Allens

In alliance with Linklaters

> 'The average level of Burnout in our sample meets or surpasses that reported... for frontline healthcare workers in the aftermath of the COVID-19 pandemic.'[1]

Why organisations must embed mental health and wellbeing support into cyber incident response planning

APRIL 2024

Mental health and wellbeing support for cyber professionals, incident response teams and staff targeted in cyber incidents, is now essential to cyber risk management and incident response planning.

As cyber incidents become commonplace and threat actors increasingly target, harass and intimidate key decision-makers to coerce them to pay cyber ransoms, information is now emerging on the heavy toll cyber incidents can take on the individuals involved.

Investing in mental health and wellbeing initiatives and implementing support structures—both before and during a cyber incident – can:

- **reduce burnout** and help retain cybersecurity talent
- enhance the effectiveness of cyber defence and incident response teams and **enhance organisational cybersecurity**
- **reduce the risk of potentially devastating consequences** that can follow targeted harassment campaigns by threat actors determined to extract cyber extortion payments from decision-makers
- **facilitate compliance with Work Health and Safety (*WHS*) legislation** given recent amendments focussed on the proactive management of psychological risks in the workplace.

This guide explains:

- the pressures faced by cyber professionals, incident response team members and senior executives and directors (who are increasingly being personally targeted in cyber incidents)
- WHS obligations in the context of cyber incidents
- nine actions to take to prepare and support employees and your organisation.

Note: this guide contains reference to some sensitive topics.

1 Andrew Reeves, Malcolm Pattinson and Marcus Butavicius, 'Is Your CISO Burnt Out Yet? Examining Demographic Differences in Workplace Burnout amongst Cyber Security Professionals' (2023) *Human Aspects of Information Security and Assurance* 11.

A multitude of stressors

'Burnout at such an unsustainably high level in the cyber sector can have serious implications, not only for the individuals affected but also for the organisations they serve and the broader society whose data they protect.'[2]

Before and after an incident

Even *before* a cyber incident occurs, cyber defence teams generally operate in a state of hypervigilance. They're also acutely aware that effective cybersecurity is rarely visible and is therefore generally underappreciated, despite the high cost of failure.

In the *aftermath* of a cyber incident, key decision-makers (including senior executives and directors) and cyber incident response teams can experience:

- **Long working hours over extended periods**, resulting in disruption to routines and eating habits, lack of sleep and increased reliance on others to assume day-to-day care and other responsibilities. Insufficient sleep also inhibits recovery from stress, can result in elevated anxiety and adversely impacts decision-making.
- **Anxiety that accompanies uncertainty** as to what has happened, the impact of the incident and how long it will take to resolve.
- Potentially **significant regulatory exposure** (including personal liability).
- **Intrusive inquiries and investigations** by regulators, law enforcement and other government agencies (and internally), both during and after cyber incidents.
- **Concern for affected individuals and others**, particularly where the compromised data is sensitive or relates to vulnerable individuals, or where the incident impacts critical infrastructure.
- A stress response from being quite literally **under attack** from cybercriminals (who may, in some cases, be state actors).
- **Harassment by the threat actor** of the individual and their loved ones.
- **Customer backlash.**
- **Media attention and speculation.**
- Feelings of **guilt** and a sense they could have done more to prevent the incident.
- Stress related to the **responsibility of having to make hard judgment calls** (eg whether to pay a ransom to a cybercriminal and the potential implications of that choice).

All of these factors are recognised psychosocial risks which, if not managed proactively, can lead to significant psychological harm to individuals and expose the organisation (or individuals) to both liability under WHS legislation and serious security risks.

Evolving threat actor tactics

As governments adopt measures to discourage ransom payments and organisations bolster their security controls, threat actors are increasingly deploying more harmful tactics to pressure key decision-makers and staff to pay ransom demands or provide access to systems or data.

1 Swatting

This involves making a false report to law enforcement, usually of an ongoing critical incident like a live-fire or hostage situation, to draw a heavy armed police response to a specific location against an unsuspecting individual or company. The 2017 Wichita swatting incident in the US tragically resulted in an innocent man's death.

2 Violence-as-a-service

Reports of violence-as-a-service (ie the payment of others to commit physical attacks such as firebombing houses, beatings, slashing tyres and throwing bricks through windows) are on the rise. Often advertised on internet noticeboards or Telegram and typically associated with threat actors focussed on SIM swapping, these services are now also bleeding into other threat actor activities.

3 Blackmail and sextortion

In this tactic, threat actors use sensitive or damaging information about key individuals within an organisation or their family members (often obtained through data breaches or targeted hacks) to pressure them to make decisions in favour of the attacker's interests under threat of exposure. For example, in the 2014 Sony Pictures hack, the threat actors used personal emails as leverage against executives. Sextortion is a type of blackmail involving threats to share sexual imagery with the public.

4 Harassment and intimidation

Other forms of harassment include threats of violence and sending other intimidating messages or packages to family members.

2 Andrew Reeves, Malcolm Pattinson and Marcus Butavicius, 'Is Your CISO Burnt Out Yet? Examining Demographic Differences in Workplace Burnout amongst Cyber Security Professionals' (2023) *Human Aspects of Information Security and Assurance* 11.

Nine actions to take

‘Left unaddressed, this level of stress will cause talent attrition and may allow vulnerabilities to go unaddressed in organisational information systems which can be readily abused by attackers.’[3]

These should be embedded in cyber-readiness activities and (where relevant) documented in cyber incident response plans and playbooks.

1. **Acknowledgment:** openly acknowledge the mental health and wellbeing challenges confronting cyber defence and incident response teams and key decision-makers (including senior executives and directors) with those stakeholders as part of incident response planning.
2. **Preparation and training:** proactively train staff on what to expect during a cyber incident (including evolving threat actor tactics) and incorporate relevant challenges into cyber simulations—this helps reduce fear and uncertainty, which can be significant stressors during such an event. Training for leaders should address how best to manage and support staff during a major incident. Training for the broader executive, cyber defence and incident response teams should include coping strategies for stress management and a focus on building resilience. Organisations like Cybermindz can also help provide proactive support for cyber professionals.
3. **Mental health first aid officers:** establish a team of trained mental health first aid officers who can provide initial support and guidance to those experiencing mental health difficulties during a crisis.
4. **Employee Assistance Programs (EAP):** EAPs offer confidential counselling services to employees dealing with personal or work-related problems that might impact their job performance, health and wellbeing. Ensure these services are well-advertised and easily accessible. Most EAPs can also provide proactive 'check-in' calls or onsite support to ensure staff at high risk are provided with support and coping strategies during the incident, rather than after.
5. **Regular communication:** keep lines of communication open before, during and after an incident. Regular updates (even where there is no new information) can help alleviate some of the stress that comes with uncertainty.
6. **Monitoring and check-ins:** working hours should be monitored, with time off scheduled during peak periods. Wellbeing check-ins should also be conducted. If leaders are going to be involved in high-stress activities with reduced sleep, ensure they have someone (either a leader not doing long hours or EAP/similar) undertaking regular check-ins.
7. **Flexible work arrangements:** during high-stress periods, allow flexible work arrangements to help staff balance their workload with other life responsibilities.
8. **Resourcing:** consider the potential for additional resourcing to assist through the crisis period to help manage high workload and demands.
9. **Post-incident support:** after the immediate threat has passed, continue providing resources for staff to cope with any lingering stress or trauma related to the incident—this could involve debriefing sessions or continued access to counselling services.

3 Andrew Reeves, Malcolm Pattinson and Marcus Butavicius, 'Is Your CISO Burnt Out Yet? Examining Demographic Differences in Workplace Burnout amongst Cyber Security Professionals' (2023) *Human Aspects of Information Security and Assurance* 11.

WHS regulatory activity and the management of psychosocial risks

Organisations have had a general safety obligation to manage psychological risks to their workforce for some time now. However, the risk of psychological injury arising out of factors present in the work environment has received significantly more focus in the past few years, particularly with the introduction of WHS regulations (in all states except Victoria) that specifically address psychosocial risk.

Under safety legislation, businesses must proactively identify psychosocial hazards arising from the workplace environment and put in place measures to control those hazards as far as is reasonably practicable.

Regulatory activity arising out of psychosocial risk factors has also increased. In some states, specialist psychosocial inspectors have been appointed and enforcement action arising out of alleged failures to manage psychosocial risk are becoming more common.

A recent example was the prosecution of the Court Services Victoria (CSV) following the death by suicide of one worker and numerous others taking stress leave. CSV, which is the independent statutory body that administers Victoria's court system, was sentenced in the Melbourne Magistrates' Court last year and fined $379,157 after earlier pleading guilty to failing to provide and maintain a safe workplace. The court heard that, from December 2015 to September 2018, workers at the Coroner's Court were at risk from exposure to traumatic materials, role conflict, high workloads and work demands, poor workplace relationships and inappropriate workplace behaviours.

The decision reflects the importance of organisations ensuring that, as far as is reasonably practicable, they identify risks inherent in the work their employees do every day, and implement effective control measures to prevent harm from arising. This obligation extends to the foreseeable stressors that could arise for staff in the event of a cyber incident.

Key contacts

Cyber

Valeska Bloch
Partner, Head of Cyber
T +61 2 9230 4030
Valeska.Bloch@allens.com.au

Gavin Smith
Partner, Co-head of Corporate, Head of Technology, Media and Telecommunications
T +61 2 9230 4891
Gavin.Smith@allens.com.au

Phil O'Sullivan
Partner
T +61 2 9230 4393
Phil.O'Sullivan@allens.com.au

David Rountree
Partner
T +61 7 3334 3368
David.Rountree@allens.com.au

Isabelle Guyot
Managing Associate
T +61 2 9230 4752
Isabelle.Guyot@allens.com.au

Lauren Holz
Senior Associate
T +61 2 9230 4283
Lauren.Holz@allens.com.au

Employment & Safety

Sam Betzien
Partner
T +61 7 3334 3091
Sam.Betzien@allens.com.au

Simon Dewberry
Partner
T +61 3 9613 8110
Simon.Dewberry@allens.com.au

Veronica Siow
Partner
T +61 2 9230 4135
Veronica.Siow@allens.com.au

Sikeli Ratu
Partner
T +61 2 9230 5046
Sikeli.Ratu@allens.com.au

Tarsha Gavin
Partner
T +61 2 9230 5181
Tarsha.Gavin@allens.com.au

If this guide has raised issues for you and you need information or support, please contact Lifeline on 13 11 14.

Allens is an independent partnership operating in alliance with Linklaters LLP.

19849D 3/24