Building Cyber Resilient Organisations: Beyond Technical Expertise

Rhiannon Taylor

17 July 2024

KEY ATTRIBUTES TO CYBER RESILIENCE

1. Develop a **Cyber Resilience Strategy** apart from or in partnership with an organisations Cyber Security Strategy

2. Obtain **Leadership Commitment** from the Board down

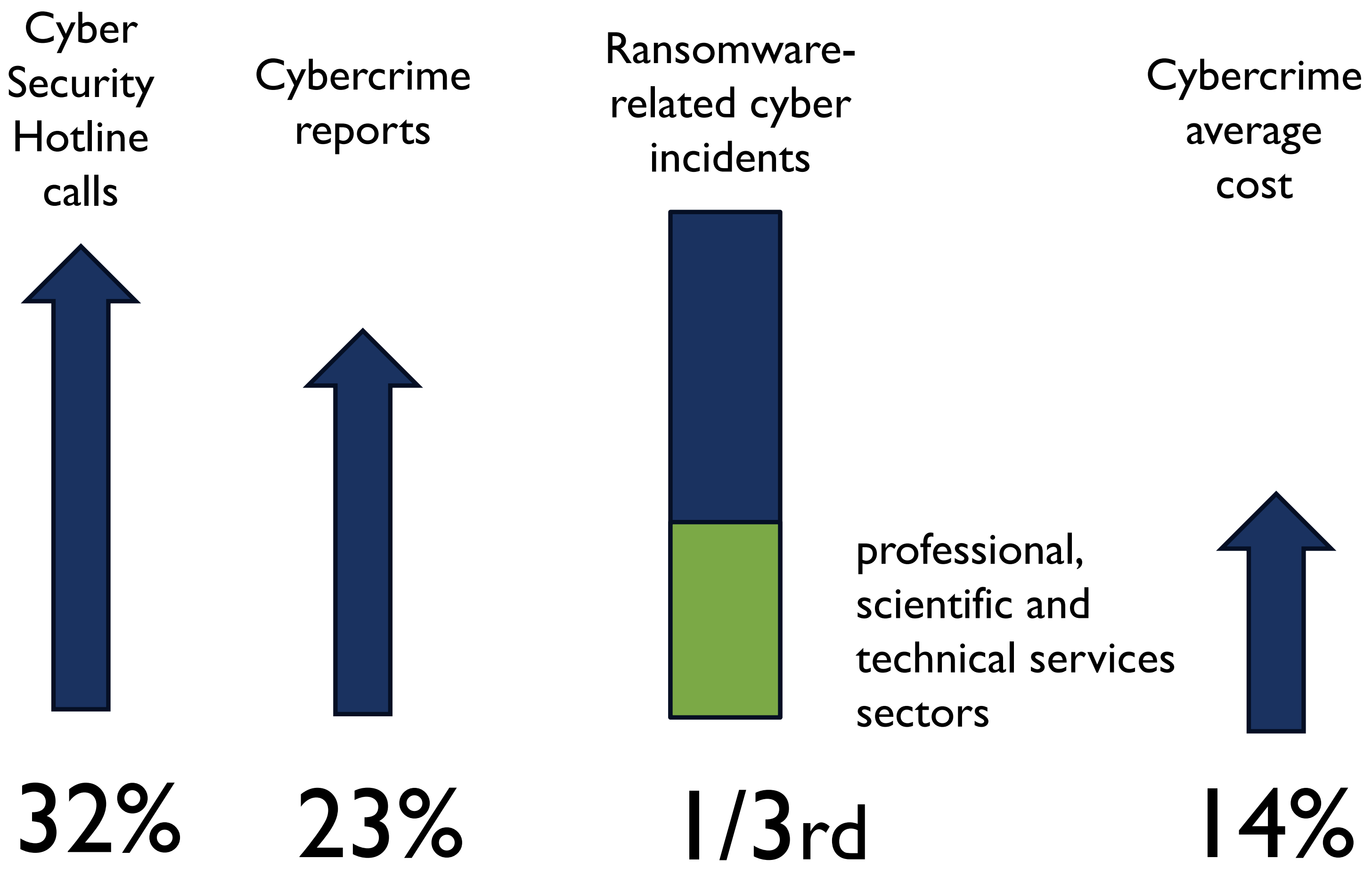
3. Develop a **Security Behaviour and Culture Program (SBCP)** and include human factors and a multidisciplinary approach to cyber resilience

INTRODUCTION

ASD Cyber Threat Report 2022-2023 reported that "…47% of Australians said they would close their account or stop using a product or service provided by an organisation that experienced a data breach."

CURRENT STATE - **2022-2023 ASD CYBER THREAT REPORT**

Almost **$80 million in losses** due to **business email compromise** fraud was self-reported to ReportCyber



Cyber Security Hotline calls

32%

Cybercrime reports

23%

Ransomware-related cyber incidents

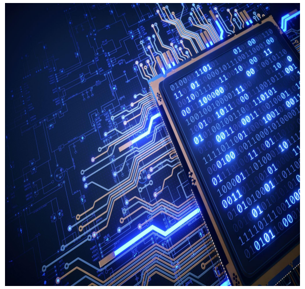
1/3rd

professional, scientific and technical services sectors

Cybercrime average cost

14%

FUTURE TRENDS – GARTNER TOP CYBERSECURITY TRENDS FOR 2024

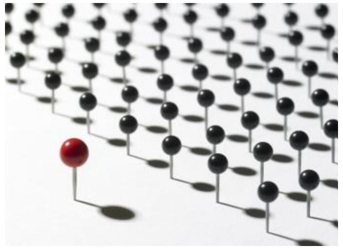


Generation AI

Outcome Driven Metrics (ODMs)

Security Behaviour and Culture Programs

Resilience Drive, resource-efficient 3rd party cyber security Risk Management



Continuous Threat Exposure Management (CTEM)

Extending the role of Identify & Access Management (IAM) to improve cyber outcomes

CYBER RESILIENCE AS A CULTURAL MINDSET

- Comprehensive Protection
- Human Factor Acknowledgement
- Adaptability and Agility
- Risk Management
- Organisational Resilience
- Reputation and Trust

CYBER RESILIENCE - LEADERSHIP & COLLABORATION

Leadership

- Demonstrating a **commitment** to cybersecurity
- Establishing **clear expectations** and accountability
- Fostering a **culture of security**
- Providing the **necessary resources, training, and support**

Collaboration and Communication

- Sharing threat intelligence and **security insights**
- Coordinating **incident response** efforts
- Aligning **cybersecurity initiatives**
- Building **strong partnerships** with external stakeholders

CYBER RESILIENCE - HUMAN FACTORS AND INTERDISCIPLINARY APPROACH

Human Factors

- Humans the weakest Link
- Humans the strongest Link
- Decision Making
- Human-Centric Approach
- Continuous Improvement

Interdisciplinary Approach

- Psychology
- Sociology
- Business Management

EXAMPLE

Organisation Vs Phishing Event

NEXT STEPS

1. Develop a **Cyber Resilience Strategy** apart from or in partnership with an organisations Cyber Security Strategy

2. Obtain **Leadership Commitment** from the Board down

3. Develop a **Security Behaviour and Culture Program (SBCP)** and include human factors and a multidisciplinary approach to cyber resilience

THANK YOU

E:mail
Rhiannon.taylor1234@gmail.com

Linked In:
https://www.linkedin.com/in/rhiannon-taylor1234/

QUESTIONS & ANSWERS