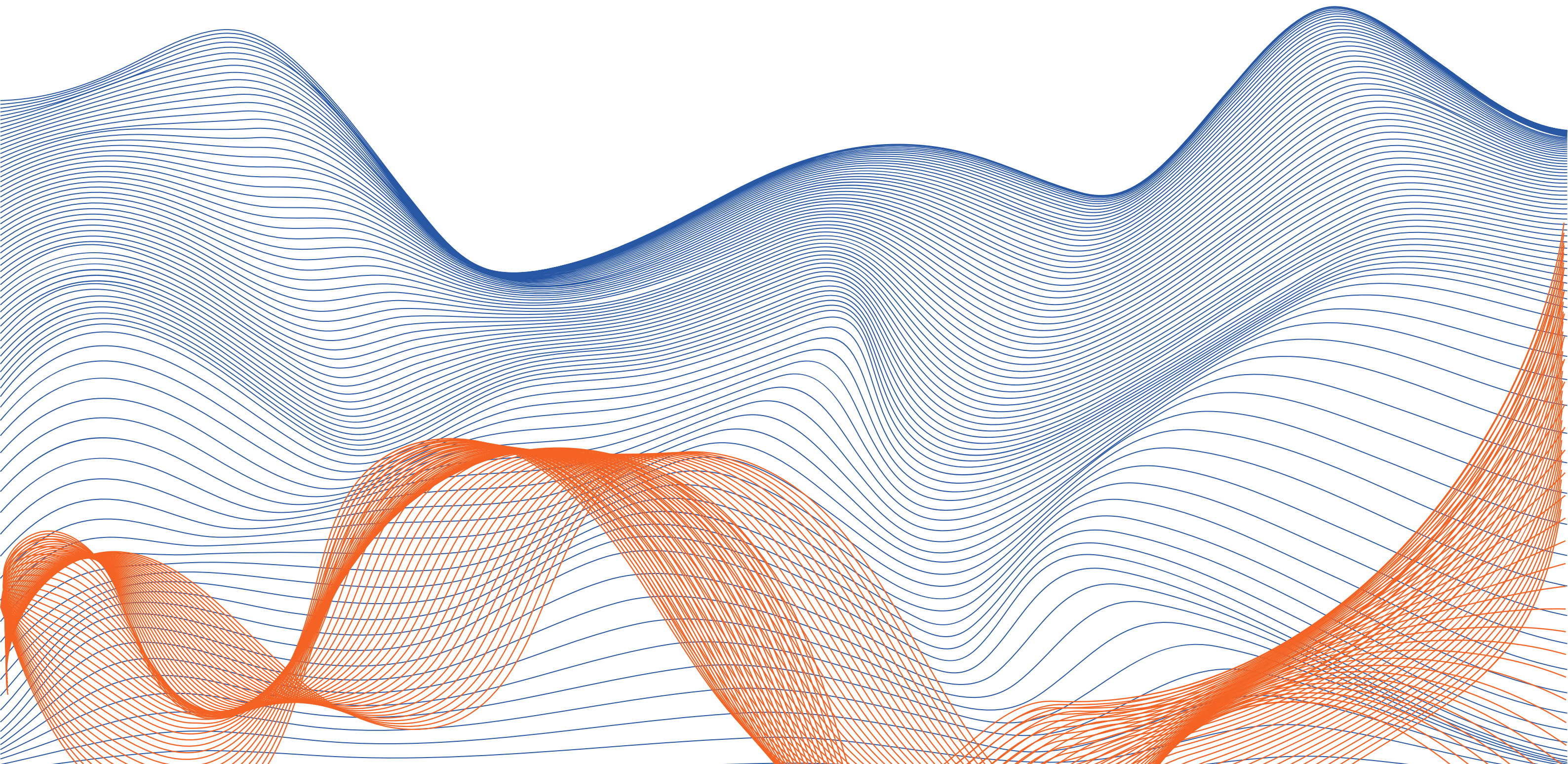
NORTHBRIDGE

BY VOIP PTY LTD

THE COST AND EFFECT OF POOR CYBER SECURITY MANAGEMENT

FY 24/25 LOCAL COUNCILS EDITION

PROTECT YOUR COMMUNITY DATA TODAY.



THE COST AND EFFECT OF POOR CYBER SECURITY MANAGEMENT

FY 24/25 LOCAL COUNCILS EDITION

INTRODUCTION

Neglecting to manage cybersecurity risks properly puts local councils at risk of experiencing extensive and potentially serious consequences.

In a world where cybercriminals are becoming increasingly sophisticated, the stakes have never been higher. Every moment without robust protection heightens the vulnerability of our communities, leaving personal information exposed and trust shattered.

Act now to prevent damaging impacts to your council and your community.

FINANCIAL IMPACTS

- A cyber incident can cost a medium-sized organization almost $100,000 each time it occurs, according to the Australian Cyber Security Center (ACSC).
- Poor cyber security measures can result in the theft of funds from council accounts.

DATA LOSS AND INFORMATION THEFT

- Insufficient cybersecurity is not just a minor oversight; it poses an imminent threat to councils, putting sensitive information at grave risk of theft.
- The potential compromise of personal data belonging to citizens and ratepayers isn’t a distant possibility—it’s a pressing reality that demands immediate attention.

SERVICE DISRUPTIONS

- Cyber attacks pose a significant threat, potentially crippling vital council services and infrastructure, leaving communities vulnerable and unprotected.
- The disruption could lead to severe delays in municipal services, waste collection, and payment portals, jeopardising the essential functions that keep our local government running smoothly.

SYSTEM COMPROMISE

- Inadequate security measures can result in devastating denial of access to essential technology systems, crippling vital operations and services.
- In the worst-case scenario, cyber attackers could seize control of council systems, putting sensitive data and community trust at grave risk.

DAMAGE OF COMMUNITY TRUST & REPUTATION

- Security breaches and data loss incidents can severely damage a council's reputation and erode public trust.
- This leads to a profound sense of vulnerability among constituents who rely on the council for their safety and well-being.

RECOVERY COSTS

- Councils face staggering financial repurcussions after a cyber incident.
- This includes potential legal liabilities and costs associated with recovery efforts, diverting valuable resources away from essential services and community development.

REGULATORY ISSUES

- Non-compliance with data risk regulations can lead to serious legal penalties and long-term reputational damage.
- Remediation and legal fees can reach millions, diverting resources from vital public services.

COMMUNITY IMPACT

- Community welfare is at stake when councils are compromised, severely impacting local communities and critical infrastructure.
- Compromise of essential services like healthcare and emergency response, and financial loss for local businesses, hindering economic growth.

STRENGTHEN YOUR DEFENCES TODAY FOR AN EMPOWERED TOMORROW

It's never too late to take charge.

Let us worry about the nitty gritty so you can focus on serving citizens who rely on you. By collaborating with a cyber defence accelerator like us, you can save both time and resources while reducing risks to the community.

Champion community trust, confidently.

ACCELERATE CYBER DEFENCE