From Prevention to Recovery: Confronting Inevitable Cyber Threats

BY **FOO SIANG-TSE** and **HOWIE LAU**

The increasing sophistication and frequency of cyber attacks have made it abundantly clear that no organisation is immune to breaches and outages. Hence, shifting the focus from a purely defensive posture to a comprehensive approach encompassing not only prevention but also robust recovery, is essential for achieving stronger cyber security resilience and corporate capabilities.

“Nothing is certain except Death and Taxes,” American statesman Bejamin Franklin famously observed in 1789.

In our highly digitalised world, we could add Outages to the equation.

As more companies and governments become more digital, the total surface area of cyber threat and vulnerability of any organisation has increased. The importance of interconnection with customers, employees, suppliers and partners in doing business has deepened and expanded this conundrum.

The benefits of robust recovery

Recognising the inevitability of cyber breaches and outages necessitates a shift in focus from solely relying on prevention to building robust recovery capabilities. Many organisations already have in place a business continuity plan, a disaster recovery strategy and a cyber security incident response plan.

Recovery capabilities enable organisations to effectively respond to breaches, minimise their impact, and restore normal operations in a timely manner. By investing in recovery capabilities, organisations can strengthen their overall cyber security resilience with several benefits.

- Reduced downtime: Minimising downtime during and after a breach is crucial for maintaining business continuity and minimising financial losses.
- Reduced data loss: Robust recovery mechanisms can help prevent or minimise data loss, protecting valuable assets and maintaining customer trust.
- Enhanced reputation: Organisations that demonstrate effective recovery capabilities inspire confidence in their ability to safeguard data and maintain business operations, protecting their reputation and brand image.

The cyber security stages

To effectively address the multifaceted nature of cyber security, the Cyber Security Stages framework outlined by the US National Institute of Standards and Technology (and widely adopted by cyber security professionals) provides a structured approach that encompasses five key phases:

1. **Identify:** Establish a clear understanding of the organisation's assets, threats and vulnerabilities to prioritise cyber security efforts.

2. **Protect:** Implement appropriate safeguards to minimise the likelihood of successful cyber attacks. These safeguards include technical controls such as firewalls, intrusion detection systems and data encryption, as well as operational controls such as risk management policies and training programmes.

3. **Detect:** Implement monitoring and logging mechanisms to identify signs of cyber security breaches. Early detection is critical for minimising the impact of attacks and facilitating timely response.

4. **Respond:** Have a well-defined incident response plan in place to enable the organisation to take effective action upon detecting a breach. This plan should clearly outline roles, responsibilities, communication protocols and containment procedures.

5. **Recover:** Restore normal operations, mitigate damage and learn from the incident. The recovery phase includes restoring data, repairing systems and conducting thorough post-incident reviews to identify areas for improvement.

Despite best efforts to protect and prepare, cyber breaches and outages are inevitable. No organisation, regardless of size or resources, is entirely immune to these threats. The ever-evolving tactics and techniques employed by cyber criminals, coupled with human error (IBM reports that 95 per cent of cyber breaches are down to human error) and the increasing complexity of IT systems, create a challenging environment where breaches are bound to occur.

How can organisations be prepared for a world filled with rising cyber risk? A comprehensive approach would include strengthening the following three areas of development, as shown in "Organisational Focus on Cyber Resilience".

1. Business continuity capabilities.
2. Reporting mechanisms.
3. Crisis communications.

Bringing it together

Effective crisis communications requires a concerted effort from all levels of the organisation, including the board of directors. Boards play a critical role in setting the tone for crisis communication, ensuring that the organisation has the necessary resources and capabilities in place, and providing guidance and support to management during a crisis.

The organisation should have a strong in-house communications team with expertise in crisis communications. This team should have the skills and resources necessary to monitor emerging threats, and develop and implement crisis communication plans. Beyond that, all employees should be trained and equipped with skills to handle tough conversations and manage stakeholders and potential reputational risks.

Organisational Focus on Cyber Resilience

Focus 1: Business continuity capabilities

Doubling down on strong business continuity planning (BCP) is crucial to ensure the organisation can continue to operate during disruptions or disasters.

First, the board should work with senior management to clearly define the scope of the BCP (e.g., types of disruption) and specific objectives (e.g., to minimise downtime, protect critical assets and ensure employee safety).

A thorough risk assessment to identify potential threats and vulnerabilities should be conducted before implementing risk mitigation strategies to minimise the likelihood and impact of disruptions. Businesses should prioritise critical business functions and processes based on their impact on their organisation.

For example, a business impact analysis to assess the potential financial and operational impact of disruptions on critical business functions could include an evaluation of maximum tolerable downtime (the longest acceptable period of interruption) for each function. Businesses could then move to develop recovery time objectives and recovery point objectives based on their assessments.

Roles and responsibilities should be clearly defined within the BCP framework, establishing a chain of command for decision making and ensuring that all personnel are aware of their responsibilities.

Planning an effective response can include developing detailed procedures for responding to different types of disruption. Businesses should identify alternate locations and resources for conducting critical business functions. And communication protocols to inform and update stakeholders during emergencies should be established.

Regular testing and training should be carried out to test the BCP through simulations, drills and exercises. This will help identify and address any gaps and weaknesses in the plan. Training for all personnel to familiarise them with their roles and responsibilities in the BCP is important, as are regular reviews and updates of the BCP to reflect organisational restructure and the evolving threat landscape. Backup systems and data recovery procedures should be reviewed and periodic audits to ensure the BCP is effective and meets regulatory requirements.

Increasingly, the BCP is not a "just-in-case" plan. It should be a regular part of the business cadence where it is tested, practised and updated regularly.

For this to happen, silos between communications and business units should be avoided. Organisations should foster a collaborative environment where communications professionals are actively involved in crisis planning and response from the outset. The communications teams should be empowered to partner with business owners in developing and implementing crisis communication strategies.

Crisis communication planning should be integrated into the organisation's disaster recovery and BCP processes. Clear lines of authority and communication protocols should be established to facilitate a rapid and coordinated response to a crisis.

By implementing these recommendations, boards can empower their organisations to effectively manage

Focus 2: Reporting mechanisms

An often-overlooked aspect is the reporting mechanisms and risk culture within the organisation. Mitigating cyber security risks depends on a robust reporting mechanism and a strong security culture, which creates a mindset among employees to report potential incidents early and quickly without compromising the "crime scene".

For example, NCS rolled out an internal campaign across all 12,000 employees with the key message: "Be Secure, Be Clean, Be Fast". This exercise was implemented with a combination of training, incentives and internal communications to build a stronger culture and mindset that cyber security is everyone's responsibility.

In terms of developing a cyber security culture and awareness within the organisation, it is important for leadership to demonstrate a commitment to cyber security by allocating resources, promoting awareness initiatives and leading by example. Employee education and regular training are key to educating personnel on cyber security best practices, phishing trends, password hygiene, data security protocols and incident reporting procedures.

The reporting mechanism should be easily accessible to all employees, regardless of their technical expertise or position within the company. This could include multiple channels like email, a dedicated hotline, internal reporting platform, or in-person reporting to designated personnel. Employees should feel comfortable reporting potential incidents without fear of retaliation or blame. Allowing anonymity encourages reporting and provides valuable insights into potential threats.

An incident response plan should have clear instructions on the types of incidents to report, and how and when to report them. This is useful to ensure consistency and reduce confusion. Incidents should be promptly investigated and addressed. And implementing a clear escalation process ensures timely resolution and minimises potential damage.

Employees should receive feedback on their reports, even if the reported incident is not deemed a threat. This encourages continued reporting and employee engagement, and demonstrates the importance of cyber security awareness. The organisation should strive to foster an environment where employees feel comfortable discussing cyber security concerns and openly reporting incidents without fear of judgement or punishment.

Tracking and analysing data can help identify trends, patterns and areas for improvement. The reporting mechanism should be integrated with the organisation's security operations centre to ensure efficient incident response and threat analysis. In addition, vendor management should encompass policies and procedures to ensure that vendors, suppliers and partners adhere to the organisation's security standards and best practices.

By implementing these elements, corporations can establish a robust reporting mechanism and a strong security culture, ultimately leading to better risk management and a more secure digital environment.

crises, minimise reputational damage and maintain stakeholder trust in the face of challenging situations. Effective crisis communications is not just about managing the immediate aftermath of a crisis; it is about demonstrating a commitment to strong governance, transparency, accountability and responsible corporate citizenship.

Building a culture of recovery within an organisation involves promoting awareness, providing training, and conducting regular exercises to test and refine recovery plans. By embedding recovery into the organisation's DNA, businesses can foster a proactive approach to addressing cyber security incidents.

Focus 3: Crisis communications

Beyond BCPs and cyber incident response plans, crisis communications is key. Communications has taken on a heightened significance for crisis management as expectations of stakeholders impacted by outages continue to evolve. The speed at which information spreads and the interconnectedness of society have amplified the potential impact of crises, making effective crisis communications more crucial than ever.

To effectively manage crises in the current environment, organisations must adapt their crisis communication strategies to address several key shifts that have transformed the landscape of crisis communication.

1. Need for speed
In the digital age, the time to respond to a crisis is measured in minutes, not days. The rapid circulation of information through social media and online news outlets means that organisations must be prepared to respond promptly and transparently to minimise speculation and control the narrative. Delays in communication can fuel anxiety, spread misinformation and erode public trust.

2. Inside-out and outside-in
Effective crisis communication is no longer a one-way street. Organisations must recognise the importance of internal communication as the foundation for external communication. Employees are often the first to perceive a crisis and can become valuable sources of information for the media and the public. By informing employees first and addressing their concerns, organisations can foster a sense of unity and empower employees to serve as informed ambassadors.

3. All communication platforms
The media landscape is more fragmented than ever before. Organisations must leverage a variety of communication channels to reach their target audience, including traditional media outlets, social media platforms, their own websites and corporate blogs. Each platform has its own unique strengths and audience demographics, and organisations must tailor their messages and engagement strategies accordingly.

4. Not just shareholders but all stakeholders
Crisis communication must recognise the diversity of stakeholders that organisations have a responsibility to inform. While shareholders remain important, organisations must also consider the needs of employees, customers, partners and the communities in which they operate. Each stakeholder group has unique concerns and information needs, and organisations must craft tailored messages that resonate with each audience segment.

5. Communicate with empathy
Transparency is essential in crisis communication, but it should not come at the expense of empathy. Organisations must strike a balance between providing accurate information and acknowledging the impact of the crisis on those affected. Conveying empathy and understanding can help maintain stakeholder trust and build goodwill.

Not a matter of if, but when

In summary, cyber resilience is not just about protection but recovery. It is not so much the technologies and processes but the people that we have to invest in. And recovery is not so much about systems and policies, but also about communicating effectively and building trust with stakeholders.

After all, nothing is certain except for death, taxes and outages. ●

Foo Siang-tse is Senior Partner of Cyber, NCS.
Howie Lau is an SID Governing Council member and Managing Partner, Corporate Development and Partnerships, NCS.