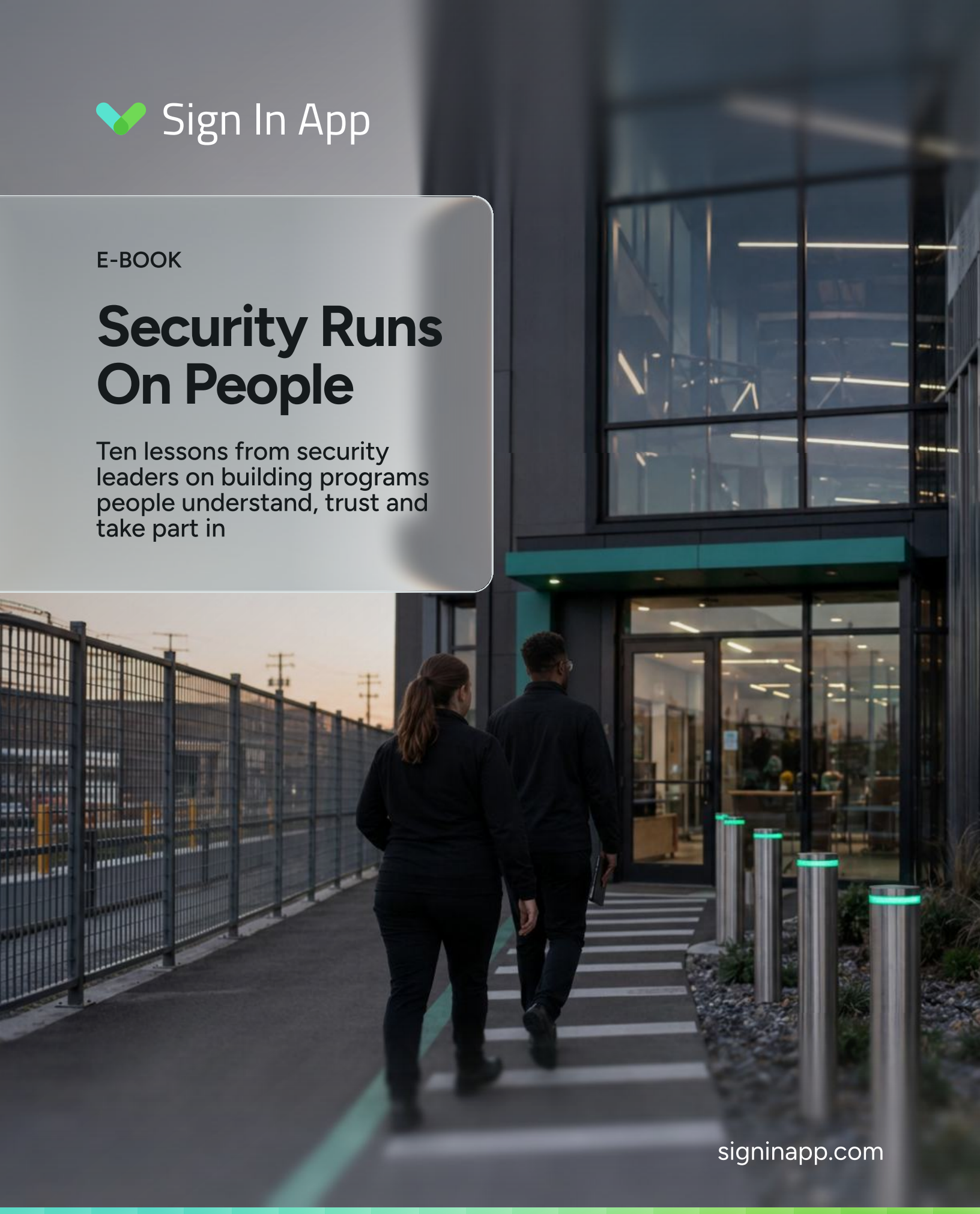
Sign In App

E-BOOK

Security Runs On People

Ten lessons from security leaders on building programs people understand, trust and take part in



signinapp.com

CONTENTS

Inside this e-book.

Ten lessons from security leaders on building programs people understand, trust and take part in.

01 Introduction: Security is a team sport.

02 Foreword from John Dillard, founder of ThreatSwitch

03 The leaders behind the lessons

04 Ten lessons at a glance

05 Lesson 1: Earn your seat by acting like a business partner

06 Lesson 2: Leadership has to listen
Lesson 3: Be the group that says yes

07 Lesson 4: Listen before you change anything

08 Lesson 5: Learn the business first
Lesson 6: No sends people around

09 Lesson 7: Kindness is an operational skill

10 Lesson 8: When a rule keeps breaking, ask why

11 Lesson 9: Make it safe to speak up

12 Lesson 10: Communication is the skill

13 What it adds up to: Security runs on people

14 Team discussion guide

15 Industrial Security & Compliance, from Sign In App.
Secure by design. Human by nature.

INTRODUCTION

Security is a team sport. Most companies don't run it that way.

Policies, processes and technology all matter. But none of them work without people.

Every day, security programs depend on employees completing training, reporting travel, raising concerns, following processes and sharing the information security teams need to make good decisions.

That makes participation one of the most important, and often overlooked, parts of a strong security program.

The question is how you earn it.

Across conversations on the Secure Access podcast, security leaders from defense, government, technology and the military kept returning to the same themes: listen before you lead. Understand the business. Make the secure path easier. Build trust. Communicate clearly.

Different careers. Different organizations. Remarkably similar lessons.

This e-book brings ten of those lessons together - practical ideas for facility security officers and security teams building a security program people understand, trust and actively take part in.

Because the more people participate, the clearer the picture security has and the better equipped it is to act.



The risk

During an emergency, incomplete visitor records can leave teams unsure who is still on site or safely accounted for.

FOREWORD

A program runs on everyone.

Like a lot of people in this business, I got here a bit by accident. My first job out of college was at the CIA, working on nuclear nonproliferation. I left to try business, then found myself pulled back into security again and again, by the work and by the people doing it.

Since then, I've seen security from several sides. I helped push for security clearance reform during the Afghanistan surge, alongside leaders like the Army's Tricia Stokes, and served on industry policy councils working on many of the same problems. Later, I founded ThreatSwitch, helping cleared contractors run their security programs until it became part of Sign In App | The Access Intelligence Platform.

Hosting Secure Access has given me the chance to sit down with some fascinating people from across the security world and ask how they approach the challenges security leaders deal with every day.



John Dillard, host of Secure Access and founder of ThreatSwitch

> Across those conversations, one idea has kept surfacing: **Security is a people business.**

We tend to divide security into boxes: personnel, physical, cyber, compliance. Those distinctions can be useful. But they can also make us forget how connected the work really is. A requirement on paper doesn't protect an organization by itself. It works when people understand what's expected of them, believe there's a good reason for it and know what to do next.

That conviction shaped how we built ThreatSwitch. When we looked closely at how companies handled security compliance, we realized much of the work wasn't actually being done by the security team. It was being done by everyone else: engineers, program managers, sales teams, delivery teams and employees completing training, submitting forms and reporting travel. A security program runs on all of them. So we built ThreatSwitch for the whole company, not just the security office.

This book brings together ten lessons from conversations on Secure Access, alongside some of what we learned building ThreatSwitch. Different organizations. Different challenges. One recurring idea: better security starts by making it easier for people to take part.

The best way to become a better security leader is to become a really good leader. I hope these lessons help you do both.

SECURITY LEADERS

The leaders behind these lessons.

These lessons draw on conversations from the Secure Access podcast with security leaders who have run programs at major defense contractors, at the State Department and the CIA, at SpaceX and Walmart, and in the Army, Navy, Marine Corps, and Secret Service.

Their backgrounds are different. Their lessons have more in common than you might expect. A thanks to all of the leaders for sharing their insights:

John Dillard
Host of Secure Access. Ex-CIA, Navy Veteran, author of Microslices, and founder of ThreatSwitch.

Michelle Lambiasi
Chief Security Officer at SAIC; started as an HR intern backing up a one-person security office.

Sarah Stull
Security leader who has built programs across defense and government services companies through roughly ten mergers.

Josh Allen
Director of Safety & Security at Cirkul; formerly the Marine Corps, the State Department, and Walmart's global security team.

Tim Wenzel
Co-author of The Kindness Games and MD at Kroll; global security experience spanning the State Department and Facebook.

Debbie Gordon
Founder of Cloud Range; cybersecurity entrepreneur with decades of experience in cybersecurity education and training.

Sean Blackman
Co-Founder and CEO of Nooks. A defense tech entrepreneur specializing in secure infrastructure.

Paul "IX" Kemppainen
Founder of SISU. Built SpaceX's security program; formerly the Navy, the Secret Service, and the CIA.

Yanek Korff
Co-Founder and COO of Expel; seasoned cybersecurity leader with a background at AOL and Mandiant.

James Bourie
Founder of Torchlight and former Army Special Forces officer, specializes in predictive security and threat intelligence.

Secure Access is now called Intelligent Access. Listen to all episodes here: signinapp.com/intelligent-access

AT A GLANCE

Ten lessons at a glance.

1. **Earn your seat by acting like a business partner**
   Security gets a seat at the leadership table when it thinks at the level of the business, not the level of the task.

2. **Leadership has to listen**
   Wherever security reports, it works when senior leaders make a point of listening to it and trusts their decisions.

3. **Be the group that says yes.**
   Many see security as the team that says no. Show people what security makes possible, not only what it forbids.

4. **Listen before you change anything**
   Learn what every team already does before you introduce a new requirement.

5. **Learn the business first**
   Understand the work and the mission before you apply security to it.

6. **A flat no sends people around you**
   Find a safe way to yes, or people will find their own way without you.

7. **Kindness is an operational skill**
   It's not about avoiding difficult conversations. It's about recognizing the person behind them and finding the best outcome.

8. **When a rule keeps breaking, ask why**
   Repeated violations are a signal about the process, not only the people.

9. **Make it safe to speak up**
   People often wait until they are sure before they say anything. Rank, ego, and friction make it worse.

10. **Communication is the skill**
    The quality of your work is limited by how well you explain it to employees, executives, and finance alike.

LESSON 1

Earn your seat by acting like a business partner.

For a long time, security was easy to put in a box: badges, paperwork, compliance, overhead. The programs that move beyond that have something in common. Their leaders understand what the business is trying to achieve, where it is exposed and how security can help it move forward with confidence.

That changes the conversation. Instead of arriving with another requirement, security arrives with context and answers. It becomes part of planning rather than something consulted after the decisions have already been made.

Often the work itself opens the door. When cleared contractors were required to run insider threat programs, security had to work closely with HR, legal, and IT for the first time. The teams that did that well earned a lasting place in those conversations.

> "You have to show that you're a business enabler.
>
> Michelle Lambiasi, Chief Security Officer, SAIC



A question for you

Where does security show up in your company's planning today, and where is it missing?

LESSON 2

Leadership has to listen.

Security can report to legal, HR, IT, or operations, and any of those structures can work. What makes the difference is whether senior leaders make a point of listening to security, and whether they trust the security leader they hired to make decisions.

That becomes especially important in smaller companies, where security may be a team of one. If every decision has to crawl through another approval chain, the program slows down and so does everyone depending on it.

Good leadership gives security a real voice. It trusts the people it hired to make decisions, holds them accountable for the outcomes and steps in quickly when something genuinely needs escalation.

> **Get to yes faster**
>
> Josh Allen, Director of Safety and Security, Cirkul, on what executives can do for their security leaders

A question for your team

If leadership asked security for its view on one decision this quarter, which decision would you want it to be?

LESSON 3

Be the group that says yes.

Many employees see security as the department of no. Changing that is not about lowering standards. It is about how security shows up: explaining what it makes possible, helping teams reach their goals safely, and treating requirements as a shared responsibility rather than a gate.

Done well, security becomes an asset the company can point to. A program that clearly cares, and shows it to customers and government partners even when nothing is wrong, builds the kind of confidence that wins and keeps business.

> **Go to security to see the possibilities of what you can get.**
>
> Sarah Stull, security leader

A question for your team

Who in your organization would describe security as the group that says yes, and who would not?

LESSON 4

Listen before you change anything.

There's a temptation when you inherit a security program or a new requirement lands to arrive with the answer. Resist it. Teams across the business are often already doing more than security realizes. They've developed processes, workarounds and informal knowledge that may never appear in a policy manual.

The leaders who build momentum fastest start by listening. They learn what each team already does, what it struggles with, and who inside it people already trust. Those people become security champions, carrying the message to colleagues in a way no outside voice can.

Before introducing a new workflow, ask:

1. What are people doing today?
2. Where does the current process create friction?
3. What can we make simpler without compromising the outcome?

> "I think it's the ability to listen."
>
> Sarah Stull, security leader, on how to get people working across silos

A question for your team

Which team in your company do you understand least, and who there could help you learn?

LESSON 5

Learn the business first.

Security expertise only helps when it fits the work. Before applying controls, the strongest leaders understand how the business operates, what a typical employee's day looks like, and what would slow them down. Some security teams spend time doing frontline work for exactly this reason.

Starting with the mission, rather than the threat, leads to programs that are simpler and more practical. Instead of asking, “How do we apply security here?”, ask, “How do we help this work happen securely?”

That shift leads to programs that protect the business without getting in its way, which is also why people follow them.

> **The key isn't thinking about security problems through a security lens.**
>
> Paul "IX" Kemppainen, who built SpaceX's security program

A question for your team

When did someone on your security team last spend time doing the work of the people you protect?

LESSON 6

A flat no sends people around you.

In government, no usually means no. Inside a company, things are messier. People still have deadlines. Customers still need answers. Work still needs to happen. When security blocks the route without providing another one, people have an incentive to find their own path. That can push the activity outside the process and outside security’s visibility. Security then learns about it later, usually after something has gone wrong.

The better response is to understand what people need to accomplish and find the safest way to get them there. A safe yes keeps people inside the process, where security can see what is happening and help when it matters.

> **In business, if I tell you you're not going there, they're going to find another way to get there.**
>
> Josh Allen, Director of Safety and Security, Cirkul

A question for your team

Who in your organization would describe security as the group that says yes, and who would not?

LESSON 7

Kindness is an operational skill.

Security work is often intrusive. It asks people for personal details, for reports on their travel and relationships, and sometimes it means having conversations they would rather avoid or delivering an answer they don't want to hear. That is exactly why kindness matters.

Kindness is not the same as being nice. Being nice often means avoiding conflict. Kindness means recognizing the person on the other side and working toward the best outcome available to them, even when the situation is difficult.

That isn't separate from good security. It helps create it. People who trust the security team are more likely to be honest, ask questions and come forward early when something doesn't look right. Thorough security and respectful security aren't competing ideas.

> "People conflate kindness with being nice.
>
> Tim Wenzel, Kroll, co-author of The Kindness Games

A question for you

Think of the last time someone dreaded a conversation with security. What would the best available outcome have looked like for them?



LESSON 8

When a rule keeps breaking, ask why.

A policy that is broken again and again is telling you something. Sometimes people need more training. Often the process itself is confusing, slow, or out of step with how the work actually gets done.

Instead of treating every violation as an isolated problem, look for the pattern underneath it. Where are people getting stuck? What are they trying to accomplish? Could you achieve the same security outcome with less friction?

Treating repeated violations as a signal, rather than only as a discipline problem, helps security fix root causes. It also earns credibility with the people security depends on, because it shows that security is trying to make their work easier, not just catch them out.

> **What policy is always being broken? Like should that policy even be there?**
>
> Tim Wenzel, Kroll

A question for your team

Which of your rules gets broken most often, and what is that telling you?

The right software can help remove some of that friction too.

Automating routine reminders, self-reporting, training and compliance tasks gives employees a clearer path to follow and gives security teams less administration to chase.

With tools like Sign In App, 40% of compliance workflows start automatically from visitor sign-ins, so security teams don't have to re-key that data.

LESSON 9

Make it safe to speak up.

Every security program depends on people saying something: reporting travel, flagging a concern, admitting a mistake while it is still small. Yet people often wait until they are certain before they speak, and by then the moment may have passed.

Three things make it worse. Rank, when junior people do not feel free to question senior ones. Ego, when admitting a mistake feels like losing face. And friction, when reporting is slow or confusing enough that people put it off.

Good security tackles all three. Build a culture where speaking up is expected. Give people trusted contacts. Then make the practical act of reporting simple enough that people actually do it.

> **There's no rank in the cockpit**
>
> Sean Blackman, former Navy pilot and co-founder of Nooks, on the culture he carried from aviation into his company

A question for your team

When someone sees something unusual, what makes them hesitate to say so?

Make it easier to act

Changing rank and ego takes culture. Removing friction is something you can start doing today.

If reporting is easy to find, easy to understand and easy to complete, there's one less reason to put it off. Self-reporting software can give employees a direct route to security, while automated reminders help keep required actions from slipping through the cracks.

Over the past year, 58,000+ employees filed more than 100,000 security reports and forms through Sign In App's Industrial Security & Compliance solution.

LESSON 10

Communication is the skill.

Security is a technical discipline, but its success depends on explanation. Employees need to understand why a requirement exists. Executives need risk described in business terms. Finance needs to see value, not just cost.

Leaders who learn to speak each audience's language get more support, more budget, and more cooperation. Plain language helps too. Acronyms and jargon shut people out of the very conversations security needs them in.

> **The quality of your work is restricted entirely by the quality of your communication.**
>
> Yanek Korff, co-founder, Expel

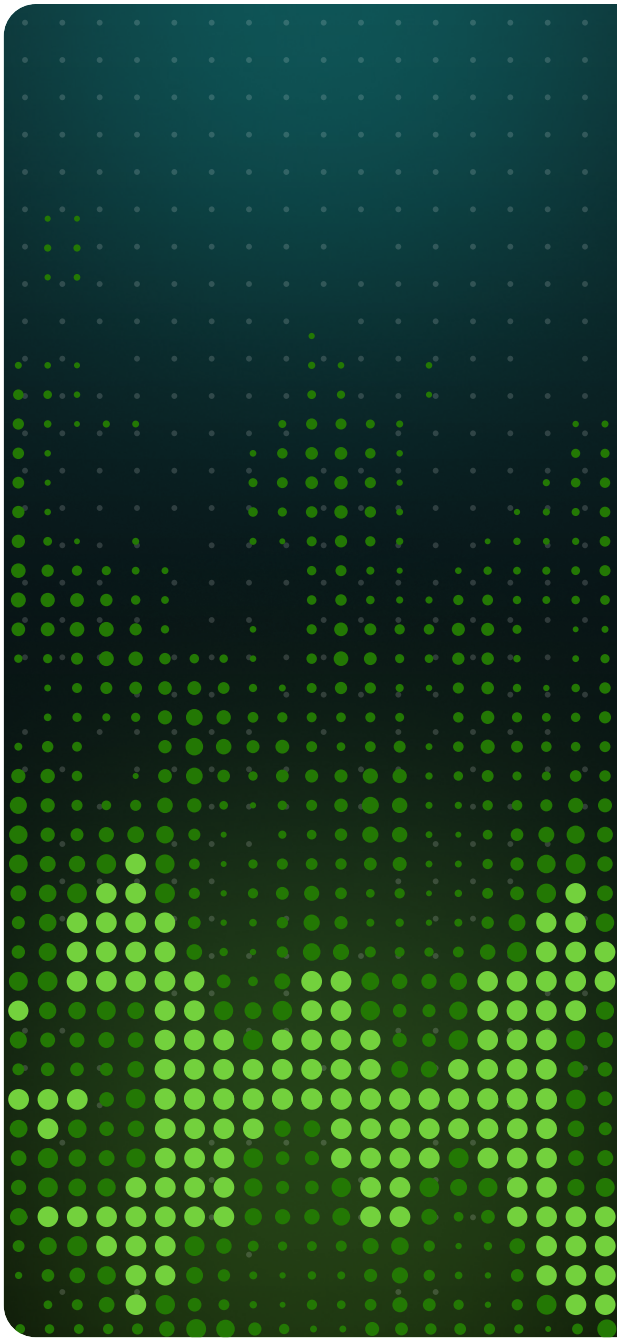
A question for your team

Who in your company would benefit most from hearing security's story in their own terms?



SUMMARY

What it adds up to.



Security runs on people.

Read together, the ten lessons describe one idea. Security is not something a security team does to a company. It is something the whole company does, with security leading the way.

Every report filed. Every training course completed. Every concern raised early. Every record kept current. Each action gives security another piece of the picture. And when participation becomes easier, that picture gets clearer. Security teams can spend less time chasing information and more time understanding what it means. They can spot gaps earlier, make better decisions and focus their attention where it matters most.

That thinking shaped ThreatSwitch: security compliance designed for the whole company to take part in, not just the security team. Now part of Sign In App, those same principles continue at a much broader scale. Better security starts with better information about the people interacting with your organization - and making it simple for people to provide it.

When people take part, you always know where you stand.

Reporting what they should, finishing their training, raising concerns early: that is what makes a security program current and visible.



Listen to the full conversations

The conversations that helped shape this book are available in full on Intelligent Access, formerly Secure Access, hosted by John Dillard, on YouTube, Spotify, and Apple Podcasts.

RESOURCE

Team discussion guide.

Reading the lessons is one thing. Putting them into practice is another. Use this 45-minute session in a security team meeting or offsite to identify one thing you can change.

Before the session

Ask everyone to read "Ten lessons at a glance" and one lesson of their choice.

Opening (5 minutes)

Which of the ten lessons is our program strongest at today, and which is hardest for us?

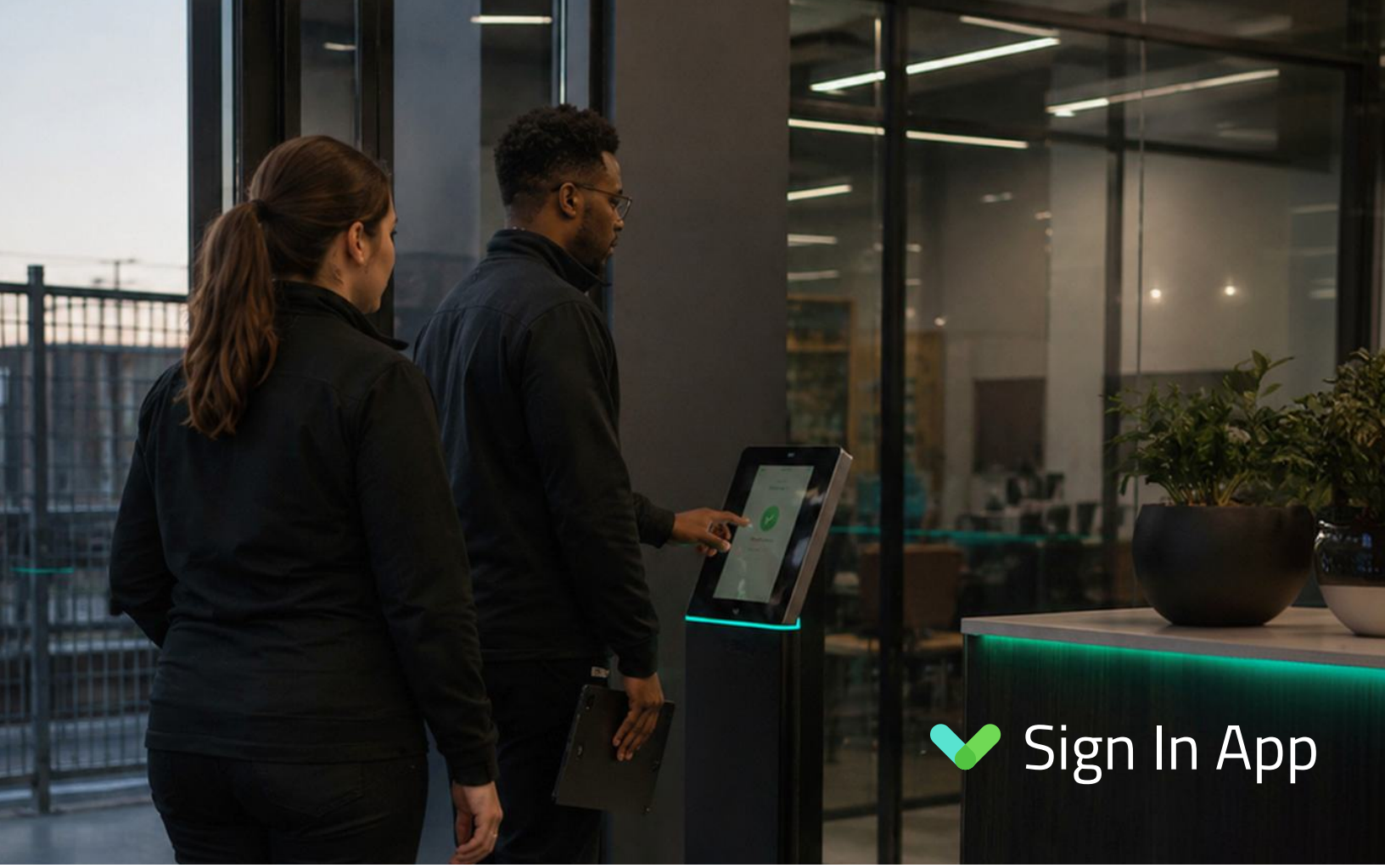
Discussion (30 minutes)

Pick two or three questions that fit your team:

1. If leadership asked security for its view on one decision this quarter, which decision would we want it to be? (Lesson 2)
2. Who in our organization would describe security as the group that says yes, and who would not? (Lesson 3)
3. Where does our program say no today, and what would a safe yes look like? (Lesson 6)
4. Think of the last time someone dreaded a conversation with security. What would the best available outcome have looked like for them? (Lesson 7)
5. Which of our rules gets broken most often, and what is that telling us? (Lesson 8)
6. When someone sees something unusual, what makes them hesitate to say so? (Lesson 9)

Close (10 minutes)

Agree on one change that would make it easier for people to do their part, who will own it, and when the team will check back in.



About Sign In App

Industrial Security & Compliance, from Sign In App. The industrial-security platform cleared and public trust contractors have relied on since its ThreatSwitch days. Sign In App is industrial security compliance software that helps facility security officers and their teams make compliance easier.

Employees can complete self-reporting and training themselves. Automated reminders keep requirements moving. Security teams get current records and clearer visibility without spending their day chasing people for updates.

It's the same human-first thinking that shaped ThreatSwitch, now part of Sign In App's broader approach to Access Intelligence: giving organizations the information they need to make smarter, earlier security decisions.

See how your whole cleared workforce can take part.
Request a demo at **signinapp.com**.

Secure by design.
Human by nature.
Trusted worldwide.