Commugen Unveils AI-Powered Cyber Risk Quantification Agent

New CRQ AI Agent helps CISOs quantify cyber risk, calculate ALE, and explain financial exposure with greater speed and confidence.

LONDIN, UNITED KINGDOM, June 23, 2026 /EINPresswire.com/ -- Commugen today announced the launch of its CRQ AI Agent, a new capability within the Commugen Cyber Risk Quantifier platform designed to help organizations accelerate, strengthen, and scale Cyber Risk Quantification (CRQ) programs.

The announcement comes as organizations face increasing pressure to demonstrate the business impact of cyber risk, justify security investments, and communicate risk exposure to executive leadership and boards of directors. While cybersecurity teams have historically relied on qualitative risk ratings such as "High," "Medium," and "Low," organizations are increasingly adopting Cyber Risk Quantification methodologies to translate cyber risk into measurable financial exposure.

Commugen's new CRQ AI Agent is designed to help organizations quantify cyber risk more efficiently by combining organizational context, external intelligence, historical incident data, industry benchmarks, and advanced risk analysis methodologies to generate explainable risk quantification recommendations.

The new capability expands Commugen's Cyber GRC platform and reflects growing industry demand for technologies that support Cyber Risk Quantification, cyber risk analysis, cyber risk assessment, financial risk modeling, board reporting, security ROI measurement, and risk-based decision making.

The Growing Importance of Cyber Risk Quantification

Over the past decade, cybersecurity has evolved from a technical function into a strategic business discipline.

Today's CISOs are expected not only to reduce cyber threats, but also to support business objectives, justify investments, prioritize initiatives, communicate with executive leadership, and demonstrate measurable value.

As a result, organizations are increasingly adopting Cyber Risk Quantification (CRQ) as a framework for understanding cyber risk in financial terms.

Cyber Risk Quantification enables organizations to estimate the financial impact of cyber events and determine the level of exposure associated with specific risks, vulnerabilities, assets, business processes, vendors, and threat scenarios.

Rather than asking whether a risk is "High" or "Critical," Cyber Risk Quantification helps organizations answer questions such as:

What is the potential financial impact of this cyber risk?
What is our annual risk exposure?
Which risks create the greatest business impact?
Which mitigation efforts provide the greatest reduction in exposure?
Which security investments generate the strongest return?
How should cyber risks be communicated to executive leadership and boards?

As cyber programs mature, these questions become increasingly important.

Boards are demanding greater visibility into cyber exposure. Regulators are placing increased focus on cyber governance and accountability. Executive teams are seeking stronger justification for cybersecurity spending.

In response, many organizations are moving toward quantified approaches that allow cyber risk to be measured, compared, prioritized, and communicated using financial metrics.

Moving Beyond Traditional Risk Assessments

Traditional cyber risk assessments often rely on qualitative scoring models.

These approaches remain useful for identifying and categorizing risks, but they can create challenges when organizations attempt to prioritize competing initiatives or justify investments.

For example, two risks may both be classified as "High."

However, one risk may represent a potential business impact of several hundred thousand dollars while another may expose the organization to losses measured in millions.

Without financial context, stakeholders may struggle to distinguish between them.

Cyber Risk Quantification addresses this challenge by estimating financial exposure using structured methodologies and quantitative models.

One of the most widely recognized concepts in Cyber Risk Quantification is Annualized Loss Expectancy (ALE).

ALE estimates expected annual financial exposure using the following formula:

ALE = Single Loss Expectancy (SLE) × Annualized Rate of Occurrence (ARO)

Within this framework:

Single Loss Expectancy (SLE) represents the estimated financial impact of a single cyber event.
Annualized Rate of Occurrence (ARO) represents the estimated frequency at which a cyber event is expected to occur.
Annualized Loss Expectancy (ALE) represents the estimated annual exposure associated with a given risk.

These concepts help organizations compare risks using a common financial metric and support more informed investment decisions.

However, implementing Cyber Risk Quantification consistently across an enterprise remains a significant challenge.

The Challenge of Scaling Cyber Risk Quantification

While the principles behind Cyber Risk Quantification are relatively straightforward, maintaining a quantification program across hundreds or thousands of risks can be difficult.

Organizations must continuously:

Identify emerging risks
Assess changing threat conditions
Evaluate business impacts
Track mitigation effectiveness
Recalculate risk exposure

Maintain risk registers
Support audits and compliance activities
Prepare reports for executive leadership and boards

Many organizations begin this process using spreadsheets and manual calculations.

As cyber programs expand, manual approaches often become difficult to maintain.

Risk assessments may become inconsistent.

Assumptions may vary between analysts.

Calculations may become difficult to defend.

Documentation may become fragmented.

The challenge is amplified when organizations operate across multiple business units, geographies, regulatory environments, and threat landscapes.

This is one of the reasons demand for Cyber Risk Quantification software, Cyber Risk Quantification platforms, and Cyber GRC solutions continues to grow.

Commugen's Cyber Risk Quantifier

Commugen's Cyber Risk Quantifier was developed to help organizations operationalize Cyber Risk Quantification at scale.

The platform enables organizations to connect risks, controls, vulnerabilities, assets, business processes, vendors, and mitigation activities within a centralized Cyber GRC environment.

Capabilities include:

Cyber Risk Quantification
Financial risk modeling
Risk exposure analysis
Inherent and residual risk calculations
Mitigation effectiveness tracking
Risk visualization
Board reporting
Risk trend analysis
Risk prioritization
Risk-based decision support

The platform also supports advanced simulation capabilities, including Monte Carlo simulation, enabling organizations to model uncertainty and evaluate a wide range of potential outcomes.

Rather than relying on single-point estimates, organizations can evaluate realistic ranges of likelihood and impact.

This approach helps create more defensible risk assessments and better reflects the statistical nature of cyber risk.

According to Commugen, the objective is not to predict the future with perfect accuracy.

Instead, the goal is to support more informed business decisions by helping organizations understand their likely exposure and the effectiveness of potential mitigation strategies.

Introducing the CRQ AI Agent

The newly announced CRQ AI Agent is designed to address one of the most difficult aspects of Cyber Risk Quantification: estimating impact and likelihood accurately and consistently.

Traditional quantification programs often rely heavily on expert judgment.

While expert judgment remains important, it can also introduce challenges related to consistency, scalability, documentation, and explainability.

Commugen's CRQ AI Agent was developed to augment this process.

The AI Agent analyzes organizational risk information while simultaneously leveraging external intelligence sources to strengthen quantification assessments.

These inputs may include:

Historical cyber incidents
Industry-specific attack trends
Geographic threat patterns
Public breach information
Known attack frequencies
Threat intelligence
Industry benchmarks
Regulatory environments
Historical loss data
Typical financial impacts of similar cyber events

By combining these sources, the AI Agent helps generate realistic recommendations for:

Single Loss Expectancy (SLE)
Annualized Rate of Occurrence (ARO)
Risk exposure ranges
Risk assumptions
Quantification rationale

The objective is to help security teams produce more consistent and defensible Cyber Risk Quantification assessments.

Explainable Cyber Risk Quantification

One of the defining characteristics of the CRQ AI Agent is explainability.

According to Commugen, organizations increasingly require transparency when using AI within risk management processes.

For this reason, the CRQ AI Agent does not simply generate numerical outputs.

Instead, it provides supporting context and reasoning behind each recommendation.

For every quantified risk, users can review:

Recommended SLE ranges
Recommended ARO ranges
Supporting assumptions
Historical references
Industry benchmarks
External intelligence sources
Contributing factors
Quantification rationale

This information helps security leaders understand how calculations were derived and provides additional confidence when presenting quantified risks to stakeholders.

The capability is intended to support executive reporting, board communication, audit preparation, regulatory discussions, and risk review activities.

By providing both numerical outputs and explanatory narratives, the AI Agent helps transform Cyber Risk Quantification from a calculation exercise into a business communication tool.

Supporting Better Board Communication

Board reporting continues to be a significant challenge for many cybersecurity leaders.

While technical metrics remain important for security operations, executive stakeholders often require a different perspective.

Cyber Risk Quantification provides a mechanism for communicating cyber exposure using business language and financial impact.

Rather than discussing vulnerabilities, attack techniques, or risk heatmaps alone, organizations can discuss:

Financial exposure
Potential loss scenarios
Risk reduction value
Investment effectiveness
Security ROI
Business impact

This can help create more productive conversations between cybersecurity leaders, executive teams, and boards.

The addition of explainable AI further strengthens this process by providing contextual reasoning that stakeholders can review and understand.

The Future of Cyber Risk Quantification

Commugen believes Cyber Risk Quantification will continue to become a foundational component of modern cyber risk management programs.

As organizations seek more objective ways to evaluate cyber exposure, justify investments, and align cybersecurity with business objectives, demand for quantification capabilities is expected to increase.

The company also expects artificial intelligence to play an increasingly important role in helping organizations scale Cyber Risk Quantification programs.

By combining organizational data, external intelligence, financial modeling, simulation technologies, and explainable AI, organizations can move toward a more mature and data-driven approach to cyber risk management.

The launch of the CRQ AI Agent represents Commugen's latest step in that direction.

New Cyber Risk Quantification Guide Released

Alongside the announcement, Commugen has released a new educational resource titled "The CISO's Guide to Cyber Risk Quantification: How to Translate Cyber Risk into Financial Impact and Make Better Security Decisions."

The guide provides practical guidance on:

Cyber Risk Quantification methodologies
Annualized Loss Expectancy (ALE)
Single Loss Expectancy (SLE)
Annualized Rate of Occurrence (ARO)
Financial risk modeling
Risk prioritization
Security ROI
Board communication
Cyber Risk Quantification programs
AI-assisted Cyber Risk Quantification

The resource is intended for CISOs, cyber risk leaders, GRC managers, security executives, and organizations seeking to improve their cyber risk management capabilities.

About Commugen

Commugen is a Cyber GRC platform that helps organizations manage cyber risk, compliance, vendor risk, mitigation activities, and security operations through automation, advanced analytics, and AI-powered workflows.

The platform supports Cyber Risk Quantification, Vendor Risk Management, Policy Management, Risk Management, Compliance Management, Mitigation Planning, Evidence Analysis, and Cyber GRC automation.

Commugen's AI-powered capabilities are designed to help organizations reduce manual effort, improve consistency, accelerate execution, and make more informed cyber risk decisions.

For more information about Commugen's Cyber Risk Quantifier and CRQ AI Agent, visit http://www.cyber.commugen.com.

Adam Babayoff
Commugen
+44 20 4591 9206
email us here
Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/921527508

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.