

TOP 10 CYBER RISK MYTHS debunked

MYTH #1:

Cybersecurity risk cannot
be financially quantified.

*swipe for the
debunk*



TOP 10 CYBER RISK MYTHS

MYTH #1: **debunked**

PAST: Cyber Risk Quantification (CRQ) was applied to derive a basic notion of the likelihood of cyber loss.

TODAY: Advances in the cyber insurance industry have enabled a full actuarial analysis of risk—actuarial CRQ (ACRQ) relevant to enterprises.

Thrivaca™ captures relevant data using a multi-source automated process that assembles regulator-approved and audit-friendly composite financial analysis in rapid order.

Follow us for the Top 10



Eradicate risk | get real resilience | #ACRQ

TOP 10 CYBER RISK MYTHS debunked

MYTH #2:

“Likelihood” is as useful as probability when it comes to cybersecurity risk.

*swipe for the
debunk*



TOP 10 CYBER RISK MYTHS

MYTH #2: debunked

Obsolete static models can't solve modern real-time challenges.

Predictive results with an actuarial risk profile — that's how to manage today's cybersecurity risks, optimization, and compliance across NIST 800-53, CSF 800-171, ISO 27001, and MITRE Att&ck.

Follow us for the Top 10



Eradicate risk | get real resilience | #ACRQ

TOP 10 CYBER RISK MYTHS debunked

MYTH #3:

Cybersecurity risk
assessment is just another
compliance requirement.

*swipe for the
debunk*



TOP 10 CYBER RISK MYTHS

MYTH #3: **debunked**

Risk assessment is a critical component of an organization's overall risk management strategy; rather than merely a compliance checkbox.

It plays an essential role in safeguarding an organization's assets, reputation, and long-term success —when utilizing full, commercial-grade actuarial science, not an obsolete static VaR model.

Follow us for the Top 10



Eradicate risk | get real resilience | #ACRQ

TOP 10 CYBER RISK MYTHS debunked

MYTH #4:

No one really knows what any organization's cyber risk is, and people should not make the effort.

*swipe for the
debunk*



TOP 10 CYBER RISK MYTHS

MYTH #4: **debunked**

Actuarial risk quantifications are about preventing incidents and building resilience. Understanding potential risks allows an organization to develop robust response and recovery plans, ensuring business continuity in the face of cyber threats.

Understanding and managing cyber risks can translate into tangible business benefits, such as increased trust and competitive advantages.

Follow us for the Top 10



Eradicate risk | get real resilience | #ACRQ

TOP 10 CYBER RISK MYTHS debunked

MYTH #5:

The “FAIR Model” based on Value-at-Risk from the 90s is perfectly sufficient for determining cyber risk exposure in today’s environment.

*swipe for the
debunk*



TOP 10 CYBER RISK MYTHS

MYTH #5: **debunked**

Cyber risk management today is increasingly integrated with enterprise risk management (ERM) frameworks.

This requires modern actuarial quantification that align cyber risk with other risk domains, considering overall business risk and strategic objectives.

Cyber threats are more sophisticated and varied, making it impossible for a static, opinion-based VaR model from the 90s to keep pace.

Follow us for the Top 10



Eradicate risk | get real resilience | #ACRQ

TOP 10 CYBER RISK MYTHS debunked

MYTH #6:

Most organizations have a realistic notion of how much cyber insurance they really need.

*swipe for the
debunk*



TOP 10 CYBER RISK MYTHS

MYTH #6: **debunked**

Determining the right amount of cyber insurance involves understanding your specific risks, evaluating potential financial impacts, consulting with experts, and regularly reviewing your coverage.

Without an actuarial-based risk profile, it would be difficult to ensure that your organization is adequately protected against the financial consequences of cyber incidents.

Follow us for the Top 10



Eradicate risk | get real resilience | #ACRQ

TOP 10 CYBER RISK MYTHS debunked

MYTH #7:

The practice of Cybersecurity is all about just getting enough specific solutions and addressing as many vulnerabilities as possible to neutralize exposure to threats.

*swipe for the
debunk*



TOP 10 CYBER RISK MYTHS

MYTH #7: **debunked**

Cybersecurity must be an organizational-wide concern, encompassing technical, human, strategic, and procedural elements. Addressing it solely as a technical vulnerability problem leads to an incomplete and potentially ineffective security posture.

With a holistic approach, organizations can better protect themselves against the full spectrum of cyber threats and ensure resilience in the face of evolving risks.

Follow us for the Top 10



Eradicate risk | get real resilience | #ACRQ

TOP 10 CYBER RISK MYTHS debunked

MYTH #8:

Unlike Engineering, Medicine, or Accounting, the Cybersecurity profession does not benefit from a consistent set of standards and practices.

*swipe for the
debunk*



TOP 10 CYBER RISK MYTHS

MYTH #8: **debunked**

Cybersecurity does benefit from structured frameworks for ensuring consistency, quality, and reliability in cybersecurity efforts, such as the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and CIS Controls, to name a few.

THE CHALLENGE?

Enforcing adoption and adherence to these frameworks to ensure trust in cybersecurity efforts, much like the standards in engineering, medicine, aviation...

Follow us for the Top 10



Eradicate risk | get real resilience | #ACRQ

TOP 10 CYBER RISK MYTHS debunked

MYTH #9:

Cybersecurity risk is simply too complex to be adequately understood using any type of quantitative methods.

*swipe for the
debunk*



TOP 10 CYBER RISK MYTHS

MYTH #9: **debunked**

72% of 3,260 enterprises surveyed by EY report being unable to determine their own cyber risks. Experience and litigation have shown that a NIST-driven quantitative analysis is a cybersecurity program's most compliant and defensible basis.

NIST-approved Thrivaca™ provides a baseline Risk Profile within one day in an intuitive, graphical UI. 12+ use cases are pre-supplied, and users require less than one hour of training.

Follow us for the Top 10



Eradicate risk | get real resilience | #ACRQ

TOP 10 CYBER RISK MYTHS debunked

MYTH #10:

All the talk about aligning cybersecurity and overall business strategy is just theoretical.

Cybersecurity should be left to the technology professionals and can't be understood by boards or senior leadership.

*swipe for the
debunk*



TOP 10 CYBER RISK MYTHS

MYTH #10: **debunked**

By demonstrating how cybersecurity supports business objectives, protects assets, and mitigates risks, boards and senior leadership can better understand its value and prioritize necessary investments and initiatives.

This holistic strategic planning + quantified risk management approach equips CISOs to safeguard the organization's reputation, financial health, and operational continuity.



Eradicate risk | get real resilience | #ACRQ

TOP 10 CYBER RISK MYTHS

Do you know your cyber risk
profile score?

learn
more:

arxnimbus.com

info@arxnimbus.com

Toll-free: 1.888.422.6584



Eradicate risk | get real resilience | #ACRQ