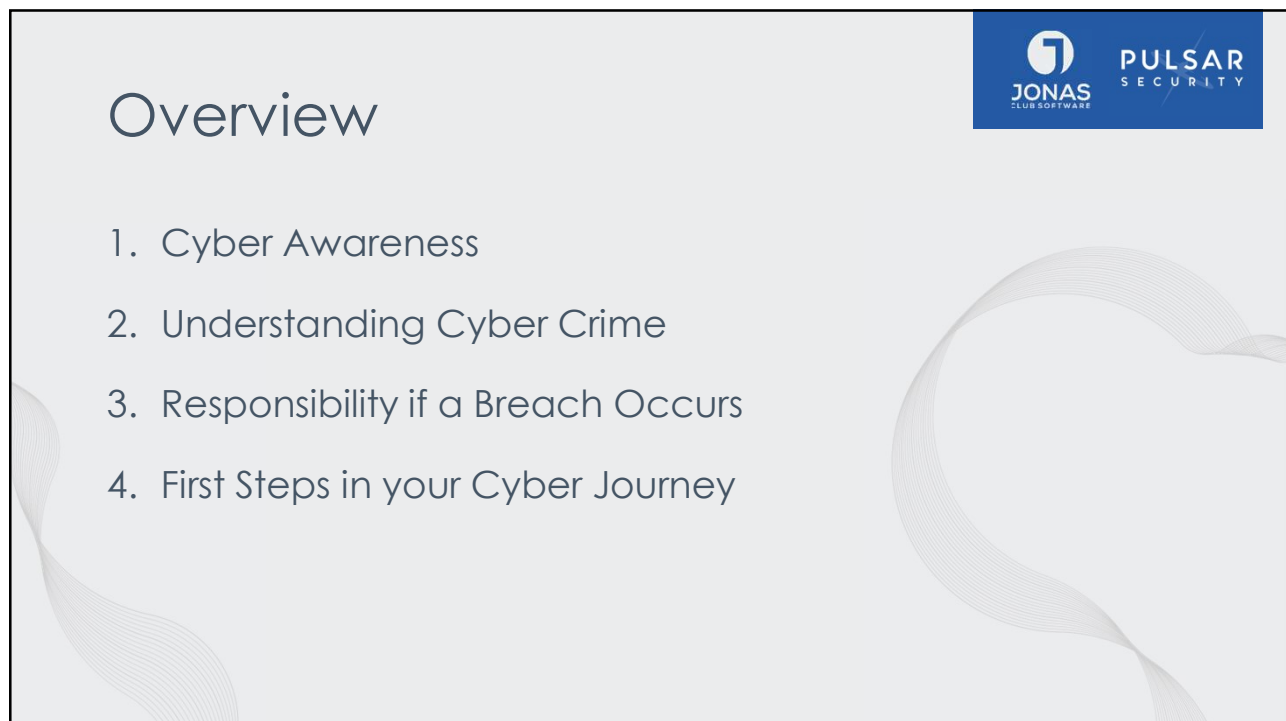




1



2



About Us

JONAS CLUB SOFTWARE **PULSAR SECURITY**


Trevor Coughlan

- General Manager, ClubHouse Online
- Jonas Club Software

Duane Laflotte

- CTO and Red Team Leader
- Pulsar Security

3



Awareness

JONAS CLUB SOFTWARE **PULSAR SECURITY**

What are Criminals After and How Prevalent is Cybercrime?

4



5



6



7



8

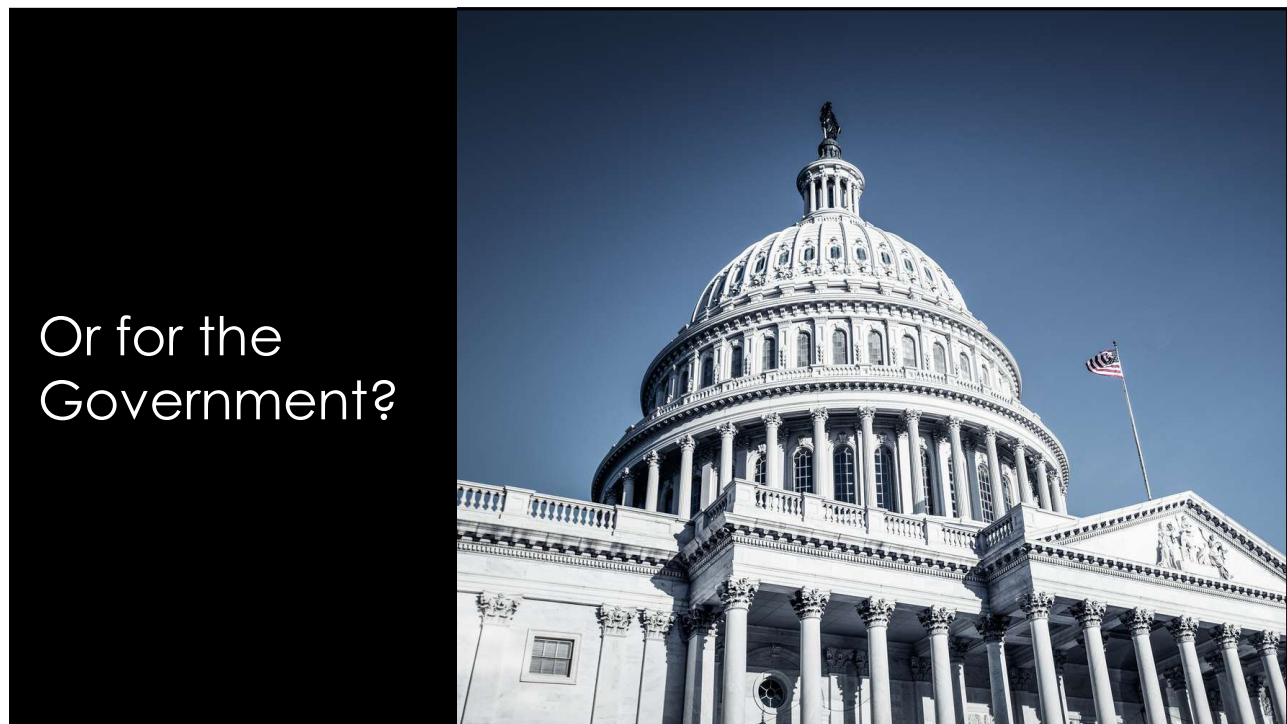


9

How many of your members work for Fortune 500 companies?

 Abbott			
 AVON			
 PEPSICO			

10



11



12

Turke & Strauss LLP

608.237.1775 | info@turkestrauss.com | 613 Williamson Street, Suite 201, Madison, WI 53703

PRACTICE AREAS | OUR TEAM | BLOGS | CONTACT US | DIVERSITY

Attorney Alex Phillips writes about the harm stemming from data breaches in the Wisconsin Lawyer

Hi there, have a question about a potential case? Text us here.

A team of exceptional professionals.

Text us

13

TCO

If you received a breach notification letter from [REDACTED]:

We would like to speak with you about your rights and potential legal remedies in response to this data breach. Please fill out the form, below, or contact us at (608) 237-1775 or sam@turkestrauss.com.

If you were impacted by [REDACTED] data breach, you may consider taking the following steps to protect your personal information.

1. Carefully review the breach notice and retain a copy;
2. Enroll in any free credit monitoring services provided by [REDACTED];
3. Change passwords and security questions for online accounts;
4. Regularly review account statements for signs of fraud or unauthorized activity;
5. Monitor credit reports for signs of identity theft; and
6. Contact a credit bureau(s) to request a temporary fraud alert.

14

Why is Your Club a Target?




High net worth individuals

- President's, CEO's, Board Members
 - People with high level access to large & important corporations
- Targeting your club may be more about gaining access to these organizations than it is about accessing your accounts
 - The Country Club at WoodField
 - Target of breach was sensitive data about members
 - Hackers gained access to the system a month prior
 - Club can be held legally liable

15

Why is Your Club a Target?



Lax security standards are prevalent throughout the industry

- Password123
- G0lf
- pr0sh0p!!
- Summer2022

16



17



18

Data: What is Sensitive?



PULSAR
SECURITY





- Not just Credit Card Data
- The Joy of Regulations
 - CCPA – California Consumer Privacy Act
 - GDPR – General Data Protection Regulation
 - Right to Delete, View, Request, and Restrict
- So what is Sensitive?
 - Credit cards, phone numbers, addresses
 - Spouse and kids names?
 - Purchases at the club?
 - Scheduled spa visit time?

19

Protection against Cybercrime is about more than securing your club.

It's about safeguarding members.

20

Understanding

What Does Cyber Crime Look Like?

21



22



APTs and You

Advanced Persistent Threats

- OSINT: Open Source Intelligence
- Dark Web: Who you are and what do we know
- Digital Recon: What do you have and what have you bought
 - Supply Chain, Software, MSP, Partners

23

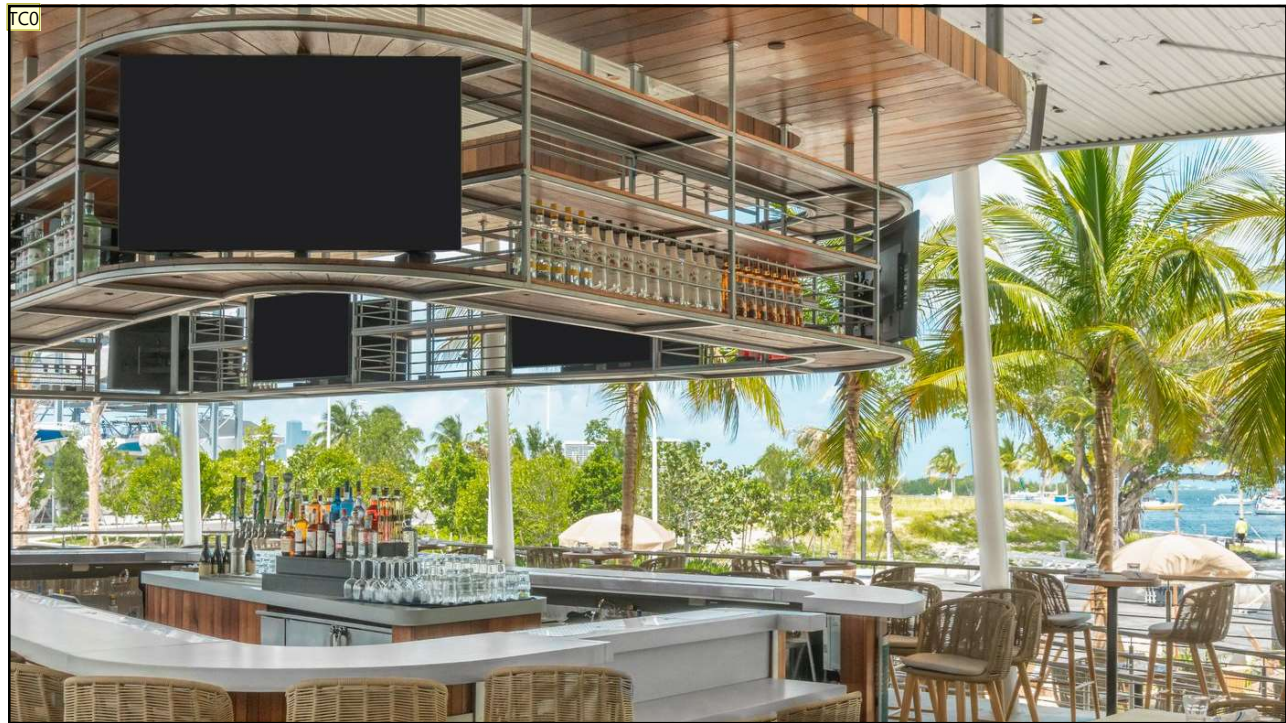


Types of Attacks

What Should We Be Worried About?

- Everything! Seriously though...
 - **IoT:** Fish Tanks, Cameras, Irrigation Systems, Thermostats, Wireless Speakers, Vacuums, TV
 - **External Surface of attack:** Website, Email, Some IoT, Cloud, Virtual Private Networks, Vendor Software
 - **Internal Threats:** End-Users (Phishing, USBs, etc), Vendor Software, Servers, Clients, Mobile Devices

24



25

Responsibility
What if the Unthinkable Happens to Your Club?

JONAS
CLUB SOFTWARE

PULSAR
SECURITY

26

Responsibility



PULSAR
SECURITY

If the Unthinkable Happens

- Mitigate risk immediately; worry about blame later
- Determine what data was stolen or encrypted
 - Who, if anyone, do you need to notify
 - What is the plan for recovery
 - How quickly will you be back online and servicing your members
 - What was the root cause? How do you prevent it from happening again?
- What can legally be said to members, the board, and employees

27

TCO

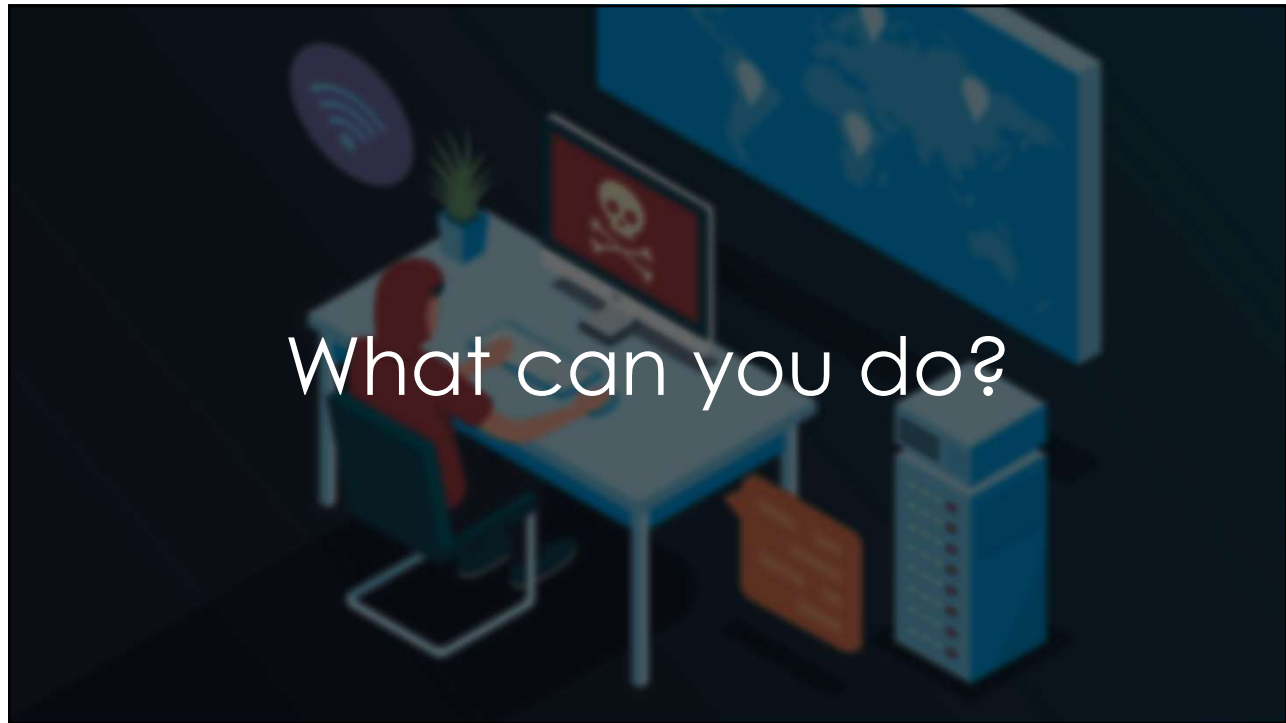


PULSAR
SECURITY

First Steps

How to Begin Preparing Your Club?

28



What can you do?

29

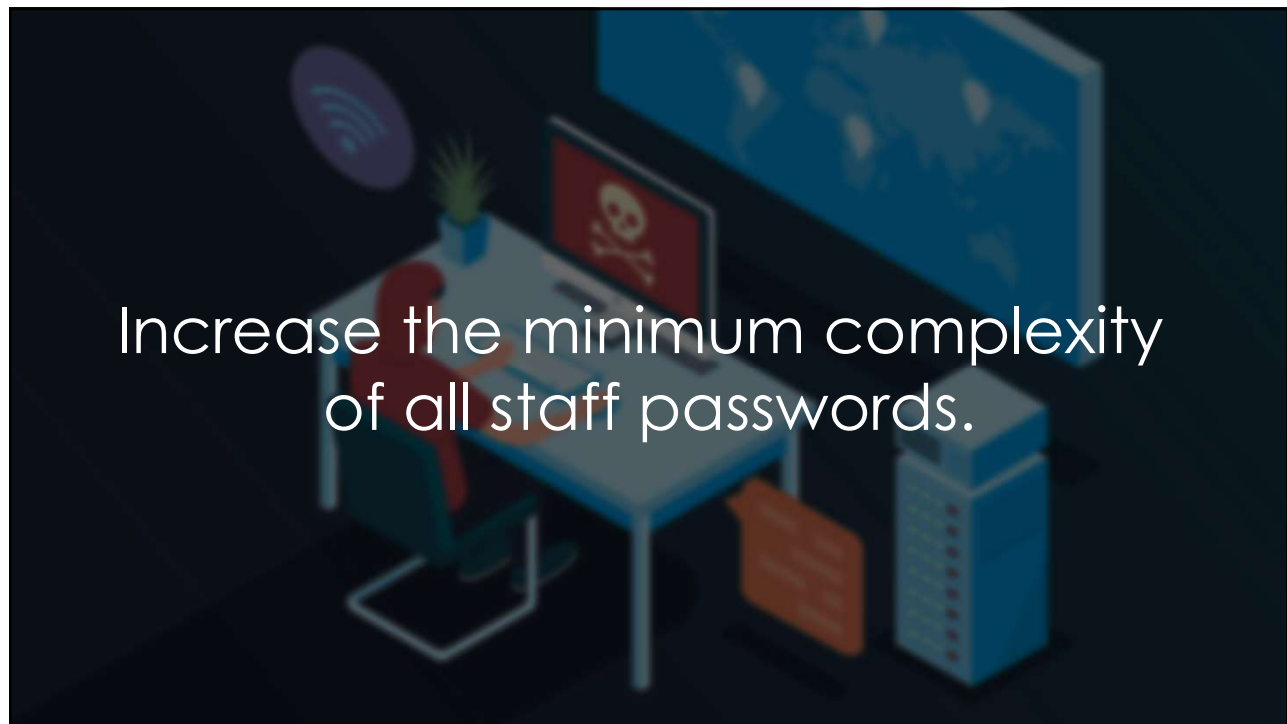
TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

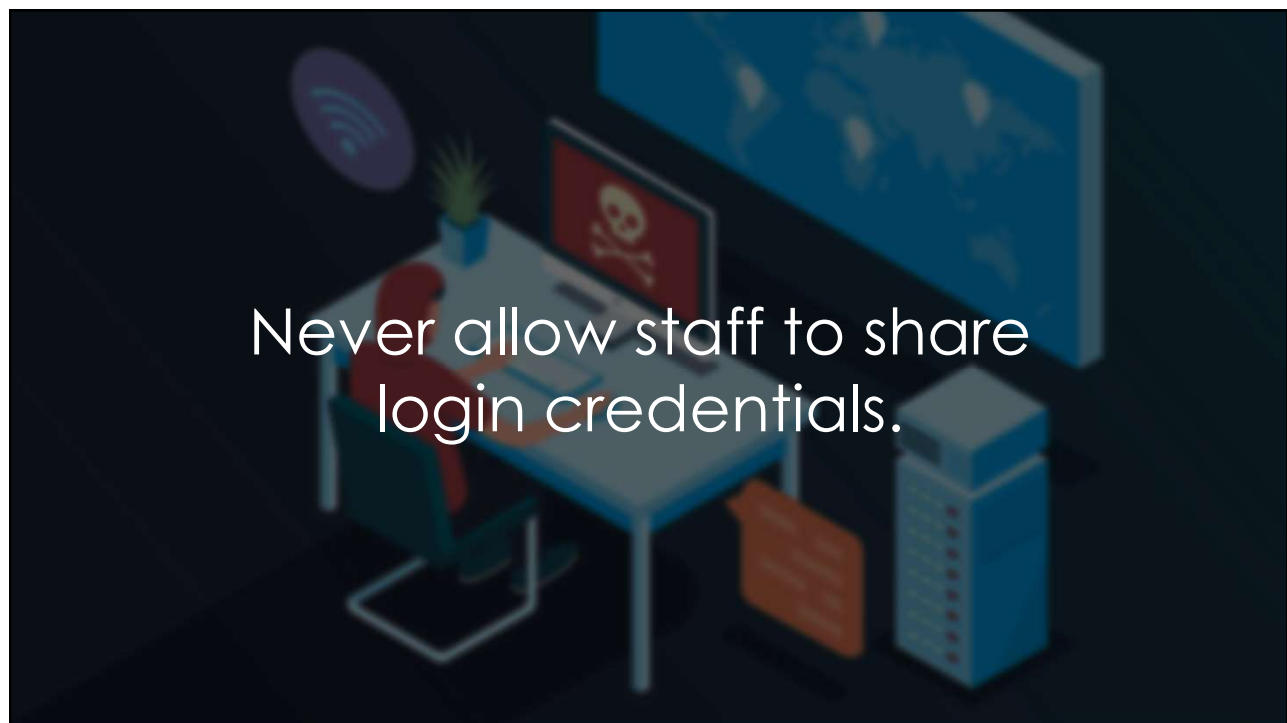


> Learn how we made this table at hivesystems.io/password

30



31



32

An isometric illustration of a person sitting at a desk in a dark room. The person is wearing a red shirt and is looking at a laptop. On the desk, there is a small potted plant and a blue folder. In the background, there is a large blue screen displaying a world map and a server tower. The text is overlaid on the image.

Educate your staff on cyber security standards regularly.

Up to 95% of all cyber security breaches occur due to human error.

33

An isometric illustration of a person sitting at a desk in a dark room. The person is wearing a red shirt and is looking at a laptop. On the desk, there is a small potted plant and a blue folder. In the background, there is a large blue screen displaying a world map and a server tower. The text is overlaid on the image.

Ensure your club is backing up data to a secure off-site location.

34



35




Ask Your Supply Chain



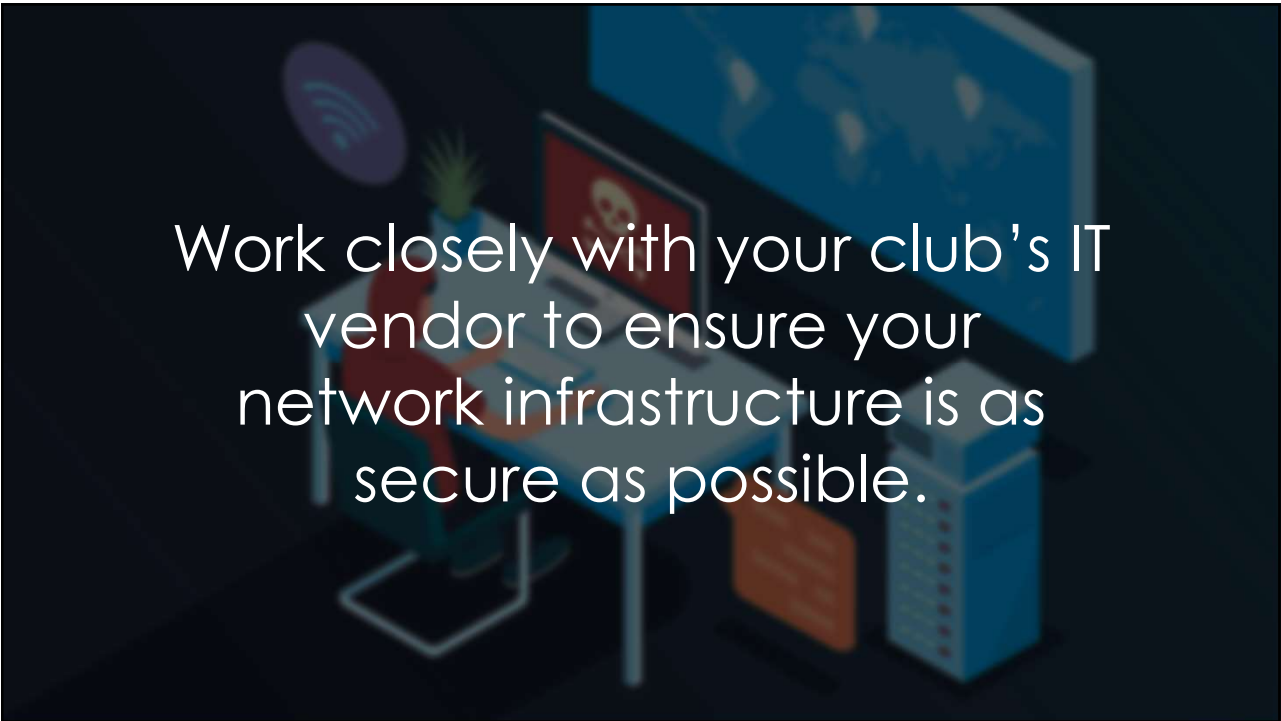
- Do you perform secure code reviews?
- How do you protect our club data at rest and in motion?
- Do you perform external and internal penetration testing?
- Do you have procedures around who has access to our data?
- What is the lifecycle of our data?
- Backups? RPO/RTO?
- What is the process for reporting data breaches involving our club data?
- What are your security best practices for implementation that we should follow?
- Do you have internal processes and reviews of your vendors who may potentially have access to our data?

36



Ensure that sensitive information
is only stored in known locations
with the appropriate
safeguards.

37



Work closely with your club's IT
vendor to ensure your
network infrastructure is as
secure as possible.

38

Security Checklist



PULSAR
SECURITY

Start with the Basics



- ☐ Security Awareness Training
- ☐ Email Protection
- ☐ Password Policies and Managers
- ☐ Wireless Security
- ☐ Client/Server – Antivirus and Patching
- ☐ Employee On and Off-boarding Processes
- ☐ External Review
- ☐ Backup and Recovery
- ☐ Ensure Vendors aren't your Weakest Link

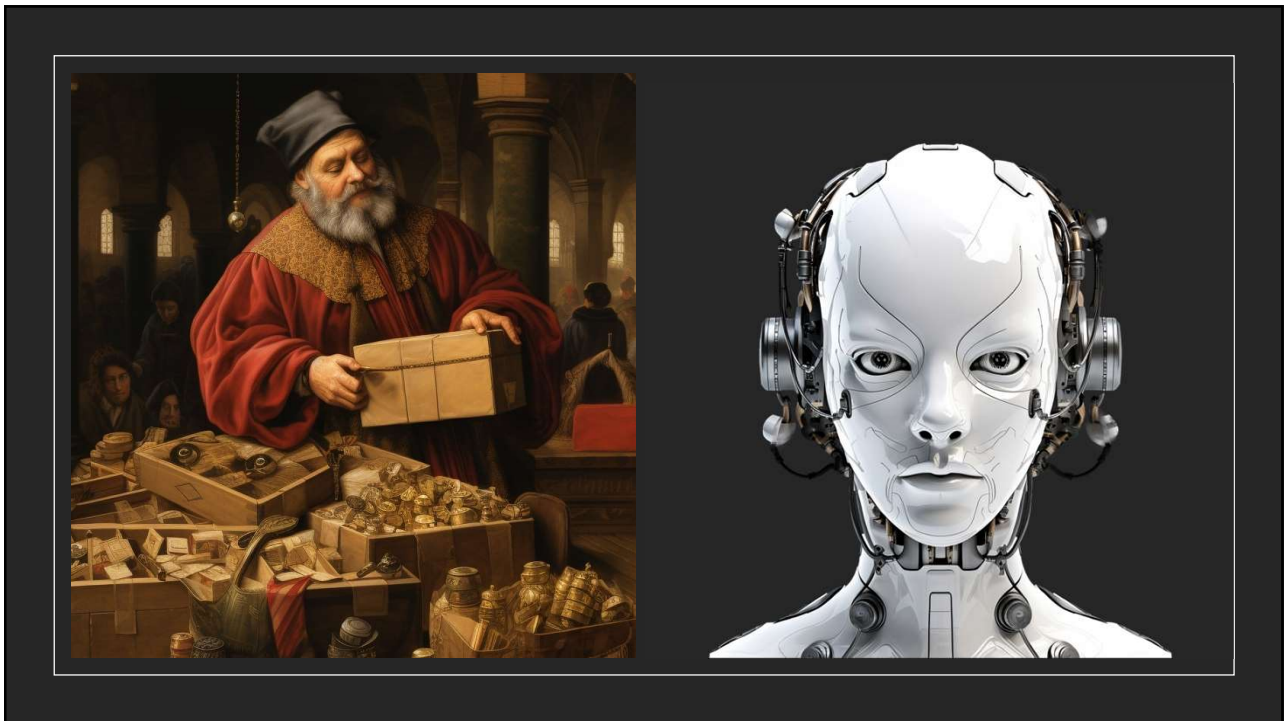
39



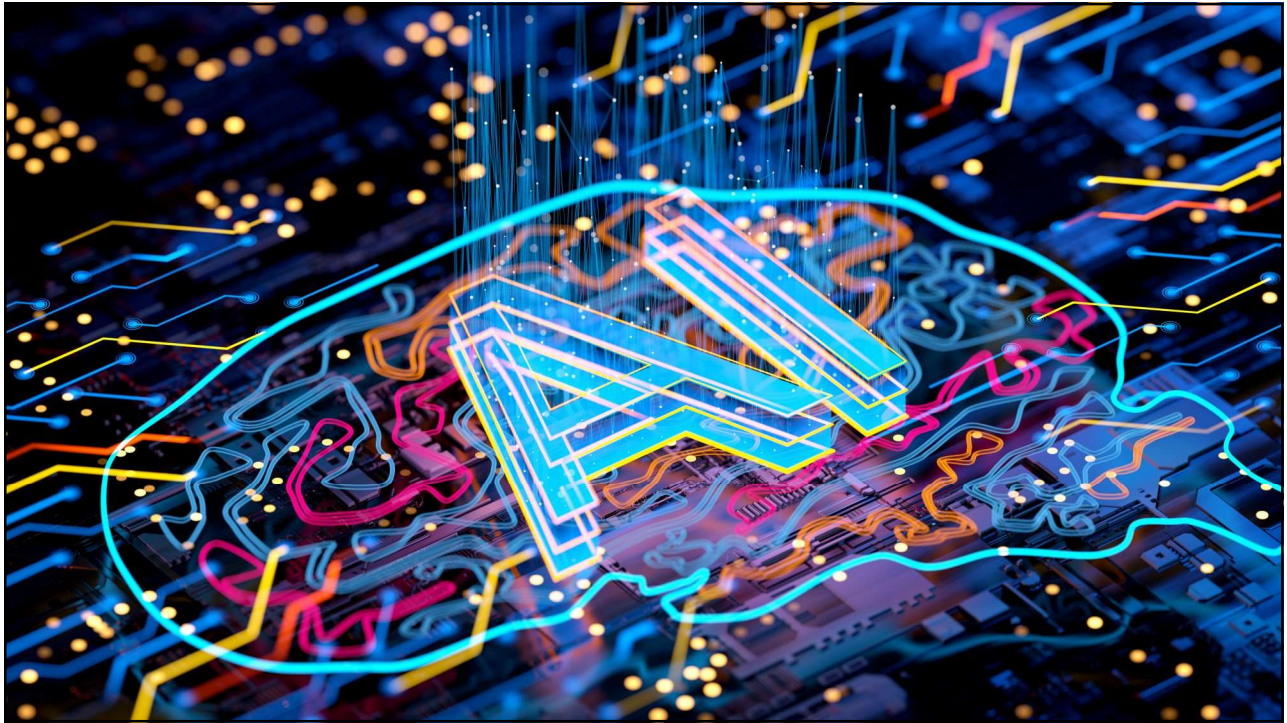
40



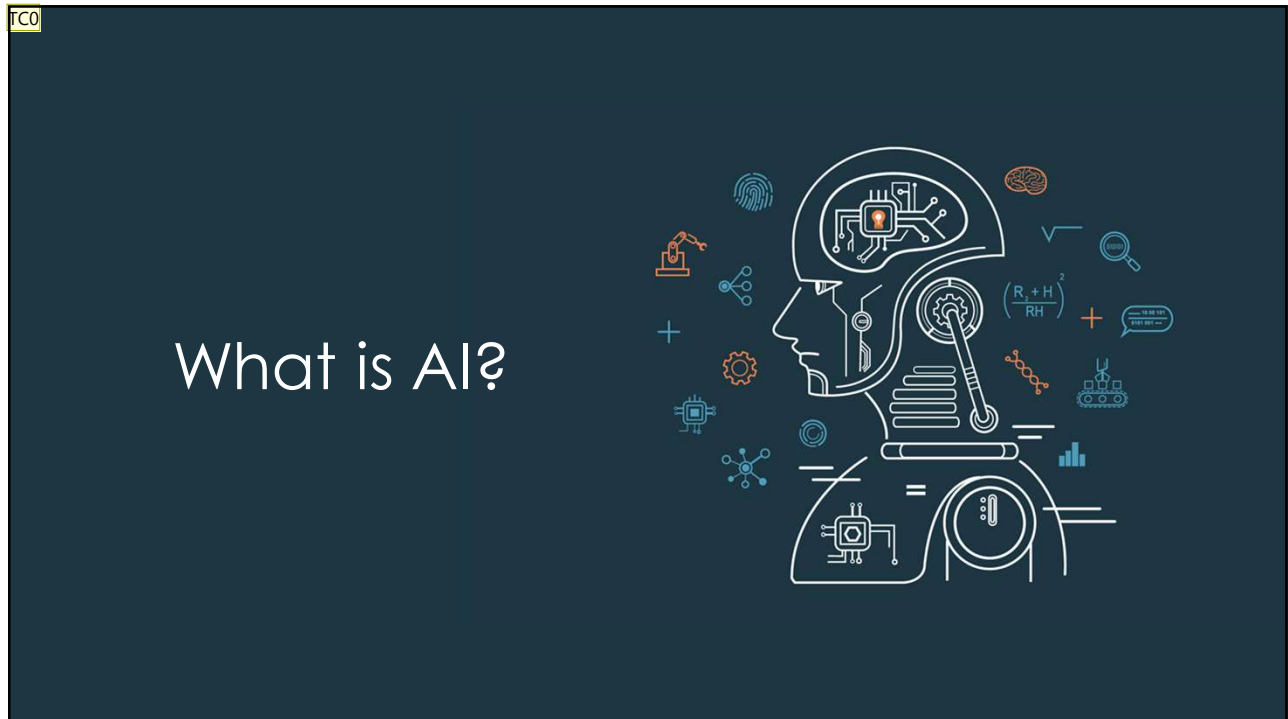
41



42



43



44

Artificial Intelligence (AI)

Root of the field

Artificial Intelligence

A field of study that seeks to enable computing systems to emulate human behavior including learning, decision making, language use, recognition of patterns and solving complex problems

45

Artificial Intelligence (AI)

A field of study that seeks to enable computing systems to emulate human behavior including learning, decision making, language use, recognition of patterns and solving complex problems

Machine Learning (ML)

AI sub field that enables recognition

Machine Learning

AI sub field that uses large data sets to detect patterns such that even unique examples have a high probability of being correctly identified

46

Artificial Intelligence (AI)

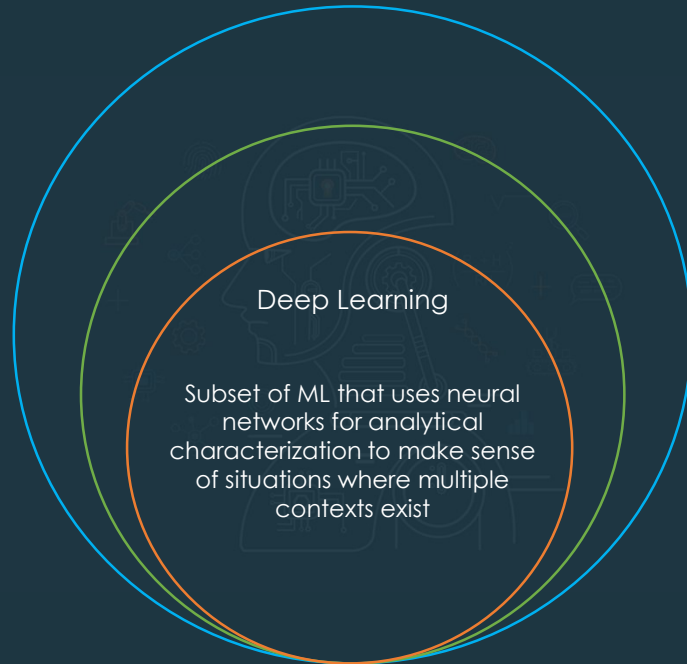
A field of study that seeks to enable computing systems to emulate human behavior including learning, decision making, language use, recognition of patterns and solving complex problems

Machine Learning (ML)

AI sub field that uses large data sets to detect patterns such that even unique examples have a high probability of being correctly identified

Deep Learning (DL)

ML sub field that helps navigate context



47

Artificial Intelligence (AI)

A field of study that seeks to enable computing systems to emulate human behavior including learning, decision making, language use, recognition of patterns and solving complex problems

Machine Learning (ML)

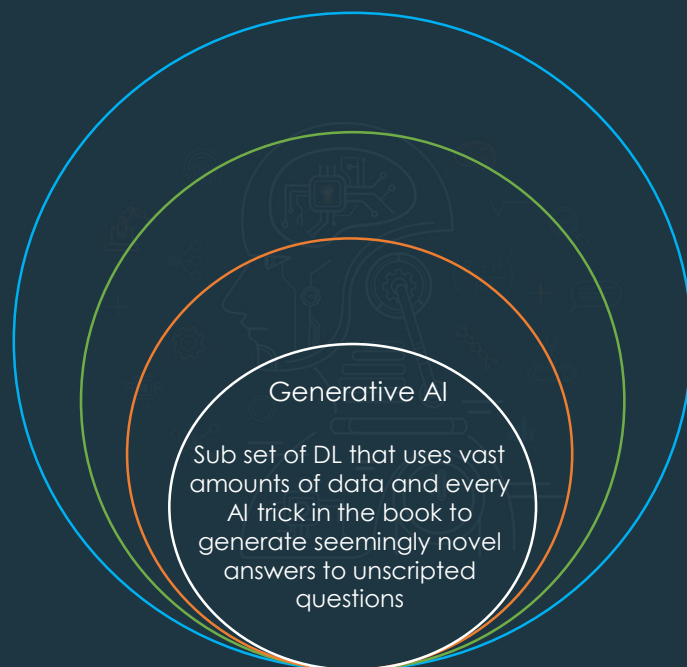
AI sub field that uses large data sets to detect patterns such that even unique examples have a high probability of being correctly identified

Deep Learning (DL)

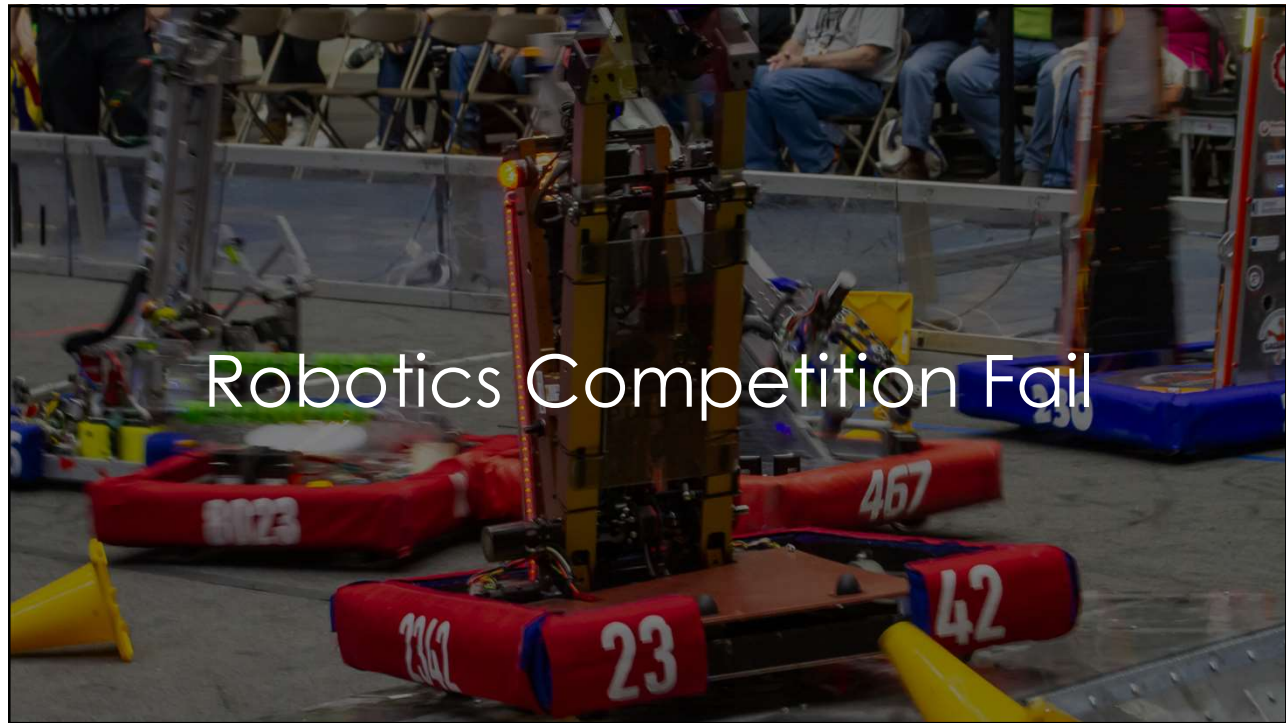
ML sub field that uses neural networks for analytical characterization to make sense of situations where multiple contexts exist

Generative AI (Gen AI)

DL sub field that can meld data from its vast library to deliver seemingly creative answers



48



49

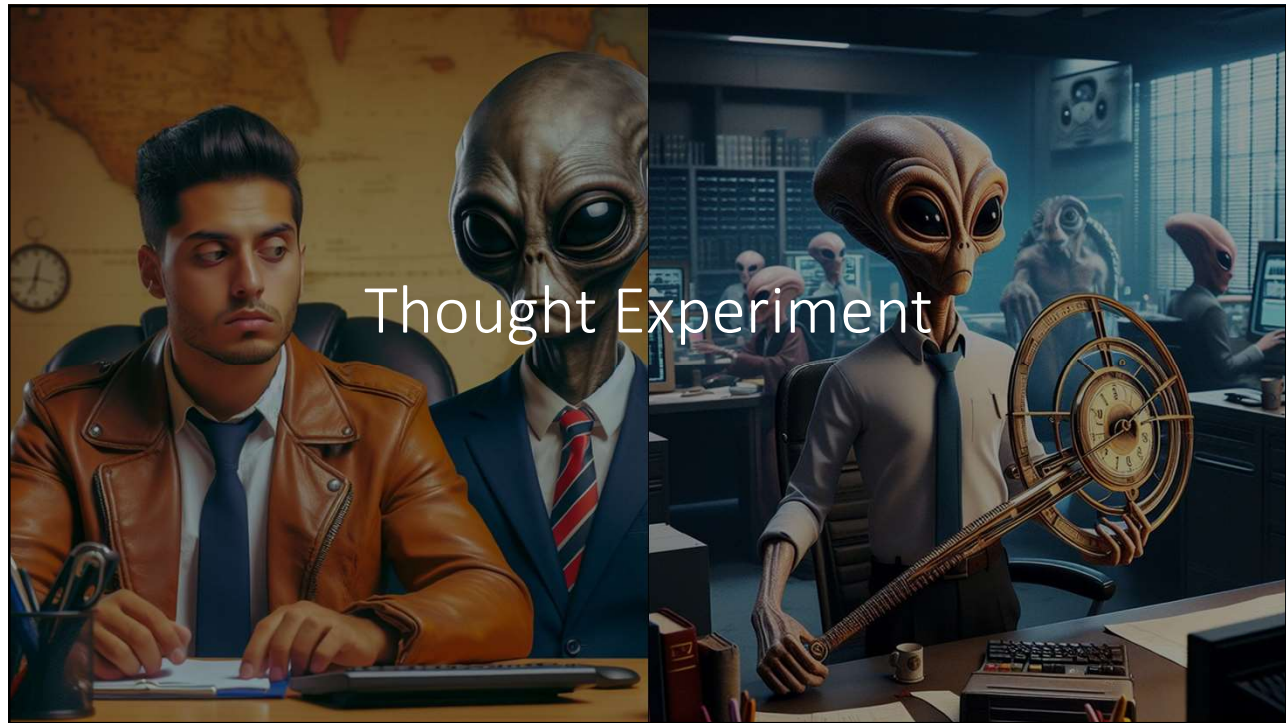
Is AI smart and/or dangerous?



PULSAR
SECURITY

- The answer is complicated, but ultimately what we see today is good at making us believe it is smart which seems dangerous
- In all cases so far, the technologies we call AI are just really, really good at making us believe they are brilliantly smart
- The reality is that none of them know anything of the significance of what is asked of them, we are not at a point where any of them would be considered sentient
- They are only dangerous if we abuse them like any other tool, but we can expect plenty of people to abuse them

50



51

Hallucinations

- AI systems are mostly working without a net and so to be as creative as possible they can make up “facts” and thereby provide false answers. We call this hallucination.
- Microsoft has added a Temperature setting that helps tamp down the chance of hallucination.
- Tread carefully!
- LiveOverflow

52

The Data Out Problem



PULSAR
SECURITY

- Users interacting with AI should NEVER:
 - Ask about proprietary ideas or methods since the maker of the AI system is a third party
 - Upload a document or other materials to an AI system that is not OK to share with the public
 - Reveal client data to an AI system they would not reveal to a random stranger
 - Think that it is impossible for the info they share with the AI to not be accessible in some way by a malicious third party (we don't know what vulnerabilities we will find in these system)
 - Trust output from an AI system without verifying it, outside that AI system

53

The Data In Problem



PULSAR
SECURITY

- Users interacting with AI should NEVER:
 - Be allowed to access proprietary data indexed by the AI system that they would not normally be given access to via normal file system permissions
 - Credentials for AI systems are likely to be just as critical as banking and other high value system access. Protect them accordingly
 - Trust output from an AI system without verifying it, outside that AI system
 - Even if the answers are not factually wrong, they can be biased based on the data that trained the model. Do not blindly follow lest you regret it later.

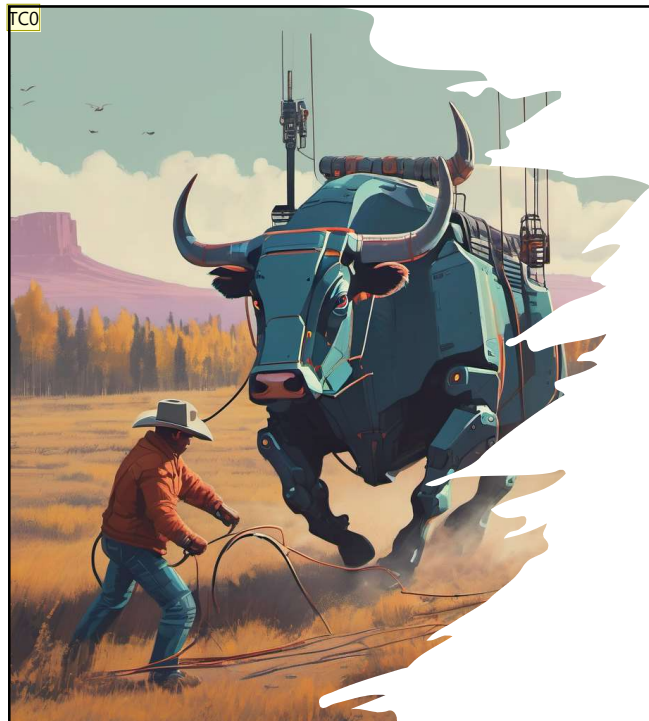
54

Questions You NEED TO ASK

- Every Software vendor is now adopting AI
- What should you ask:
 - Pseudonymization?
 - Where is your data?
 - Who owns the data?
 - How is my data isolated?
 - Is my data used in any other customers training models?
 - What protections do they have in place to prevent certain data from being accessed?
(i.e. can anyone request how much the GM is paid or PII on a particular member)




55



Manage AI Use Before It's Too Late

- Staff must first receive approval from the Business Manager to evaluate the security of any AI tool. This includes **reviewing the tool's security features, terms of service, and privacy policy**. Employees must also **check the reputation of the tool developer and any third-party services used by the tool**.
- Employees **must not upload or share any data that is confidential, proprietary, or protected by regulation** without prior approval from their Business Unit Manager. **This includes data related to customers, employees, or partners.**


56



Manage AI Use Before It's Too Late

- Any AI tool used by employees **must meet our security and data protection standards.**
- Employees must **exercise discretion when sharing information publicly and comply with international regulations. Evaluate whether the information should be shared outside the company and whether it would be appropriate in a public context.**

57



General Principle

Don't input anything into AI you wouldn't post publicly online (Passwords, PII, Sensitive Info, etc.)

58

