

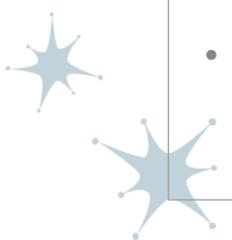
DATA PRIVACY

A USER'S PERSPECTIVE

PRESENTED BY: JIM STOKER

Finishing Before I Start

- I am a data security optimist: I believe that we can adapt to effective regulations with minimal business impact if we are smart
- Don't forget the role of the user in the process of developing rules, oversight, and processes around data security
 - This applies to all of us: Regulatory Agencies, Oversight, and Business (often, mostly business)
- Don't underestimate the complexity of the what we are discussing
 - Something that takes a book to write down, even a small one, is complex
- Technical solutions are much better than policy, but are *much* harder than you think to implement
- Treat analytics as a part of a business process, not a business process itself





OUR CLIENTS RELY ON US TO SAFEGUARD THEIR CONFIDENTIAL DATA - IT'S A RESPONSIBILITY SHARED BY EVERY TEAMMATE IN EVERY ROLE.



Technical Controls

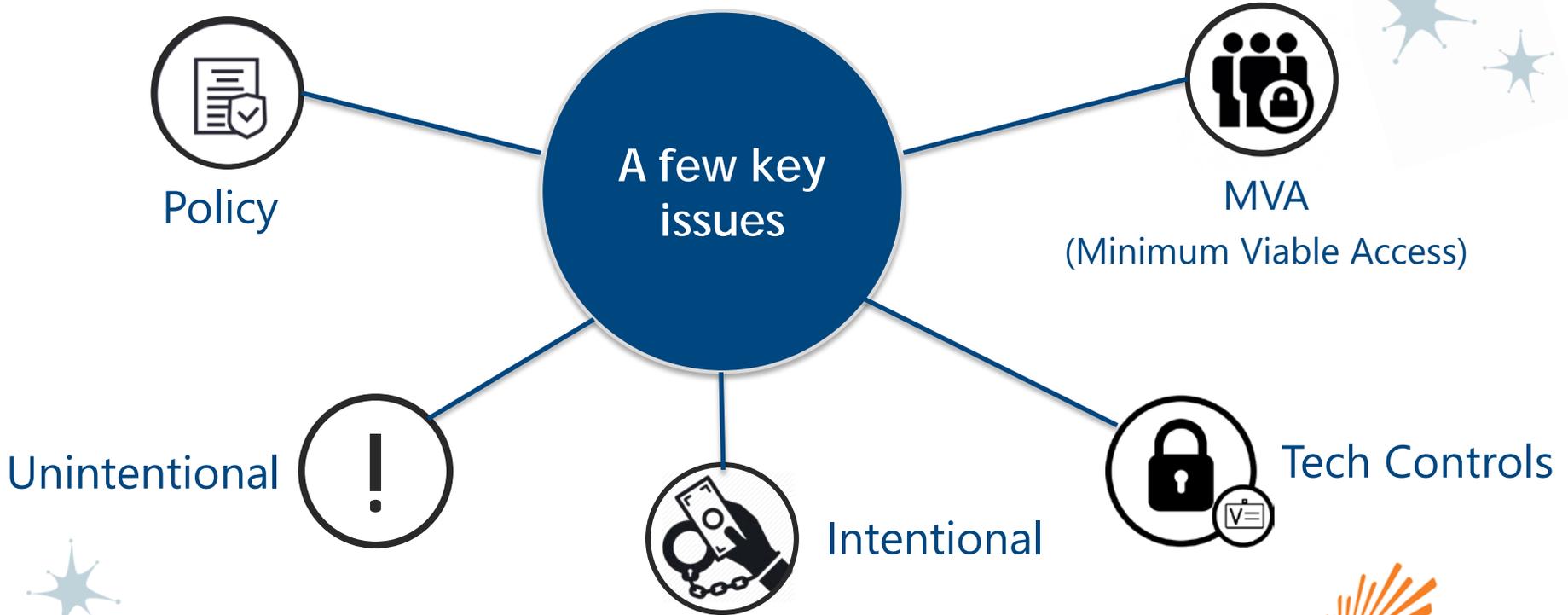
Policy



Brought to you by Cyber Security Education and Awareness



Background



Types of Data Privacy Risks: Intentional

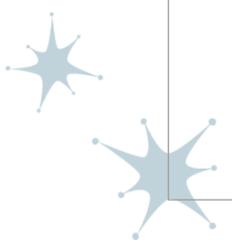
Internal Fraud: Prevention and detection of intentional sale/use looks a lot like external fraud

Prevention uses similar tools: monitoring, rules/models

Things we worry about: False positive rates, privacy concerns, creepiness

Physical controls also effective

- Phones
- Printers
- Thumb drives



Types of Data Privacy Risks: Unintentional

How is data used? This can be roughly divided between production work (reporting, dashboards, the running of models) and non-production (analytics)

PRODUCTION DATA WORK: EASY (RELATIVELY)

- Process Should be untouched by human hands
- Should be recorded
- Risk at end usage (access control)

NON PRODUCTION: HARD

- Data needs are unclear
- Very touched by human hands (in prod)
- Not recorded
- Complex results
- *MUST BE IMPLEMENTED!*

Unintentional Fraud Prevention

Reminder: Data privacy is complicated!

California Data Privacy Act

GDPR

What Next?

Change your organizational structure: Centralize data (at least a little)

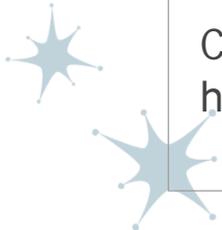
Fewer points of contact between sensitive data and users

Change your data: Smart data (masking, binning, etc)

Not as easy as it looks!

Change your business process around analytics: Have a clear handoff from non-production to production data

Implementation controls are a strong risk mitigant



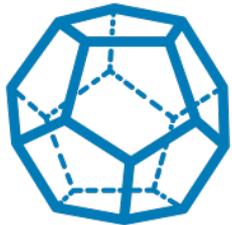
CLOSING THOUGHTS



- Technical controls are the best answer, but they are both complicated and linked to data strategy, all of which is linked to usage. This is hard.



- Treat analytics as a business process, control where data is sourced from, who touches it and how results are implemented



- Don't underestimate complexity
 - Everyone can't be an expert
 - Don't create a process that requires people to be know more then they will
 - Org structure can help here