RSM

Key lessons and insights from the CrowdStrike outage

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

Helping you protect your assets, your reputation and your future.

Executive summary

CrowdStrike, a leading cyber security firm, experienced a significant outage in July 2024 that impacted millions of computers and a wide range of organisations relying on its services globally. According to CrowdStrike's update, ~99% of the impacted Windows sensors had restored functionality as of 5pm on 29 July.

In a day and age when there is dependence on technology to deliver services across every sector from transportation, supply chain to healthcare and emergency services, the event was catastrophic and a reminder for organisations to examine their resilience and readiness for such disruptions. As a result of this incident, organisations experienced financial losses, disruptions to critical operations, impact to community and citizen services and ongoing costs for recovery, legal and regulatory impact management.

With the increasing digitisation of business processes and the growing threat landscape posed by cyber-attacks and data breaches, there is a heightened focus on digital resilience today. This event provided critical lessons for organisations, particularly in Australia, emphasising the importance of robust contingency planning measures, cyber security planning, and the need for investments towards wider operational resilience.

This paper intends to focus on the key lessons learned from this incident and provides actionable relevant insights for organisations to consider so as to maintain operational resilience.

Kaustubh Vazalwar
Director, RSM Cyber Security & Privacy Risk Services

Key lessons

This incident and the follow-on impact are a stark reminder for organisations that even the most trusted solutions / tools can fail and it is vital to review and eliminate, where possible, single points of failures in technology as well as the processes that support critical business systems.

Whether its Information Technology (IT) or Operational Technology (OT) environment supporting production/ critical operations, this incident has provided important learnings for every organisation across a range of areas.

1. Incident Response Planning

The incident highlighted the importance of well-defined incident response plans covering every critical system and sub-system, including clearly documented and tested protocols across people, technology and processes.

2. Regular Scenario based Testing

Regular testing of documented recovery plans and disaster recovery drills can significantly improve employee awareness at every level and an organisation's readiness to handle outages.

The need to identify specific scenarios custom to the organisation which can cause widespread business impact, emphasising the need for a well-defined and supported resiliency function.

3. Redundancy, Failover and Scalability Mechanisms

The incident highlighted the need for effective redundancy and failover mechanisms for critical systems, manual workarounds across every layer as well as the importance to identify and regularly review interdependencies (upstream and downstream) for every critical process to ensure service continuity.

At the same time, the ability to scale and manage loads efficiently can prevent service disruptions during high-demand periods. Designing and developing systems with security, resilience and scalability in mind, can enable effectively managing peak loads as well as periods of disruptions.

4. Third Party Risk Management

This incident was a clear reminder on the importance of effective and thorough third party risk management. Organisations today depend on third parties and partner organisations (in country and / or outside) for a wide range of services. Reliance on third-party services requires ongoing due diligence, risk assessments as well as continuous monitoring as part of governance.

Regulatory frameworks such as APRA CPS 230 for financial services organisations in Australia have placed particular importance on effective third party risk monitoring and management by the senior leadership.

5. Service Level Agreements (SLAs)

The incident has emphasised the need for clearly defined SLAs that outline performance metrics and enables the senior management to monitor performance. In incidents where remediation activities are dependent on external teams and can run over days / weeks, clearly documented, agreed and communicated SLAs are important for critical business operations.

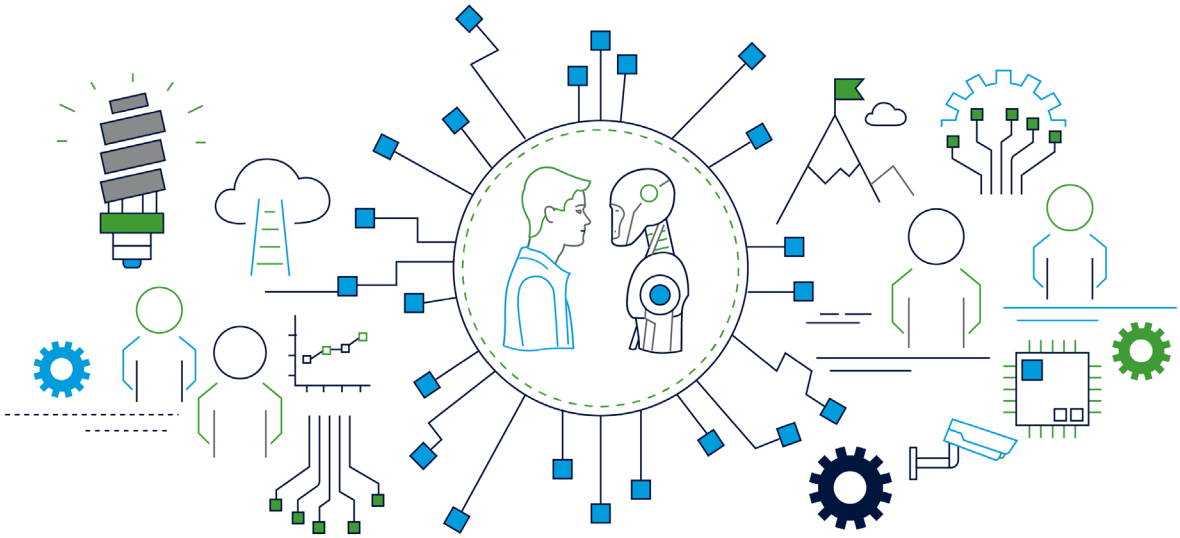
6. Focussed Communication

Consistent, timely and relevant communication during an outage or critical incident is crucial to maintain stakeholder and customer trust. The incident has clearly highlighted the importance of effective communication planning and execution for organisations in every sector, while managing critical incidents.

7. Continuous Monitoring and Alerts

Proactive monitoring and real-time alerts are essential for early detection and mitigation of issues. Many organisations, especially small and medium enterprises, detected and realised the impact of the outage quite late (in certain cases subsequent working Monday) and had longer disruption to their operations.

The incident highlighted the importance of investing in capabilities and implementing processes for continuous monitoring of systems supporting critical business operations.



8. Complexity of environments

IT and OT environments that support critical 24x7 operations (E.g., Water, Energy & Gas, etc.) often involve a complex network of interdependent systems.

The incident highlighted the criticality of continuity planning focussed on safety, operational integrity and system availability in such environments.

This includes processes for testing and implementing updates and security patches for supporting systems.

> Even the most trusted solutions/ tools can fail and it is vital to review and eliminate single points of failures in technology as well as processes that support critical business systems.

9. Investments in Resourcing

Technical and Customer support teams in almost every organisation went through an unprecedented stress during this incident, especially managing expectations and queries from internal and external stakeholders and working across long hours.

The outage underscored the need for robust local technical resourcing as well as customer support to handle increased queries expected during incidents and the need for dedicated investments in this space.

10. Mental Health Support

Incidents such as these can involve long working hours trying to recover all systems and often complex coordination efforts across multiple internal and external teams.

It is important to make sure employees supporting the recovery from such incidents are provided with the right mental health support considering the long and stressful nature of recovery process they may go through.

Key insights on way forward

So how do organisations prepare for the next such inevitable incident and what are some of the key questions to introspect on as they work towards the wider goal of operational resilience?

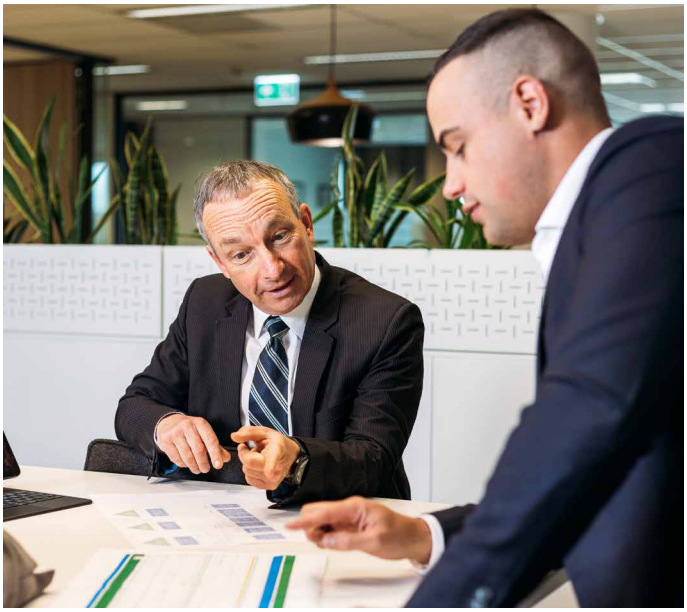
Let us evaluate these focus areas and questions as below:

1. Holistic Enterprise Risk Management

Organisations need to adopt a comprehensive approach to enterprise risk management that considers all potential threats, including cyber, operational, and environmental risks. It is important to regularly update risk assessments based upon applicable emerging threats and develop mitigation strategies for a wide range of custom applicable scenarios relevant to the organisation, including third party risks.

Key questions

- Do we have a regular and monitored process for Risk Assessment and Business Impact Analysis?
- Are our current risk assessments up to date and inclusive of all potential threats?
- Are employees at every level aware of the risk management process and protocols for reporting, management and escalation?
- Do we conduct regular risk assessments for any third party services / capabilities supporting critical business operations?



2. Incident Response Planning

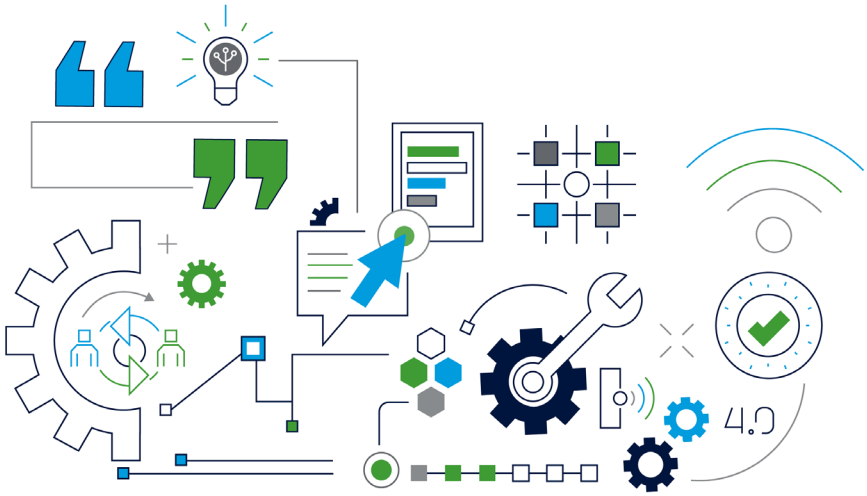
Maintaining up-to-date Business Continuity, IT and OT Disaster Recovery and Cyber Incident Response plans that address various scenarios, relevant to the organisation, ensures the organisation can continue operating during disruptions.

Business continuity and cyber incident management intersect closely, particularly in today's digital landscape where cyber threats pose significant risks to organisations. It is vital that that there is dedicated investment for the resiliency function in the organisation and aligned leadership support to drive key actions to ensure readiness.

The resiliency function needs to account for preparedness not only for internal processes but also any critical third party / partner teams that support critical operations.

Key questions

- Are our Business Continuity plans (BCP), Disaster Recovery Plans (DRP) and Cyber Incident Response Plans (CIRP) comprehensive and up to date?
- Do we have visibility over the disaster recovery preparedness measures of any third party teams / organisations supporting critical operations including Cloud / Data centre providers and SaaS platforms?
- Is there clarity in terms of interdependencies (Upstream and Downstream) for all critical systems as part of Business Impact Analysis?
- How often do we test our Incident Response Plans?
- Is there clarity and awareness amongst staff members at every level on roles and responsibilities in a crisis situation?
- Do our incident response plans provide appropriate details for stakeholder management?
- Is there clarity on communication management responsibilities and requirements as part of the response plans?



3. Resilience Strategy

Developing an integrated resilience strategy that aligns with the organisation's overall business objectives and risk appetite is vital. Regulatory requirements in almost every industry today demand focussed and organisation wide aligned efforts for resilience to ensure compliance with standards and guidelines.

Cross departmental and team collaboration across as part of resiliency strategy enables the organisation to ensure a coordinated and unified response to disruptions.

Driving design of infrastructure and systems with resilience in mind should be a key part of resiliency strategy. It should provide appropriate guidelines to implement redundant systems, failover mechanisms, and backup solutions to ensure the availability and integrity of data and applications in the event of a critical incident.

The strategy should also guide safely testing security updates and patches for systems and applications supporting critical operations in test environments before application and rollout to production systems and end devices.

The other aspect to review as part of resilience strategy are the avenues to bring in automation, incorporate new solutions as well as technologies such as Artificial Intelligence (AI) and machine learning as part of monitoring and management capabilities. Implemented post a Cost vs Risk assessment, these can provide significant benefits with faster and potentially more effective response times to incidents and threats.

Key questions

- Do our resiliency investments align with our organisational risk appetite?
- Is the organisational risk appetite and identified resilience strategies aligned with the regulatory requirements and stakeholder expectations?
- Do we have clarity on the resiliency requirements of every critical business unit?
- Are we designing and assessing critical applications and system architectures for their resilience and identifying single points of failures?
- How do we test updates and security patches for critical systems in a safe environment before applying to production?
- Who is responsible for overseeing resilience initiatives, and is there clear accountability up to the leadership?
- How is the organisation monitoring and adapting to changes in regulatory requirements?
- Are there focussed investments in internal and external measures such as internal audits or external benchmarking assessments to review resiliency readiness of regulated systems?

> Designing and developing systems with security, resilience and scalability in mind, can enable effectively managing peak loads as well as periods of disruptions.

4. Resource Management

Allocating sufficient resources and support, including budget and personnel, to initiatives focussed on maintaining operational resiliency ensures they are effectively implemented and maintained.

Managing incidents in a connected enterprise requires cross team collaboration across multiple teams and business units under time sensitive stressful conditions.

These situations can potentially be further complicated when working with third party teams, partner organisations, managing regulatory requirements as well as timely stakeholder communications.

Mental health can be a key factor for executive, technical as well as customer support team members during periods of critical incidents running over days / weeks.

It is important for set the tone from the top with executive sponsorship and commitment and a proper review of resource requirements for every team under critical incident situations, relevant to the organisation.

Key questions

- How did we perform in each team under any recent incidents critical to the organisation?
- Do we have the necessary resources allocated to our customer service team to manage large scale critical incidents?
- What measures / resources do we have in place within the organisation to support the mental health of staff members?
- Do we have representation of non-technology teams such as Human Resources during the testing of documented recovery plans?

5. Culture

Fostering a culture of resilience within the organisation is essential, emphasising the importance of preparedness and adaptability at all levels. To support proactive resilience, it is important to promote a security-first and resiliency by design culture that encourages and provides incentives for proactive engagement in safeguarding information & systems.

Equally, it is vital to commit to continuous improvement within the organisation learning from incidents, ensuring alignment with change management and regularly testing and reporting on documented plans and procedures.

Key questions

- Have we allocated appropriate resources, established policies and set the accountability tone from the leadership?
- Do we have training and testing programs in place to educate employees and test preparedness?
- How do we encourage and reward proactive identification and mitigation of risks?
- How do we capture and implement lessons learned from past incidents?
- Do we track and report learnings from exercises focussed on testing documented BCP, DRP and CIRP?
- Do we involve third party and partner teams supporting critical operations as part of the approach to discuss learnings from any incidents or exercises?

Conclusion

Critical incidents such as the CrowdStrike outage are the unavoidable reality that organisations across every sector and every geography face today.

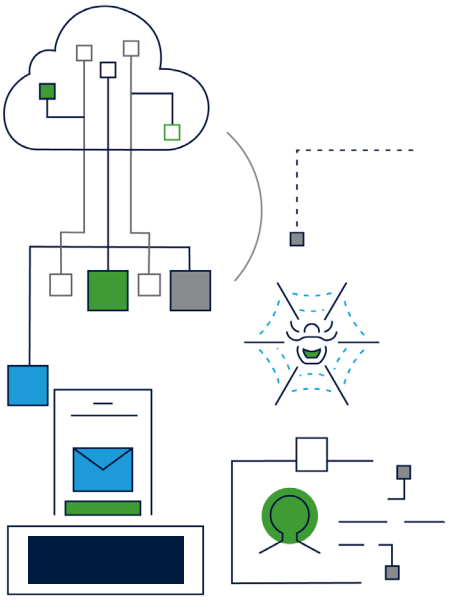
It serves as a crucial reminder to every organisation on the importance of investing in operational resilience and effective risk management. Transitioning from traditional business continuity management (BCM) to operational resilience involves shifting focus from merely recovering from disruptions to ensuring the continued operation of critical business operations under a wide range of applicable scenarios.

By focussing efforts on learning from this incident and implementing the insights outlined in this report, organisations can enhance their preparedness and ability to withstand and recover from disruptions as well as ensure operational integrity and business continuity of their critical operations.

Our cyber security and privacy team

RSM is an international leader in providing security, resiliency and privacy services to clients across a variety of organisations and can help you assess as well as implement resiliency practices.

Get in touch with one of our cyber security, resilience or technology risk experts below



Darren Booth
Partner
darren.booth@rsm.com.au

Ashwin Pal
Partner
ashwin.pal@rsm.com.au

Riaan Bronkhorst
Partner
riaan.bronkhorst@rsm.com.au

Kaustubh Vazalwar
Director
kaustubh.vazalwar@rsm.com.au

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

rsm.com.au