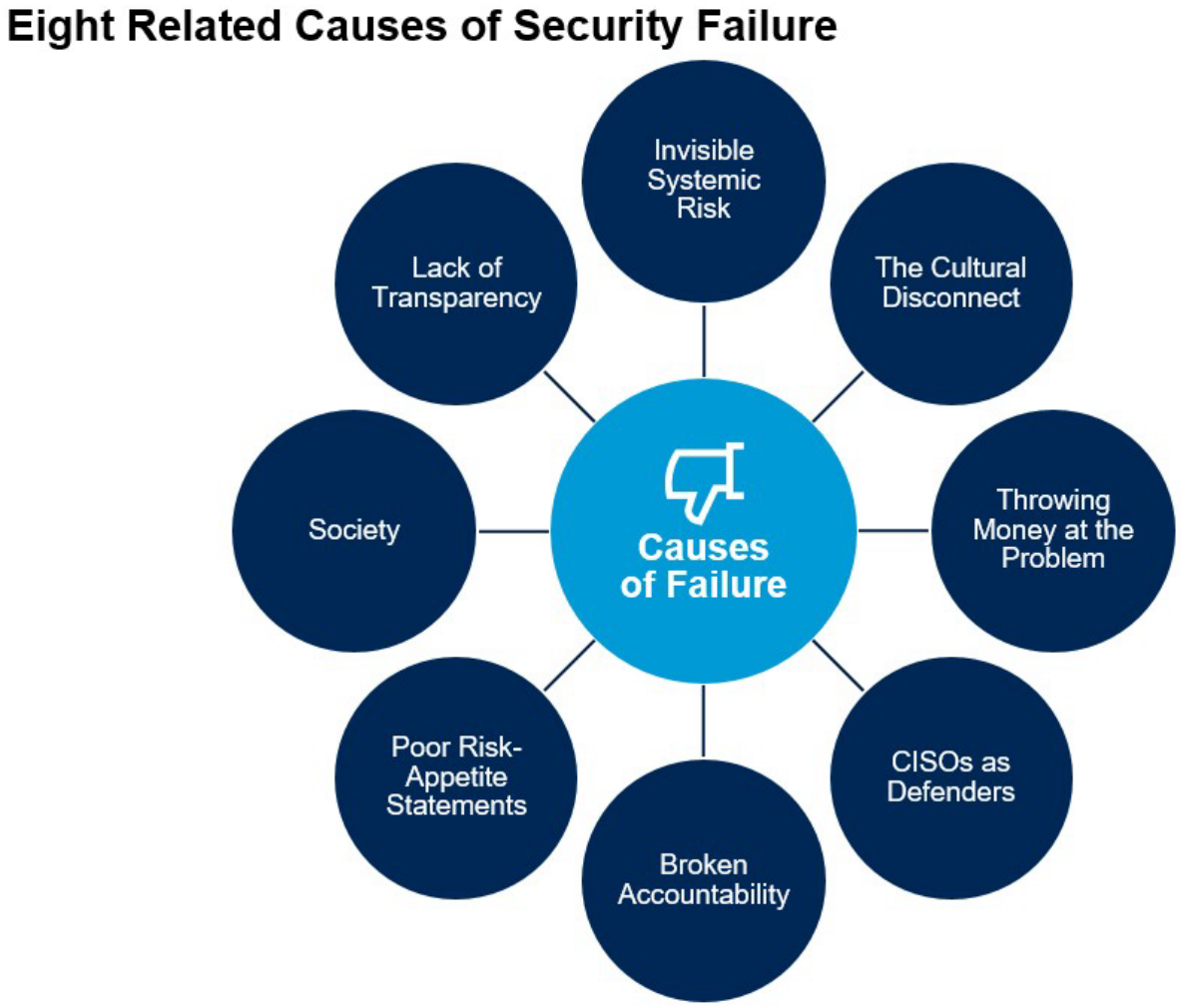


Source: https://iapp.org/media/images/resource_center/State_Comp_Privacy_Law_Map.png

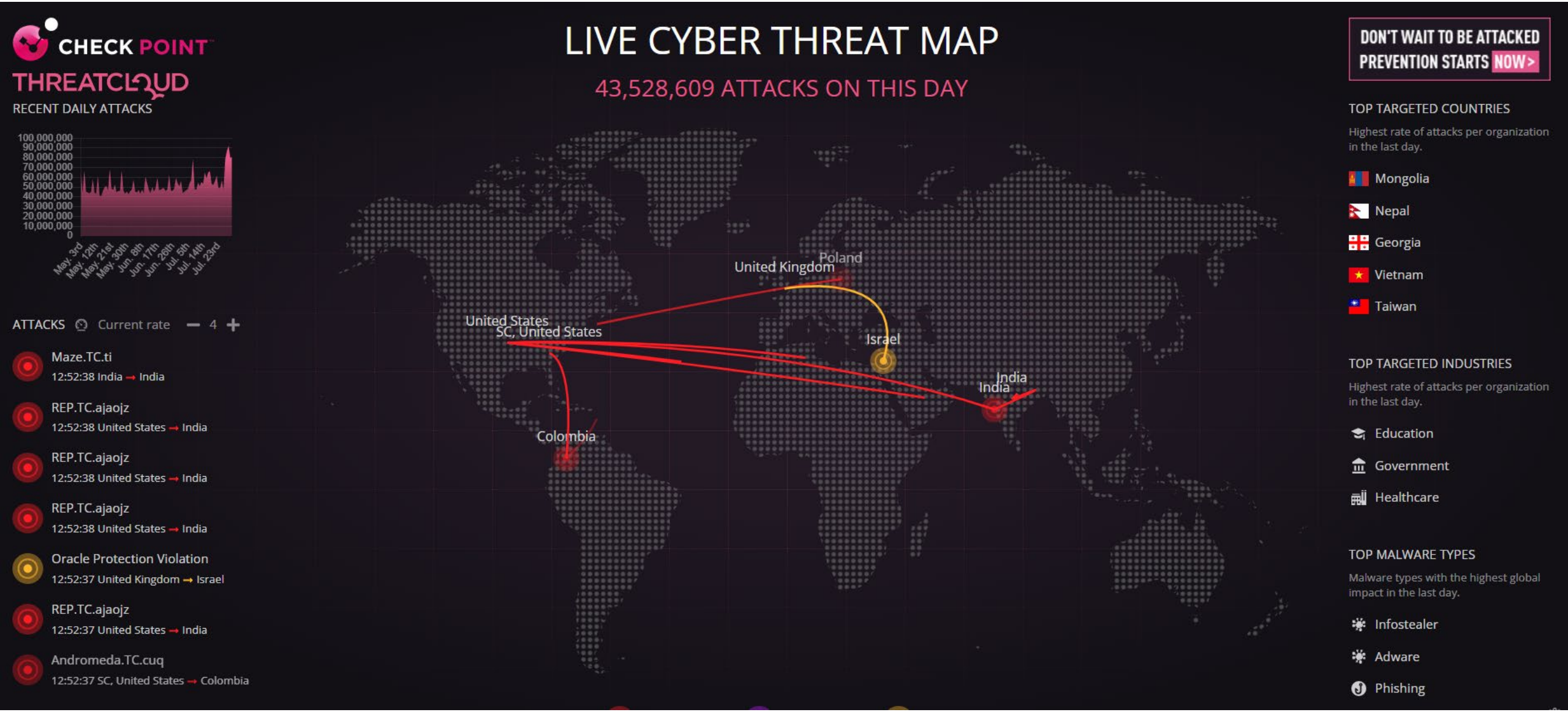
Strategic Planning

What does this all mean?

- Define the eight reasons



Source:https://www.gartner.com/document/3904673?ref=solrAll&refval=225616225&qid=0df98fbb9b466bc69199efad/


CHECK POINT
THREATCLOUD
LIVE CYBER THREAT MAP
43,528,609 ATTACKS ON THIS DAY
DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW>
RECENT DAILY ATTACKS
100,000,000
90,000,000
80,000,000
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
May. 3rd
May. 12th
May. 21st
May. 30th
Jun. 8th
Jun. 17th
Jun. 26th
Jul. 5th
Jul. 14th
Jul. 23rd
ATTACKS
Current rate
4
Maze.TC.ti
12:52:38 India → India
REP.TC.ajaojz
12:52:38 United States → India
REP.TC.ajaojz
12:52:38 United States → India
REP.TC.ajaojz
12:52:38 United States → India
Oracle Protection Violation
12:52:37 United Kingdom → Israel
REP.TC.ajaojz
12:52:37 United States → India
Andromeda.TC.cuq
12:52:37 SC, United States → Colombia
United Kingdom
Poland
United States
SC, United States
Israel
India
India
Colombia
TOP TARGETED COUNTRIES
Highest rate of attacks per organization in the last day.
Mongolia
Nepal
Georgia
Vietnam
Taiwan
TOP TARGETED INDUSTRIES
Highest rate of attacks per organization in the last day.
Education
Government
Healthcare
TOP MALWARE TYPES
Malware types with the highest global impact in the last day.
Infostealer
Adware
Phishing

Case Study

Ransomware forces shutdown

- The incident led to the cancellation of 2,800 patient appointments at the NHS Trust.
- Took 3 days to resolve
- Hospitals are an appealing target for cyberwar…why?

Source: Getty Images/iStockphoto
https://www.zdnet.com/article/ransomware-blamed-for-cyber-attack-which-forced-hospitals-to-cancel-operations-and-shut-down-systems/

Vulnerability

What puts users at risk?

- Forms of malware?
- Who is impacted?
  - Are we safe?
- Can this problem be solved?
  - Combat strategies?

Source: https://www.itweb.co.za/content/KWEBb7yaExK7mRjO

Password Strength

How secure are your passwords?

- Use numbers, letters, and symbols
- Make them as long as possible

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Source: https://community.isc2.org/t5/Tech-Talk/How-long-does-it-take-to-crack-passwords/td-p/32546

Password Management

Password Basics

- Keep them in your head?
- Don't change them?
- Reuse them?

Password Management

- Consider a passphrase
  - Access a vault of your passwords
- Two-Factor Authentication

Source: https://youtu.be/a6iW-8xPw3k

Protection

Considerations

- Antivirus
- Ad blocker
- Avoid dodgy plugins
- Back-up files
- Disable macros
- Don’t just open attachments
- Firewall
- VPN

Source: https://www.pcmag.com/roundup/256703/the-best-antivirus-protection

Phishing Scams

Case Study

- Google and Facebook targeted
- Lost $100 million

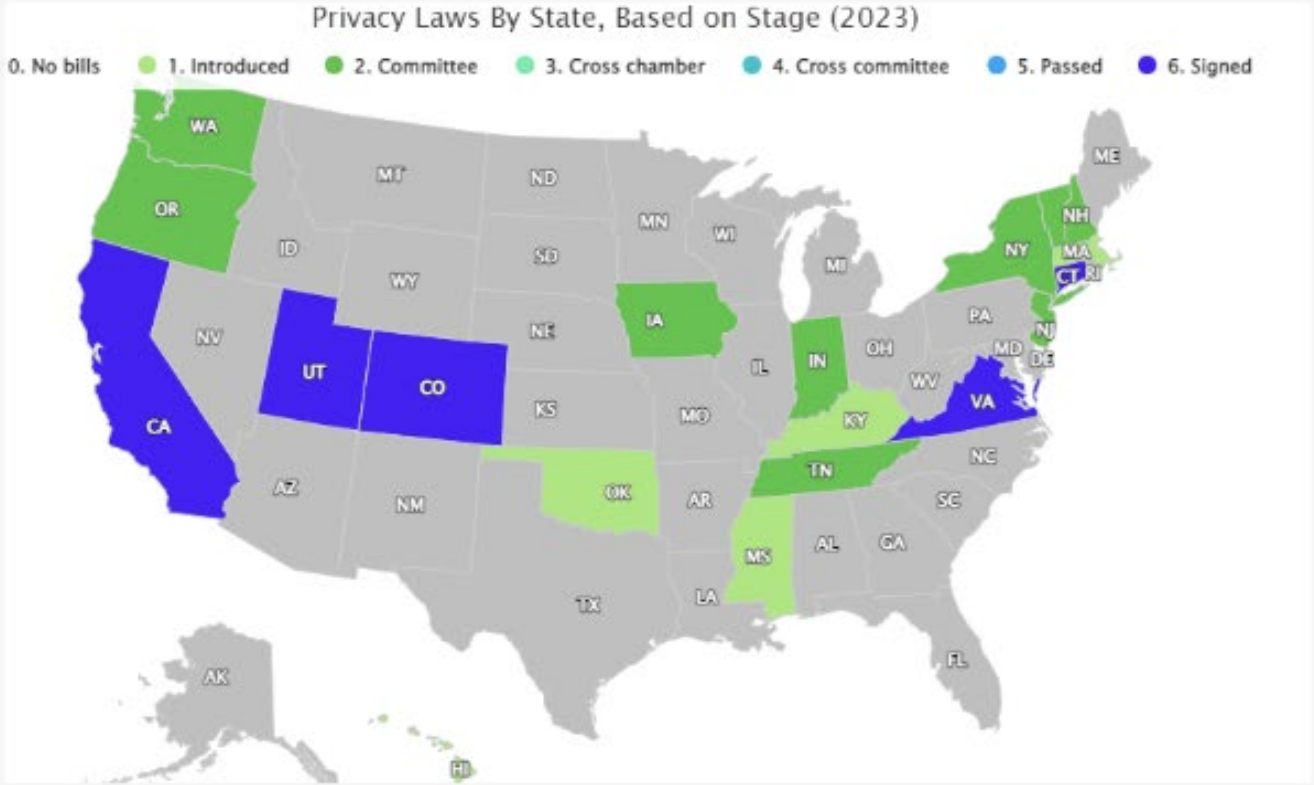
Best Practices

- Careful of any suspicious emails
- Don’t click on random links

Source: https://www.nouveau.co.uk/content-hub/avoidphishing/

Data Privacy Laws

- Govern how companies handle the data of users & citizens
- Permission, access, ownership
- Varies by state

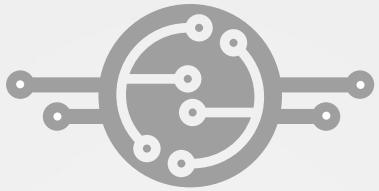


Cybersecurity

Hijacking your systems!

- Who borrows flash drives?
- How else do you share data?
- Vectors for Virus & Malware

Source: http://www.ommdvd.com/images/services/USB-Pile.jpg



Artificial Intelligence

MIS2901

Lavin - Spring 2023

What Is AI?

"A field which combines computer science and robust datsets, to enable problem solving"

- Human Approach:
  - Systems that think like humans
  - Systems that act like humans

- Ideal Approach:
  - Systems that think rationally
  - Systems that act rationally

AI Applications

Speech Recognition

Uses Natural Language Processing to process human speech into a written format

Customer Service

Online virtual agents, frequently asked questions, message bots, voice assitants

Computer Vision

Enables computers & systems to derive meaningful information from digital images, videos, visual inputs and then take action

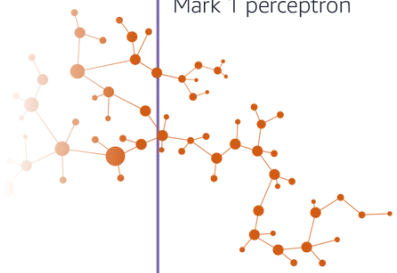
Recommendation Engines

Using past data, use algorithms to uncover trends and make recommendations

1950s

BIRTH OF AI

Psychologist Frank Rosenblat creates the Mark 1 perceptron



1970s

AI WINTER

The 70s and 80s deliver little progress towards the promise of AI

1997

IBM DEEP BLUE

IBM's chess computer defeats grandmaster Garry Kasparov

2005

ERA OF BIG DATA

1000101010010010011
0101010100101001010
1010101001010100111

'Big data' is coined as data goes beyond data warehouses

2006

CLOUD COMPUTE

AWS begins offering cloud infrastructure

2009

GPUs & SOCIAL

GPUs accelerate AI and social media data feeds AI's need for data

2011

AI WINS JEOPARDY

An artificial intelligence beats the top two jeopardy contestants

DIGITAL ASSISTANTS

Apple launches Siri

2015

DRIVERLESS CARS

Tesla announces Autopilot and Waymo takes to the streets

2016

COZMO AI TOY

Anki releases AI-powered Wall-E inspired toy

2017

FACEBOOK FACE AI

Facebook rolls out facial recognition to help with tagging

2018

JUST WALK OUT

Amazon releases Just Walk Out tech to streamline retail

2021

DELIVERY BOTS

Amazon begins testing delivery robot "Scout" in select cities

Personal Applications

1

E-COMMERCE

Personalized Assistants
Fraud Prevention

LIFESTYLE

2

Autonomous Vehicles
Spam Filters
Facial Recognition
Recommendation Systems

EDUCATION

3

Content Curation
Personalized Learning

Business Applications

1 HUMAN RESOURCES

Hiring

Candidate Pool Curation

2 MARKETING

Content Marketing

Targeted Ads & Personalization

3 FINANCE

Fraud Detection

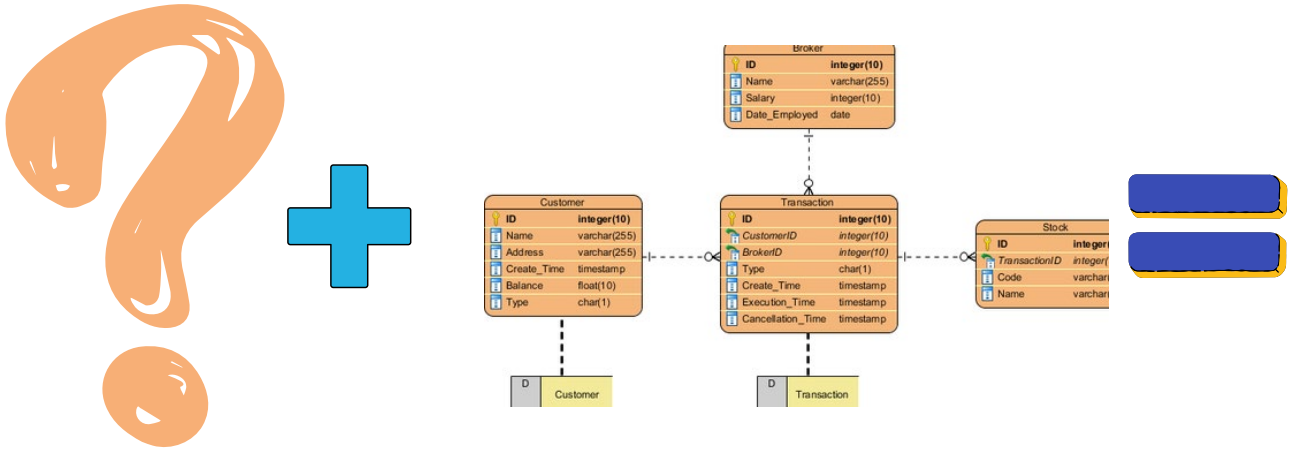
Stock Trading

Loan Risks

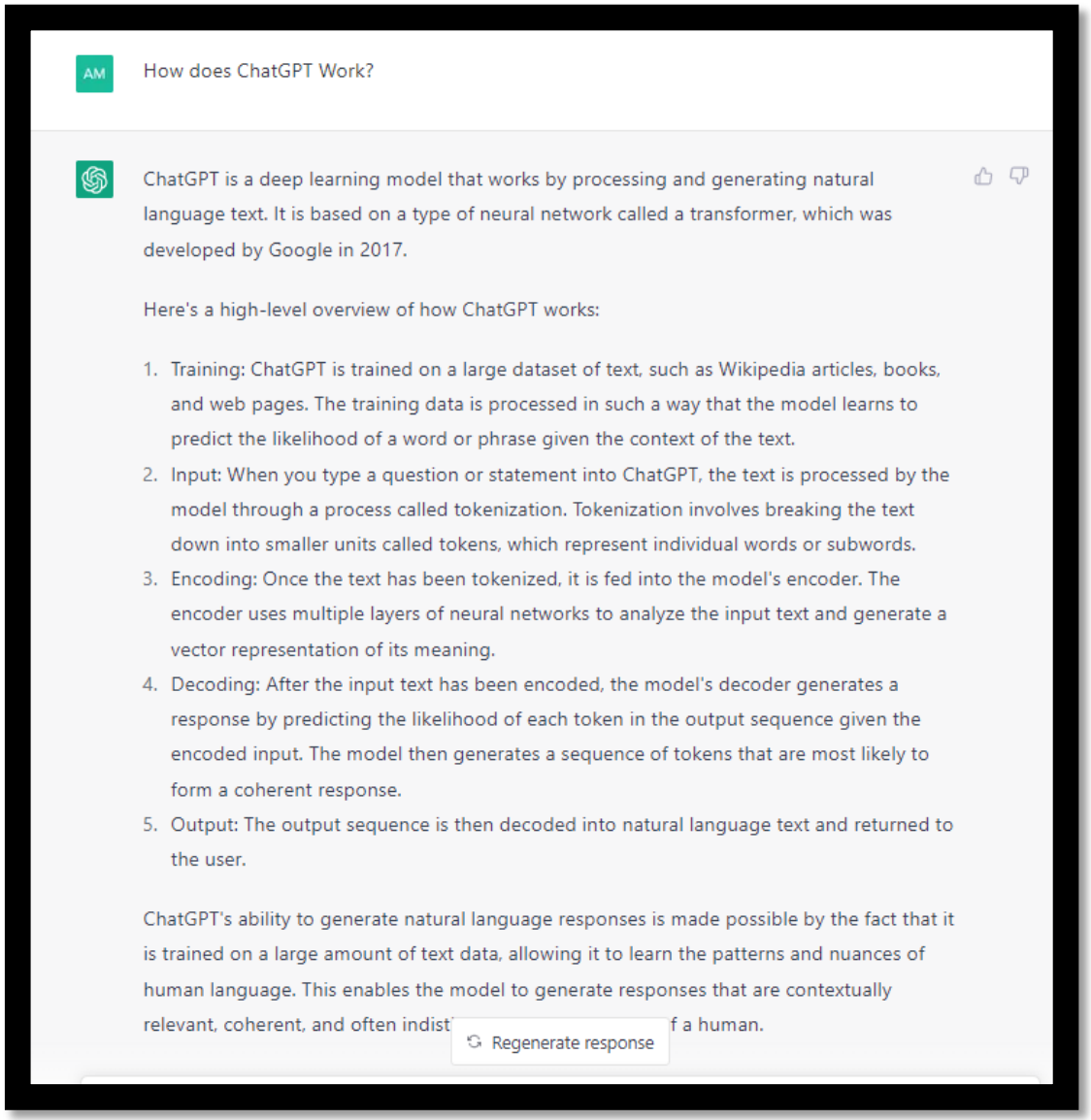
ChatGPT

BUSINESS APPLICATIONS

- Customer Support & Service
- Sales & Marketing
- Personalized Customer Recommendations
- Content Creation
- Employee Training and Support



How does it work?



DISCUSSION:

WHAT ARE THE ACADEMIC IMPLICATIONS OF CHATGPT?

WHAT ARE THE BUSINESS IMPLICATIONS OF CHATGPT?

More to Come

Prepare with Readings & Videos before our next class!!!