RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **HUM-R06**

Transforming Security Through Design

J Wolfgang Goerlich

Advisory CISO
Cisco Secure
@jwgoerlich

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

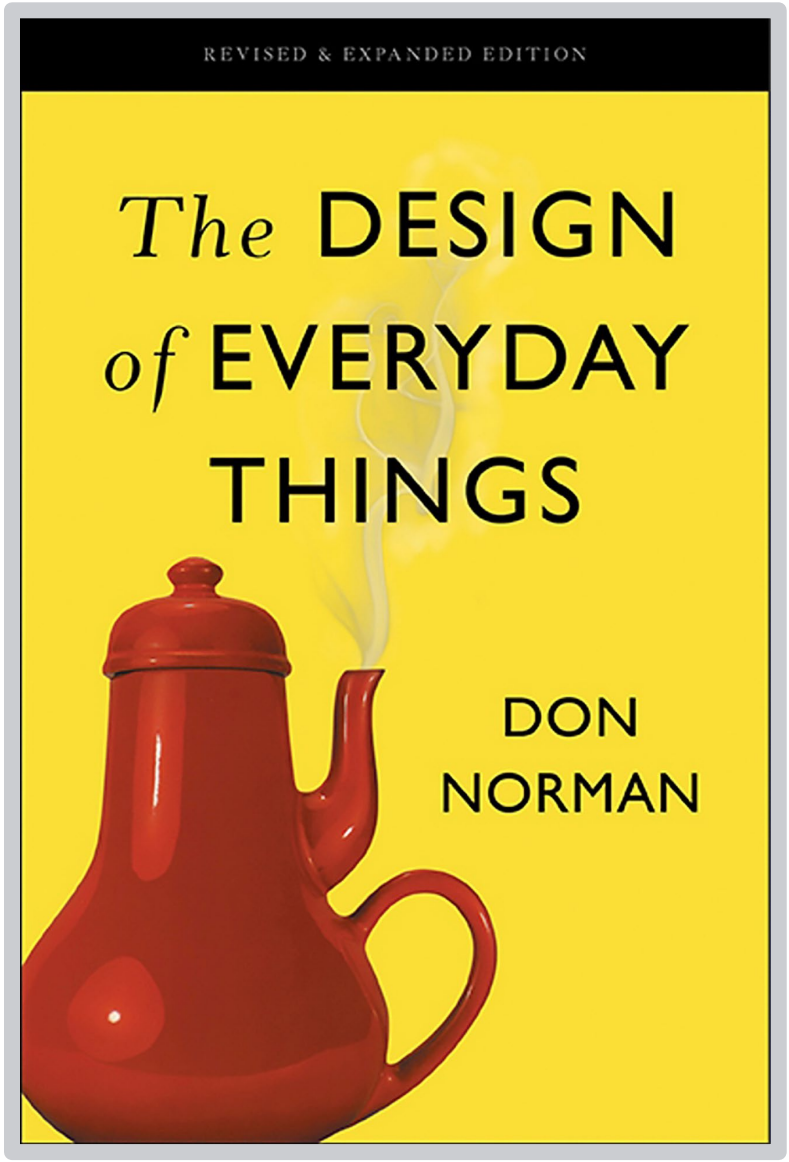
90%

of breaches are caused by people

(not an actual statistic)

Most industrial accidents are caused by human error. Estimates range from **75 to 95%.**

How is it that so many people are incompetent?



“

Answer: They aren't. It's a design problem.

-- Don Norman, *The Design of Everyday Things*

”

RSAConference2022

A Design Approach

The Model (Usability)

Paths They Take

- Number of steps
- Familiarity of each step
- Friction at each step

Choices They Make

- Number of choices
- Predictability of each choice
- Cognitive load for each choice

Usability

- Behavior or journey maps
- Control Frameworks (CSC)
- Reduce steps
- Reduce choices
- Simplify
- Clarify

“

Affordance is what the environment offers the individual.

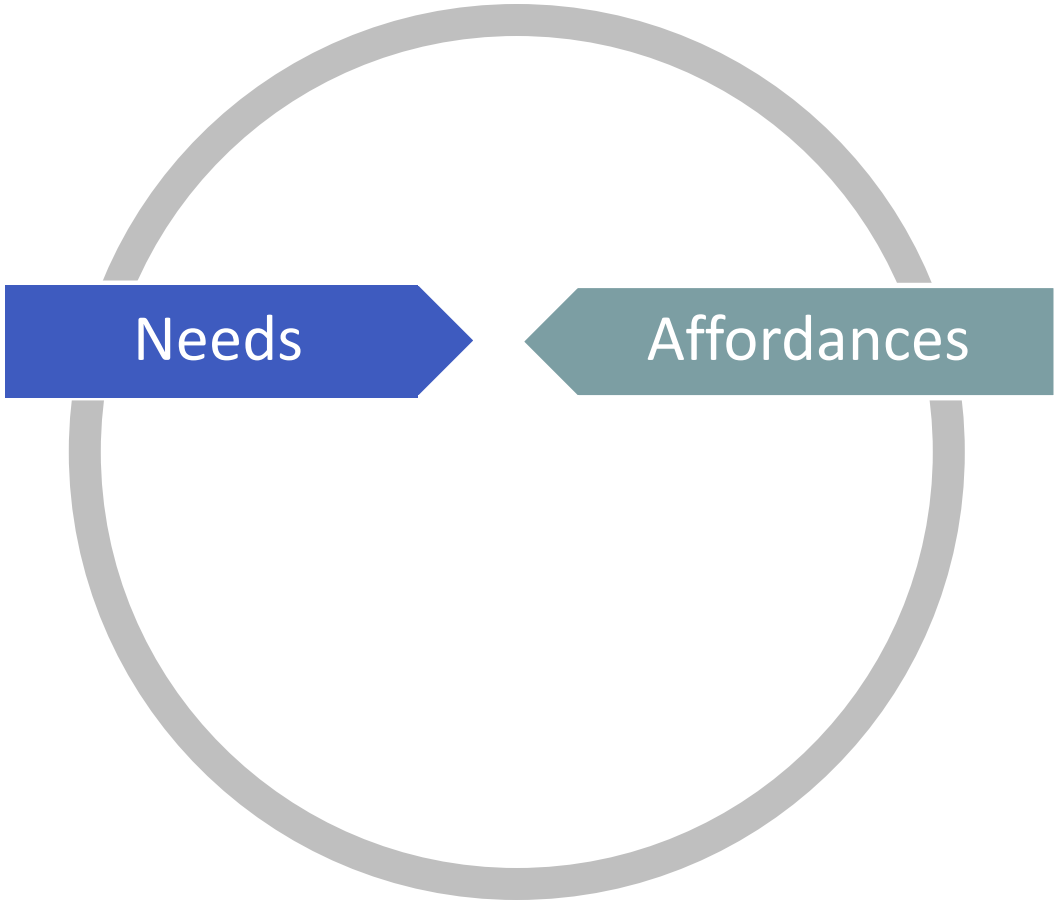
-- James J. Gibson

”

Classic affordances

End Users

- Functional
- Emotional
- Cognitive
- Physical
- Sensory



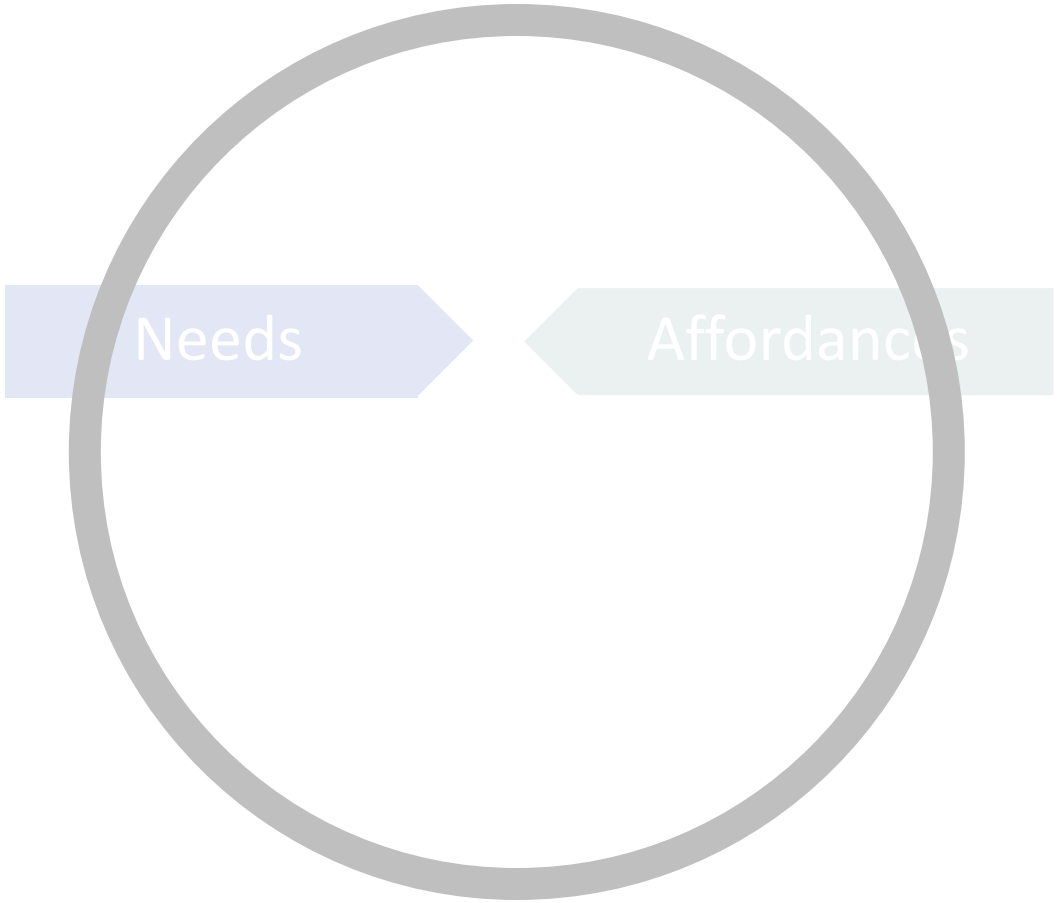
Security Design

- Functional
- Emotional
- Cognitive
- Physical
- Sensory

Cognitive, physical, sensory, and functional affordances in interaction design. BIT 22(5) (pp.315-338)

End Users

- Functional
- Emotional
- Cognitive
- Physical
- Sensory



Security Design

- Functional
- Emotional
- Cognitive
- Physical
- Sensory

Cognitive, physical, sensory, and functional affordances in interaction design. BIT 22(5) (pp.315-338)

- Security depends upon how well the needs of people are met by the affordances of the security controls.
- If they don’t meet, people will creatively satisfy their own needs with their own affordances.

Constrained users are creative, and creative users are dangerous.

RSAConference2022

Feedback

“

Nudge was written as an alternative to rules and mandates.

-- Richard Thaler

”


Nudge


Sludge

“

Sludge: friction and bad intentions.

-- Richard Thaler

”

Look at the paths they take

- Process analysis
- Journey mapping
- Behavior mapping
- Wayfinding

No. Really look.

- Expected path: IT operations
- Exception handling: Security
- Is it the path? Choices?
- What can be learned?

Bad friction along the path encourages users to bypass or avoid security.


80

Good friction is the natural consequence of poor security behaviors.

Problem: our typical metrics

"What percentage of the organization's identified vulnerabilities have not been remediated in a timely manner?"

"What percentage of the organization's hardware assets have not recently been scanned to identify unauthorized network boundaries?"

"What percentage of the organization's network devices are not located on dedicated Virtual Local Area Networks (VLANs)?"

"What percentage of the organization's accounts are not included in the organization's inventory?"

Measuring Tool: HEART

	GOALS	SIGNALS	METRICS
Happiness	User Satisfaction	Survey Ratings	Satisfaction
Engagement	User Content Discovery	Time Spent Analytics	Page Views
Adoption	User Onboarding	Signup Analytics	Signup Rates
Retention	User Loyalty	Returning User Data	Seven-day Activity, Earnings
Task Success	User Accomplishment	Usability Studies	Task Completion

Metrics

- Measure compliance rates, ***BUT ALSO***
- Measure process and communication sludge

RSAConference2022

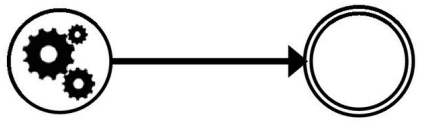
Exception Handling

Again, look at the paths they take

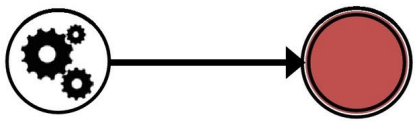
- Why do users follow the path?
- When do they forge their own?
- Expected path: IT operations
- Exception handling: Security

People breaking the rules are people communicating to us our design problems.

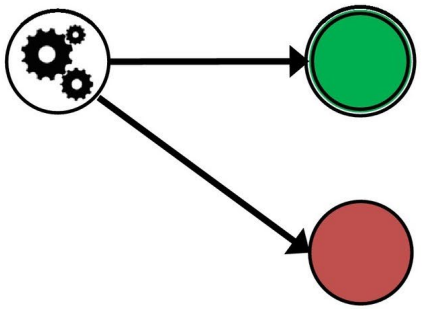
(A) No treatment effect



(B) Backfiring



(C) Treatment offset by negative side effect



(D) No treatment effect, but positive side effect

(E) Only proxy changes, not actual criterion

(F) Treatment offset by later behaviour

(G) Environment does not support change

(H) Intervention triggers counteracting forces

RSAConference2022

Culture Change


getConnection
connection.
ctSQL = "SELECT
statement.
next()


Dev ops


eCommerce
Market

Security Champion

A security champion is a member of the business itself, who collaborates with the security team on best practices.

- Share and contextualize security knowledge
- Plan to turn action to behavior
- Provide peer support

Security Advocate

A security advocate is a member of the security team who focuses on getting practices into the hands of the workforce.

- Share and contextualize business knowledge
- Fight sludge and security fatigue
- Connect champions to wider community

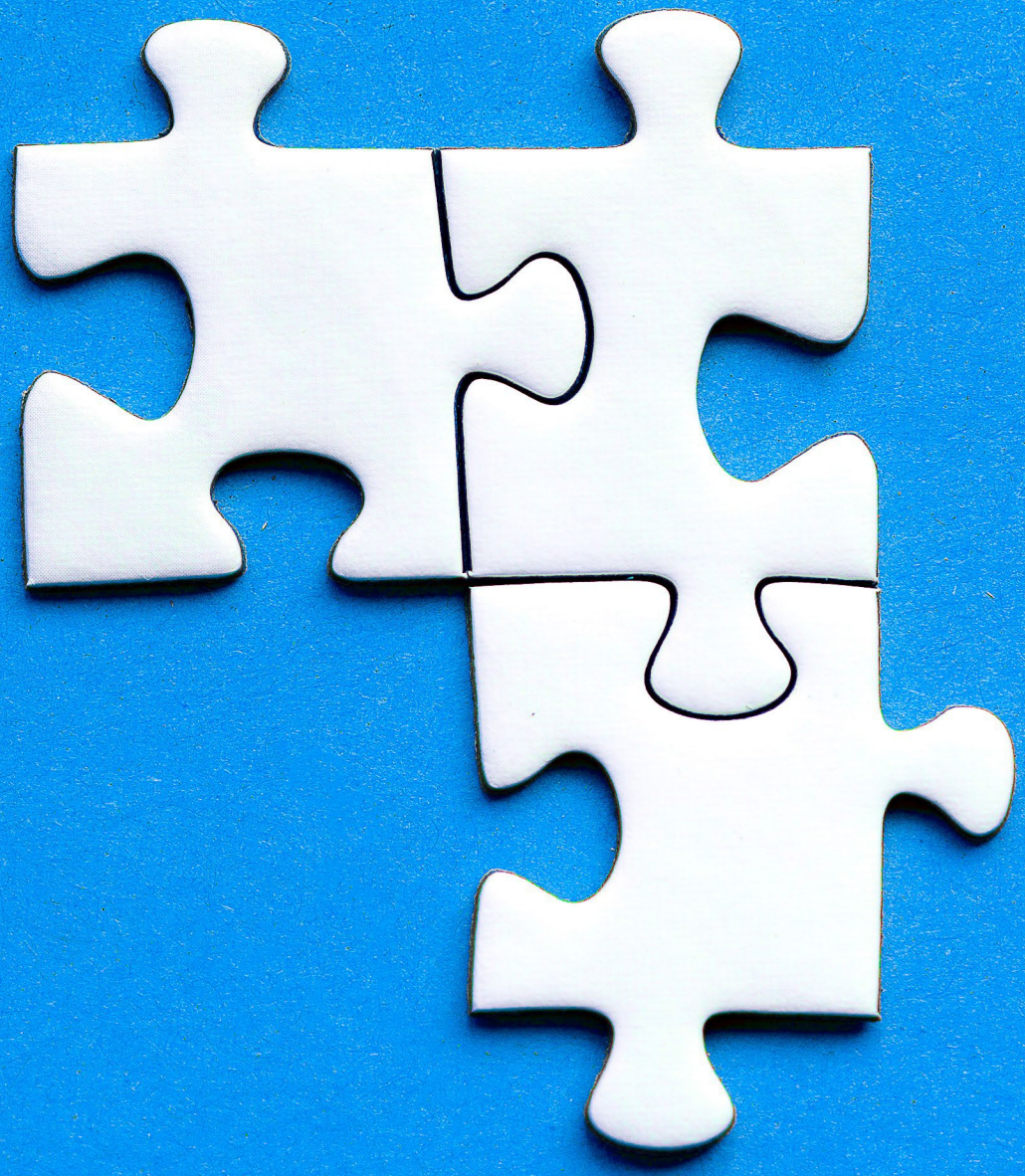
Security **Advocate**

Security **Champion**

Security SME

Business SME

Advocate/champion programs are for making informed decisions, not simply carrying out things already decided.

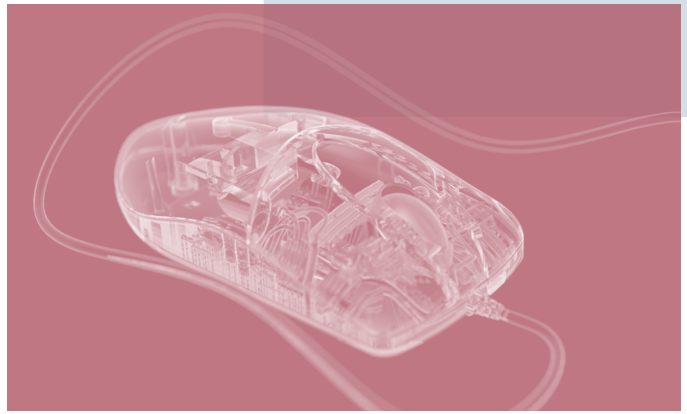


RSAConference2022

Defend

Usability

Defensibility



Manageability

Auditability

Fifth Ability: Marketability (out of scope)

Business case

- What does the capability enable?
- What does the capability prevent?
- How easier will it be to run?
- How compliant will it make us?

The Model (Defensibility)

Paths They Take

- Number of steps
- Familiarity of each step
- Friction at each step

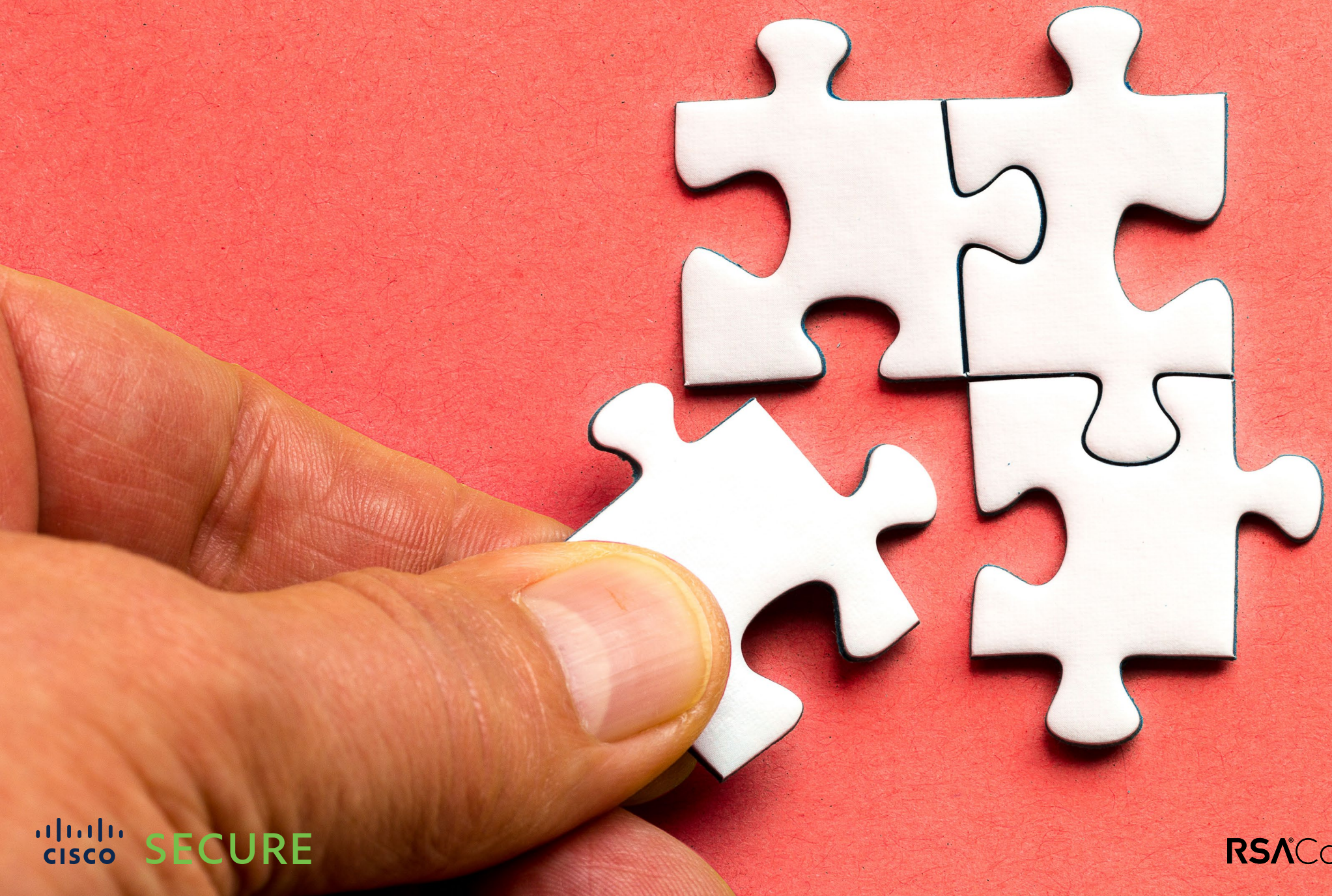
Choices They Make

- Number of choices
- Predictability of each choice
- Cognitive load for each choice

Defensibility

- Threat model or attack path
- Mitre ATT&CK
- Increase steps
- Increase choices
- Complicate
- Confound

Good security gets out of the way of users while getting in the way of adversaries.



RSAConference2022

Final Thoughts

Roadmap depends on where we are

- Before: using this design approach for security architecture and planning
- During: using this design approach as part of an active security initiative
  (example: building an IAM program)
- After: using this design approach to troubleshoot and address security problems in an ongoing business area
  (example: securing DevOps)

Introducing design into security programs

- Next week you should:
  - Identify an area that would benefit from a human-centric design approach
- In the first three months following this presentation you should:
  - Map out the processes (usability)
  - Map out the attack paths (defensibility)
  - Evaluate controls and establish metrics
- Within six months you should:
  - Map out manageability and audit
  - Implement the controls and establish feedback
  - Tune the controls and policy to reduce impact on users while increase impact on adversaries

Thank you!

cisco SECURE