KI und Cybersecurity:
Die größte Führungsfrage des Jahres 2026

Von Leif Steen und Punit Thakkar

1. Das 22-Sekunden-Problem

Hier ist eine Zahl, die verändert, wie jeder über Cybersecurity denken sollte.

Auf der RSA Conference 2026 enthüllte Sandra Joyce, VP von Google Threat Intelligence, dass die Zeit zwischen dem ersten Netzwerkzugang und der Weitergabe an andere Angreifer von acht Stunden im Jahr 2022 auf nur 22 Sekunden im Jahr 2025 geschrumpft ist. Zweiundzwanzig Sekunden. So viel Zeit bleibt einem Verteidiger, bevor ein Angreifer übergibt und tiefer in die Systeme eines Unternehmens vordringt.

Kein Mensch kann so schnell reagieren. Genau deshalb verändert KI die Cybersecurity von Grund auf.

Die Zahlen sprechen eine klare Sprache. Laut einem Kiteworks-Report von 2026 setzen 77 % der Organisationen bereits generative KI in ihrem Security-Stack ein. Doch nur 37 % haben eine formale KI-Richtlinie. Die Kluft zwischen Einsatzgeschwindigkeit und Governance ist enorm.

Und Angreifer schauen genau hin. Eine Umfrage von Dark Reading vom Februar 2026 ergab, dass 48 % der Cybersecurity-Fachleute agentische KI (also autonome Systeme, die eigenständig planen, sich anpassen und hartnäckig weiterarbeiten) als den gefährlichsten Angriffsvektor betrachten. Diese Systeme stoppen nicht nach einem gescheiterten Versuch. Sie versuchen es erneut.

Die Botschaft ist eindeutig. Angriffe werden heute in Sekunden gemessen. Die KI-Adaption in den meisten Unternehmen wird noch in Quartalen gemessen.

2. Eine neue Art von Organisation

Was bedeutet das in der Praxis?

Es bedeutet, dass sich das Organigramm weiterentwickeln muss. Das ist etwas, woran wir seit einiger Zeit arbeiten, und wir haben unsere Erkenntnisse kürzlich im Berlin Capital Club präsentiert.

Die Kernidee ist das, was wir die „augmentierte Organisation“ nennen. In der alten Welt wurde jede Sicherheitsaufgabe von einem Menschen erledigt. In der neuen Welt arbeiten hybride Teams aus Menschen und KI zusammen. Einige Funktionen übernimmt die KI vollständig. Andere werden durch KI-Unterstützung leistungsfähiger. Das Ergebnis ist eine Organisation, die schneller lernt, präziser entscheidet, effektiver schützt und in einem größeren Maßstab arbeiten kann als je zuvor.

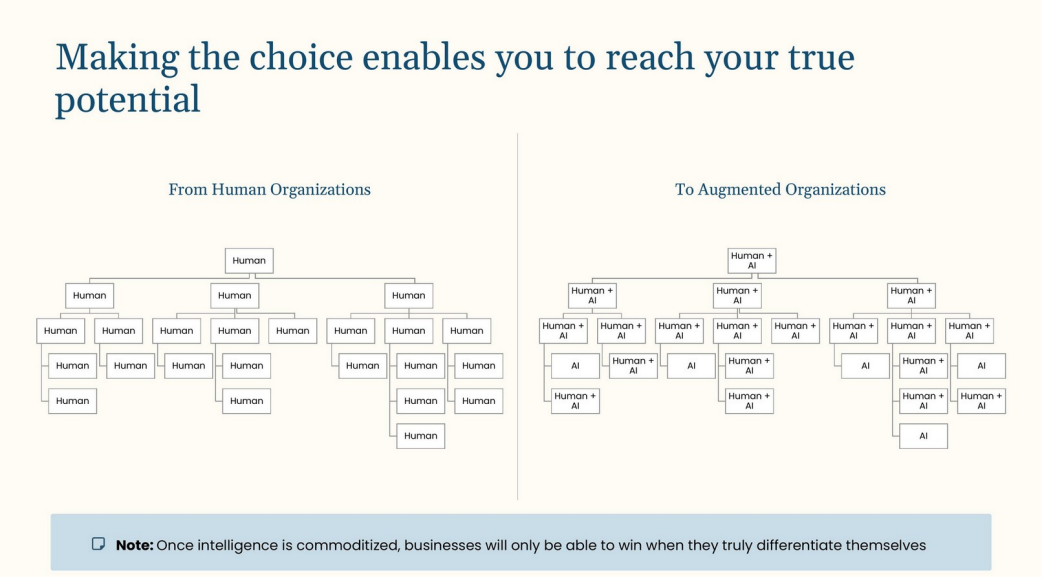

Abbildung: Von Human-Organisationen zu augmentierten Organisationen (© Leif Steen / Punit Thakkar)

Das erfordert neue Rollen. Einen Chief AI Security Officer (CAISO), der Technologie und Geschäftsstrategie gleichzeitig versteht. Ein AI-Governance-Team, das Regeln definiert, bevor etwas schiefgeht. Eine Unternehmenskultur, die KI-Kompetenz als Grundvoraussetzung behandelt, genauso wie wir heute grundlegende Computerfähigkeiten voraussetzen.

Leif bringt acht Jahre Erfahrung in Wachstumsstrategie, Marketing und Unternehmensaufbau mit. Punit bringt elf Jahre Erfahrung aus Technologie, Unternehmensführung und Medien mit, darunter als Frontier-AI-Research-Consultant am Fraunhofer HHI. Wir haben beide an der ESMT Berlin studiert und dort auch den MBA-Kurs „AI for Managers“ entwickelt. Wir teilen die Überzeugung, dass KI eine Führungsaufgabe ist.

Die zentrale Erkenntnis aus unserer Arbeit: Sobald Intelligenz zur Massenware wird, können Unternehmen nur noch gewinnen, wenn sie sich wirklich differenzieren. Diese Differenzierung muss auf ganzer Linie erfolgen, auch bei internen Strukturen. Das Organigramm von gestern ist für die Herausforderungen von morgen schlicht nicht gemacht.

3. Vom Feuerlöscher zum Architekten

Viele CISOs verbringen ihre Tage im Krisenmodus. Ein Angriff hier, ein Datenleck dort. Sie haben das Gefühl, ständig Brände zu löschen. Definitiv etwas, das auf Dauer niemandem Freude macht.

Wer immer nur Feuer löscht, baut nie ein feuerfestes Haus.

Die KI-Revolution verlangt drei fundamentale Denkwechsel von Security-Führungskräften.

Erstens: Von der Führung von Menschen zur Führung von Intelligenz. Wer heute ein Team leitet, wird morgen auch KI-Agenten leiten. Das erfordert neue Fähigkeiten, vor allem das, was wir „Agent Engineering“ nennen: die Kunst, KI-Systeme so zu konfigurieren, dass sie zuverlässig arbeiten. Es läuft auf eine klare Definition von Rolle, Aufgabe und Kontext hinaus.

Zweitens: Von individueller KI-Kompetenz zu organisationsweiter KI-Fluenz. Es reicht nicht, wenn der CISO weiß, wie man ChatGPT oder Claude benutzt. KI-Wissen muss durch

die gesamte Organisation fließen. Peer-to-Peer-Lernen, interne Sessions, eine gemeinsame Plattform für KI-Erfolge. All das gehört zur Strategie.

Drittens: Vom Fragenstellen zum Erteilen von Missionen. Statt Mitarbeitern eine einzelne Aufgabe zu geben und auf Ergebnisse zu warten, sollten Führungskräfte Missionen definieren. Mit Hilfe einer Impact-vs.-Capability-Matrix (einer einfachen Methode, die wir zur Priorisierung von KI-Projekten nach Wirkung und Umsetzbarkeit entwickelt haben) wird klar, wo die größte Hebelwirkung liegt.

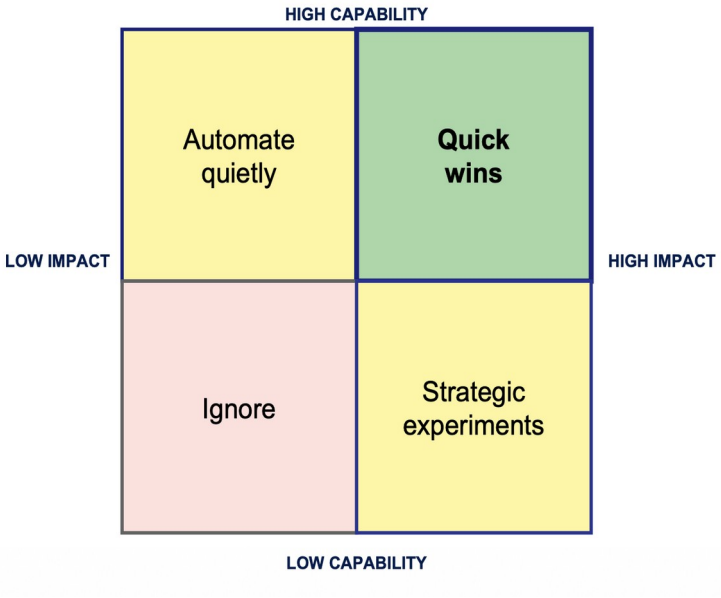

Abbildung: Impact-vs.-Capability-Matrix (© Leif Steen / Punit Thakkar)

Vertrauen, Transparenz und erklärbare KI sind hier entscheidend. Sie sind das Fundament, das verhindert, dass KI-Initiativen am internen Widerstand scheitern. Wer eine Kultur aufbauen will, die KI-Experimente ermöglicht und gleichzeitig Compliance schützt, braucht klare Leitplanken. Und den Mut, sie durchzusetzen.

4. Ein Kompass für den Einstieg

Hier sind die konkreten Lektionen aus unserer Praxis und Forschung.

Do’s

- ✓ Definieren Sie eine KI-Richtlinie, bevor der erste Mitarbeiter KI einsetzt. Regeln vor Werkzeug.
- ✓ Starten Sie mit einem Quick Win. Ein überschaubares Projekt (zum Beispiel automatisierte Log-Analyse), das innerhalb von 30 Tagen Ergebnisse liefert.
- ✓ Machen Sie KI-Wissen zur Teamaufgabe. Peer-to-Peer-Lernen, „Prompt der Woche“-Sessions, eine gemeinsame Plattform für KI-Erfolge.
- ✓ Erstellen Sie eine „Soul File“ und eine „Constitution File“: Dokumente, die beschreiben, wie Sie und Ihr Team denken und mit KI arbeiten. So handeln KI-Agenten im Interesse der Organisation.
- ✓ Priorisieren Sie mit der Impact-Capability-Matrix. Alles, was möglich ist, ist spannend. Konzentrieren Sie sich auf das, was auch sinnvoll ist.

Don’ts

- ✗ KI nur als IT-Projekt behandeln. KI gehört in die gesamte Führungsebene.
- ✗ Ohne Governance starten. Shadow-AI (KI-Nutzung ohne Wissen der Führung) ist das neue Shadow-IT.
- ✗ Auf den perfekten Moment warten. Es gibt ihn nicht. Die Welt bewegt sich bereits.
- ✗ KI-Ergebnissen blind vertrauen. KI ist ein mächtiges, aber fehlbares Werkzeug. Menschliche Aufsicht bleibt unerlässlich.
- ✗ Kulturwandel ignorieren. Die beste Technologie der Welt scheitert, wenn die Menschen dahinter zurückgelassen werden.

5. Wie geht es weiter?

Gartner prognostiziert, dass 40 % der Unternehmensanwendungen bis Ende 2026 aufgabenspezifische KI-Agenten integrieren werden, gegenüber weniger als 5 % im Jahr 2025. Das ist ein achtfacher Anstieg in einem einzigen Jahr. Proofpoints Cybersecurity-Ausblick warnt, dass autonome Copiloten bis 2026 Menschen als Hauptquelle von Datenlecks übertreffen könnten. Unternehmen führen KI-Assistenten in rasantem Tempo ein, ohne zu erkennen, dass sie die gleichen Datenhygiene-Probleme übernehmen, die bereits in ihren Umgebungen existieren.

Die Chance ist enorm. Die Unternehmen, die KI-Cybersecurity richtig umsetzen, werden einen strukturellen Vorteil gewinnen, der sich über die Zeit potenziert. Wer heute Governance-Rahmenwerke aufbaut, wird morgen mit Zuversicht skalieren können.

Das ist eine Zukunft, die es wert ist, gebaut zu werden. Die Frage ist: Sind Sie bereit, sie zu führen?

Über die Autoren

© Leif Steen

Leif Steen, Go-to-Market- & Wachstumsstratege

Leif Steen kommt aus acht Jahren im Bereich Wachstumsstrategie, Marketing und Unternehmensaufbau. Nach Stationen unter anderem als Incubation Manager, Co-Founder und Digitalmarketing-Stratege studierte er an der ESMT Berlin (MBA, #1 in Deutschland laut FT Rankings 2025) sowie an der HEC Paris. Heute verbindet er seine Go-to-Market-Erfahrung mit dem Thema KI-Führung.

© Punit Thakkar

Punit Thakkar, KI-Forscher, Unternehmer & Technologieberater

Punit Thakkar ist Frontier-AI-Research-Consultant am Fraunhofer Heinrich-Hertz-Institut (HHI) in Berlin und Absolvent der ESMT Berlin (MBA). Mit elf Jahren Erfahrung aus Technologie, Unternehmensführung und Medien verbindet er Forschung und Praxis. An der ESMT Berlin hat er den Executive-MBA-Kurs „AI for Managers“ mitentwickelt. Er ist zudem Autor des Newsletters „Hello Universe“ auf Substack.

Dieser Beitrag erscheint als Gastbeitrag auf datensicherheit.de

ENGLISH VERSION

AI and Cybersecurity:
The Biggest Leadership Question of 2026

By Leif Steen and Punit Thakkar

1. The 22-Second Problem

Here is a number that changes the way anyone should think about cybersecurity.

At RSA Conference 2026, Google Threat Intelligence VP Sandra Joyce revealed that the time between initial network access and attacker hand-off has collapsed from eight hours in 2022 to just 22 seconds in 2025. Twenty-two seconds. That is the window a defender has to respond before an attacker completes a hand-off and moves deeper into a company's systems.

No human can react that fast. This is why AI is transforming cybersecurity from the inside out.

The numbers tell a striking story. According to a 2026 Kiteworks report, 77% of organisations now run generative AI in their security stack. Yet only 37% have a formal AI policy in place. That gap between deployment speed and governance is staggering.

And attackers are paying attention. A Dark Reading poll from February 2026 found that 48% of cybersecurity professionals now see agentic AI as the single most dangerous attack vector. These are autonomous systems that can plan, adapt, and persist with minimal human input. They do not stop after a failed attempt. They try again.

The point is clear. The speed of attacks is now measured in seconds. The speed of AI adoption at most companies is still measured in quarters.

2. A New Kind of Organisation

So what does this mean in practice?

It means the org chart needs to evolve. This is something we have been articulating for some time, and we recently presented our thinking at the Berlin Capital Club.

The core idea is what we call the "augmented organisation." In the old world, every security task was done by a human. In the new world, hybrid teams of people and AI work together. Some functions are handled entirely by AI. Others become more capable because of AI support. The result is an organisation that learns faster, decides more precisely, protects more effectively, and operates at a larger potential scale than ever before.

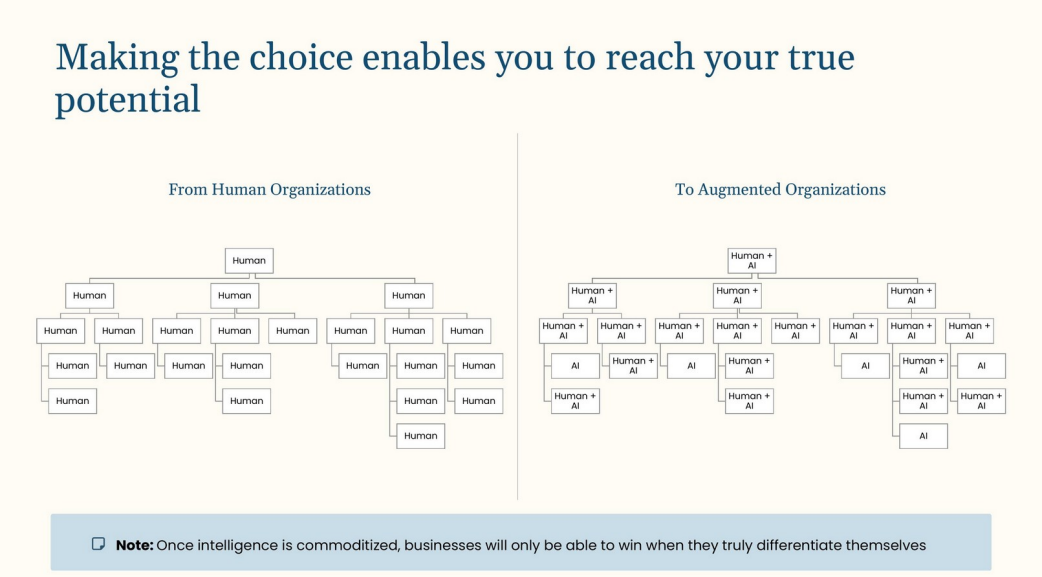

Figure: From human organisations to augmented organisations (© Leif Steen / Punit Thakkar)

This requires new roles. A Chief AI Security Officer (CAISO) who understands technology and business strategy at the same time. An AI governance team that defines rules before something goes wrong. A corporate culture that treats AI literacy as a baseline requirement, the same way we treat basic computer skills today.

Leif brings eight years of experience in growth strategy, marketing, and business building. Punit brings eleven years across technology, business leadership, and media, including work as a frontier AI research consultant at Fraunhofer HHI. We both studied at ESMT Berlin, and also developed an executive MBA course “AI for Managers”. We share a conviction that AI is a leadership responsibility.

The key insight from our work is that once intelligence is commoditised, businesses can only win when they truly differentiate themselves. This differentiation needs to occur across the board, including internal structures. Yesterday’s org chart is simply not built for the challenges of tomorrow.

3. From Firefighter to Architect

Many CISOs spend their days in crisis mode. An attack here, a data breach there. They feel like they are fighting fires, which is not that pleasant an experience.

Anyone who only keeps fighting fires never builds a fireproof house.

The AI revolution calls for three fundamental mindset shifts from security leaders.

First: from leading people to leading intelligence. Anyone who leads a team today will also lead AI agents tomorrow. This requires new skills, especially what we call “agent engineering,” the art of configuring AI systems so they work reliably. It comes down to a clear definition of role, task, and context.

Second: from individual AI literacy to organisation-wide AI fluency. It is simply not enough for the CISO to know how to use ChatGPT or Claude. AI knowledge must flow through the entire organisation. Peer-to-peer learning, internal sessions, a shared platform for AI wins. All of this is part of the strategy.

Third: from asking questions to assigning missions. Instead of posing a single task to employees and waiting to see results, leaders should define missions. With the help of an impact-vs.-capability matrix (a simple method we developed for prioritising AI projects by effect and feasibility), it becomes clear where the greatest leverage lies.

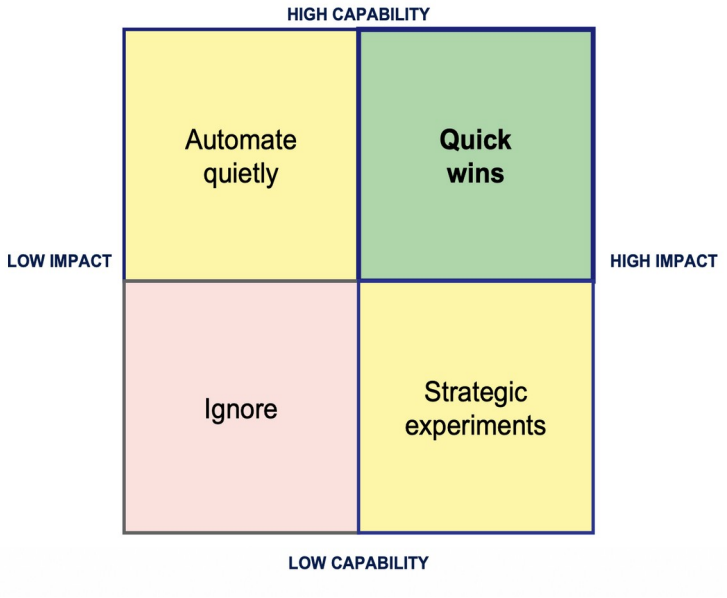

Figure: Impact-vs.-Capability Matrix (© Leif Steen / Punit Thakkar)

Trust, transparency, and explainable AI are critical here. They are the foundation that prevents AI initiatives from failing because of internal resistance. Anyone who wants to build a culture that allows AI experimentation and protects compliance at the same time needs clear guardrails, and the courage to enforce them.

4. A Compass for Getting Started

Here are the concrete lessons from our practice and research.

Do’s

- ✓ Define an AI policy before the first employee starts using AI. Rules before tools.
- ✓ Start with a quick win. A manageable project (for example, automated log analysis) that delivers results within 30 days.
- ✓ Make AI knowledge a team effort. Peer-to-peer learning, “Prompt of the Week” sessions, a shared platform for AI wins.
- ✓ Create a “soul file” and a “constitution”: documents that describe how you and your team think and work with AI. This way, AI agents act in the organisation’s interest.
- ✓ Prioritise with the impact-capability matrix. Everything that is possible is exciting. Focus on what is also sensible.

Don’ts

- ✗ Treat AI as just an IT project. AI belongs across the C-suite.

- ✗ Launch without governance. Shadow AI (AI usage without leadership's knowledge) is the new shadow IT.
- ✗ Wait for the perfect moment. It does not exist. The world is already moving.
- ✗ Trust AI results blindly. AI is a powerful but fallible tool, human oversight remains essential.
- ✗ Ignore cultural change. The best technology in the world fails when the people behind it are left behind.

5. Where Do We Go From Here?

Gartner projects 40% of enterprise applications will embed task-specific AI agents by the end of 2026, up from less than 5% in 2025. That is an eight-fold increase in a single year. Proofpoint's cybersecurity outlook warns that by 2026, autonomous copilots may surpass humans as the primary source of data leaks. Enterprises are rushing to roll out AI assistants without realising they inherit the same data hygiene issues already present in their environments.

The opportunity here is enormous. The companies that get AI cybersecurity right will gain a structural advantage that compounds over time. The ones that build governance frameworks today will be the ones that scale confidently tomorrow.

This is a future worth building. The question is: are you ready to lead it?

About the Authors

© Leif Steen

Leif Steen, Go-to-Market & Growth Strategist

Leif Steen brings eight years of experience in growth strategy, marketing and business building. After roles including incubation manager, co-founder and digital marketing strategist, he studied at ESMT Berlin (MBA, #1 in Germany according to FT Rankings 2025) and HEC Paris. Today he combines his go-to-market expertise with the topic of AI leadership.

© Punit Thakkar

Punit Thakkar, AI Researcher, Entrepreneur & Technology Consultant

Punit Thakkar is a frontier AI research consultant at the Fraunhofer Heinrich Hertz Institute (HHI) in Berlin and a graduate of ESMT Berlin (MBA). With eleven years of experience across technology, business leadership and media, he bridges research and practice. At ESMT Berlin he co-developed the executive MBA course “AI for Managers.” He also writes the “Hello Universe” newsletter on Substack.

This article appears as a guest contribution on datensicherheit.de