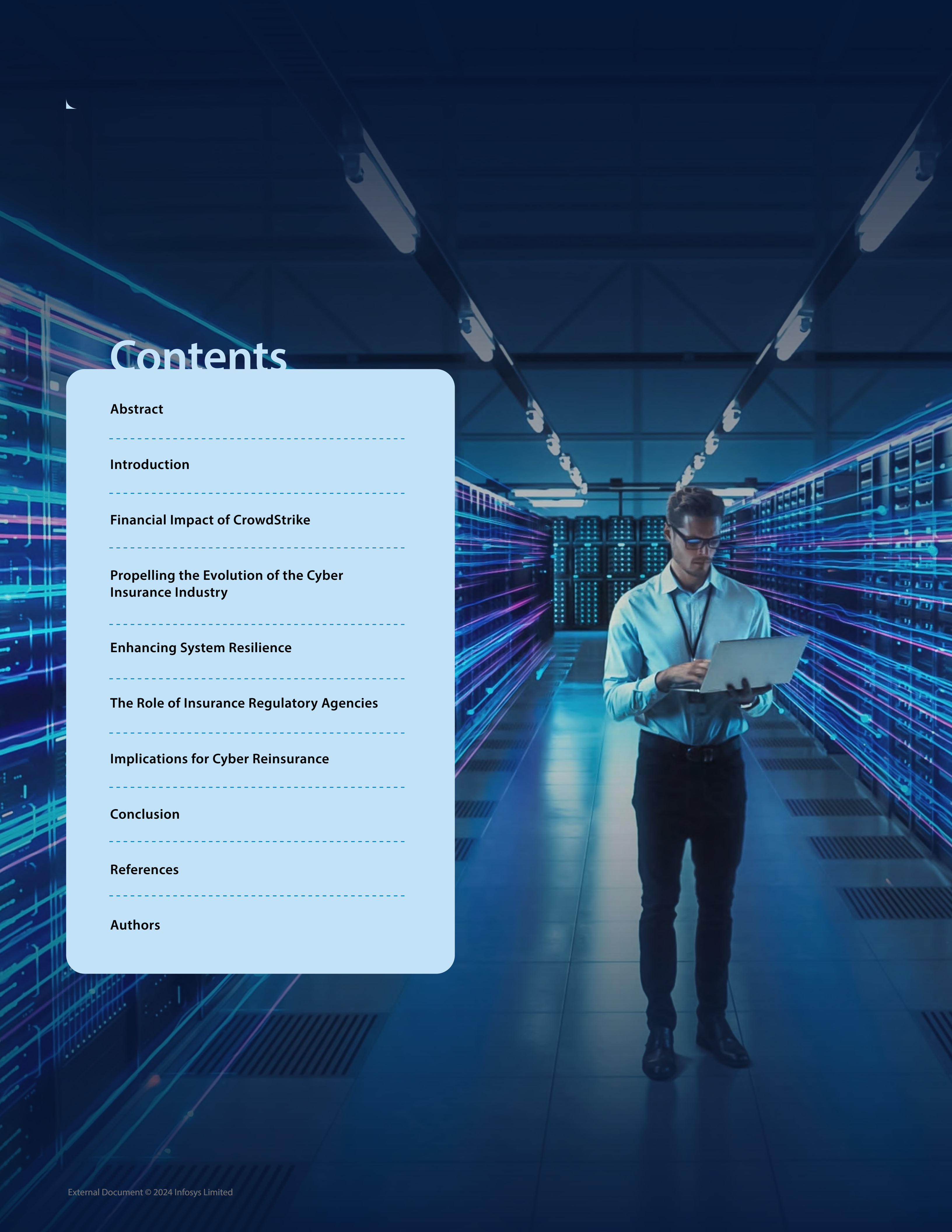
SEIZING OPPORTUNITIES IN ADVERSITY: CYBER INSURANCE AFTER THE CROWDSTRIKE OUTAGE

Navigate your next

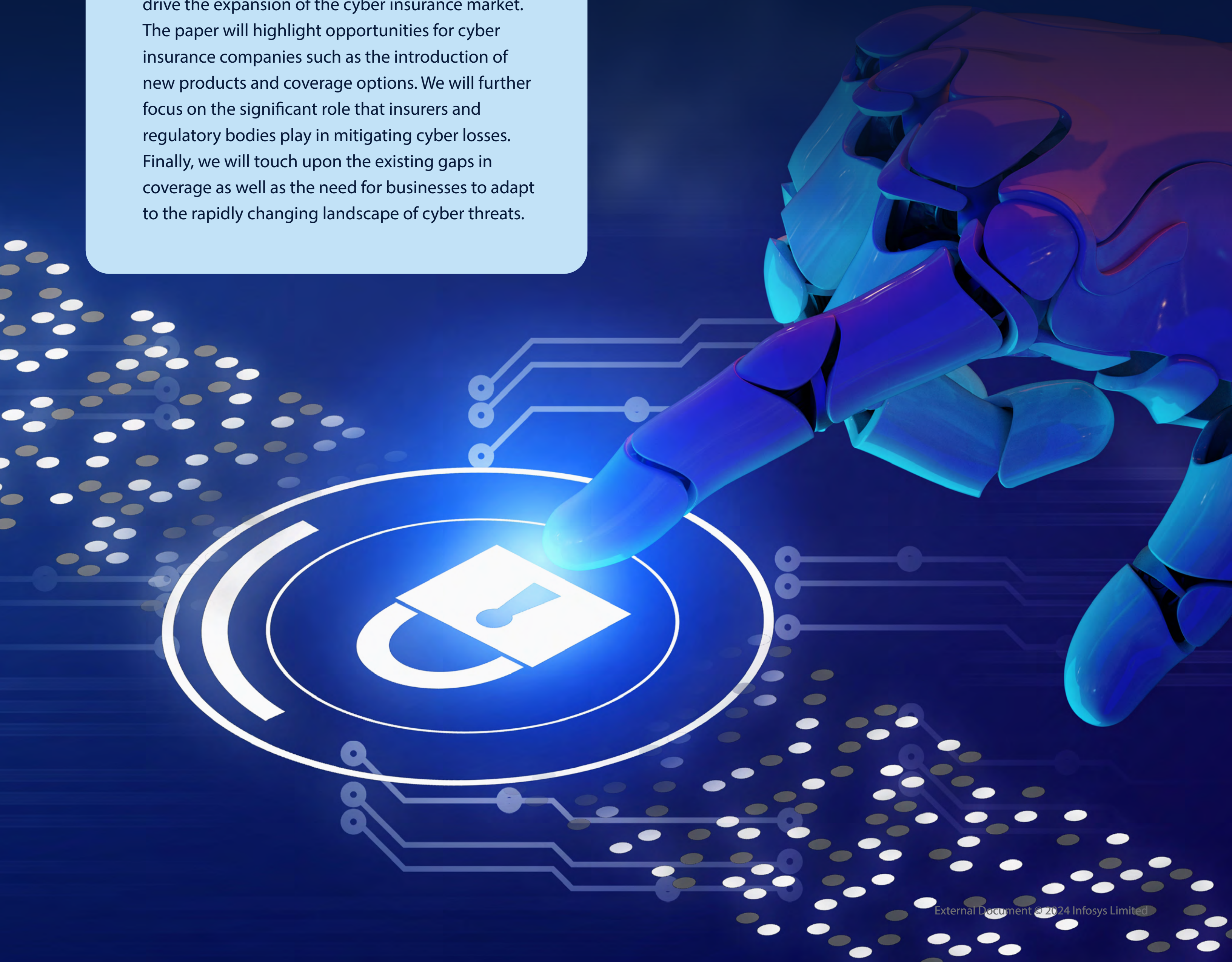


Contents

Abstract

The faulty Falcon update from CrowdStrike for Microsoft Windows caused a widespread system outage with a blue screen of death sweeping across industries leading to huge financial losses. The incident highlighted the gaps in cyber insurance coverage[1,2] and the acute need for better system resilience. This event will inevitably trigger an increase in premiums. It will also lead to the introduction of new regulations, drive innovations in cyber insurance product offerings, and help tighten underwriting risk assessments.

In this white paper, we will discuss how potential losses arising from the CrowdStrike incident will drive the expansion of the cyber insurance market. The paper will highlight opportunities for cyber insurance companies such as the introduction of new products and coverage options. We will further focus on the significant role that insurers and regulatory bodies play in mitigating cyber losses. Finally, we will touch upon the existing gaps in coverage as well as the need for businesses to adapt to the rapidly changing landscape of cyber threats.



Introduction

The rapidly evolving IT landscape is hyper-connecting the world of business across sectors. Digital transformation, while revolutionizing business, has introduced new challenges – particularly in cybersecurity. Recently, a faulty software update from CrowdStrike led to system outages, impacting essential industry sectors globally. This was not a malicious cyber-attack but the result of inadequate processes and controls as well as human error. Insurance carriers are yet to fully assess the CrowdStrike impact on their books. However, it is obvious that the implications will be far-reaching, affecting many areas including policy coverage, wording, and regulations – all leading to a new evolutionary phase for the cyber insurance market growth.

The impact of the CrowdStrike incident for the cyber insurance industry is analogous to the impact of COVID-19 on digital transformation. It will accelerate the development of innovative insurance products to address evolving needs of clients. New products will have broader cyber insurance coverage spanning malicious attacks, such as ransomware, malware, phishing, and non-malicious incidents such as human errors and system failures. Insurers will adopt stricter underwriting risk assessments to evaluate potential business interruptions caused by security vulnerabilities in the supply chains of their clients.

Financial Impact of CrowdStrike

The CrowdStrike outage impacted approximately 8.5 million Microsoft Windows devices across the world. Over 3000 flights were canceled and 23,900 were delayed. The healthcare sector experienced disruption in essential services such as surgery, access to patient records, appointment schedules, and emergency call centers. Stock exchanges delayed trading while banking digital services were severely affected[4].

According to estimates, the outage resulted in US $5.4 billion in direct losses for Fortune 500 companies, excluding the impact on Microsoft. These losses stem from operational disruptions, lost revenue, and costs associated with system recovery and mitigation efforts. About 10% to 20% of these losses are likely to be covered by insurance[3].

Usually, direct losses are underreported, and it is very complex to assess indirect losses. Some organizations do not report cyberattacks due to fear of reputational damage or the notion that the costs of reporting outweigh the benefits from insurance payouts. Two large components of the cost of cyberattacks are indirect losses such as business disruption and reputational damage. Such losses are hard to quantify. Quantifying the global financial impact of cyberattacks over the past five years is highly challenging. However, available data suggests that ransomware alone could cause damages of approximately US $265 billion by 2023[5]. The large financial impact highlights the urgency with which businesses must invest in comprehensive cybersecurity as well as cyber insurance measures to protect against the growing threat of cyberattacks.

Propelling the Evolution of the Cyber Insurance Industry

The CrowdStrike event has catalyzed the evolution of the cyber insurance industry, driving innovation in products to better meet the complex needs of modern businesses.

Current status of cybersecurity coverage

Cybersecurity coverage typically falls into two main categories – first-party coverage and third-party coverage. First-party coverage includes support services for system restoration, legal compliance, and business interruption compensation, as well as coverage for cyber extortion and cybercrime-related losses. Third-party cyber liability coverage, on the other hand, protects businesses from claims made by third parties due to a cyberattack, covering legal costs, media liability, and technology errors and omissions.

New opportunities with the surge in demand

After the CrowdStrike outage, businesses realized that comprehensive cyber insurance coverage is no longer a choice but a necessity. The protection gap is now obvious and visible. Uninsured and/or underinsured organizations are in a hurry to prioritize coverage to protect against such incidents. This will create a surge in demand fueling unprecedented cyber insurance growth. Insurers need to tap into these opportunities with improved and innovative offerings.

Comprehensive coverage with enhanced product offerings

Despite the growing importance of cyber insurance, significant coverage gaps persist, leaving businesses vulnerable to substantial financial losses. These gaps arise from insufficient coverage limits, underinsured businesses, and policy exclusions for events such as nuclear incidents, terrorism, and specific cyberattacks. The CrowdStrike incident has exposed inherent vulnerabilities and underscored the need for comprehensive coverage that extends beyond traditional cyber threats. Previously, cyber insurance policies focused on covering losses resulting from malicious attacks such as ransomware, malware, and phishing. However, the CrowdStrike event highlights the need for broader coverage that also addresses non-malicious incidents such as human error and software flaws.

Innovative products covering the entire supply chain

There is a growing need to cover business interruptions caused by the failure of third-party vendors on which businesses rely. Insurers are likely to develop policies that offer broader protection for business interruptions caused by security vulnerabilities in the insured companies' supply chains.

Stricter underwriting risk assessment

The growth opportunity also presents new challenges for insurers. To build a profitable book of business, they must avoid adverse selection. This will lead to the adoption of stricter underwriting standards. To better assess the risks, carriers will leverage close cooperation with cybersecurity organizations. Broader assessment of risks using emerging technologies and AI/ML-based modeling will help create a better risk assessment framework. This will ensure accurate ratings based on the actual risk exposure.

Risk monitoring and management

Risk monitoring is another key opportunity for insurers. This includes providing risk management advice and consulting to help businesses better manage their cyber risks.

Increased premium rate

The increasing frequency and severity of cyberattacks have driven up premiums. Major factors affecting cyber insurance premiums include the current cyber security posture, coverage limits, deductibles, nature of business and its size, and claims history. The premium also depends on the type of coverage chosen – comprehensive or specialized policies. Increased premium rates will help insurers achieve a better bottom line while increasing the cost for insured businesses. Businesses should carry out due diligence to balance cost and coverage before arriving at a decision about their insurance.

Cyber insurance pool for uninsured and underinsured

The demand for cyber insurance coverage is rising rapidly. However, carrier reach and coverages are limited. Currently around 25 insurance carriers offer coverage. Looking at this protection gap, the concept of insurance pools, where multiple entities contribute to a common fund, may offer a promising solution. Such pools can provide affordable options for small and medium-sized businesses to obtain adequate coverage. To be successful, cyber insurance pools must have effective governance and regulatory compliance in place. Regulators need to step in and address challenges such as accurate risk assessment.

Enhancing System Resilience

The CrowdStrike event has highlighted the importance of system resiliency for organizations. Businesses should be in a permanent state of readiness to mitigate cyber incidents (malicious or non-malicious) and undertake comprehensive resiliency measures. These include vulnerability management, technology debt remediation, site reliability engineering (SRE), and strong disaster recovery (DR) practices.

Insurers have the opportunity to offer system resilience or risk advisory service to their clients, especially in the SME sector. This calls for close cooperation among insurers, regulators, customers, industry forums, and cyber security firms. Insurers can leverage their partnership with industry forums, cybersecurity firms, and regulators for access to the latest threat intelligence and thereby enhance their ability to improve incident response.

Vulnerability management

Organizations need to monitor and sharpen their defense mechanisms as the threat landscape is constantly shifting. Cybersecurity carriers have an opportunity to provide comprehensive consultancy and help improve the cybersecurity posture of the insured who have been assessed as subpar. Close cooperation between the insurers, cybersecurity firms, and the insured will mitigate risks to a large extent. The key actions recommended for risk mitigation are mentioned below:

Zero trust security architecture

Zero trust architecture has gained traction after recent security breaches. The basic principle is never to trust but to always verify and grant minimal privilege and access to perform an authorized function for a stipulated period. No resources such as users, devices, applications, or APIs are automatically trusted because they are in the network.

Security automation and orchestration

To reduce the mean time to detect (MTTD) and mean time to respond (MTTR), organizations must automate security threat identification and trigger responses through security orchestrations while keeping human guidance in the loop.

Cloud security enhancements

Security is a shared responsibility between the cloud service provider (CSP) and the organization. Most cloud service providers offer security for facilities, infrastructure, networks, and software running the cloud. However, organizations are responsible for cloud security. To fill this gap, organizations must have a well-defined policy addressing security KPIs and adopt cloud security enhancements, including identity and access management, encryption, and monitoring.

Enhanced threat intelligence integration

A well-orchestrated and coordinated security information and event management (SIEM) system can obtain inputs from multiple sources such as feeds from endpoint detection and response, penetration testing, threat intelligence, and log data. AI/ML-based analytical models process this data and produce high-fidelity alerts instead of thousands of siloed false alarms. This enables security analysts to channelize their bandwidth to protect the organization from real threats.

Endpoint detection and response

Antivirus-based protection using signature matching is not enough. Rapid detection of potential threats with endpoint detection and response (EDR) solutions to monitor real-time endpoint activities can provide better protection.

Multi-factor authentication

Multi-factor authentication (MFA) has become a de facto standard for accessing critical systems. This can save organizations even in situations where credentials are compromised.

In-sprint penetration testing

Many organizations do penetration testing once or twice a year. However, it is important to realize that every piece of new code introduces a possibility of vulnerability. So, in-sprint vulnerability tests and continuous monitoring are key to identifying and mitigating vulnerabilities before hackers can exploit them.

Phishing and security awareness training

Regular security awareness training within organizations is important to minimize the possibilities of phishing and social engineering attacks.

Incident response drills

Similar to regular fire drills and DR exercises, incident response drills are important to ensure preparedness during an attack.

Site reliability engineering

Site reliability engineering (SRE) focuses on enhancing the reliability and availability of systems. It automates actions across software, hardware, monitoring, and logging to keep the product up and running across the entire organization. Potential failures can be programmatically identified and solved ahead of a crisis. Logged events are analyzed to identify the root cause for failures and build resiliency and redundancy into the system. This reduces system outages and enables quick recovery from incidents.

Technology debt remediation

Over the years, all organizations accumulate technology debt such as outdated or unsupported software. Timely remediation is essential to secure such systems and build the capability to defy new cyber threats.

Strengthening disaster recovery practices

Despite taking all safety measures, unforeseen failures may still happen. This calls for a disaster recovery (DR) plan to ensure business continuity. A regular dry run of the DR plan is key for a successful recovery without jeopardizing business operations. Maintaining redundancy is critical to restore systems with minimum MTTR when an incident happens.

Infosys leverages its insurtech partners to help carriers and organizations improve their end-to-end cybersecurity posture. We also help create a resilient landscape that enhances proactive risk management. By elevating their security posture, organizations can protect their business operations and increase eligibility for preferential rating and policy coverage.

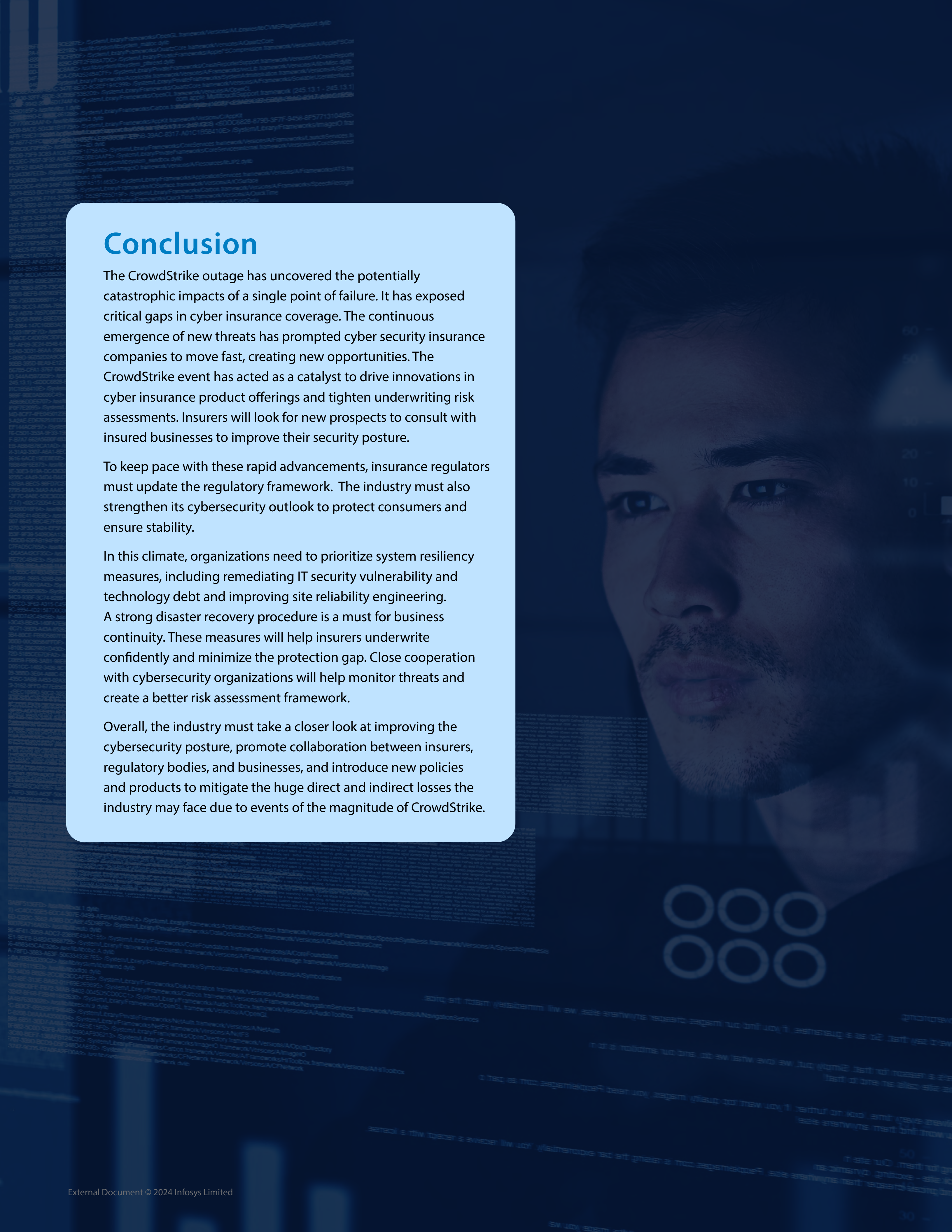
The Role of Insurance Regulatory Agencies

The CrowdStrike event is a wake-up call for regulators to keep pace with the evolving cyber threat landscape. Regulators must step up to strengthen the security posture of the entire cybersecurity industry. Increased collaboration among industry stakeholders and regulators is vital to protect consumers and ensure market stability. Given the new realization about the magnitude, severity, and frequency of cyber events such as CrowdStrike, regulatory authorities should focus on formulating new controls and regulations to address cyber risks. To improve the oversight of cyber insurance, regulatory bodies can introduce new controls and measures such as:

- Formulating a standardized cybersecurity framework
- Mandating regular risk assessments and reporting
- Enforcing stringent data protection regulations

Implications for Cyber Reinsurance

The recent surge in volume and spread of cyber losses has also impacted reinsurers. Due to the uneven cyber security posture of the insured, reinsurers encounter significant challenges in assessing cyber risks accurately. Reinsurers need to rely on the underwriting judgments of primary insurers. Some reinsurers have focused on developing accurate underwriting models to account for the evolving new threats. The volume and spread of threats across the world present a significant growth opportunity for reinsurers. However, they need to be prudent in evaluating the assumed risks. New offerings such as cyber catastrophes and excess liability will soon dominate the landscape. This will provide additional layers of protection for insurers and their clients.



Conclusion

The CrowdStrike outage has uncovered the potentially catastrophic impacts of a single point of failure. It has exposed critical gaps in cyber insurance coverage. The continuous emergence of new threats has prompted cyber security insurance companies to move fast, creating new opportunities. The CrowdStrike event has acted as a catalyst to drive innovations in cyber insurance product offerings and tighten underwriting risk assessments. Insurers will look for new prospects to consult with insured businesses to improve their security posture.

To keep pace with these rapid advancements, insurance regulators must update the regulatory framework. The industry must also strengthen its cybersecurity outlook to protect consumers and ensure stability.

In this climate, organizations need to prioritize system resiliency measures, including remediating IT security vulnerability and technology debt and improving site reliability engineering. A strong disaster recovery procedure is a must for business continuity. These measures will help insurers underwrite confidently and minimize the protection gap. Close cooperation with cybersecurity organizations will help monitor threats and create a better risk assessment framework.

Overall, the industry must take a closer look at improving the cybersecurity posture, promote collaboration between insurers, regulatory bodies, and businesses, and introduce new policies and products to mitigate the huge direct and indirect losses the industry may face due to events of the magnitude of CrowdStrike.

References

1. David Jones, Cybersecurity Dive, July 25, 2024 CrowdStrike disruption direct losses to reach $5.4B for Fortune 500, study finds | Cybersecurity Dive
2. Parametrix, CrowdStrike's Impact on the Fortune 500, July 2024 CrowdStrike's Impact on the Fortune 500 - Parametrix (parametrixinsurance.com)
3. Kenneth Araullo, CrowdStrike incident unlikely to materially impact re/insurers – Fitch Ratings, July 23, 2024 CrowdStrike incident unlikely to materially impact re/insurers – Fitch Ratings | Insurance Business America (insurancebusinessmag.com)
4. Parametrix, CrowdStrike's Impact on the Fortune 500, July 2024 CrowdStrike's Impact on the Fortune 500 - Parametrix (parametrixinsurance.com)
5. Steve Morgan, Editor-in-Chief, Cybercrime Magazine, July 7, 2023 Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 (cybersecurityventures.com)

Authors

Prashanth Dwarkanath

Prashanth Dwarkanath is an Industry Principal with the Insurance Domain Consulting Group at Infosys. He has over 21 years of experience in IT and business consulting engagements in the insurance industry. With his extensive expertise across the life and property and casualty lines of businesses, Prashanth has led multiple transformational programs across the insurance value chain.

Tapas Das

Tapas Das is an Industry Principal with the Insurance Domain Consulting Group at Infosys in North America. He has over 20 years of experience in the insurance industry, with specialization in the property and casualty and reinsurance domains. He has worked with top insurance and reinsurance companies across USA and Europe and led several digital transformation initiatives.

Srinita Pradhan

Srinita Pradhan is a Lead Consultant with the Insurance Domain Consulting Group at Infosys. She has over 18 years of experience in business analysis and consulting across US life insurance and global financial market clients. Her expertise lies in life insurance and annuities, managed investments, regulatory compliance, and banking domains.

Robin Lindstedt

Robin Lindstedt is a Senior Consultant with the Insurance Domain Consulting Group at Infosys. Robin has more than 20 years of experience in defining new digital processes and leading business system enhancements for financial services, life insurers, and retirement plans.

For more information, contact askus@infosys.com

Infosys®
Navigate your next