TrustCloud®

THE STRATEGIC CISO PLAYBOOK:

How five security leaders turned risk constraints into business advantage

Lessons from the Strategic CISOs Series

TrustCloud®

CONTENTS:

1 **Introduction: the end of the checkbox**
Sravish Sridhar, TrustCloud

2 **Part 1. Run security as a profit center**
Dave Brown, Andesite

3 **Part 2. Replace questionnaires with evidence**
Myke Lyons and Jon Zayicek, Cribl

4 **Part 3. Build a security culture beyond the security team**
Lori Kevin, IMO Health

5 **Part 4. Learn creativity within constraints**
Matthew Martin, Western Carolina University

6 **The playbook: five moves that define a strategic CISO**

7 **Keep going**

INTRODUCTION: THE END OF THE CHECKBOX

I started the Strategic CISOs conversation series for a simple reason. I kept meeting security leaders who ran security as a way to help the business grow, not just a way to pass the audit, and I wanted more people to hear how they did it.

For years, GRC programs operated with a point-in-time model. This may have been adequate when environments were stable and change was slow. Neither is true now. Every new AI agent, every integration, and every vendor widens the risk surface faster than an annual review can check.

I have started thinking about the CISO role in terms of a historian and a navigator. A historian can tell you in detail what risk used to look like. The leaders in this series wanted to navigate: to see risk as it forms and steer clear before it becomes an incident. That is what cyber risk assurance makes possible: a posture that is current, not accurate as of last quarter.

Each of them runs their program differently, and they do it while working under real constraints. Dave Brown had to run his program like a profit center, proving every dollar he spent was tied to future revenue. The team at Cribl was buried under security questionnaires. Lori Kevin needed to cultivate a security culture across the whole business. Matt Martin walked into higher education with a fraction of the budget he was used to. Four very different problems, and in every case the constraint became the reason they built something better.

I am grateful for what each of them was willing to share, and for how candid these conversations have been. The common thread across all four is trust: once they were able to see risk continuously, they could bring business stakeholders into the process and clearly demonstrate the business value of trust.

That is what this series is for. Real conversations with the leaders redefining the CISO role. Here are my top lessons from the Strategic CISOs series, and the playbook you can borrow from all of them.

Sravish Sridhar
Founder and CEO
TrustCloud

PART 1:
RUN SECURITY AS A PROFIT CENTER

Dave Brown, CISO and CIO, Andesite

Dave Brown spent 21 years in the Coast Guard, ran a computer incident response team, did a stint at the Department of Homeland Security, and served eight years as a CISO at a company later acquired for 1.2 billion dollars. He authored a book called The Lean CISO. So when he built Andesite's security, compliance, and IT program from scratch, he did not start with a control framework.

He started with questions most security leaders skip:

- Do I understand how this business actually makes money?
- How can the security program help it make more?

Dave defines a profit center in plain terms that a CFO can evaluate: look for three numbers moving in the right direction at the same time. Revenue up, costs flat or falling, and overall risk down. If all three are true, the program is paying for itself. If you can only speak to security's impact on the third number, you are still running a cost center. Dave treats risk reduction as a measured business outcome he can put in dollars, not a soft claim.

When security operates as a profit center, its influence on all three of these is visible. The overall risk picture, where most CISOs focus, is only one of these important metrics to track.

When Dave joined Andesite, he spent his first 90 days working to understand the business and its inner workings, mapping security objectives to organizational objectives. He wanted stakeholders to see security as a vital part of business operations. In his own worked example, Dave put roughly 150,000 dollars into the compliance priorities that opened specific markets, against a pipeline of about 3 million dollars, and closed 1.5 million of it. Pitched in those terms, that spend is an investment the finance team can weigh like any other.

Transparency is essential here. Rather than answering the same security questionnaires deal after deal, Andesite gives buyers a real-time view of its posture, and that changes how fast deals move.

"When a customer asks about our security posture, we don't send them a 200-question spreadsheet. We give them a real-time view of our compliance and controls. That transparency shortens deal cycles."

— Dave Brown, CISO and CIO, Andesite

The payoff shows up everywhere once you start measuring it. Using a trust center, Andesite cut questionnaire turnaround from three or four weeks down to three or four days. Automating evidence collection took a task that used to run about 50 minutes per control down to seconds. And Dave watches what customers actually download, because a document nobody opens is a signal to stop spending time maintaining it.

> ***"That's what allows our team to optimize budget. Not just spend more, but spend smarter."***
>
> — Dave Brown, Andesite

Dave's lesson for any security leader is to focus on order of operations. Learn the business first. Tie the program to outcomes the business already cares about. Then report those outcomes the way every other function reports results.
Do that, and the business will credit security for growth it can measure.

PART 2:
REPLACE QUESTIONNAIRES WITH EVIDENCE

Myke Lyons, CISO, and Jon Zayicek, former Customer Security Assurance Leader, Cribl

Nobody enjoys the security questionnaire. At TrustCloud, we like to say, “Friends don’t send friends security questionnaires.” Jon Zayicek believes that wholeheartedly. But behind the joke is a serious argument. A questionnaire is a survey-driven way to assess risk, a low-trust exchange of high-stakes information that buries both sides in manual work. Cribl set out to replace the questionnaire with something better. In doing so, they turned the assurance team into one of the most measurable revenue contributors in the company.

"We decided to be transparent, and it's really worked out well for us."

— Jon Zayicek, former Customer Security Assurance Leader, Cribl

Transparency, at Cribl, means showing rather than telling. Their trust portal publishes real artifacts: attestations, pen test summaries, current policies, and a notification center that gets ahead of a vulnerability and tells customers where they stand before they have to ask. That posture deflects repeat questions and builds buyer confidence at the same time.

Transparency does two jobs at once: fewer questions, more trust.

Jon estimates that approximately 80% of closed-won deals go through his assurance team. When a buyer needs to judge the risk of working with Cribl, this is the team that answers. The team tracks it the way a revenue function tracks pipeline: share of deals touched, SLA turnaround on questionnaires, and cycle time. Two years ago a questionnaire could take them four to six weeks to complete. Now most turn around in about two days, sometimes 24 hours, because they put AI on the highest-volume, lowest-risk work first: drafting questionnaire answers from a maintained knowledge base.

THE QUESTIONNAIRE

- Send a questionnaire
- Four to six weeks
- Low-trust exchange
- A document you send
- Invisible to sales

THE TRUST EXPERIENCE

- Publish real evidence
- Days, sometimes 24 hours
- Continuous, verifiable evidence
- A portal, refreshed monthly
- Logins flag buying intent

"Every business is being asked to do things with AI. This is absolutely the most no-brainer opportunity for you to provide value back to your business."

— Myke Lyons, CISO, Cribl

Myke Lyons reframes compliance itself along the same lines. He treats each new attestation as a pipeline-generating decision, evaluated on the potential market it unlocks rather than the boxes it checks.

In other words, GRC becomes RGC: revenue-generating compliance, not governance for its own sake.

> ***"Make the trust portal not just 'we really take security seriously in the company.' Of course you do. Give some substance to your trust portal."***
>
> — Myke Lyons, Cribl

Substance means artifacts, tested evidence, and advisories, refreshed close to monthly cadence. And because those portal logins flow back into the CRM, they double as buyer-intent signals. When the person who runs compliance at a prospect logs in three times in a week, the seller can read that as a deal getting more serious, and act on it.

Revenue-generating compliance gets noticed. Cribl's CRO put Jon forward for President's Club and sent him to Hawaii for what his team had built, because the sales organization kept telling the CRO how much that work was worth to them.

Cribl's assurance work connects into Salesforce and the sales motion, so the team describes what it does in the language the business already uses, and trust becomes part of how deals move forward. For most organizations that connection is the missing piece. The evidence exists, but it sits to the side of the deal, and the assurance team is measured on questionnaires cleared rather than revenue supported.

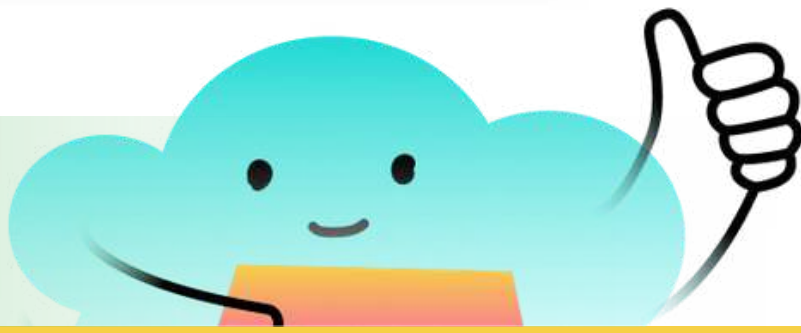
There is a further horizon. TrustCloud is building toward assessments that run agent to agent, a third-party risk tool on one side talking to the vendor's system on the other, with far less human handling in between. That is coming. What a team can do today does not wait on it. Cribl's advantage came from moves any organization can make now: evidence a buyer can reach without asking, and an assurance function wired into the sales motion to drive revenue.

MEASURED ON QUESTIONNAIRES CLEARED

↓

MEASURED ON REVENUE SUPPORTED.

Assurance wired into sales gets noticed. Assurance off to the side gets overlooked.



PART 3:
BUILD A SECURITY CULTURE BEYOND THE SECURITY TEAM

Lori Kevin, VP of Security and Compliance, IMO Health

Lori Kevin leads with a strong conviction: a security culture across the business cannot be built by the security team alone. She has spent six years working through that at IMO Health, and her starting point makes all the difference. It begins with values.

"Trust is the foundation of everything my team does. We're building a security function around the core values of trust, accessibility, clarity, and strong communication. We want the whole organization to know how to access security policies and see the strategic value security offers to their department."

— Lori Kevin, VP of Security and Compliance, IMO Health

Lori arrived in cybersecurity through customer support, operations, and the software side of the business, and she draws on all those experiences in her current role. **Those insights help her translate risk into terms the rest of the business already understands.**

> ***"I haven't just been in security. I've really been in the weeds of software development and customer support, and that's helped me evolve a security approach that's transformative and looks at it through a business lens too."***
>
> — Lori Kevin, IMO Health

Inside her own team, the discipline Lori is proudest of is learning to get out of the way. Everyone brings different strengths, and a leader's job is to recognize them instead of making everyone fit the same mold. That's important in security, where teams separate into silos or lean too hard on a few key people. She is candid that she was not good at letting go when she started, and she credits her team for telling her when it is time.

“I want my team to kick me out of meetings,” Lori says. The growth she cares about happens when people step up and take ownership.

> ***"The more that I am involved, the less development opportunity there is for the team. That is where trust comes in for me. If I keep stepping in, I get in the way of someone else being able to develop. As managers, our job is to create those opportunities so our teams can explore and grow."***
>
> — Lori Kevin, IMO Health

Her approach to reporting is to think the way leadership thinks and translate everything into risk language, focusing on the risk, why it matters to the business, and what her team is doing about it. She treats those updates as an ongoing dialogue layered on top of a set reporting rhythm.

"Conversations with executive leadership cannot be overly technical. You have to figure out what story will actually lead to action. For me, that means framing things from a risk perspective, because that’s what’s going to resonate."

— Lori Kevin, VP of Security and Compliance, IMO Health

My favorite security initiative from IMO Health is its security champions program. Most champions programs work closely with product and engineering teams, and Lori does that too, because secure development is non-negotiable. But she refused to stop there. Her program runs more than 30 champions across an organization of roughly 350 people, pulled deliberately from marketing, admins, HR, and the individual-contributor ranks, not only managers.

The best delegation move a security leader makes is getting out of the way.

Champions were asked, never volun-told. The forum rarely has an agenda. And the culture shows up in small, human ways: when someone spots a simulated phishing test and fires her a screenshot, their running joke is "not today, Lori."

That reach, from product all the way to HR, is what turns security from one team's mandate into shared ownership of risk across the company.

STARTING A SECURITY CHAMPIONS PROGRAM

1. **SIZE IT PROPORTIONALLY**
   ~1 in 10, weighted to product and engineering
2. **RECRUIT BY INVITATION**
   Source names from leaders and team, never volun-tell
3. **OPEN WITH A KICKOFF**
   Set the mission, purpose, and time ask up front
4. **KEEP THE FORUM LOOSE**
   Members bring topics and host discussions
5. **GAMIFY PARTICIPATION**
   Phishing leaderboards, quizzes, small rewards
6. **RENEW ANNUALLY**
   Members stay or nominate a successor, seats rotate
7. **HAND OFF THE RUNNING**
   Move day-to-day ownership to the GRC team

PART 4:
CREATIVITY WITHIN CONSTRAINTS

Matthew Martin, Chief Information Security and Privacy Officer, Western Carolina University

I first knew Matt as the leader who spends his own time flying to Ghana and Uganda to share cybersecurity expertise with executives and students, work that began with a cyber resiliency conference in Accra and grew into an ongoing nonprofit partnership. That instinct, more than any tool or certification, is the key to how he leads.

After two decades running security in financial services, where budget requests were typically granted, Matt made a deliberate choice to lead security at a university. He wanted to test his belief that strong security fundamentals hold even in an environment where the budget, the team, and the operating model vary greatly from the enterprise. He calls the approach creativity within constraints, and the first thing he learned was that he was focusing on the wrong constraint.

"I thought I was dealing with constraints around dollars. It turned out the dollar constraint was actually one of the smaller constraints."

— Matt Martin, Chief Information Security and Privacy Officer, Western Carolina University

The real constraint was the environment itself. Faculty don't all report to the CISO, departments run themselves, and a university built on open, shared knowledge can feel like family. That culture creates genuine trust, and it means security has to be designed to work with how the place already runs. You cannot mandate your way through it. You build through influence. Matt shared that his early mistake was trying to fix before he understood.

Eventually he stepped back to listen and learn first: sit with the environment, ask how things actually work, and document before changing anything. Listening first also showed him where he could streamline without piling new work on anyone. Access, for instance, was being approved one person at a time rather than by role or use case. Moving to use cases made the program consistent, auditable, and defensible.

On the perennial question of where to start, risk or compliance, he does not hesitate.

> ***"If you do risk well, compliance comes almost for free."***
>
> — Matt Martin, Western Carolina University

Start with a real risk register and name an owner for each risk. That gives you a shared language for every conversation with leadership, and it maps each risk to the person accountable for retiring it. You also make those owners part of the solution, because the solution belongs to the person who raised the problem.

Capacity was the next honest constraint. Matt cannot hire a team of analysts to test every control or spend weeks each year on a self-assessment, so automation is the only way he can get reliable evidence on every control.

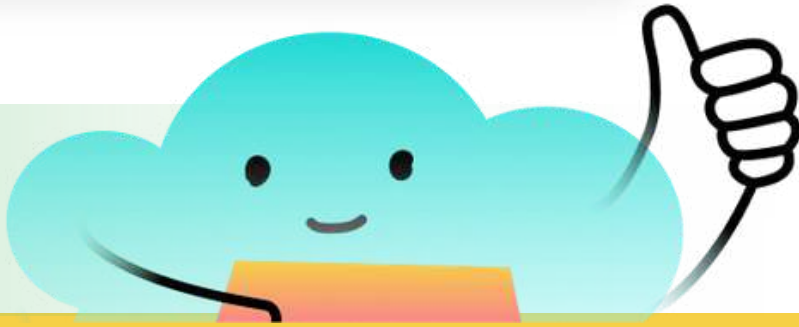
> ***"I can't go hire a team of risk analysts. The only way I could do that was to embrace technology."***
>
> — Matt Martin, Western Carolina University

He leaned hard into automation and continuous monitoring. It spared his small team the manual evidence collection, and more than that, it gave him continuous visibility into whether a control was actually working, ground truth instead of opinions that changed depending on who he asked. Once the testing was in place, the payoff went beyond cleaner attestation.

"With that testing in place, we can see when things aren't working when they're supposed to be, and we're having better conversations."

— Matt Martin, Chief Information Security and Privacy Officer, Western Carolina University

Automate to get ground truth, not opinions that change with who you ask.



Higher ed's tighter budgets sharpened a discipline Matt would send back to his own enterprise days: before buying, ask whether a three-million-dollar feature is really three million dollars better than what you already own.

The mindset matters as much as the mechanics. Matt's advice to anyone stepping into a resource-constrained role is to be part of the community you serve, understand the real risks rather than the ones on paper, and lean on automation to clear the manual work. Beyond that, it comes down to temperament. You have to want to get your hands dirty, be creative enough to build what isn't the industry standard, see the business-enablement side of the job and not only the technical one, and hold the mission loosely.

"If you come in and you're like 100% security or bust, you won't last long in higher ed."

— Matt Martin, Chief Information Security and Privacy Officer, Western Carolina University

THE PLAYBOOK:
FIVE MOVES THAT DEFINE A STRATEGIC CISO

Although these leaders are working in very different environments, with different constraints, five similar threads show up in each one.

1. **ALIGN TO BUSINESS OBJECTIVES BEFORE SECURITY OBJECTIVES.**
Spend your first months learning how the organization actually succeeds, then map your program to support those objectives. Dave Brown's profit-center math and his first-90-days discipline both start here. This is GRC transformation in practice: security counted as a valuable part of the business.

2. **PROVE VALUE WITH EVIDENCE, NOT SURVEY-DRIVEN ATTESTATION.**
Publish real proof and let buyers serve themselves, the way Cribl and Andesite both do. Replace the questionnaire with a trust center, and support the claim "we take security seriously" with artifacts anyone can verify. Deals move faster when buyers don't have to wait on a questionnaire.

3. **MAKE SECURITY EVERYONE'S JOB THROUGH CHAMPIONS.**
A high regard for security doesn't spread on its own. Lori Kevin's champions program, built deliberately across marketing, HR, and admins rather than just product, turns security into a habit in every business unit and promotes shared ownership of risk.

Point security outward. Align to how the business wins, prove value with evidence buyers can verify, and make it everyone's job through champions.

4 **UNDERSTAND YOUR REAL CONSTRAINTS BEFORE YOU ACT.**
Matt Martin assumed that budget would be his biggest challenge, but overlooked the cultural differences of a new sector. Identify the true constraints in your environment, listen before you start to fix, and move from one-off decisions to repeatable use cases. Assess risk clearly, name an owner for each one, and compliance follows almost for free.

5 **USE AI AND CONTINUOUS MONITORING TO DO MORE WITH LESS.**
Every one of these leaders reached the same conclusion: continuous monitoring proves a control is operating and maps it to the risk it mitigates, so you see risk continuously instead of once a year. This is the backbone that makes the other four moves sustainable when the team is small and the environment never stops changing.

The connective tissue across all five is trust: trust made measurable, so security drives the business instead of chasing it. The strategic CISO is the leader who turns whatever they've been handed into an advantage for the business, and brings the whole company along.

Of these five moves, which one could you put into practice next?

KEEP GOING

These conversations are part of the Strategic CISOs series, where security leaders share how they are turning GRC into continuous cyber risk assurance.

SEE WHAT THIS LOOKS LIKE IN YOUR OWN PROGRAM

Walk through continuous control monitoring, AI governance, and customer assurance with our team

Request a walkthrough

GO DEEPER ON THE PLAYBOOK

CONTINUOUS CONTROL MONITORING
Proof on demand instead of a point-in-time snapshot

AI GOVERNANCE
Lead on AI without slowing the business down

CUSTOMER ASSURANCE
Turn trust into a faster sales cycle

WATCH THE FULL CONVERSATIONS, WITH CLIPS AND HIGHLIGHTS

http://trustcloud.ai/strategic-cisos/

TrustCloud®

© 2026 TrustCloud, Inc. All rights reserved.