The Human Data Perimeter:

Mapping the Employee Threat Surface in an AI-Powered World

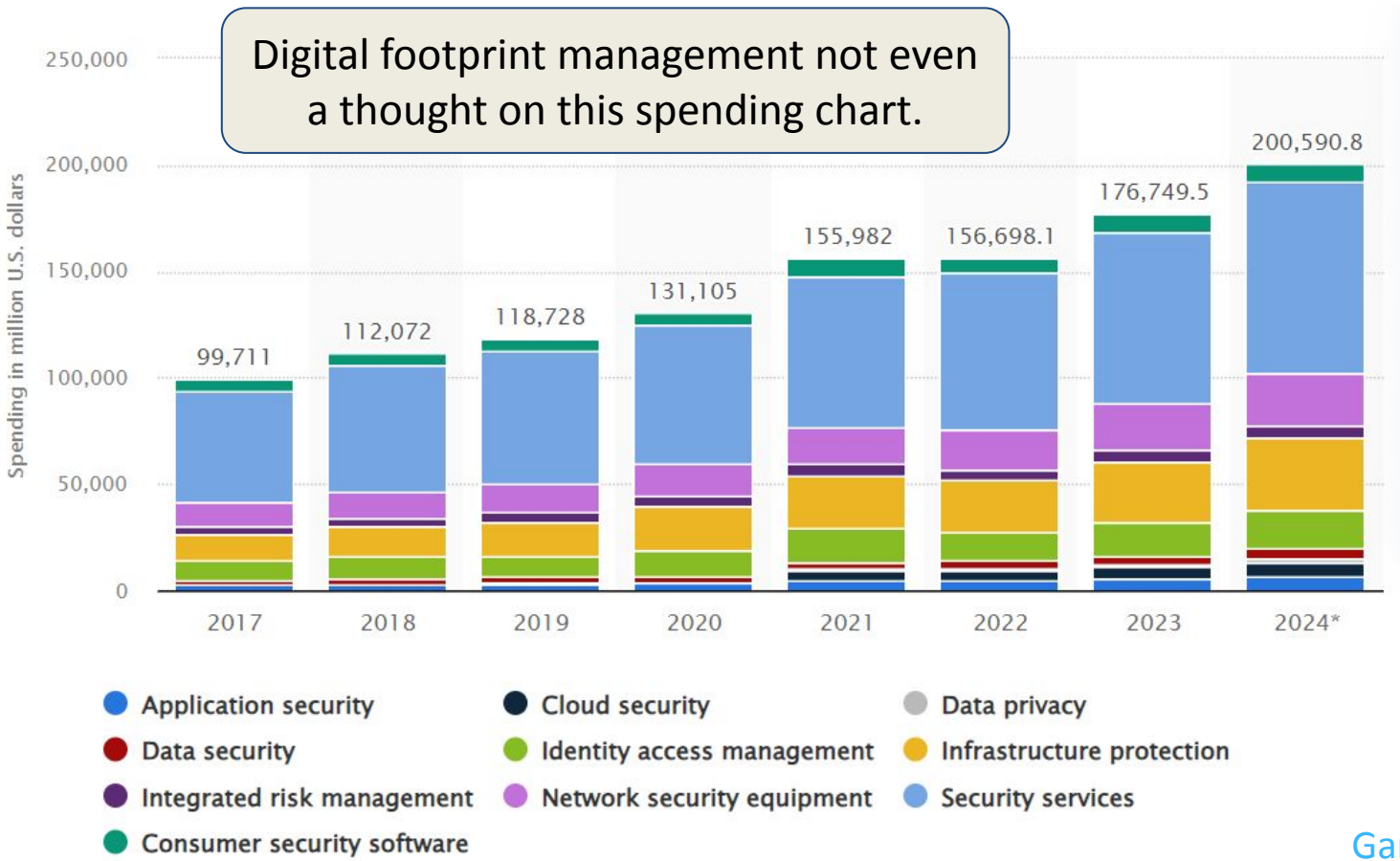
ObscureIQ 2025

Gartner expects Information Security spending to grow from $183 billion in 2024 to $292 billion by 2028.

Gartner projects that 60% of organizations will adopt digital footprint mgt tools by 2026 to protect high-risk employees from cyber threats.

Security and Risk Management End-User Spending

Digital footprint management not even a thought on this spending chart.



Gartner 2023

Let’s make a list of cyber attacks that did not utilize some form of social engineering to accomplish its goal:

1.

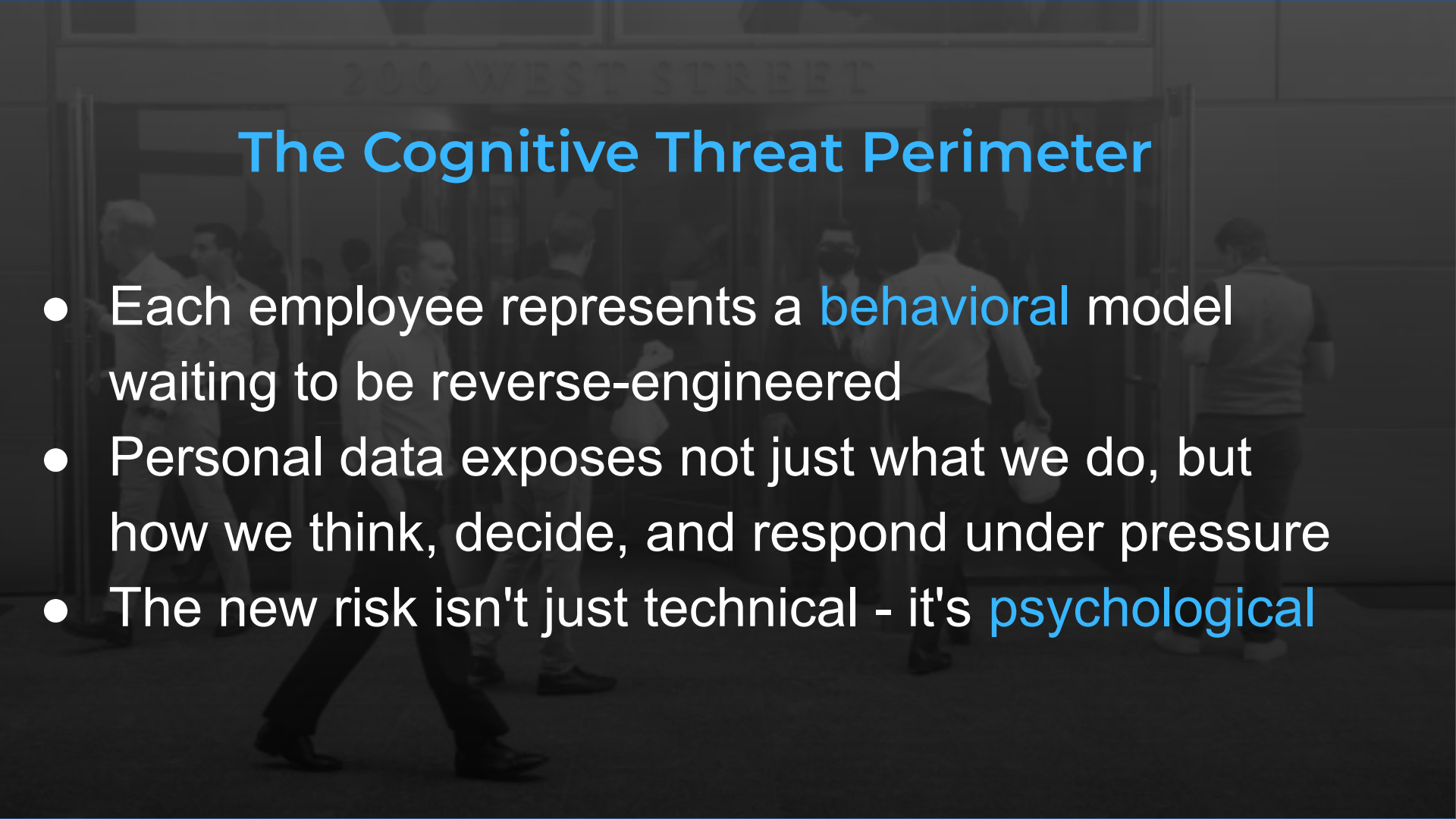
Almost all cyber attacks have a social engineering component. Humans are the easiest mechanisms to exploit.

90+% of data breaches are facilitated via employees who are inside organizational security.
And via social engineering attacks like phishing.

Social Engineering Attacks

- Phishing
- Whaling
- Baiting
- Diversion Theft
- Business Email Compromise
- Smishing
- Quid Pro Quo
- Pretexting
- Honeytrap
- Tailgating/ Piggybacking

CrowdStrike 2023

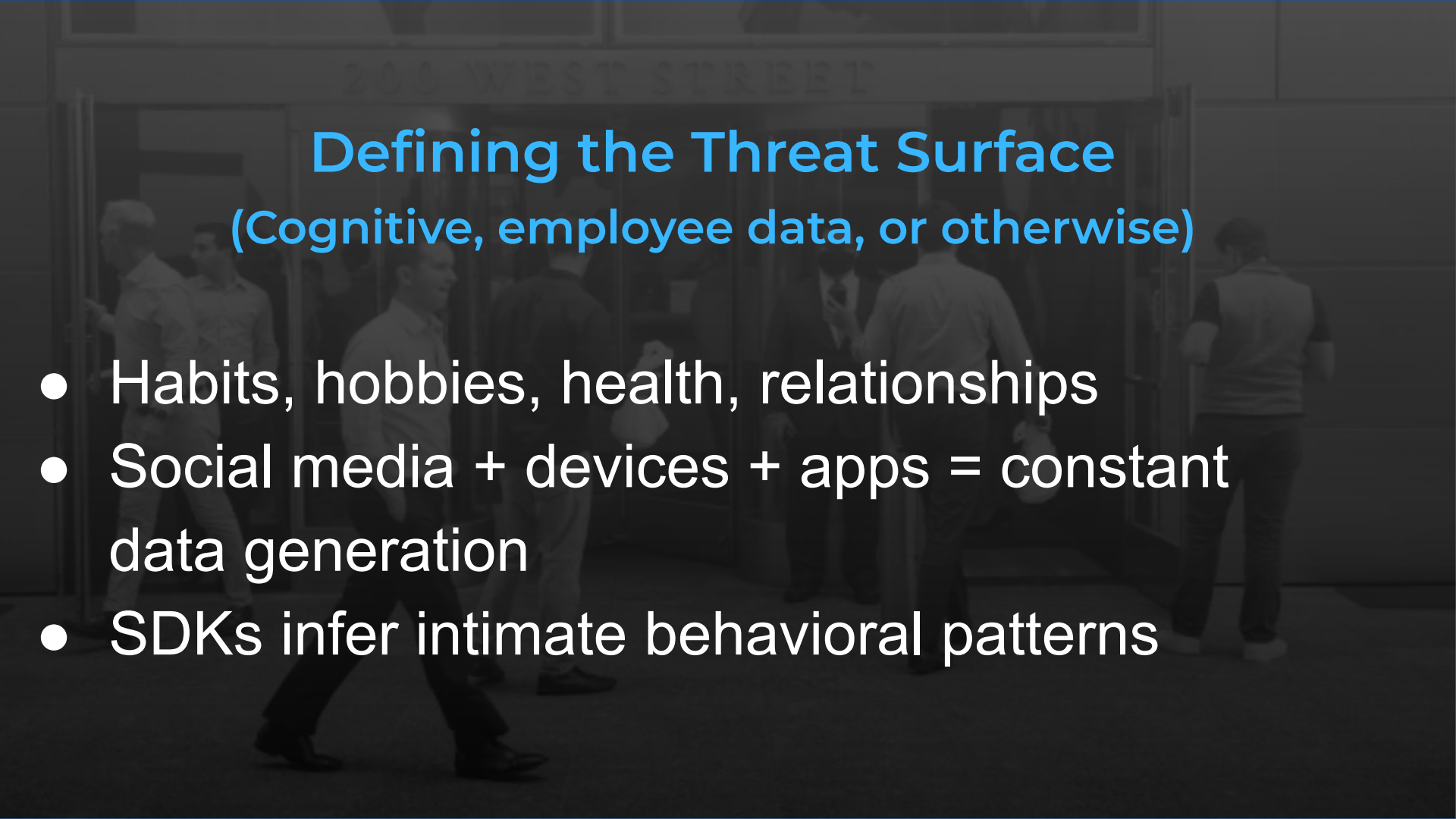


The Cognitive Threat Perimeter

- Each employee represents a behavioral model waiting to be reverse-engineered
- Personal data exposes not just what we do, but how we think, decide, and respond under pressure
- The new risk isn't just technical - it's psychological

Cognitive Engineering Vectors

- Attacks mimic trusted mental models
  - authority, urgency, reciprocity
- Success depends on hijacking **attention**, overriding **skepticism**, and exploiting **emotional bandwidth**
- These are not technical attacks - they are psychological manipulations wrapped in code



Defining the Threat Surface

(Cognitive, employee data, or otherwise)

- Habits, hobbies, health, relationships
- Social media + devices + apps = constant data generation
- SDKs infer intimate behavioral patterns


Bad actors use personal data to target & trick employees.
This is a threat surface.
Are you thinking about employee personal data as a threat surface?
Loves the Chicago Cubs
Works in the finance department
Joined a new dating site
Going on vacation next week
Going through divorce
Taking new meds

Devices can collect and infer more than we imagine! SDKs from companies like NumberEight allow CRAZY targeting.

Iceberg Model of Threat Exposure

- Top: visible data (social, career, public records)
- Submerged: ad tracking, location, breaches, profiles
- Most threats lie below the surface

Most of the personal data collected about us is hidden.

Social Media

People Search

Career Related

Public Records

Marketing Data

Advertising Tracking

Profilers & Aggregators

Data Breaches & Leaks

Credit & Risk

Location History

ObscureIQ
PRIVACY RECOVERY TECH

Data Broker Taxonomy 5.0

3rd Party Data

Companies you have likely never met or done business with

1st Party Data

Companies you know

Searchers

People Search Engines

- **Don't Know Name**
- People search: by Phone
- People search: by Email
- People search: by DOB
- People search: by Address
- People search: by Username
- People search: by Face
- People search: by Domain
- People search: by Vehicle VIN/Plate

- **Already Know Name**
- People search: General
- People search: Ancestry
- People search: Education / Alumni
- People search: Employment
- People search: Business Leads
- People search: Real Estate
- People search: Background Check
- People search: Public recs
- People search: Criminal recs
- People search: Marriage recs
- People search: Death recs
- People search: Court cases
- People search: Business Directory
- People search: Professional Dir
- People search: Membership Org
- People search: Special Interest

- People search: Leaked / Breaches Data

Screeners

Credit Bureaus/Risk Screeners

- Credit reporting: Alt
- Credit reporting: Automotive
- Credit reporting: Employment
- Credit reporting: International
- Credit reporting: Medical
- Credit reporting: Payday lending
- Credit reporting: Rental
- Credit reporting: Screening
- Credit reporting: Utilities

- Screening: Check/bank
- Screening: Employment
- Screening: General
- Screening: Risk mitigation
- Screening: Social Media
- Screening: Tenant
- Screening: Phone

Data Providers

Profilers/Aggregators

- Data Provider: **Largest Brokers**

- Data Provider: Location
- Data Provider: Biometric
- Data Provider: Demographic
- Data Provider: Education
- Data provider: Property records
- Data provider: Social media
- Data provider: Automotive

More sub-cats coming

AdTech

Advertising Technology

- AdTech: Multi

- AdTech: Identity Resolution
- AdTech: Identity Verification
- AdTech: Identity Mgt

- AdTech: Attribution / Analytics
- AdTech: Retargeting / Optimization

- AdTech: Ad Exchange
- AdTech: Ad Network
- AdTech: Ad Platform
- AdTech: Ad Server
- AdTech: DMP
- AdTech: DSP
- AdTech: SSP

- AdTech: Ad Agency
- AdTech: Market research / Survey

- AdTech: General
- AdTech: Email Verification
- AdTech: Tag Management

Monetizers

Data Monetizers

- Monetizer: Social Media
- Monetizer: Cloud / Hosting
- Monetizer: Collaboration / CRM
- Monetizer: Email
- Monetizer: Job Search
- Monetizer: Dating Site
- Monetizer: Payments / Banking
- Monetizer: Telecom
- Monetizer: ISP
- Monetizer: Shopping / Retail
- Monetizer: Fitness

- Monetizer: Search
- Monetizer: Search: Music
- Monetizer: Search: Trademark
- Monetizer: Search: Specialty

- Monetizer: Publisher Related
- Monetizer: Service Provider

- Monetizer: News: News Site
- Monetizer: News: PR
- Monetizer: News: Newspaper
- Monetizer: News: TV Station
- Monetizer: Nonprofit
- Monetizer: School

- Monetizer: Cannabis
- Monetizer: Chat
- Monetizer: City: Data

Synthetic Cognition as a Weapon

- LLMs generate targeted scripts based on personal cognitive traits
- AI mimics trust signals, emotional tone, and communication rhythms
- Attacks are now designed for your brain, not your firewall

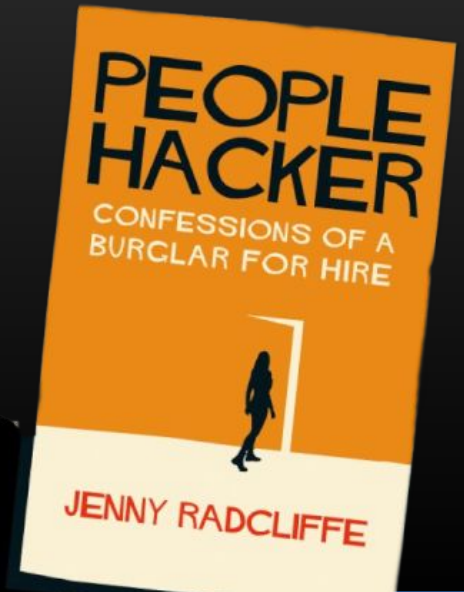
- **A New Toolkit**
  LLMs are being used to craft convincing phishing content

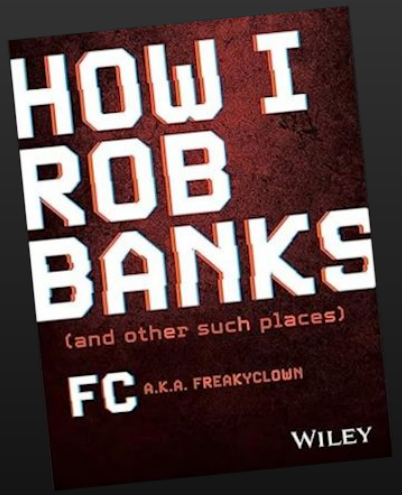
- **An Underground Economy**
  Ready-made AI phishing templates sold on the dark web
  FraudGPT, WormGPT, WolfGPT, DarkBard, etc.

- **The New “Script Kiddies”?**
  LLMs lower the technical barrier, letting less-skilled attackers create convincing attacks

What if everyone could be as good as social engineers like FC and Jenny Radcliffe?

With AI they can be...





Marks & Spencer Cyberattack (2025)

- British retailer suffered a cyberattack that disrupted ops, compromised customer data.
- Scattered Spider - known for sophisticated social engineering tactics.
- Attackers impersonated M&S employees, contacting IT help desks to request password resets. leveraging detailed knowledge of employee roles and comm styles.

Reuters coverage

AI Mimicry: Tinder Case Study

- The researcher used LLMs to craft empathetic, personalized responses, adjusting tone and content based on each match’s style, photos, and replies.
- Demographics, emotion, timing
- Phishing potential: deep personalization

GIZMODO

This Guy Used ChatGPT to Talk to 5,000 Women on Tinder and Met His Wife

Aleksandr Zhadan built a program with ChatGPT to find love, and it worked.

By **Maxwell Zeff** Published February 7, 2024 | Comments (95)

Aleksandr Zhadan and Karina Vyalshakaeva. Photo: Aleksandr Zhadan

What did Zhadan accomplish?

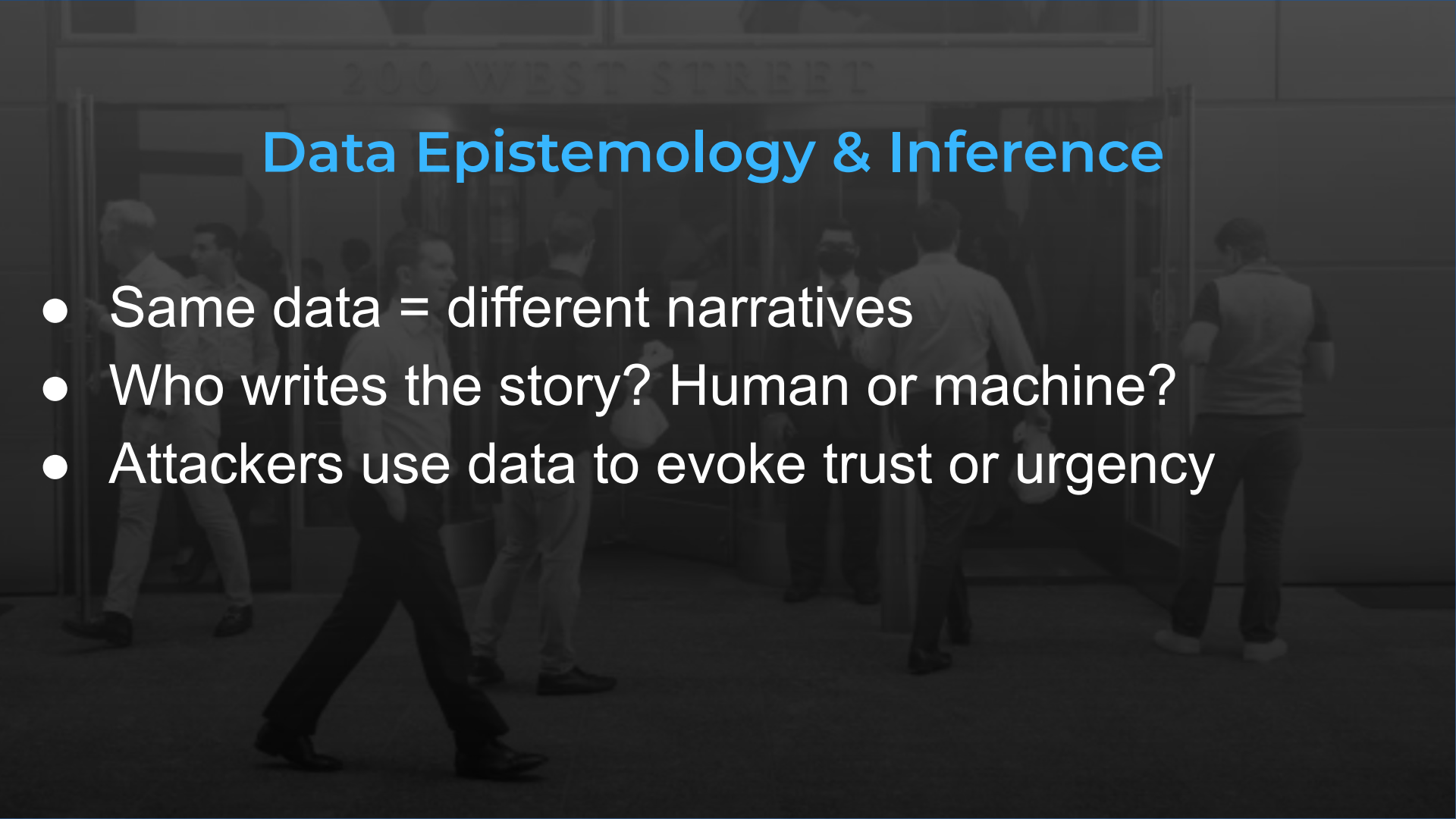
- Target demographics
- Target physical characteristics
- Target character attributes
- Interact over time
- Pass Turing Test…

Many elements of an ideal phishing campaign.

Gizmodo 2023

Arup Deepfake Video Scam (2024)

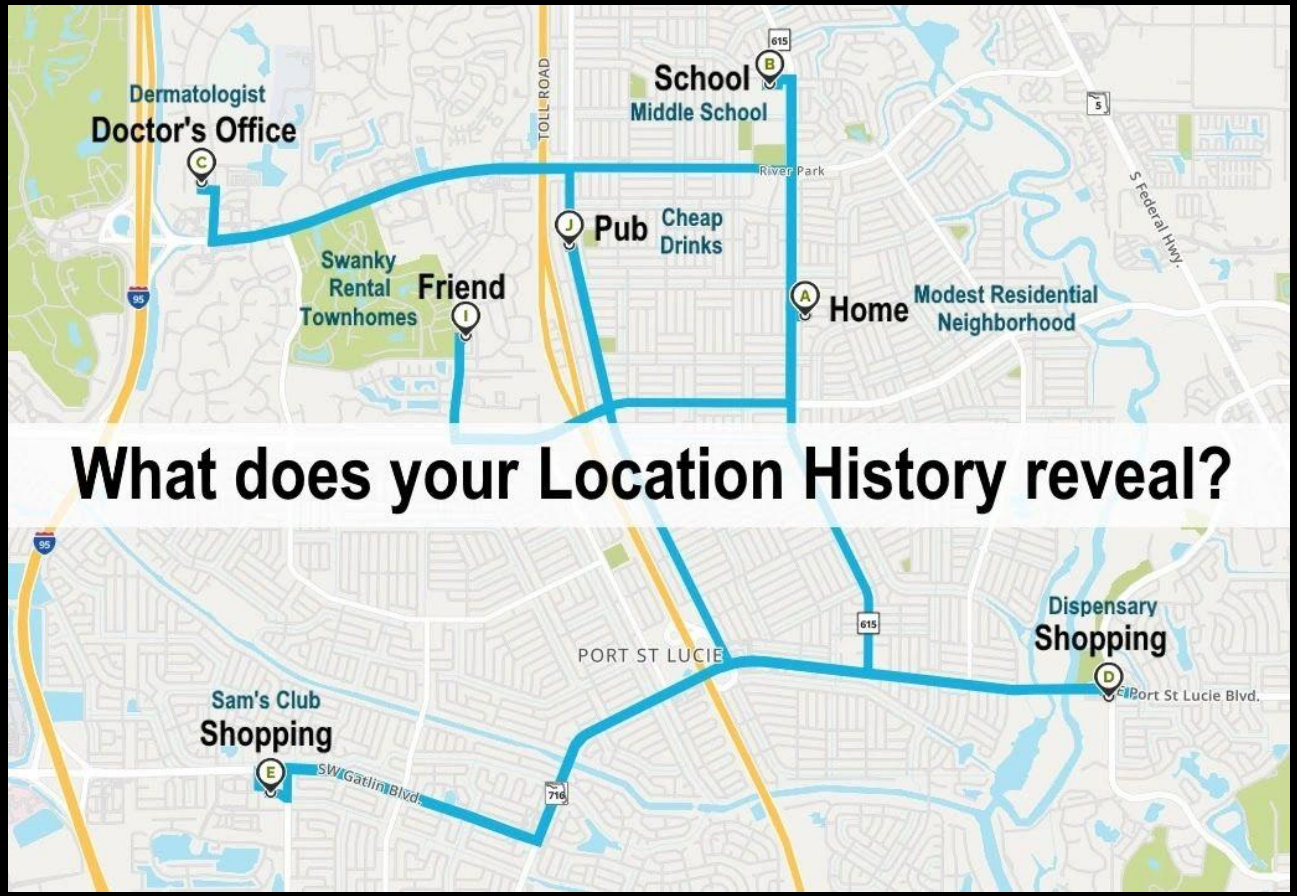
- Attack Vector: AI-generated deepfake video conference impersonating senior executives
- AI-generated deepfakes convincingly mimicking the appearance and voices of Arup's executives.
- Employee sent 15 transactions totaling approximately HK$200 million (around $25M USD)



Data Epistemology & Inference

- Same data = different narratives
- Who writes the story? Human or machine?
- Attackers use data to evoke trust or urgency

What can your location history reveal about you?



Is this the location history of a Mom with a kid in middle school who parties 🎉 a lot?

She has a skin condition, goes out on school nights, visits a friend's house for an hour almost every evening, and then hits the bar. And she appears to have a medical marijuana card.

Or is this a Single Mother working two jobs to make ends meet and caring for a sick parent?

he's working at a Doctor's office and at a bar, occasionally picking up her Father's medical marijuana order to treat his nausea. And she still manages to drop off and pick up her kid from school each day.

Enhanced for Cognitive Depth

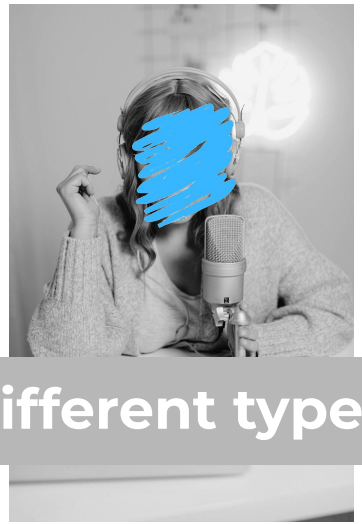
The Psychology of Exploitability

- Cognitive biases are no longer accidental vulnerabilities—they're intentional design targets
- Attacks are crafted to:
  - Confirm your preconceptions
  - Borrow credibility from familiar voices
  - Trigger emotional urgency faster than logic can intervene
- Phishing emails don't fool our systems -they fool our stories!

Threat Stratification by Role

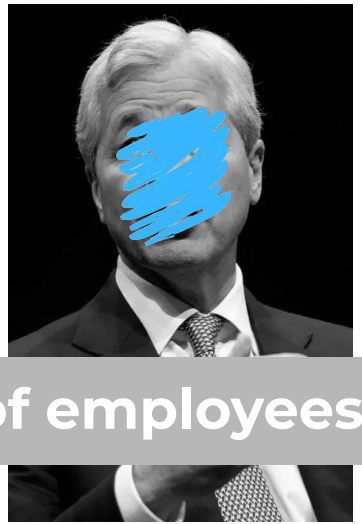
- High Visibility: Executives, influencers
- High Net Worth: C-suite, founders
- High Touch: Customer-facing staff
- High Risk: Trust & Safety, InfoSec

White Glove Service for executives and highly-visible employees
+ inexpensive packages for low-risk employees



HIGH VISIBILITY

Corporate Evangelists or Influencers



HIGH NET WORTH

C Suite & VP Level

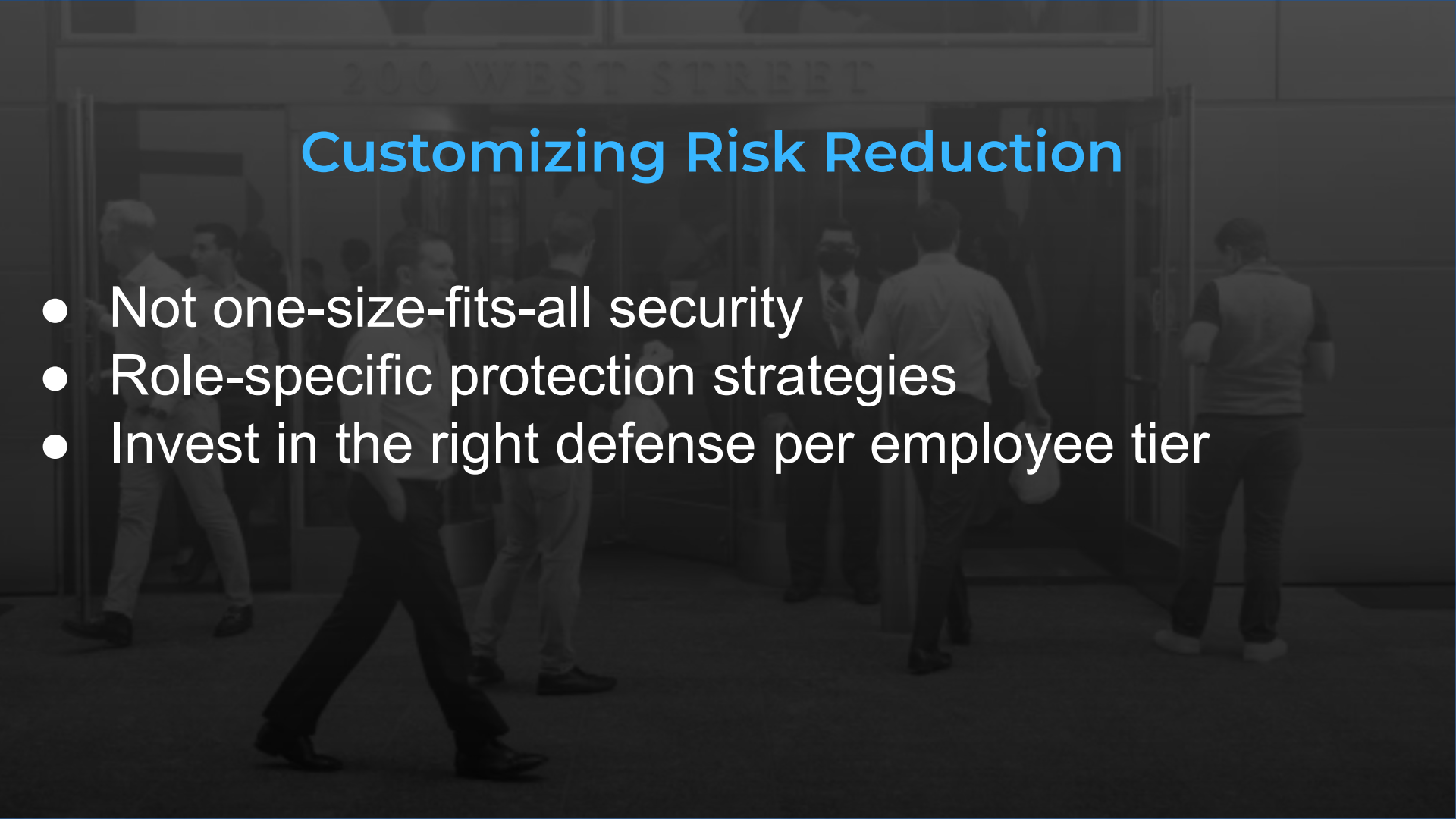
HIGH TOUCH

Front line employees

HIGH RISK

Trust & Safety Teams

Different types of employees have different needs and risks.



Customizing Risk Reduction

- Not one-size-fits-all security
- Role-specific protection strategies
- Invest in the right defense per employee tier

Strategies: Reduce the Surface

- Digital footprint management = proactive defense
- Remove data before attackers can use it
- Move from awareness to control

Strategies: Monitor for Threats

- Continuously monitor for exposed data and threats to high-risk individuals
  - Across surface web, deep web, dark web
  - Monitor for
    - Doxing detection
    - Impersonation
    - Credential and data leaks
    - Surveillance

Privacy as a Layer of Defense

- Not just IP: protect your people
- Data privacy = brand trust + internal resilience

Security as Cognitive Ecology

- Treat human security behaviors as part of an organizational cognitive system
- Build adaptive schemas, not just awareness campaigns
- The goal: reduce cognitive load, reinforce threat detection mental models, and cultivate resilience to deception

The Future is Human-Centric Security

- Continuous learning and simulation
- Behavioral monitoring + privacy controls
- Adaptive tools for evolving threats

So, let's summarize...

Summary

- Employees = modern threat surface
- AI escalates attacker capabilities
- Strategic threat surface reduction and monitoring will be the key
- Empower employees to be the first line of defense - but realize their limitations


Privacy is power.
It’s not just your corporate IP
you need to protect;
it’s your people.

Jeff JOCKISCH

ObscureIQ Co-Founder & Partner

Leading Data Privacy Researcher

Recognized Expert on Data Brokers

LinkedIn Top Voice / **YBYR**

Colby SCULLION

ObscureIQ Founder & CEO

Automation Expert

Open Source Intelligence Expert

B14ckBear Digital Recon Team Leader

CODEX of Commercial Surveillance

Over 8,600+ companies who collect personal data and who are part of the consumer surveillance economy.

The largest and deepest dataset, categorized, tagged, and scored.