FORTIUM

CYBER RESILIENCE IN 2025:
INVESTING NOW OR PAYING LATER

WHITE PAPER



CONTENTS

1. INTRODUCTION **3**

2. THE GROWING CYBER THREAT LANDSCAPE **5**

3. THE FINANCIAL CASE FOR CYBERSECURITY INVESTMENT **7**

4. KEY BUDGETING PRIORITIES FOR 2025 **9**

5. THE COST OF INACTION **11**

6. CONCLUSION: WHY NOW IS THE TIME TO INVEST **13**

1 INTRODUCTION

INTRODUCTION



> **We've seen a significant rise in client discussions about expanding security beyond traditionally high-value asset areas, such as post-production, to encompass the entire organization.**
>
> **Security managers recognize the importance of frictionless technology that secures data for the life of the file, rather than just in transit, without disrupting daily workflows. In today's fast-moving security landscape, the best security is both agile and non-intrusive—it protects without hindering business operations.**
>
> — Iain Benson, Director at Fortium

As cyber threats escalate in scale and sophistication, the media and entertainment industry finds itself at a critical juncture. With increased reliance on digital infrastructure, cloud services, and AI-driven workflows, the attack surface has never been broader. Yet, many organizations still view cybersecurity as a cost center rather than an essential investment. The question is no longer whether you can afford to enhance security but whether you can afford not to.

This white paper explores the urgent need for increased cybersecurity investment in 2025, backed by industry data, emerging threat trends, and the financial consequences of inaction. It aims to equip Chief Information Security Officers (CISOs) with the insights they need to advocate for stronger security budgets and resilient cyber strategies.

2 THE GROWING CYBER THREAT LANDSCAPE

THE GROWING CYBER THREAT LANDSCAPE

According to Forrester's Global Tech Market Forecast, 2024 To 2029 (Forrester, 2024), software and IT services will account for 66% of global technology spending in 2025, driven largely by investments in cybersecurity and modernization of legacy systems. Gartner forecasts that global information security spending will grow by 15% in 2025 (Gartner, 2024), reflecting a heightened threat environment, cloud expansion, and a critical shortage of security talent.

In the media and entertainment sector, the risks are particularly high due to:

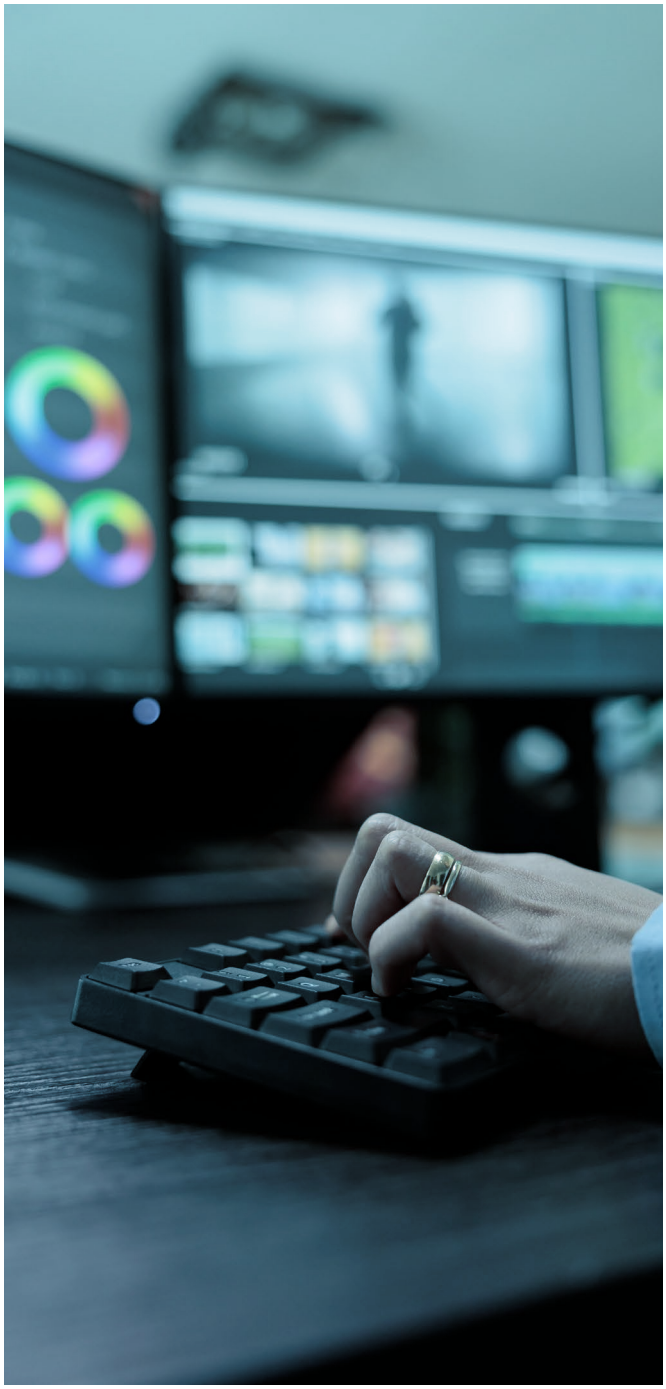
High-value digital assets: Exclusive content, intellectual property, and consumer data are prime targets for cybercriminals.

Ransomware threats: Cybercriminals increasingly target streaming platforms, production houses, and broadcasters to disrupt services and extort payments (National CIO Review, 2024).

Third-party vulnerabilities: Collaborations with post-production teams, marketing agencies, and distribution networks create complex supply chain risks.

Deepfake and AI-generated fraud: The rise of AI has introduced new security concerns, from synthetic identity fraud to reputation attacks.

Regulatory Compliance: Evolving privacy laws and data protection regulations require companies to maintain rigorous security controls or face hefty fines (Gartner, 2023).



3 THE FINANCIAL CASE FOR CYBERSECURITY INVESTMENT



THE FINANCIAL CASE FOR CYBERSECURITY INVESTMENT

The Cost of a Data Breach Report 2024 (IBM & Ponemon Institute, 2024) underscores the financial impact of cyber incidents:

The average cost of a data breach surged by 10% year-over-year to **$4.88 million**, the highest increase since the pandemic.

Ransomware victims who engaged law enforcement reduced their breach costs by **nearly $1 million**.

Organizations leveraging security AI and automation saved an average of **$2.2 million per breach** and reduced breach lifecycles by nearly **100 days.**

Companies with robust incident response plans saw **35% lower breach costs** compared to those without them.

Despite rising budgets, 28% of CISOs report dissatisfaction with their allocations, emphasizing the need for security leaders to communicate the strategic value of cybersecurity investments to executive leadership (National CIO Review, 2024).

4 KEY BUDGETING PRIORITIES FOR 2025

As CISOs prepare their budgets, they should focus on prioritizing security measures that align with Fortium Technologies' offerings and expertise:

1. COMPANY-WIDE ENCRYPTION & ALWAYS-ON SECURITY:

Organizations should implement encryption across all files—not just selected ones—to maintain a default 'always-on' security stance. This reduces reliance on trusted users and minimizes insider threat risks while ensuring continuous protection against unauthorized access and data breaches.

2. ZERO TRUST ARCHITECTURE (ZTA):

Strengthening identity and access management to counter credential-based attacks. With phishing and credential theft leading attack vectors, implementing a Zero Trust model ensures continuous verification of users and devices.

3. INCIDENT RESPONSE & BUSINESS CONTINUITY PLANNING:

Proactive breach response training can significantly cut costs associated with downtime and regulatory fines. Additionally, maintaining detailed audit records and access logs is critical for forensic investigations and regulatory compliance. These records provide visibility into security events, help detect anomalies, and ensure accountability, reducing risks associated with unauthorized access. Regular penetration testing and tabletop exercises help organizations refine their response strategies.

4. CLOUD SECURITY & DATA PROTECTION:

With 40% of breaches involving multi-cloud environments, securing cloud-based assets is crucial. Cloud misconfigurations remain a top concern, making continuous monitoring and governance essential (Computer Weekly, 2024).

5. THIRD-PARTY RISK MANAGEMENT:

Strengthening vendor security assessments to minimize supply chain vulnerabilities. Companies must enforce stringent security policies for external partners and service providers.

6. CYBER AWARENESS & EMPLOYEE TRAINING:

Employees are often the weakest link in security. Investing in comprehensive security awareness programs can prevent social engineering attacks and improve overall security posture.

7. THREAT INTELLIGENCE & CONTINUOUS MONITORING:

Real-time threat intelligence feeds and advanced monitoring systems can detect threats before they escalate. CISOs should leverage frameworks like MITRE ATT&CK to proactively anticipate attacker tactics.

8. SECURITY FOR AI & EMERGING TECHNOLOGIES:

As organizations integrate generative AI and machine learning models, new security risks emerge. Ensuring AI-driven applications are protected against adversarial attacks and data poisoning is crucial.

9. AI-DRIVEN SECURITY AUTOMATION:

AI and machine learning reduce detection and response times, mitigating potential damages. AI-powered tools are proving invaluable in threat hunting, behavioral analysis, and automated incident response (IBM, 2024). Organizations should implement encryption across all files—not just selected ones—to maintain a default 'always-on' security stance. This reduces reliance on trusted users and minimizes insider threat risks while ensuring continuous protection against unauthorized access and data breaches.

5 THE COST OF INACTION



THE COST OF INACTION

Cybersecurity is no longer just an IT issue—it is a business imperative. With breach costs skyrocketing and cyber threats growing more sophisticated, failing to invest in security could mean losing customer trust, operational downtime, and severe financial penalties.

Beyond direct financial losses, the reputational damage caused by a breach can be irreparable. Consumers and partners expect companies to take data protection seriously, and a single high-profile incident can lead to customer churn, stock price drops, and lost revenue opportunities.

Additionally, regulatory scrutiny is intensifying. Non-compliance with GDPR, CCPA, and other global data protection regulations can result in severe fines and legal repercussions. The enforcement of stricter security measures is inevitable, making proactive investment the only viable strategy.

6 CONCLUSION: WHY NOW IS THE TIME TO INVEST



CONCLUSION: WHY NOW IS THE TIME TO INVEST

For media and entertainment organizations, cyber resilience is not a choice; it is a necessity. Investing in security now will not only mitigate risks but also create a foundation for sustainable growth in the digital age.

CISOs must champion a security-first approach, aligning cybersecurity spending with business objectives. By prioritizing investments in AI-driven security automation, cloud security, and incident response, organizations can significantly reduce breach costs and minimize operational disruptions.

THE TIME TO ACT IS NOW - BECAUSE THE COST OF INACTION IS FAR GREATER

FORTIUM

For more information contact:
info@fortiumtech.com
support@fortiumtech.com

UK: +44 (0) 330 053 9690
US: +1 (310) 987-4683

fortium.com