

Crash Course in Chaos

Special report: How tech teams responded in the wake of the global CrowdStrike outage

Crash Course in Chaos

Special report: How tech teams responded in the wake of the global CrowdStrike outage

Contents

Foreword	2
Introduction	3
<hr/>	
Chapter 1	
Industry-wide transformation	4
<hr/>	
Chapter 2	
Cultural challenges remain	8
<hr/>	
Chapter 3	
Shifting vendor relationships	11
<hr/>	
Chapter 4	
Calm after the chaos: building resilience and optimising investment	13
<hr/>	
Conclusion	14





Foreword

From Jon Mort, Chief Technology Officer, The Adaptavist Group

The CrowdStrike outage on July 19, 2024¹ had a seismic impact on businesses and consumers worldwide. In the space of only a few hours, **8.5 million devices crashed across a whole host of industries**, from healthcare to aviation and emergency services, **costing Fortune 500 companies an estimated \$5.4 billion**². However, while the negative ramifications of the outage are well-known, little attention has been paid to all the positive changes that have been made in response—until now.

At [Adaptavist](#), our mission is to help businesses work better. We therefore set out to examine not only how companies around the world were impacted by the outage but - crucially - what steps they have taken since to build resilience and protect themselves from suffering an incident of this magnitude again.

Our findings show that, while painful, the CrowdStrike incident has provided a valuable call to arms. Instead of resting on their laurels, companies have seized the opportunity to overhaul software engineering practices. This has helped catalyse unprecedented levels of transformation, from massive investments in training and hiring to fundamental changes in how organisations approach development and vendor relationships.

We are now seeing boards that not only have an awareness of the challenges their development teams are facing, but first-hand experience of the consequences of failing to approach development and vendor relationships in the right way.

While the outlook is positive, there is still more work to be done. The major incident was no silver bullet, and building true resilience requires meeting deeper cultural and structural challenges with effective strategies to match. We may never be able to fully prevent another incident like CrowdStrike, but we can be far better equipped to respond to it.

¹ <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>

² <https://www.parametrixinsurance.com/in-the-news/crowdstrike-to-cost-fortune-500-5-4-billion-insured-loss-range-of-540-million-to-1-08-billion>



Introduction

The July 19 CrowdStrike incident thrust software engineering into the mainstream and starkly highlighted the severe ramifications a software outage can have. As Microsoft commented at the time, the incident demonstrated *“the interconnected nature of our broad ecosystem—global cloud providers, software platforms, security vendors and other software vendors, and customers.”*¹

But when the chaos subsides, systems come back online, and normal service resumes, what lessons are learned? And, importantly, why were organisations not sufficiently prepared?

To understand the answer to this question, and to show how companies are reacting in the months following the CrowdStrike outage, we surveyed 400 people with software development responsibilities in organisations with over \$10m in revenue across the UK, US, and Germany. The survey provides organisation-wide insights, from shifts in investment and training priorities to changes in cultural practices and attitudes toward vendors and third-party partners. Our research reveals an astounding 98% of companies were impacted by the event which affected millions of people globally as organisations raced to get their systems back online.

A significant **84% of organisations admit to not having an adequate incident response plan in place before the outage**. Of those with plans in place, only 16% found them effective during the crisis. Most organisations had never experienced such a large-scale outage or the ensuing impact on IT infrastructure, nor did they understand what was necessary to mitigate the fallout.

Six months on from the chaos, this special report investigates why **80% of organisations report positive outcomes from the CrowdStrike crisis** and reveals remarkable change among businesses. It also illuminates the remaining cultural and structural challenges that must be addressed to mitigate future risk and why, despite the progress, only 12% of organisations express high confidence in preventing similar incidents. It is clear that the event served as a wake-up call for the entire software industry—however, prevention of another similar incident is not yet guaranteed.

Methodology

The research was conducted by Censuswide on behalf of Adaptavist, part of The Adaptavist Group, between 08.10.2024 and 16.10.2024. Censuswide surveyed 400 people with responsibility for software development in organisations with \$10 million or more in annual revenue in the UK (100 respondents), US (200 respondents) and Germany (100 respondents).

¹ <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>



Chapter one:

Industry-Wide Transformation

Newfound confidence among software development professionals due to remarkably proactive and positive changes in the wake of the CrowdStrike incident.

i. 404: System stability not found

The CrowdStrike outage sent shockwaves through the software development community, exposing vulnerabilities in security and operational processes.

Prior to the outage, many organisations operated under the assumption that their existing protocols were sufficient enough to safeguard their systems and users. However, software update processes, while automated in many cases, often lack contingency planning for major disruptions to critical infrastructure like CrowdStrike's cybersecurity services. It's no surprise then that, in the wake of the outage and after a post-mortem analysis of the disruption, 84% of organisations admitted to not having an adequate incident response plan in place, and of those with plans in place, only 16% found them effective during the crisis.



84% of organisations
admitted to not having an
adequate incident response
plan in place

The CrowdStrike outage opened IT leaders' eyes to the wider robustness of their entire software development practices and processes. As a result, an overwhelming **81% of respondents have reported adopting more robust software development methodologies** and one-third of organisations have completely overhauled their software engineering processes to prevent similar disruptions in the future.

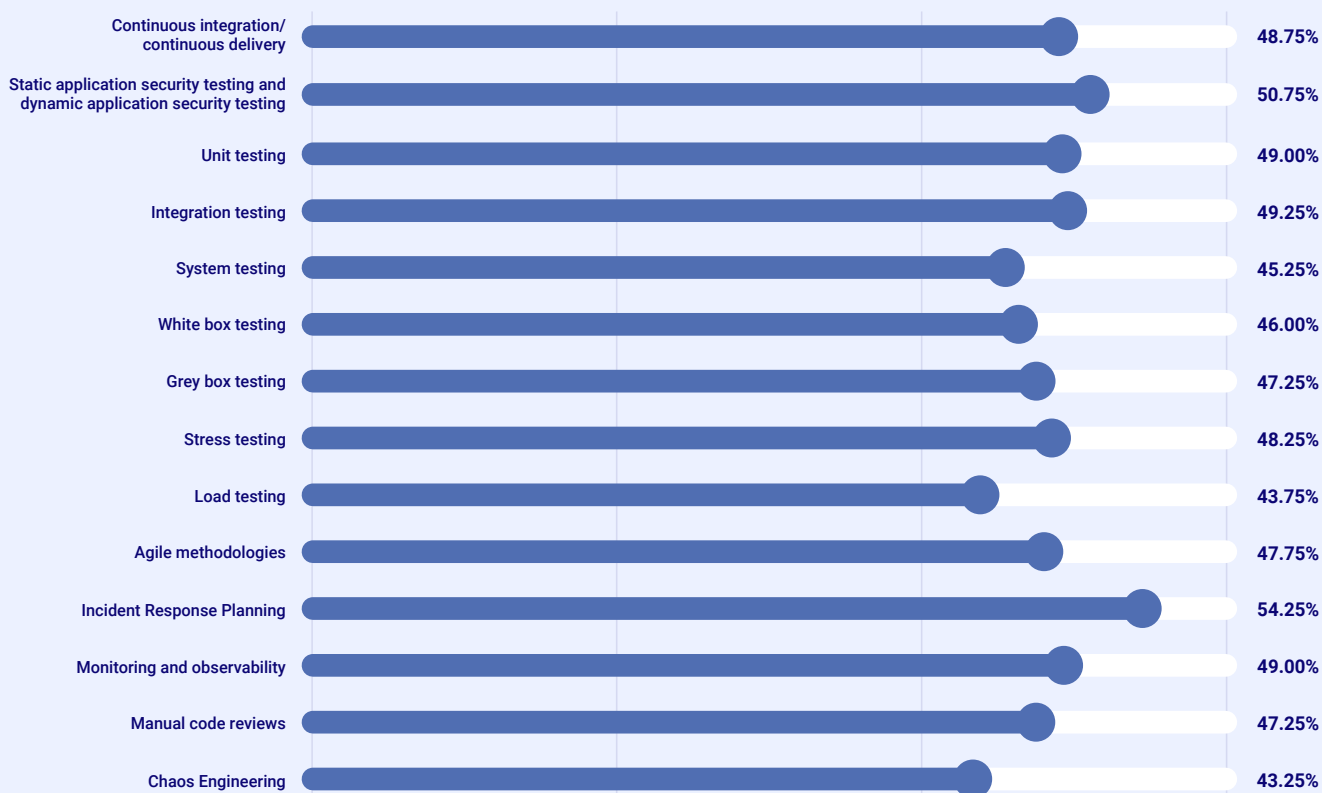
These transformations include more investment, or first-time implementation of incident response planning (54%), continuous integration and continuous delivery methodologies (49%), and monitoring and observing technologies (49%). What's more, approximately half of all software developers are introducing, or increasing investment into, a series of pertinent testing measures across the board.

By embedding these practices into their workflows, organisations aim to future-proof their software against a rapidly evolving threat landscape. This dual response - proactive process transformation and enhanced development rigour - marks a pivotal shift in how the industry approaches resilience, with lessons learned driving widespread change.



In focus

In response to the CrowdStrike outage how, if at all, does your organisation plan to adjust its software engineering practices in the next 12 months?



ii. Money talks: Shifting investment priorities

The CrowdStrike outage not only prompted operational changes, but reshaped the investment landscape in software development.

A significant **86% of businesses reported boosting financial investment in software development practices and training as a direct response to the outage**. The surge in funding underscores a widespread commitment to mitigating future risks through skill-building and process optimisation. Agile and DevOps practices emerged as the most prominent focus areas, with 89% of organisations increasing investment in training, this was followed by software testing training (89%), and cybersecurity training (88%). These methodologies, valued for their adaptability and resilience, have become essential tools in maintaining operational continuity.



In focus

In response to the CrowdStrike outage how, if at all, does your organisation plan to adjust its software engineering practices in the next 12 months?

Agile and DevOps practices and training	89.25%
Software testing training	89.00%
Cybersecurity training	87.50%
Incident response training	86.00%

There has also been a hiring spree across crucial technical roles in the aftermath of CrowdStrike, with an overwhelming 99.5% of organisations reporting plans to expand their technical teams, with quality assurance roles (36%) leading the charge. IT operations (34%), software developers (32%), and DevOps engineers (31%) follow closely, reflecting a balanced approach to strengthening the software development lifecycle across its key phases.



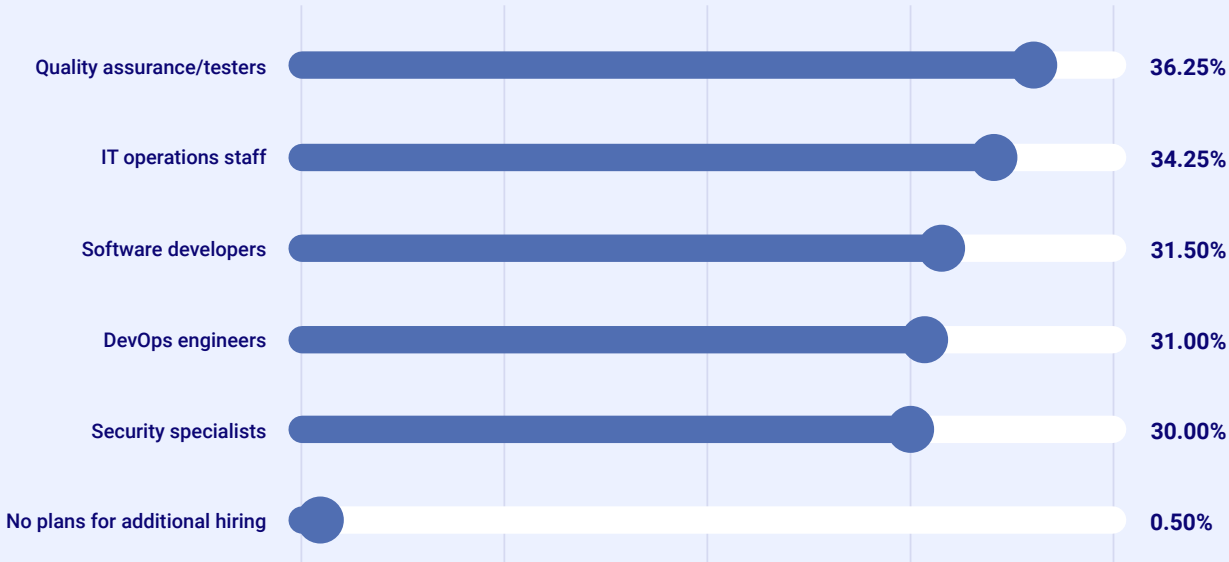
In the aftermath of CrowdStrike, **99.5% of organisations** plan to expand their technical teams.

These investment priorities signal a strategic pivot. By allocating resources to both talent acquisition and workforce training, organisations aim to build a robust foundation for a more secure and reliable software ecosystem in the post-CrowdStrike era.



In focus

In response to the CrowdStrike incident, is your organisation planning to hire additional staff in any areas?



iii. Awareness and evolving attitudes

Increased investment in training and software development processes will have no impact unless there's an inherent, company-wide mindset shift towards the regulations, security practices and operations which keep organisations secure.

Fortunately, this has been the case. In fact, organisations are increasingly embracing regulations as a means to enhance security and accountability. **Nearly half of respondents are now more supportive of regulations around cybersecurity and resilience (47%) and software quality assurance (48%).** Additionally, 49% endorse mandatory incident reporting requirements, signalling a growing recognition of the importance of transparency in mitigating threats. Support for broader software industry regulations has also increased, with 43% expressing a positive shift in attitude.



76% of organisations
note increased board-level
attention to cybersecurity.

The outage has also heightened cybersecurity awareness across organisations. Enhanced staff awareness was reported by 80% of respondents, while 74% observed improved collaboration between IT and other departments. At the leadership level, 76% of organisations note increased board-level attention to cybersecurity, a critical shift toward embedding security as a strategic priority.



In focus

As a result of the CrowdStrike incident, to what extent has your organisation experienced the following positive outcomes?

Improved incident response capabilities	79.75%
Enhanced cybersecurity awareness among staff	80.00%
Increased investment in IT infrastructure	79.25%
Improved collaboration between IT and other departments	74.00%
Adoption of more robust software development practices	80.75%
Greater focus on vendor risk management	76.25%
Increased board-level attention to cybersecurity	76.25%

With all the increased awareness and attention towards cybersecurity, now is the perfect time to double down on awareness training and security governance protocol.

“While it's encouraging to see this surge in security consciousness, business leaders must ensure that it's here to stay and results in lasting change. Robust security practices, such as automated vulnerability scanning and security testing at every stage of development and during runtime, is key to this journey, as is maintaining clear incident response protocols which every staff member is aware of.”



Jobin Kuruville
Global Head of DevOps Practice
Adaptavist



Chapter two:

Cultural challenges remain

Concerning patterns around psychological safety, fear of acknowledging mistakes and pressure to prioritise speed over quality may have contributed to widespread unpreparedness for the CrowdStrike incident.

i. Speed versus quality: A dangerous trade-off

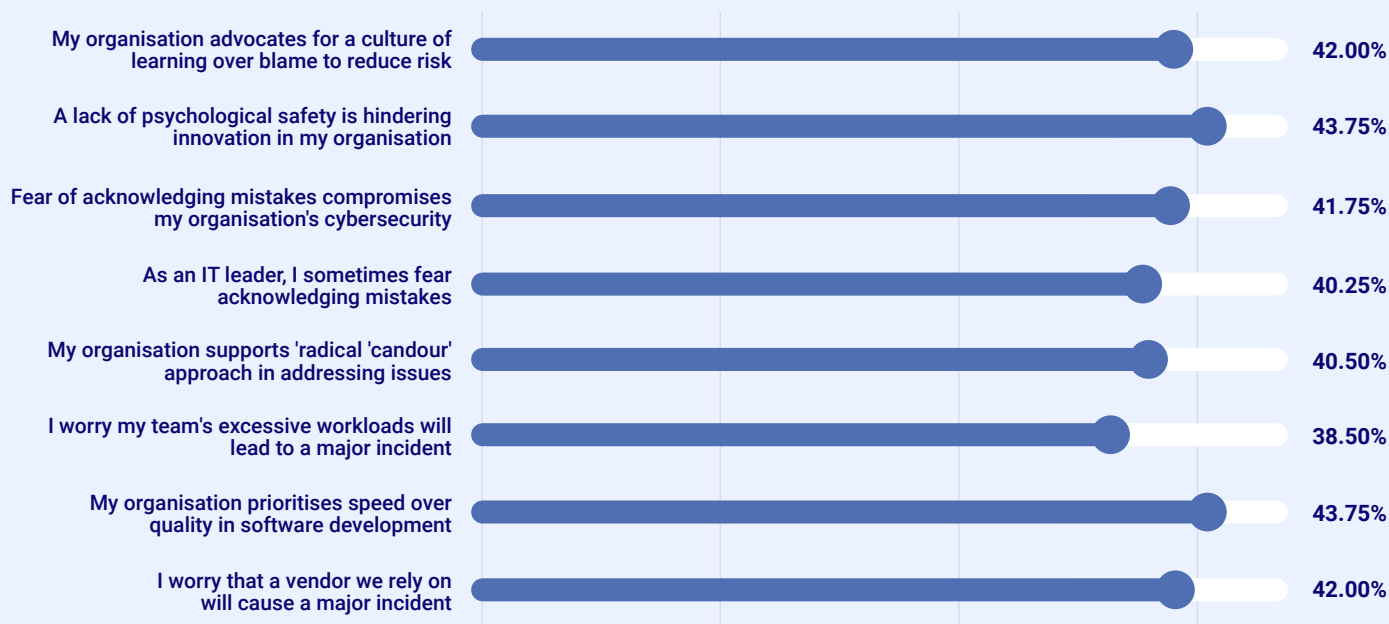
It can be easy to forget the most important factor to resilient IT operations: the human factor. This is often overlooked in favour of introducing the newest cutting-edge technologies and a focus on expanding infrastructure and operations, without real consideration of whether IT teams are equipped to deal with the increasing workload.

This typically results in overstretched and overworked teams, and worryingly, **44% of IT leaders revealed that their organisation still prioritises speed over quality in software development**, and 39% worry that their team's excessive workloads will lead to another major incident.



In focus

To what extent do you agree or disagree with the following statements?



ii. Culture crisis: The devastating impact of the 'blame game'

When a major outage occurs, it's IT teams that typically take on the bulk of the burden. Even when they're not in the midst of a catastrophe, it's often IT that is the first to be blamed if something goes wrong.


In fact, one in four IT leaders admitted that their organisation still advocates for a culture of fear over learning to reduce risk, and 40% said they still fear acknowledging their mistakes. A culture of fear can have significant repercussions on wider organisational resilience and innovation.

44% revealed that a lack of psychological safety is hindering innovation in their organisation, and 42% said that a fear of acknowledging mistakes comprises their organisation's cyber security.

In the wider context of the CrowdStrike outage, nearly two-fifths (39%) of IT leaders warn that excessive workloads could even trigger another major incident.



The ongoing war for IT talent is likely exacerbating these issues, but building a culture which invites open and honest collaboration, and addresses the issue of over-worked and over-blamed teams is the key to creating a welcoming environment for more IT professionals and delivering a far more resilient, efficient and secure IT environment.

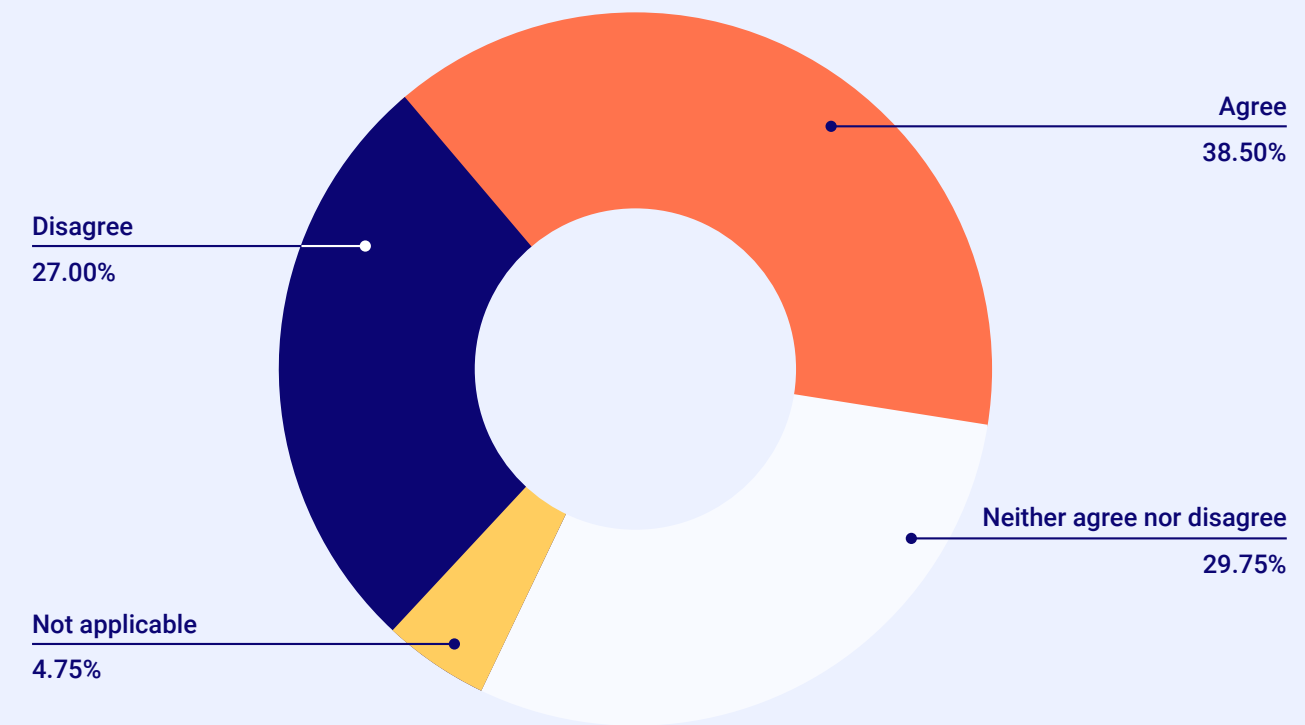
 **44% of respondents** revealed that a lack of psychological safety is hindering innovation in their organisation

‘Radical candour’ - a communication framework for specific and sincere praise and kind and clear criticism—is also key to creating an effective feedback loop that prioritises efficiency without ever inducing ‘blame’. **41% of IT leaders said their organisation already supports a radical candour approach to addressing feedback**, whereas 55% admit this is not necessarily in place.



In focus

“I worry my team’s excessive workloads will lead to a major incident”





Chapter three:

Shifting vendor relationships

The CrowdStrike outage has triggered a fundamental transformation in how organisations approach technology partnerships—a decisive shift in vendor relationships, marked by a striking loss of confidence in traditional single-vendor approaches.

i. Third parties: CrowdStrike winners and losers

The CrowdStrike outage underscored the critical importance of vendor reliability and forced organisations to reassess their third-party partnerships. This disruption revealed both vulnerabilities and opportunities, prompting a shift in how businesses approach vendor management.

Interestingly, **only 16% of organisations expressed satisfaction with their current providers**, signalling widespread concern over existing vendor capabilities. However, instead of retreating entirely from external solutions, organisations are adopting a more diversified and strategic approach to mitigate risks.



34% of organisations are expanding their vendor portfolios to reduce dependence on a single provider.



Approximately 37% of respondents are actively strengthening partnerships with current vendors, emphasising a commitment to trust and collaboration. On the other hand, 34% of organisations are expanding their vendor portfolios to reduce dependence on any single provider. Interestingly, one in three (34%) are increasing their reliance on open-source solutions to leverage flexibility and community-driven development.

31% are pivoting toward in-house development, highlighting a renewed focus on internal innovation and self-reliance. While resource-intensive, this strategy offers greater control over critical systems and reduces exposure to external outages.

However, by far the most significant shift in approach to vendor relationship management in the wake of the CrowdStrike incident is diversification: **a vast majority (83%) of organisations are either actively diversifying their providers or planning to do so.**

Evidently, leaders have realised that overreliance on a single vendor can be catastrophic if things go wrong, and as a result, 32% are already actively exploring multi-vendor solutions, and 30% have implemented more rigorous testing protocols, indicating a systematic approach to reducing future risks.



In focus

Which, if any, statements describe your organisation's shift in development philosophy following the CrowdStrike outage?

Strengthening partnerships with current vendors	37.00%
Increasing reliance on open-source solutions	34.25%
Diversifying our vendor relationships	34.00%
Moving towards more in-house development	30.75%
No significant change	16.25%
No statements in particular describe my organisation's shift in development philosophy following the CrowdStrike outage	0.75%





Chapter four:

Calm after the chaos: building resilience and optimising investment

While a lot of change has occurred in the six months since the CrowdStrike outage, it is clear that organisations still need to make strategic decisions to deliver greater digital resiliency and mitigate the risk of future crises.

This may be a mountain to climb, but the journey can be made easier with effective collaboration and a pragmatic approach to software development and IT operations. Thus, organisations must focus on the following key objectives to make the most out of their investments.



Continuous delivery:

We have seen how organisations are rethinking their relationships and reliance on vendors, and while diversifying can be a solid approach when thinking about digital resiliency, it will also increase complexity. When selecting tools and partners, the principles of continuous delivery should drive organisations' decision-making process.



DevOps/DevSecOps practices:

To be diligent in their preparations for future incidents, organisations must embed security best practices as standard, and support strategic testing and automated infrastructure. This is critical not only at the prevention stage but also for ensuring that the correct response processes are in place to allow IT teams and the wider organisation to react quickly.



Robust service management:

Implementing an effective service management strategy is the key to helping teams work better together. The right approach to service management can improve visibility and insights via proactive monitoring, and utilise automation to improve processes and workflows. This, in turn, supports organisations to focus on what really matters—safe in the knowledge that their processes will hold up to scrutiny.



Conclusion

While we're seeing promising progress, the journey to significantly reducing the risk of another global incident like CrowdStrike is far from over. True resilience requires a transformation that extends beyond technical teams—it must be embedded across the entire organisation.

Greater focus must be placed on creating systems where every function, at every level, is aligned with the right practices.

Striking the optimal balance between people, processes, and technology is essential to unlocking safer, more effective ways of working. This organisational-wide approach ensures that developers and technical teams are supported by a broader framework, enabling them to prevent and respond to issues within a cohesive and resilient ecosystem.

“ With the best intentions in the world, businesses will still face challenges in becoming more structurally and culturally resilient. It's not enough to just implement technology—organisations need to ensure they support their teams with the right processes and tools.

This holistic approach is critical. By embedding secure processes and leveraging advanced technologies within their ways of working, businesses can innovate while enhancing their ability to respond quickly and effectively to future challenges. Doing so positions organisations in increasingly complex and volatile business contexts to not just mitigate, but thrive in the face of disruptions.




As we reflect on the lessons learned, it's clear that resilience is a continuous pursuit. By focusing on strengthening organisational culture and constantly investing to make systems and practices robust, we can create a future where our businesses are better prepared for the unexpected and empowered to adapt and grow. Let us take this moment to recommit to this necessary transformation and ensure our organisations are built for long-term success. ”



Jon Mort
Chief Technology Officer,
The Adaptavist Group

Appendix

Want to optimise your organisation's IT practices?

-  Visit Adaptavist's website www.adaptavist.com
-  Contact us at: www.adaptavist.com/contact
-  For Group enquiries, visit www.theadaptavistgroup.com/contact

About Adaptavist and The Adaptavist Group

Founded in 2005, Adaptavist is a global technology and innovative solutions provider that helps organisations improve agility and overcome the challenges of digital transformation.

We are experts at delivering innovative and tailored solutions, and quality services across some of the world's most trusted technology ecosystems, including Atlassian, AWS, monday.com, GitLab, and many more.

It is the pioneer brand of The Adaptavist Group, a global family of companies with one common goal: to make business work better. We combine the best talent, technology, and processes to make it easier for our customers to excel—today and tomorrow.

The Adaptavist Group exists to support clients' day-to-day workflows, business transformation, and high-growth strategies. We offer a comprehensive but always evolving range of services across five key practices: agile, DevOps, work management, ITSM, and cloud. Our depth of knowledge across these practices unites us in our mission to help businesses embrace continuous transformation and make it their competitive advantage.

Media Contact: adaptavist@wearetf.com