

Gov-Sponsored Study: Cost of Cyber Attacks Climbs 15X Higher

Analysis of 15 years of historical data reveals that cybersecurity incidents are more common and costly than ever

VA, UNITED STATES, June 11, 2025

/EINPresswire.com/ -- The Cyentia Institute today unveiled the 2025 edition of its Information Risk Insights Study (IRIS), a definitive [research](#) publication essential for business leaders, risk managers, policymakers, and cybersecurity professionals. Sponsored by the Cybersecurity and Infrastructure Security Agency (CISA), [IRIS 2025](#) delivers comprehensive, actionable data and analysis, enabling organizations to better understand and mitigate cyber risks.

IRIS 2025 examines over 15 years of historical cybersecurity incidents and financial losses (2008-2024), identifying clear, evolving patterns that directly impact how businesses approach risk management. This data-driven study addresses critical questions:

Have cybersecurity incidents become more frequent and costly?

Are certain industries disproportionately impacted?

What emerging tactics and threats pose the greatest risk today?

How can organizations strategically allocate resources for maximum risk reduction?

Key findings from IRIS 2025 provide compelling reasons to explore this extensive report:



The Information Risk Insight Study 2025

Reported cybersecurity incidents have surged dramatically, increasing by 650% since 2008.

The financial stakes have never been higher, with median losses per incident escalating from \$190,000 in 2008 to nearly \$3 million today.

Incidents resulting in severe financial "tail losses" have seen costs multiply by five, highlighting vulnerabilities that organizations can no longer ignore.

Industry-specific trends offer targeted insights for sectors such as Professional Services, which have seen a substantial 25-fold increase in incident-related losses, and Retail, where proactive measures have significantly reduced financial impacts.

IRIS 2025 underscores the necessity of adapting cybersecurity strategies to evolving threats, particularly the rise in compromised user credentials, exploitation of public-facing applications, and targeted attacks through third-party vendors.

The report offers executives and security teams critical guidance for decision-making, risk assessment, and strategic cybersecurity investment.

By examining detailed, real-world data, readers can make informed, strategic decisions to significantly reduce their organization's cyber risk exposure.

Access the full IRIS 2025 report at www.cyentia.com/iris2025 to gain a clear understanding of contemporary cyber threats and proven strategies for effective risk mitigation.

About the Cyentia Institute

The Cyentia Institute is a renowned research firm committed to providing high-quality, data-driven insights to help organizations enhance cybersecurity and effectively manage information

Introduction

"Time isn't a straight line... It's all bumpy wumpy."
-The Eleventh Doctor

Welcome to the 2025 edition of the (roughly) biennial Information Risk Insights Study (IRIS). The last one was in 2022, so it's about time we got this to you. Thanks for your patience.

Fittingly, time is of the essence in this IRIS. Not just because it's a tad overdue, but because it's literally about time—cyber risk trends over time, to be specific.

Cybersecurity is ever-changing, and there's an implicit assumption that risk is always increasing. But is it?

Are cyber events occurring at greater frequency? Is an organization more likely to have a breach now than 15 years ago? Which types of incidents have become more common over time? Have the financial impacts of cyber events increased or decreased? Are risk factors trending the same way for all sectors and sizes of organizations?

We explore these questions and more by analyzing a huge historical dataset of cyber events and losses from 2008 through 2024. As always, our goal is to dispel the fog of FUD surrounding cyber risk so you can see it more clearly and manage it more effectively. Thanks for reading!

Acknowledgements

The Cyentia Institute wishes to acknowledge and thank the Cybersecurity Division and the Office of the Chief Economist at the Cybersecurity and Infrastructure Security Agency (CISA) for sponsoring this study. It is our sincere hope that this research will aid community efforts to manage cyber risk.

THE CYENTIA INSTITUTE | CYENTIA.COM

TABLE OF CONTENTS

| | | |
|----|---|----|
| Q1 | ARE SECURITY INCIDENTS BECOMING MORE COMMON? | 4 |
| Q2 | DO INCIDENT TRENDS DIFFER ACROSS ORGANIZATIONS? | 7 |
| Q3 | IS THE PROBABILITY OF INCIDENTS INCREASING? | 12 |
| Q4 | HAVE SECURITY INCIDENTS GOTTEN MORE COSTLY? | 16 |
| Q5 | DO TRENDS DIFFER AMONG EVENT TYPES? | 20 |
| Q6 | ARE INTRUSION METHODS CHANGING OVER TIME? | 23 |
| Q7 | WHAT ARE WE MISSING FROM CURRENT EVENTS? | 27 |
| A | METHODOLOGY & INCIDENT PATTERNS | 32 |

The Cyentia Institute is a research firm working to improve cyber risk management through our analytical services and data-driven research publications. You can download the IRIS 2025 and find related content at www.cyentia.com/iris.

IRIS 2025 Contents

IRIS 2025

KEY FINDINGS

- On average, 3,000 significant security incidents are publicly reported or discovered each quarter. That's a 650% increase over the last 15 years.
- Cyber events affecting smaller businesses are far more common overall, but relative to population size, the rate among the largest corporations is 620 times higher.
- The annual probability of any given organization experiencing a cyber event has almost quadrupled since 2008.
- The probability of a <\$1B firm suffering an incident has more than doubled, while the annual likelihood for a \$100B+ organization has fallen 50%.
- Losses from a typical security incident have absolutely exploded, rising 15-fold from a median of \$190K to almost \$3 million!
- The cost of more extreme "tail loss" events is also up 5-fold, ballooning to \$32 million.
- Cyber events aren't just costing more—they're hurting the bottom line more than ever before. We've seen an 8-fold increase in costs as a proportion of annual revenue.
- Median losses for professional services firms are up 25x over the last 15 years! Alternatively, there's been a huge decrease in loss magnitude among retailers.
- Compromising user credentials remains the most common intrusion technique over the last decade, fluctuating between 43% and 60% of all incidents.
- Exploitation of web applications is up 6x for smaller firms, while targeting third-party relationships has doubled among large organizations.

Like what you see? **Join the vision!**

We intend to continue the IRIS in the future to discover even more insights for managing information risk. If you'd like to join in that effort by contributing relevant data or sponsoring research, please reach out to us via the contact form at www.cyentia.com/iris.

THE CYENTIA INSTITUTE | CYENTIA.COM

IRIS 2025 Key Findings

risks. Through collaborations with leading industry and government entities, Cyentia continually advances cybersecurity knowledge and practice.

Wade Baker

Cyentia Institute

+1 541-852-5555

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/820792719>

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.

© 1995-2025 Newsmatics Inc. All Right Reserved.