CYBERSECURITY READINESS PODCAST SERIES Episode 106

The Invisible Attack Surface: Zero Trust for SAP and ERP Environments

with Holger Hügel, Chief Technology Officer, SecurityBridge

Host	Dr. Dave Chatterjee, Duke University
Guest	Holger Hügel, Chief Technology Officer, SecurityBridge
Topic Focus	Zero Trust for SAP / ERP Environments
Podcast Portal	https://www.cybersecurityreadinesspodcast.com/

Summary

In Episode 106 of the Cybersecurity Readiness Podcast Series, Dr. Dave Chatterjee is joined by Holger Hügel — Chief Technology Officer of SecurityBridge and a global authority on SAP cybersecurity with over 26 years of experience — to address a governance blind spot that exists inside the security perimeters of even the most mature enterprise organizations: the SAP environment.

Opening with the August 2024 ransomware attack on Stoli Group USA — where attackers went straight for the company's SAP enterprise resource planning (ERP) system, disrupting financial operations and contributing directly to a bankruptcy filing within three months — Dr. Chatterjee frames the episode's central challenge: organizations can have zero trust architecture, network segmentation, and identity governance fully deployed across their IT landscape, and still be critically exposed, because most CISOs have never formally claimed accountability for SAP security, and most SAP teams do not think of themselves as part of the security function.

Hügel explains the structural gap at the heart of this problem. SAP systems are simultaneously the most business-critical and the least security-governed assets in most large organizations. The C-suite depends on them for financial operations, payroll, procurement, and supply chain continuity, yet SAP teams and security teams speak different languages, operate under different budgets, and rarely collaborate. SAP departments typically define "security" as managing user authorizations and privileges — a narrow interpretation that leaves configuration drift, patch backlogs, and monitoring gaps entirely unaddressed.

Analyzed through Dr. Chatterjee's Commitment–Preparedness–Discipline (CPD) framework, the conversation translates SAP cybersecurity from a technical niche into a governance imperative. The Medtronic case study demonstrates what good looks like: a CISO who crossed the organizational divide, sponsored SAP hardening from the cybersecurity budget, built a continuous patch management process, and created the governance structure that allowed the team to respond to an out-of-band vulnerability within hours rather than weeks.

The episode's central message is neither technical nor abstract: the organizations that will survive the next ERP-targeted ransomware attack are not those with the most sophisticated tools — they are the ones that have claimed ownership of the problem, built the processes to address it continuously, and created the cross-functional governance structures that SAP and cybersecurity teams cannot build on their own.

Discussion Highlights

The Opening Incident: When ERP Becomes the Target

Dr. Chatterjee opens with the August 2024 ransomware attack on Stoli Group USA, the North American arm of the company behind one of the world's most recognized vodka brands. The attackers did not go for peripheral systems — they went straight for the SAP ERP platform running the company's financial operations, reporting, and core business processes. The system went down. The business stopped

running. Within three months, the company filed for bankruptcy. Court documents identify the attack on the SAP environment as a direct contributing cause.

Hügel confirms this is not an isolated case. ERP systems represent the highest-value targets in the enterprise because they contain the most sensitive financial, personal, and operational data — and because the organizations that depend on them most have often governed their security the least.

> *"When SAP is not working, you need a fix within hours, not days, not weeks. These systems are not just IT — they are the business. And unfortunately, organizations have opened them to the world through digital transformation and supply chain integration without fully understanding the risk."*
>
> **— Holger Hügel, CTO, SecurityBridge**

The Governance Gap: Why SAP Security Falls Between Chairs

Hügel identifies the structural cause of the SAP security gap with precision: the C-suite focuses on business outcomes and largely delegates technology decisions; the SAP department defines itself as a service provider to the business rather than a security stakeholder; the CISO function governs "IT security" but has historically not claimed ownership of application-layer ERP security. The result is a gap at the intersection of all three.

SAP environments are technically distinct — with their own terminology, architecture, patch cycles, access frameworks, and monitoring constraints — and that distinctiveness has made it easy for each organizational layer to assume someone else is responsible. As Hügel notes, when a CISO asks the SAP team about security posture, they will typically hear about user authorizations and privilege management. The configuration drift, the patch backlog, and the absence of continuous monitoring will not be mentioned, because the SAP team does not see those as their security problem.

> *"The C-suite has no clue what happens in their SAP environment. The SAP guys don't see themselves as part of IT. And in that gap, the organization is exposed in ways that no one has been asked to own."*
>
> **— Holger Hügel, CTO, SecurityBridge**

Zero Trust Applied to SAP: What It Actually Means

Dr. Chatterjee explains that zero trust — as a philosophy — means verifying before trusting, continuously, across every control domain. In the SAP context, Hügel translates this into specific architectural implications:

Least privilege access must be enforced not just at provisioning but dynamically and on a time-limited basis. Privileged users who require elevated access to perform specific activities should have those privileges elevated for the duration of the activity and then lowered — a pattern SecurityBridge calls privilege elevation with time-bounded scope. This approach does not just reduce the attack surface; it produces cleaner, more actionable monitoring signals, because privileged activities that occur outside of a declared elevation session become anomalies that can be detected.

Patching must be continuous, not periodic. SAP publishes security patches monthly, and in an AI-enabled threat environment, the window between disclosure and active exploitation is measured in hours, not weeks. Organizations that batch SAP patches into quarterly change management cycles are accepting a persistent, documented exposure. The Medtronic case demonstrated that a governance decision — to prioritize patch velocity over change management formality for security-critical fixes — is achievable and operationally defensible.

System hardening must follow SAP's own published security baseline — a documented set of configuration parameters that, when implemented, brings the system to a defensible security posture. Hügel notes that most organizations have never fully implemented this baseline, and that doing so is

neither technically complex nor prohibitively resource-intensive. It requires a governance decision to treat it as an obligation rather than a recommendation.

Monitoring alone cannot protect SAP environments. This is the point Hügel makes most forcefully: because SAP audit logs are written inside the system and must be pulled by external monitoring tools, there is an inherent latency between an event and its appearance in a SIEM. In an environment where administrators and attackers generate identical-looking log entries, no monitoring solution — regardless of AI capability — can consistently distinguish between the two in real time. The answer is to make the environment harder to penetrate and harder to move through, rather than to bet on faster detection.

> *"Monitoring alone won't protect an SAP system. The data is always delayed. Your reaction is delayed. It's like trying to drive a car while drunk — no matter how many assistants you have, it simply doesn't work. The answer is to harden the environment so that if someone gets in, they cannot get out."*
>
> **— Holger Hügel, CTO, SecurityBridge**

The CPD Framework Applied to SAP Security

Dr. Chatterjee applies the Commitment–Preparedness–Discipline (CPD) framework to SAP security governance, with Hügel's analysis illustrating each pillar:

CPD PILLAR	APPLICATION TO SAP ZERO TRUST
COMMITMENT	SAP security cannot improve until a named organizational leader — typically the CISO — explicitly claims accountability for it. The organizational gap exists precisely because no one has done so. Commitment means entering SAP risk in the enterprise risk register, allocating budget across the CISO–SAP divide, and establishing that SAP cybersecurity is not the SAP team's problem alone or the CISO's problem alone — it is a shared governance obligation.
PREPAREDNESS	Preparedness in the SAP context means: conducting an authorization landscape assessment (role assignments, separation of duties conflicts, inactive user access, privilege accumulation); implementing the SAP security baseline configuration; establishing a continuous patch management process with defined velocity targets; and building an incident response plan that specifically accounts for ERP-targeted ransomware. Organizations that have never done these things are not unprepared in a technical sense — they are unprepared in a governance sense.
DISCIPLINE	Discipline means that the processes built under Preparedness are executed continuously, not triggered only by audits, penetration tests, or incidents. SecurityBridge research shows that 67% of organizations address SAP security reactively — a finding that defines the absence of Discipline precisely. Continuous monitoring, periodic access reviews, configuration drift detection, and patch cadence are not one-time achievements. They are organizational habits that must be maintained, measured, and verified.

The Medtronic Case Study: What Good Looks Like

Hügel presents Medtronic as the clearest available illustration of CPD in action. The CISO approached the SAP team not with a mandate but with a question: can we join forces? The answer produced a joint governance structure in which the CISO sponsored the hardening of the SAP environment from the

cybersecurity budget — bridging the resource gap that typically prevents SAP security investment — while the SAP team provided the domain expertise to execute.

The sequence Hügel describes is instructive: rather than beginning with SIEM integration (the common but often counterproductive starting point), Medtronic started with system hardening. A hardened system produces far fewer false-positive alerts, which means that when monitoring is introduced, it produces actionable signal rather than noise. The process was then formalized — turning a one-time remediation into a repeatable governance discipline.

The governance investment proved its value when an out-of-band vulnerability was disclosed. Rather than waiting for the next scheduled change window, Medtronic assessed the risk, tested the patch within hours, and deployed to production the same day. The ability to move at that velocity was not the result of luck or urgency — it was the result of having built the process infrastructure in advance.

> *"Medtronic didn't get lucky. They built the infrastructure. They had the processes in place. The CISO committed to it, the teams were prepared for it, and the discipline was there the day the out-of-band vulnerability hit."*
>
> **— Dr. Dave Chatterjee**

Actionable Recommendations

**For CISOs: Establish Visibility First Commission an assessment of your SAP authorization landscape — role assignments, separation of duties conflicts, inactive user access, and privilege accumulation. You cannot govern what you cannot see, and most CISOs have never seen this picture.	**For CISOs: Formalize Ownership Accountability for SAP security must be formally assigned inside the CISO function. This is a governance decision, not a headcount decision. The organizational gap exists because no one has claimed it. Claim it.
**Assess and Remediate Your Patch Posture Identify disclosed, unpatched SAP vulnerabilities in your environment and document what compensating controls, if any, are in place. In an AI-enabled threat environment, patch latency is not a compliance issue — it is an active exposure.	**Implement the SAP Security Baseline SAP publishes a documented set of security configuration parameters. Most organizations have never fully implemented it. Doing so is the single highest-leverage hardening action available and requires no new tooling — only governance commitment.
**Build a Cross-Functional Governance Structure The Medtronic model — CISO sponsoring SAP hardening in partnership with the SAP team — is replicable. Budget the collaboration, not just the tools. The organizational gap will not close on its own.	**Shift from Reactive to Continuous SecurityBridge research shows 67% of organizations address SAP security only in response to audits, penetration tests, or incidents. Establish routine monitoring, periodic access reviews, and configuration drift detection as standing processes — not event-driven responses.
**Apply Time-Bounded Least Privilege Implement privilege elevation with time-bounded scope for SAP users requiring elevated access. This reduces the attack surface and dramatically improves monitoring signal quality — making it possible to distinguish administrative activity from adversarial activity in the audit logs.	**For Boards: Ask for Comparative Penetration Test Reports Board members need not understand SAP terminology. They should ask their security or SAP team to produce the last two penetration test reports side by side. If the findings are the same, the organization has not improved. That is the

	governance signal boards can act on without technical expertise.

Time Stamps

0:00	Opening scenario — the August 2024 Stoli Group USA ransomware attack on SAP and the bankruptcy that followed
0:49	Host framing: ERP as the central nervous system of the organization — and the overlooked attack surface
3:07	Holger Hügel welcome and introduction
3:23	Guest career journey — 26 years in SAP environments, from IT service management to SAP cybersecurity
6:14	SAP and ERP explained for general audiences — what they are, why they matter, why the stakes are high
9:42	The governance gap: why the C-suite, the CISO, and the SAP team each assume someone else owns SAP security
12:48	Dr. Chatterjee's observation: integrated cybersecurity governance should encompass all systems, including ERP
13:29	The CPD framework introduced — Commitment, Preparedness, Discipline as the governance lens
17:39	CPD applied to SAP security — Hügel maps each pillar to the specific SAP governance challenge
22:26	The 67% finding: most organizations address SAP security reactively — and what that means in practice
24:08	Three elements of SAP cybersecurity preparedness: patching, baseline configuration, and privileged access monitoring
29:27	Why monitoring alone cannot protect SAP — the log-pull latency problem and its governance implications
29:58	Time-bounded least privilege: SecurityBridge's approach to improving monitoring signal quality
30:58	Zero trust for SAP — what the framework means in an environment with inherent monitoring constraints
34:32	Assume the breach: hardening as the primary SAP defense strategy, not detection speed
36:15	The prison analogy: you cannot prevent entry, but you can make exit impossible
39:01	Checks and balances in SAP: building controls that limit lateral movement and trigger immediate alerts
40:18	The Medtronic case study — CISO-sponsored SAP hardening, cross-functional governance, and out-of-band patch response
44:38	Dr. Chatterjee synthesizes Medtronic through the CPD lens: they built the infrastructure, they weren't lucky

45:56	Closing recommendations for CISOs: establish visibility, formalize ownership, assess patch status
47:21	Recommendations for boards: ask for two consecutive penetration test reports — improvement is the metric
48:35	Closing remarks and episode wrap-up

Memorable Quotes

"A ransomware attack did not just cause disruption — it ended a company. Court documents cite the attack on the SAP system as a direct contributing cause of the company's collapse. This is not a theoretical risk. This is a business continuity risk that has already materialized."

— Dr. Dave Chatterjee

"SAP is not just an application — it is an environment for developing applications, for managing financial data, for running the business. When SAP is not working, the business is not working. And yet the governance structures to protect it are either absent or disconnected from the security function entirely."

— Holger Hügel, CTO, SecurityBridge

"67% of organizations address SAP security reactively — actions triggered only by audit, penetration test, or incident. There is no routine monitoring, no periodic access review, no process for identifying configuration drift. When a threat actor arrives, the organization is literally starting from zero."

— Dr. Dave Chatterjee

"Think about an SAP system as a prison for the cyber attack. They will get in — there are always ways in. But they will never get out. You don't know how they got in, but you know exactly how they will try to get out. Those are the doors you control."

— Holger Hügel, CTO, SecurityBridge

"The gap maps precisely onto the CPD pillars: Commitment — someone has to own SAP security and say so out loud. Preparedness — the baseline must be implemented and the patch process must be operational before the incident. Discipline — the organization must verify continuously that those controls are still working."

— Dr. Dave Chatterjee

"In the AI era, you need to patch everything. AI-supported attacks will use tag chains — combining vulnerabilities you never imagined together — to reach targets you thought were protected. The 80% approach that was acceptable before is not acceptable now."

— Holger Hügel, CTO, SecurityBridge