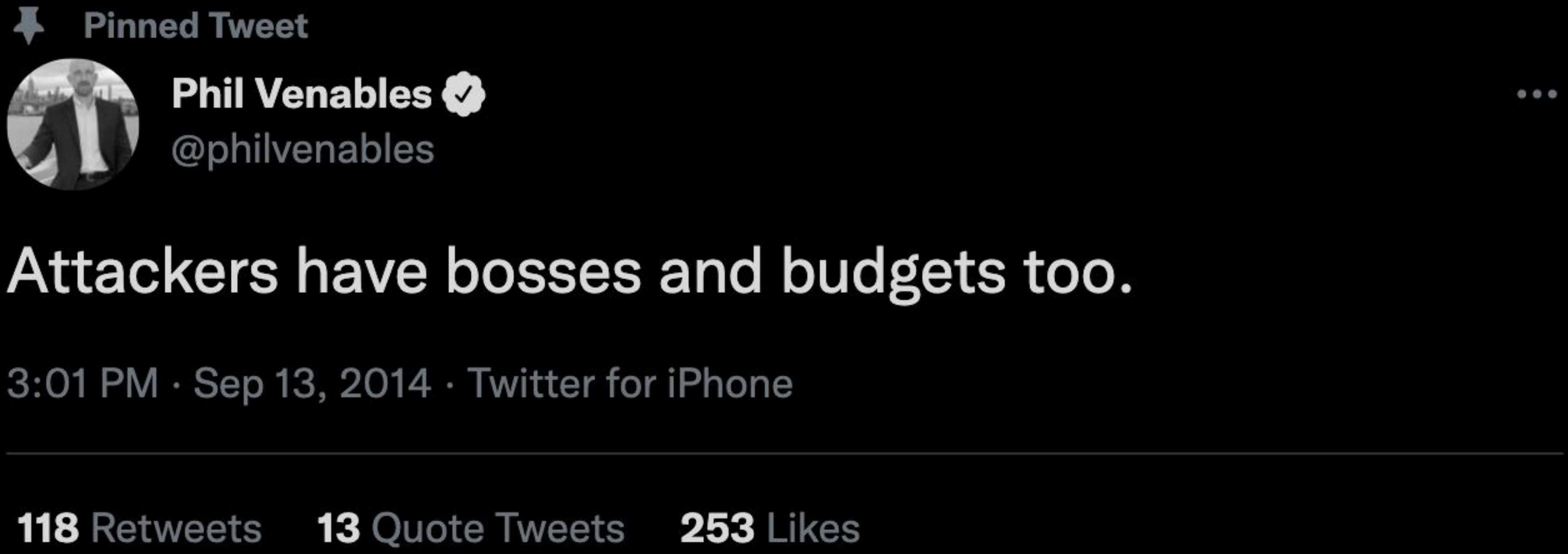
Security Checklists

Surprisingly effective
at scale

Sean Cassidy, Head of Security at Asana

December 17, 2021



Pinned Tweet

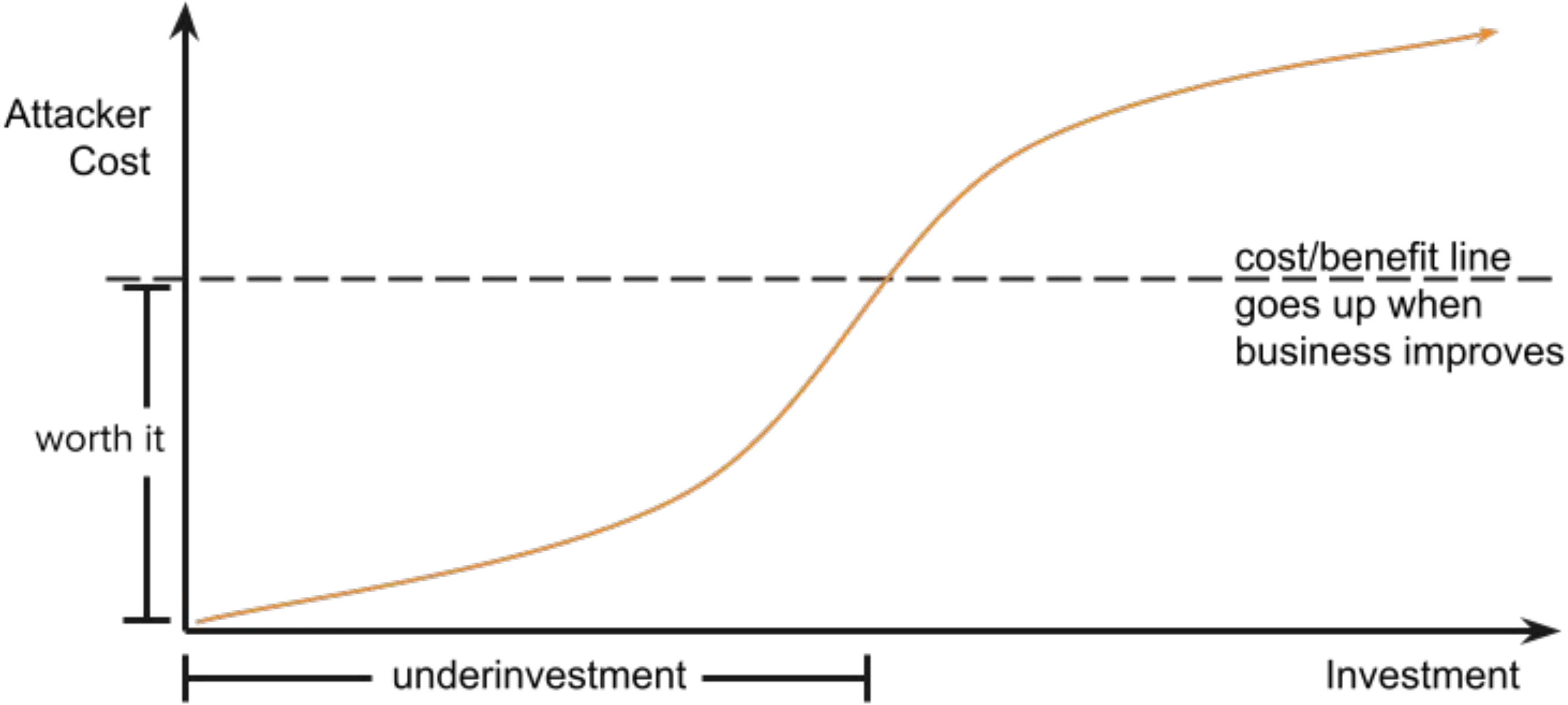
Phil Venables

@philvenables

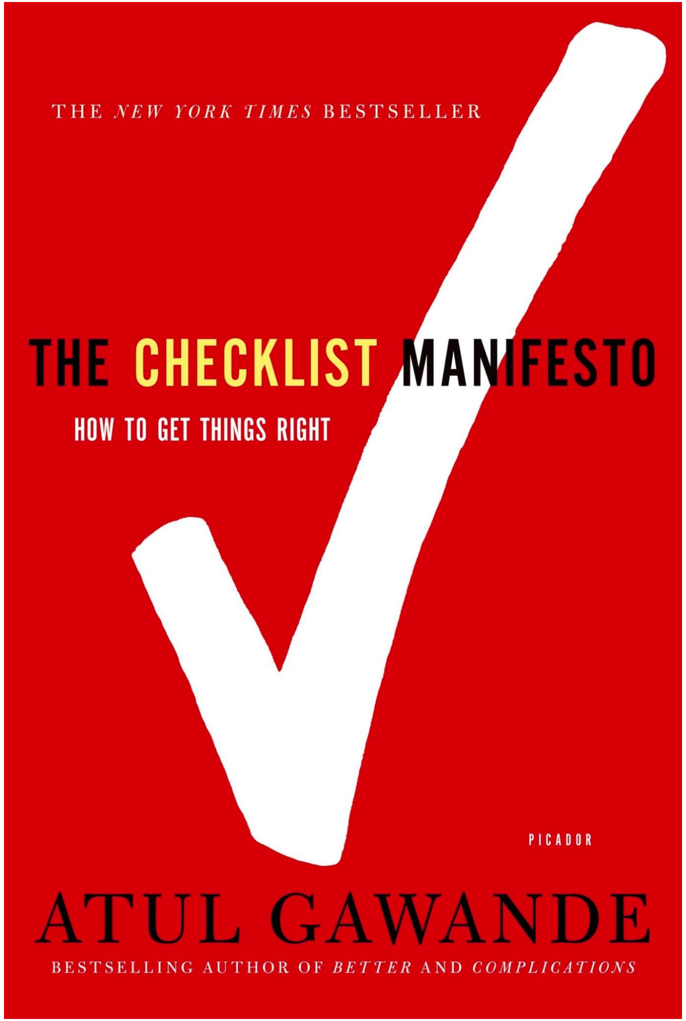
Attackers have bosses and budgets too.

3:01 PM · Sep 13, 2014 · Twitter for iPhone

118 Retweets **13** Quote Tweets **253** Likes


Attacker Cost
cost/benefit line goes up when business improves
worth it
underinvestment
Investment

Reducing internal costs is just as important as raising attacker costs



THE *NEW YORK TIMES* BESTSELLER

THE CHECKLIST MANIFESTO

HOW TO GET THINGS RIGHT

PICADOR

ATUL GAWANDE

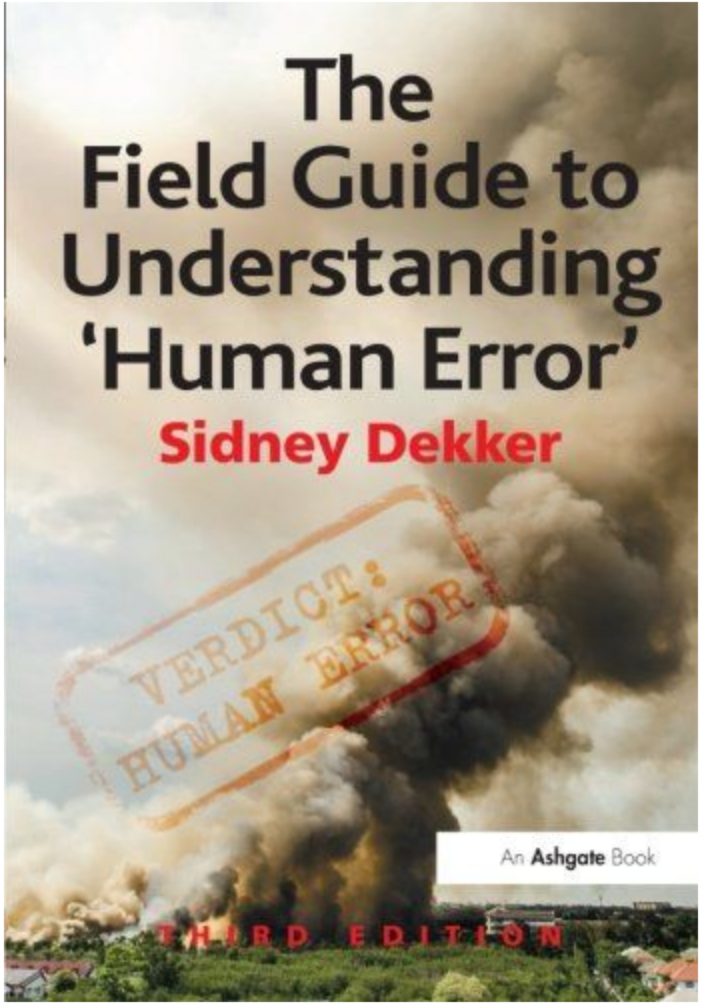
BESTSELLING AUTHOR OF *BETTER* AND *COMPLICATIONS*

When do checklists work so well?

- ❑ Complex situations that require expertise
    - ❑ Specialization leading to Super-specialization
- ❑ Time pressure
- ❑ Consistency is critical
- ❑ Situation is stressful
- ❑ There are easy-to-ignore steps

Checklists let you ignore some tradeoffs

Freedom	☑	Discipline
Craft	☑	Protocol
Specialized abilities	☑	Group collaboration



The Field Guide to Understanding 'Human Error'

Sidney Dekker

VERDICT: HUMAN ERROR

An Ashgate Book

THIRD EDITION

When do humans make mistakes?

- ❑ Complexity
- ❑ Novel situations that seem routine
- ❑ Subtle distinctions
- ❑ “Blame and train”
- ❑ Assumptions necessary for speed

Problem statement

We can only do security reviews for X% of new features.

If we don’t do them, only Y% of features have a threat model.

We’ve seen Z security incidents from features with no security review/threat model.

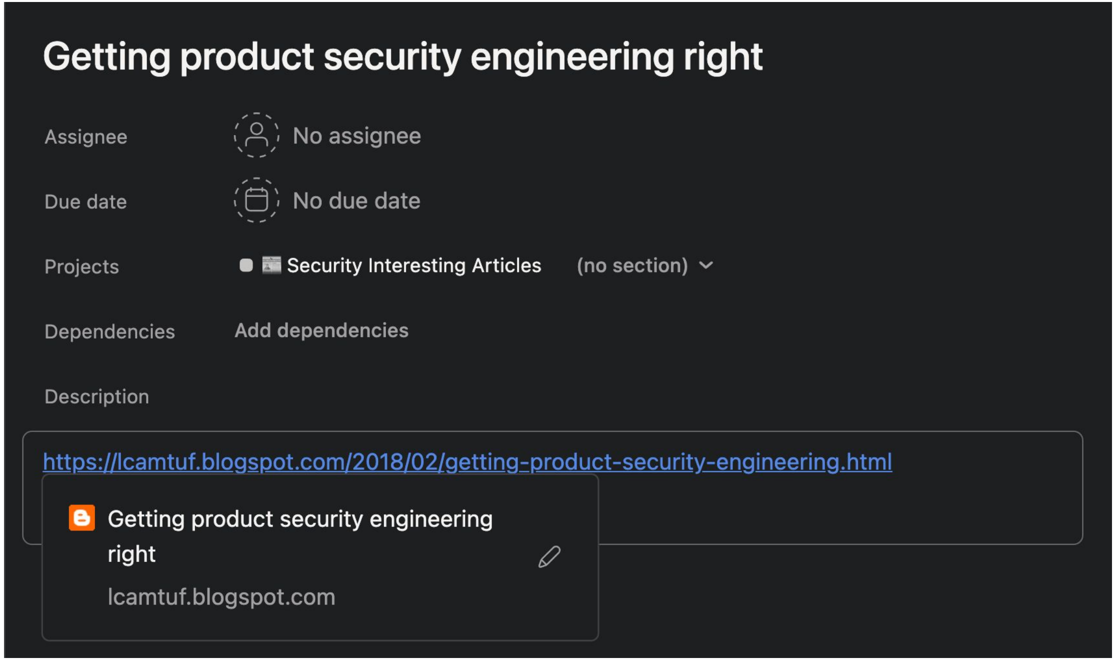
What can we do to fix it?

- ❑ Meet with teams to tell them how important threat modeling is
- ❑ Train every engineer how to threat model
- ❑ Staff up a security review team
- ❑ Block every feature on security review
- ❑ etc.

It’s not worth teaching every engineer how to threat model

Imagine this new feature

- We don’t have link previews. Our users want this. So let’s add it!



Getting product security engineering right

Assignee No assignee

Due date No due date

Projects Security Interesting Articles (no section)

Dependencies Add dependencies

Description

https://lcamtuf.blogspot.com/2018/02/getting-product-security-engineering.html

Getting product security engineering right

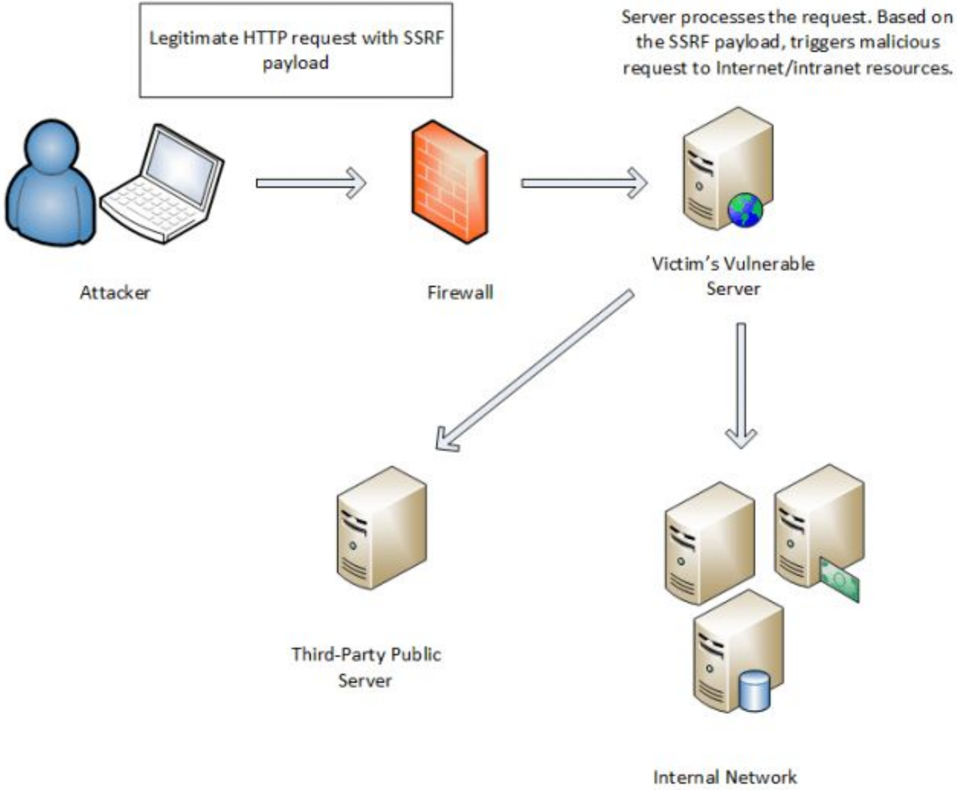
lcamtuf.blogspot.com

An example of STRIDE for a new feature

- ❑ Spoofing
  - ❑ We’re authenticating requests using our normal framework, so let’s mark as N/A
- ❑ Tampering
  - ❑ I guess someone could give us a malformed URL, but that would just error. We’re using a standard URL parsing library, so N/A
- ❑ Repudiation
  - ❑ We log requests, so we’re good, right? N/A
- ❑ Information Disclosure
  - ❑ We’re using existing frameworks, so let’s mark as N/A
- ❑ Denial of Service
  - ❑ I’m pretty sure Infra handles this, so I’ll mark as N/A
- ❑ Elevation of privilege
  - ❑ My app only has two roles, and another team owns that so I’ll mark as N/A

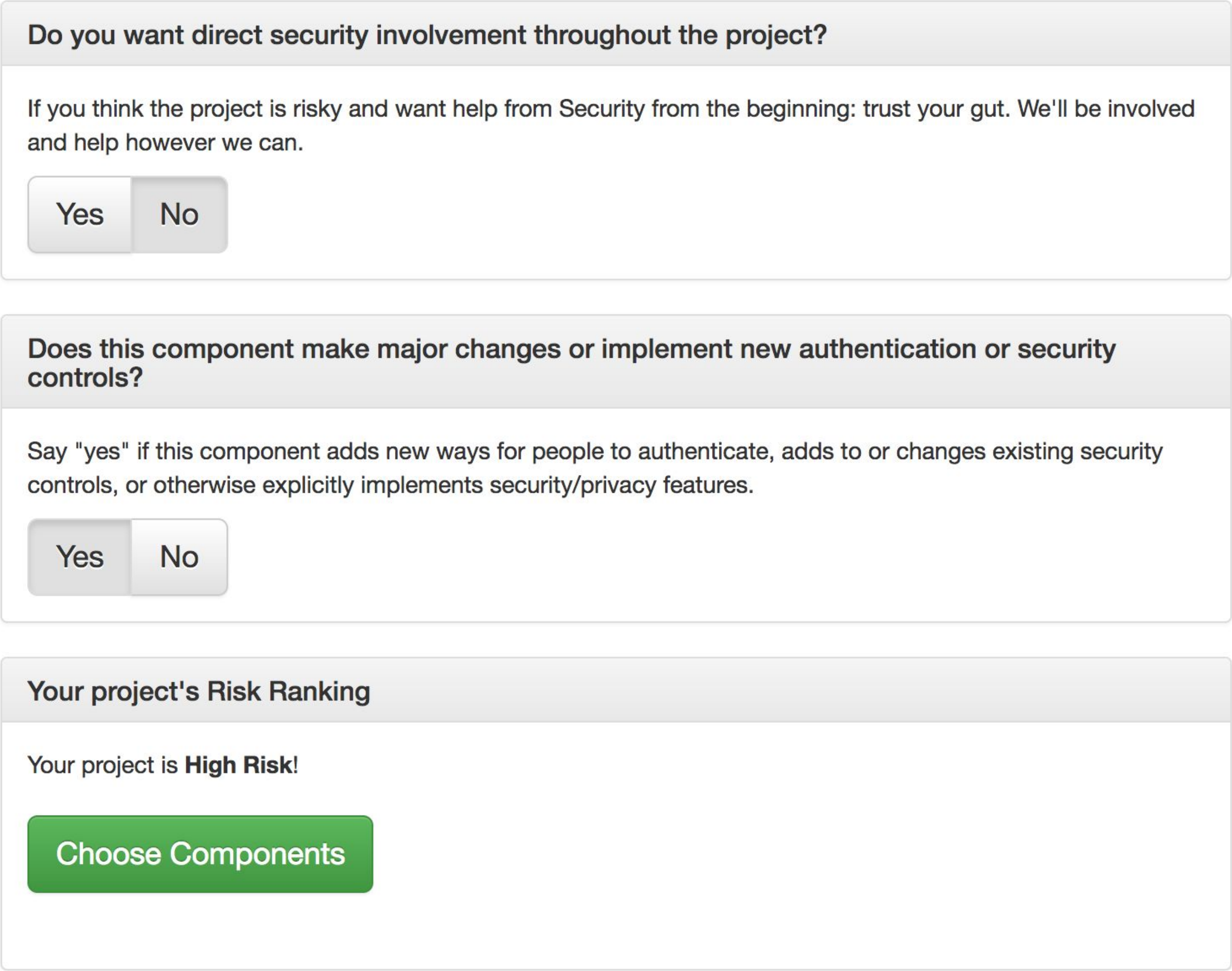
What did this threat model miss?

SSRF!


Legitimate HTTP request with SSRF payload
Server processes the request. Based on the SSRF payload, triggers malicious request to Internet/intranet resources.
Attacker
Firewall
Victim's Vulnerable Server
Third-Party Public Server
Internal Network

Counterpoints

- “They didn’t threat model properly!”
  - Yes, my point isn’t that threat modeling is useless, but that rather it takes effort to do. Busy developers are busy, and generally won’t spend enough time developing a threat model that’s good enough to catch things.
- “STRIDE isn’t the only threat model”
  - Yes, but this is representative of most threat modeling frameworks.
- “Threat models should be reviewed by security”
  - We don’t have time to review every threat model. We can only review a fraction of them.
- “Threat models are still useful”
  - Agree! When we have time to make them, we still make them. Done well, they’re very valuable.



Do you want direct security involvement throughout the project?

If you think the project is risky and want help from Security from the beginning: trust your gut. We'll be involved and help however we can.

Yes [✓ No]

Does this component make major changes or implement new authentication or security controls?

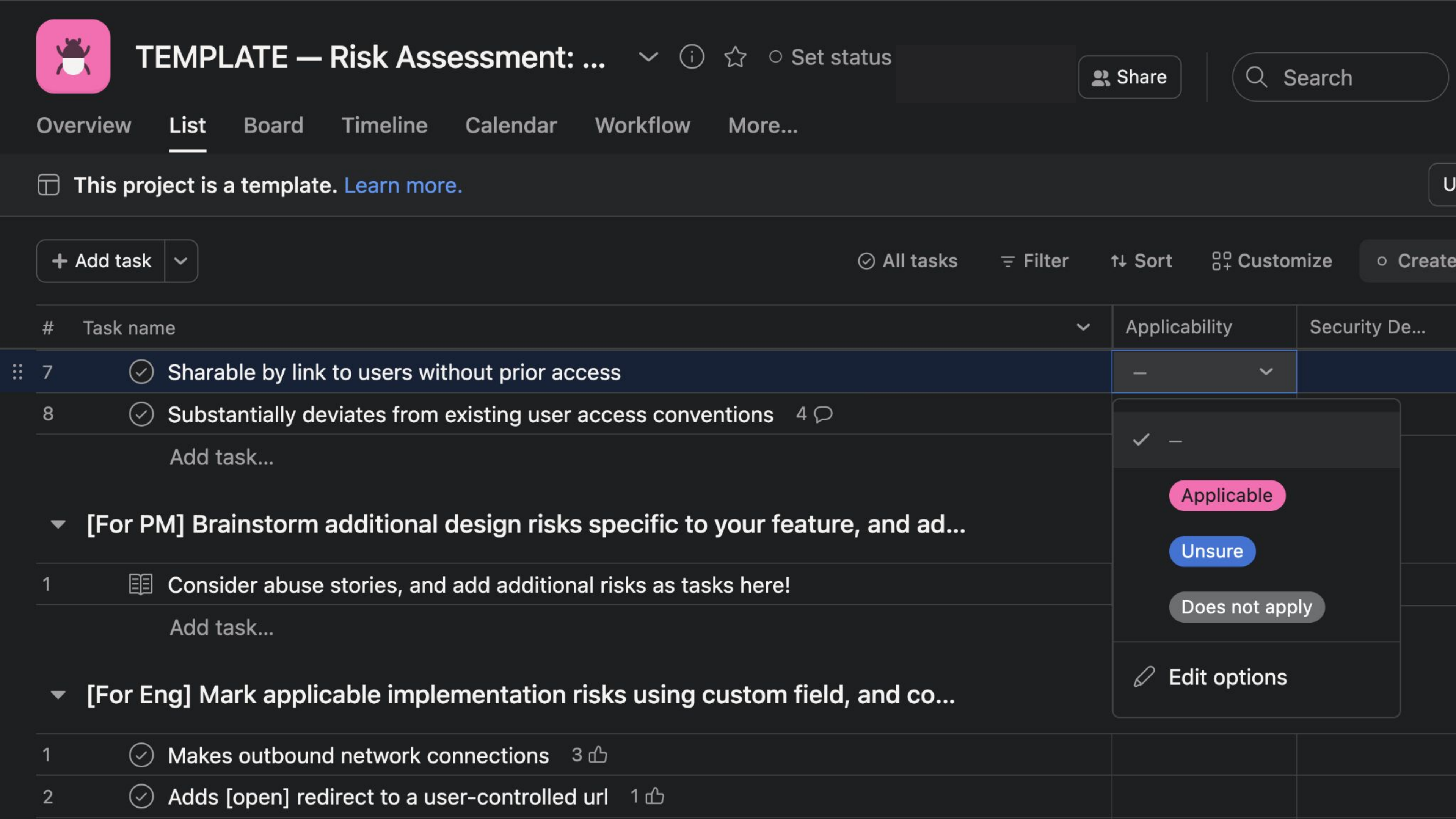
Say "yes" if this component adds new ways for people to authenticate, adds to or changes existing security controls, or otherwise explicitly implements security/privacy features.

[✓ Yes] No

Your project's Risk Ranking

Your project is **High Risk**!

Slack's goSDL



This project is a template. Learn more.

#	Task name	Applicability	Security De...
7	Sharable by link to users without prior access	–	
8	Substantially deviates from existing user access conventions 4		
	Add task...		

[For PM] Brainstorm additional design risks specific to your feature, and ad...

#	Task name
1	Consider abuse stories, and add additional risks as tasks here!
	Add task...

[For Eng] Mark applicable implementation risks using custom field, and co...

#	Task name
1	Makes outbound network connections 3
2	Adds [open] redirect to a user-controlled url 1

Here’s how it works

- ❑ Whenever a new feature is considered at Asana, a PM will add a task to a centralized project
- ❑ This task has a lot of subtasks to do various things
- ❑ One of them is fill out a security risk assessment for their feature
- ❑ It asks questions of them, like “Do you use cryptography?”
- ❑ It’s easy to fill out and serves as useful documentation
- ❑ Security team can scan and decide if they want to get more involved

Tips for using this well

- ❑ Embed this wherever your developers are doing their work
  - ❑ Design docs
  - ❑ Product management review
  - ❑ Production readiness review
  - ❑ etc.
- ❑ Don’t use another new tool, use whatever you’re already using
- ❑ Emphasis on easy: skip jargon and terms of art when you can. Include descriptions and examples.
- ❑ Read all of the filled out checklists and judge which ones to get involved with.
- ❑ Iterate.

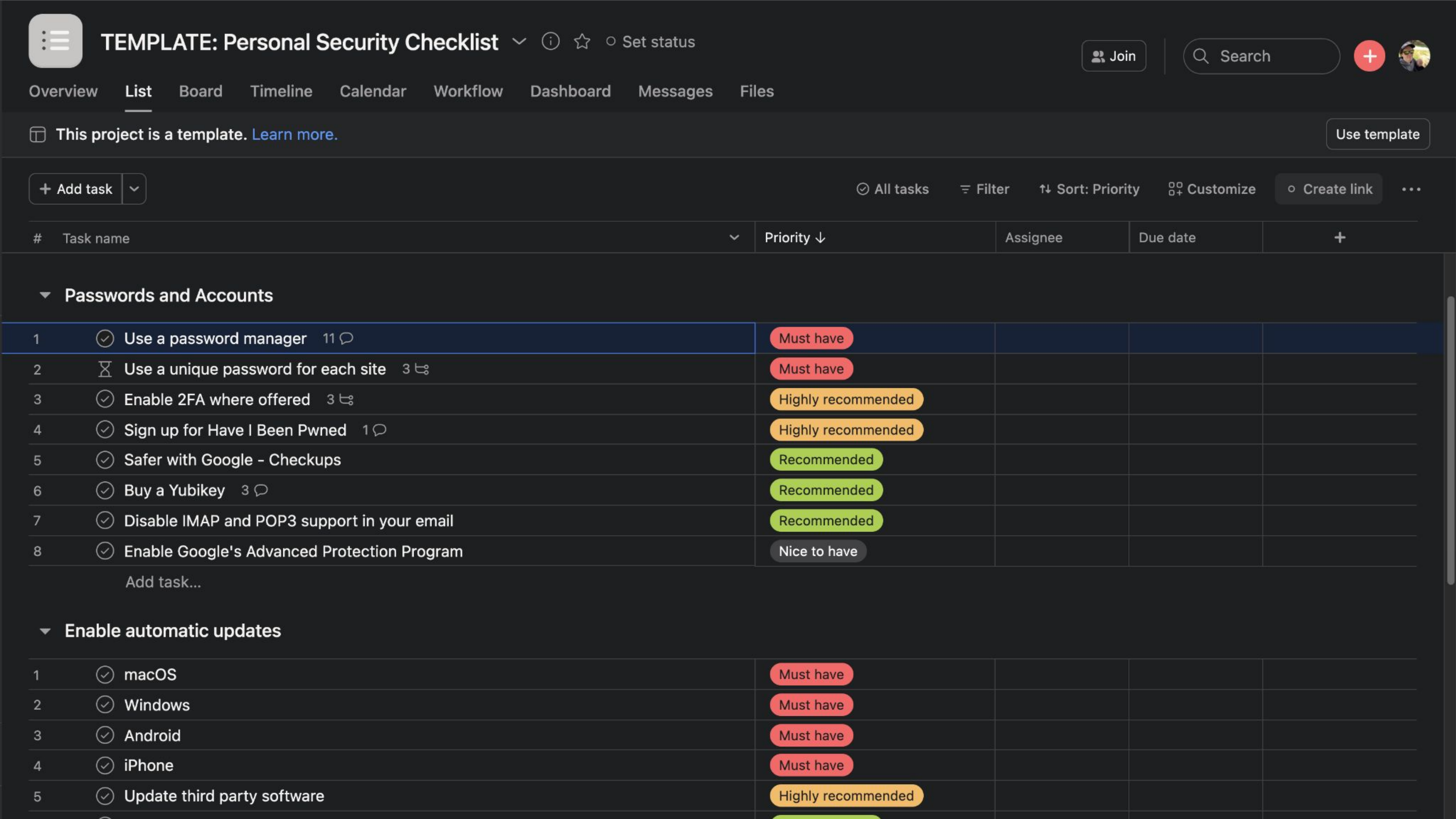
Other successful applications of checklists

Incident Response

- ❑ Incident set up
- ❑ Runbooks
- ❑ Where logs live and how to search for them
- ❑ Who to inform and when
- ❑ Incident Coordinator rotation
- ❑ How and when to contact DFIR
- ❑ Post incident action items

Vendor review

- ❑ Short checklists here make a big difference!
- ❑ Have a few questions which are absolutely disqualifying
- ❑ Don’t leave a whole lot to judgement or personal opinion



This project is a template. Learn more.

#	Task name	Priority ↓	Assignee	Due date
	Passwords and Accounts			
1	✓ Use a password manager 11 💬	Must have		
2	⧗ Use a unique password for each site 3 ⑂	Must have		
3	✓ Enable 2FA where offered 3 ⑂	Highly recommended		
4	✓ Sign up for Have I Been Pwned 1 💬	Highly recommended		
5	✓ Safer with Google - Checkups	Recommended		
6	✓ Buy a Yubikey 3 💬	Recommended		
7	✓ Disable IMAP and POP3 support in your email	Recommended		
8	✓ Enable Google's Advanced Protection Program	Nice to have		
	Add task...			
	Enable automatic updates			
1	✓ macOS	Must have		
2	✓ Windows	Must have		
3	✓ Android	Must have		
4	✓ iPhone	Must have		
5	✓ Update third party software	Highly recommended		

Questions?