CYBERSECURITY READINESS PODCAST SERIES
Episode 111

Closing the Gap Between Leadership Intention and Operational Security Reality: A CPD Lens on SMB Cybersecurity Governance

with Bruno Lecoq, CEO, BEMO

Host	Dr. Dave Chatterjee, Duke University
Guest	Bruno Lecoq, CEO, BEMO
Topic Focus	Closing the Gap Between Leadership Intention and Operational Security Reality in Small and Medium-Sized Organizations
Podcast Portal	https://www.cybersecurityreadinesspodcast.com/

Summary

In Episode 111 of the Cybersecurity Readiness Podcast Series, Dr. Dave Chatterjee is joined by Bruno Lecoq, CEO of BEMO, to examine the gap between executive intention and operational security reality in small and medium-sized organizations, and what it costs when resource trade-offs, unclear ownership, and optimism bias quietly undermine programs that look sound on paper.

Drawing on his nearly sixteen years at BEMO and twenty years at Microsoft before that, working with companies of 10 to 1,000 users across multiple verticals, Bruno argues that the recurring failure point is rarely the tools; it is the absence of clear ownership, aligned resources, and sustained discipline. The conversation moves through why IT alone cannot own security, how the function's reporting line shapes whether it is treated as a cost center or a strategic capability, and a detailed walk-through of a SOC 2 "fire drill" scenario that Dr. Chatterjee analyzes through his Commitment–Preparedness–Discipline (CPD) Framework.

The discussion also covers how BEMO uses AI-driven log review and unannounced tabletop exercises to keep clients honest about their true readiness, why Bruno turns away prospects who treat compliance as a paperwork exercise rather than a genuine security commitment, and why he believes cybersecurity and compliance, approached the right way, are a competitive advantage rather than a cost of doing business.

The Gap Between Intention and Operational Reality

Dr. Chatterjee opens the episode with two cautionary examples: an Austrian aerospace supplier that lost 50 million euros in a single business email compromise attack because no one owned the question of how to verify an unusual wire transfer request, and a small California medical practice that permanently closed after a ransomware attack, not because the attack was sophisticated, but because years of deferred backup investment left nothing to recover from. Both cases, he notes, were procedural and leadership failures rather than technology failures.

> *An Austrian aerospace supplier lost 50 million euros in a single business email compromise attack, not because they lacked tools, but because no one owned the*

> *question of how to verify an unusual wire transfer request from the CEO — a procedural gap, not a technology gap.*
>
> **— Dr. Dave Chatterjee**

Security as a Team Sport, Not an IT Function

Bruno opens with an example from his own company: every new hire is told that within three to four days of joining, they will receive a phishing-style text impersonating him personally, as a live test of how people behave when they believe no one is watching. He argues that the recurring issue across BEMO's client base, regardless of industry, is not the absence of tools but the absence of clarity around three things: who owns security, whether resources are aligned to that ownership, and whether the organization has the discipline to sustain it. Security, he insists, has to be treated the way customer satisfaction is treated — something everyone in the organization owns, not a task handed entirely to IT.

> *Security is not IT, it's a team sport. Everyone owns it, and I think very often what I see, when you ask customers those three questions — who clarifies ownership, who aligns the resources, who creates the discipline — they believe someone owns that, but when you go deep into it, they do not.*
>
> **— Bruno Lecoq, CEO, BEMO**

Where IT Reports Shapes How Security Is Valued

Dr. Chatterjee connects this to a separate guest's observation that IT departments often treat platforms like SAP as outside their core responsibility, arguing that cybersecurity strategy must be strategically aligned with business strategy rather than delegated wholesale to IT. Bruno builds on this by pointing out that an organization's reporting structure shapes how security is perceived: when IT reports into finance, security tends to be evaluated purely on cost rather than strategic value, whereas alignment with business strategy allows leadership to make informed trade-offs about what to enable and what to defer.

The SOC 2 Fire Drill: CPD Framework Applied

Bruno describes a common pattern: a company decides it needs to be SOC 2 compliant, treats it purely as an IT project, and only later discovers that a meaningful share of the required controls — onboarding, background checks, training — actually belong to HR and other functions outside IT. Dr. Chatterjee applies his Commitment–Preparedness–Discipline (CPD) Framework directly to this scenario: there was no leadership mandate distinguishing cyber readiness from a compliance checkbox, no capacity assessment before compliance ownership was assigned to already-stretched engineering leads, and no governance routine in place to detect drift after the initial certification was achieved.

> *Becoming compliant is like having a kid — the baby is born, but you have to deal with the baby for eighteen years. When the motivation to be cyber security ready is based purely on closing a deal, that's always the wrong place to start.*
>
> **— Bruno Lecoq, CEO, BEMO**

From Static Compliance to Continuous Discipline

Bruno describes how BEMO operationalizes the discipline pillar for clients: logs are automatically aggregated each month and run through AI analysis that flags the delta from the prior period and opens tickets for resolution, removing work that used to take days or months. Beyond automated review, BEMO runs quarterly tabletop exercises without announcing the date in advance, specifically to prevent organizations from over-preparing and passing artificially. Bruno also describes the access control evolution at his own company — from permanent global admin access a decade ago to today's ticketed, time-boxed credential elevation — as an example of discipline becoming an ingrained mindset rather than a periodic exercise.

> *My goal is not to say, 'Oh, we passed with flying colors.' Do I truly believe that in case of a real incident, we'll pass? So we don't set the date for the tabletop exercise. That's the only true test, because you can see how the organization reacts from the top to the bottom.*
>
> **— Bruno Lecoq, CEO, BEMO**

Vetting Clients: Walking Away When Commitment Isn't Real

Both Bruno and Dr. Chatterjee describe turning away prospective clients who are not genuinely committed. Bruno recounts a prospect who demanded CMMC Level 2 certification by a fixed deadline regardless of cost, refusing to accept that the organization's lack of internal ownership made the timeline unrealistic; Bruno ultimately ended the engagement. Dr. Chatterjee draws a parallel to his own consulting practice, where he insists that the CEO and other C-level leaders attend the first meeting as evidence of genuine commitment, and will decline engagements where that commitment is not present, framing the decision as being about protecting organizations and the broader goal of making the digital world safer, not simply about revenue.

The CPD Framework Applied to SMB Cybersecurity Governance

CPD PILLAR	APPLICATION TO SMB CYBERSECURITY GOVERNANCE
COMMITMENT	Commitment is a genuine, resource-backed decision by senior leadership to treat cyber readiness as a strategic priority rather than a delegated IT task or a compliance checkbox. Active commitment means leadership sits on an oversight function or actively monitors security performance and asks informed questions; passive commitment — simply funding a team and stepping away — is not

	enough. Ownership must be explicitly assigned, never assumed, or accountability collapses the moment something goes wrong.
PREPAREDNESS	Preparedness is the operational capacity to detect, contain, and respond to threats across every business function, not just IT. It requires a realistic capacity assessment before compliance or security ownership is assigned, clear playbooks for who owns each control, and recognition that functions such as HR, finance, and operations carry direct responsibility for specific safeguards — onboarding, background checks, training — that cannot be delegated to IT alone.
DISCIPLINE	Discipline is the sustained, continuous execution of security and compliance practices over time — monthly log review, unannounced tabletop exercises, and ongoing governance routines that catch drift before it compounds into an incident. Discipline is what separates an organization that was compliant on a single audit date from one that stays continuously secure, and it requires the same consistency an organization applies to running payroll every month.

Key Takeaways

Dr. Chatterjee distills several recurring themes from the conversation. Most cybersecurity programs fail because of leadership decisions, or the absence of them, not because of missing tools or technology gaps; the tools and frameworks already exist. Optimism bias, he argues, is the most expensive line item in a cybersecurity budget that never appears on a spreadsheet: the assumption that an internal team has the bandwidth and expertise to absorb a compliance project as a side effort is rarely malicious, but it compounds quietly until an external trigger — a deal, an audit, an incident — makes the cost visible. The antidote is honest capacity assessment before commitments are made, not after.

> *Optimism bias is the most expensive line item in a cybersecurity budget that does not appear on the spreadsheet. The antidote is not pessimism — it is honest capacity assessment, made before decisions are made, not after.*
>
> **— Dr. Dave Chatterjee**

Closing Thoughts: Security as Competitive Advantage

Asked for his final word, Bruno reframes cybersecurity and compliance not as a cost center but as a strategic differentiator: a way to show customers and partners that their data is genuinely protected, to build a defensible reputation, and to win business that less prepared competitors cannot credibly pursue. Dr. Chatterjee closes by encouraging organizations to revisit their cybersecurity governance with that same mindset before approaching a partner like BEMO, so that the engagement reflects true readiness rather than a transactional checkbox.

Actionable Recommendations

RECOMMENDATION	DETAIL
Assign Ownership Explicitly, Never Assume It	Name a specific owner for security and for each major compliance effort, with clearly assigned responsibility and resources. Ownership that is assumed rather than assigned creates confusion and allows accountability to evaporate the moment something goes wrong.
Treat Security as Cross-Functional, Not an IT-Only Task	Recognize that HR, finance, and operations own specific controls — onboarding, background checks, training, vendor access — that cannot be delegated to IT. Security succeeds only when every function treats it as part of doing business, the same way everyone is expected to own customer satisfaction.
Conduct an Honest Capacity Assessment Before Committing	Before assigning compliance or security ownership to an already-stretched team, assess realistically whether that team has the bandwidth and expertise to deliver. Optimism about internal capacity is the hidden cost driver behind most failed compliance efforts.
Automate Continuous Log Review, Not Just Point-in-Time Audits	Use automated and AI-assisted log review to surface month-over-month deltas and open remediation tickets automatically, rather than relying solely on an annual audit to reveal gaps.
Run Unannounced Tabletop Exercises	Test incident response without telegraphing the date in advance, so leadership sees how the organization genuinely reacts under pressure rather than a rehearsed, artificially clean result.
Align Security Strategy With Business Strategy	Ensure the security function understands and supports business goals rather than operating in isolation or being evaluated purely as a cost center. Where IT reports within the organization meaningfully shapes whether security is treated strategically or transactionally.
Vet Client and Vendor Commitment Before Engaging	Insist that C-level leadership participate in initial security or compliance discussions as a test of genuine commitment, and be willing to decline engagements where leadership intends only to check a compliance box rather than improve real security posture.
Reframe Compliance as a Competitive Advantage	Position cybersecurity and compliance investment as a driver of customer trust, reputation, and revenue rather than a cost of doing business, to build sustained organizational motivation for the discipline pillar of the CPD Framework.

Time Stamps

TIME	CONTENT
0:02	Introduction — Dr. Chatterjee's background and credentials
0:49	Host framing: the gap between executive intention and operational security reality, with two cautionary examples
3:37	Bruno Lecoq welcome and introduction
3:49	Guest background — 20 years at Microsoft, founding BEMO, and the cross-industry pattern of ownership gaps
5:27	Dr. Chatterjee on governance beyond compliance, and the realities facing resource-constrained SMBs
7:25	Security as a team sport: clarifying ownership, aligning resources, and creating discipline
9:24	Why the gap between intention and follow-through persists in small organizations
10:30	IT and business strategy misalignment, and the SAP security example
12:33	How an organization's reporting structure shapes whether security is seen as cost or strategy
13:46	The SOC 2 example: compliance controls that belong outside IT
14:26	The CPD Framework applied to the SOC 2 fire drill scenario — Commitment and Preparedness
17:26	Bruno on compliance rushed for deal purposes versus genuine readiness
19:03	The Epic case study parallel, and the Discipline pillar of the CPD Framework
21:54	The evolution of access control discipline — from permanent admin to ticketed elevation
23:31	Cybersecurity as a strategic opportunity, not a cost of doing business
25:36	How BEMO operationalizes continuous compliance with automated, AI-assisted log review
27:42	Key takeaway: most cybersecurity failures are leadership failures, not technology failures
29:57	Tool sprawl without ownership, and the strain on under-resourced IT teams
30:27	Key takeaway: optimism bias as the hidden, unbudgeted cost of cybersecurity programs
33:22	Bruno's real-world example: declining a prospect demanding an unrealistic CMMC timeline
35:08	Dr. Chatterjee on requiring C-level participation as evidence of genuine commitment

38:52	Monthly business reviews and unannounced tabletop exercises as tests of true readiness
40:17	The CPD Framework recap — Commitment, Preparedness, and Discipline working together
42:09	Bruno on which CPD pillar organizations struggle with most: sustaining discipline
43:52	The paycheck analogy: discipline in security as essential as discipline in payroll
48:15	Bruno's closing thought: cybersecurity and compliance as a competitive advantage
48:58	Episode wrap-up and listener call to action

Memorable Quotes

	The leadership decision that ended the practice wasn't made during the attack — it was made in every budget cycle before it. **— Dr. Dave Chatterjee**
	The bad part is the person who is responsible to check all the logs, who does the dirty job every week, every month to make sure you stay secure, never gets any kudos. If you stay secure, that person gets nothing; if there's a hack, that person gets the blame. **— Bruno Lecoq, CEO, BEMO**
	If you don't have the discipline of securing the organization in a sustained manner, the organization will also not survive. The difference is the paycheck is tangible — the adverse effect of poor security takes a while to show, but when it happens, it's too late to recover from it. **— Dr. Dave Chatterjee**
	I believe in compliance not for the paper, but for opening my system to someone outside who can find the gaps before a hacker does. I don't see that as something bad — I find it something good. **— Bruno Lecoq, CEO, BEMO**
	Cybersecurity and compliance, done the right way, are a huge competitive advantage — it's how you prove to your customers that you care about protecting their information. **— Bruno Lecoq, CEO, BEMO**