TAKE CONTROL OF THE UNEXPECTED:

ENHANCING CYBER INCIDENT EXCELLENCE THROUGH COMPREHENSIVE INCIDENT PLANS

An Integrated Approach to Managing Modern Cyber Threats

SIMONA DIMOVSKI:
www.linkedin.com/in/simona-dimovski-100/

SKYGRID INDUSTRIES:
www.skygridindustries.com.au

AGENDA

Understand the Landscape:

Explore various types of cyber attacks

Enhance Response Strategies:

Learn how to build and execute a comprehensive incident response plan.

Apply Best Practices:

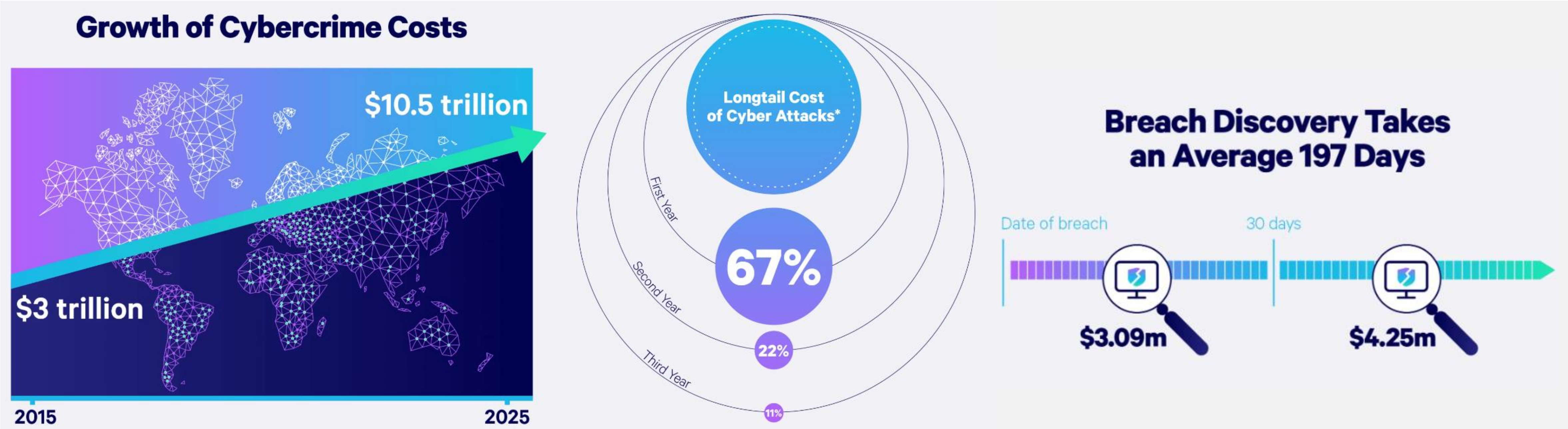
Discover actionable steps to improve crisis management in cyber events.

THE MODERN CYBER THREAT LANDSCAPE

Key Points:

- **Diverse Threats:** Modern cyber threats include ransomware, credential breaches, zero-day exploits, and insider threats.
- **Growing trends:** cybercrime is up 600% as a result of the Covid-19 pandemic. AI accelerates the attack frequency
- **Real risks:** Cyber attacks have been rated the fifth top rated risk, and have become a new norm across public and private sectors
- **Impact:** financial loss ($10.5 trillion worldwide), operational disruption, and reputational damage.

THE MODERN CYBER THREAT LANDSCAPE



A cyber incident at your organisation is a matter of “when” not “if”.

SIMONA DIMOVSKI: www.linkedin.com/in/simona-dimovski-100/
SKYGRID INDUSTRIES: www.skygridindustries.com.au

IT PAYS TO BE PREPARED FOR A CYBER INCIDENT

Why Incident Planning Matters:

Minimize Damage: A well-prepared plan helps reduce the impact of diverse threats.

Ensure Continuity: Effective management ensures business operations continue with minimal disruption.

Protect Stakeholders: Preserves the trust of customers, partners, and regulatory bodies.

Regulatory Compliance: Helps meet legal and compliance requirements.

SIMONA DIMOVSKI: www.linkedin.com/in/simona-dimovski-100/
SKYGRID INDUSTRIES: www.skygridindustries.com.au

KEY COMPONENTS OF A COMPREHENSIVE INCIDENT PLAN

The 6 steps of Incident Response:

1. **Preparation:** Develop policies, assemble a response team, and conduct regular training.
2. **Detection and Analysis:** Implement monitoring tools, set up alerts, and establish classification criteria.
3. **Containment:** Develop short-term and long-term strategies to control the situation.
4. **Eradication:** Identify and remove the threat, verify its removal, and apply necessary updates.
5. **Recovery:** Restore normal operations, monitor for reoccurrence, and communicate effectively.
6. **Lessons Learned:** Review the incident, update the plan, and share insights to prevent future occurrences.

SIMONA DIMOVSKI: www.linkedin.com/in/simona-dimovski-100/
SKYGRID INDUSTRIES: www.skygridindustries.com.au

COMMON FAILURES IN INCIDENT RESPONSE

Delayed Detection and Response: Many incidents suffered from delays in detecting breaches and initiating response measures. This often resulted in extended periods of exposure and greater damage.

Communication Failures: Inadequate or delayed communication with affected individuals, stakeholders, and the public was a recurring issue. Companies struggled with transparency and timely updates, affecting trust and reputation.

Vendor and Third-Party Management: Breaches involving third-party vendors highlighted weaknesses in managing and securing these relationships. Many companies lacked effective oversight and security measures for third-party services.

Coordination Issues: Effective incident response requires seamless coordination between internal teams and external parties (e.g., law enforcement, regulatory bodies). Many organizations faced difficulties in this area, leading to fragmented responses.

Inadequate Containment and Recovery Efforts: Failures in containment strategies and recovery efforts were common. Some organizations struggled with stopping the spread of the attack and restoring normal operations.

Public Relations Management: Managing public perception and media relations during a crisis was a significant challenge. Many companies faced criticism for their handling of media inquiries and public communications.

SIMONA DIMOVSKI: www.linkedin.com/in/simona-dimovski-100/
SKYGRID INDUSTRIES: www.skygridindustries.com.au

AUSTRALIAN BROADCASTING CORPORATION (ABC) DATA BREACH (2021)

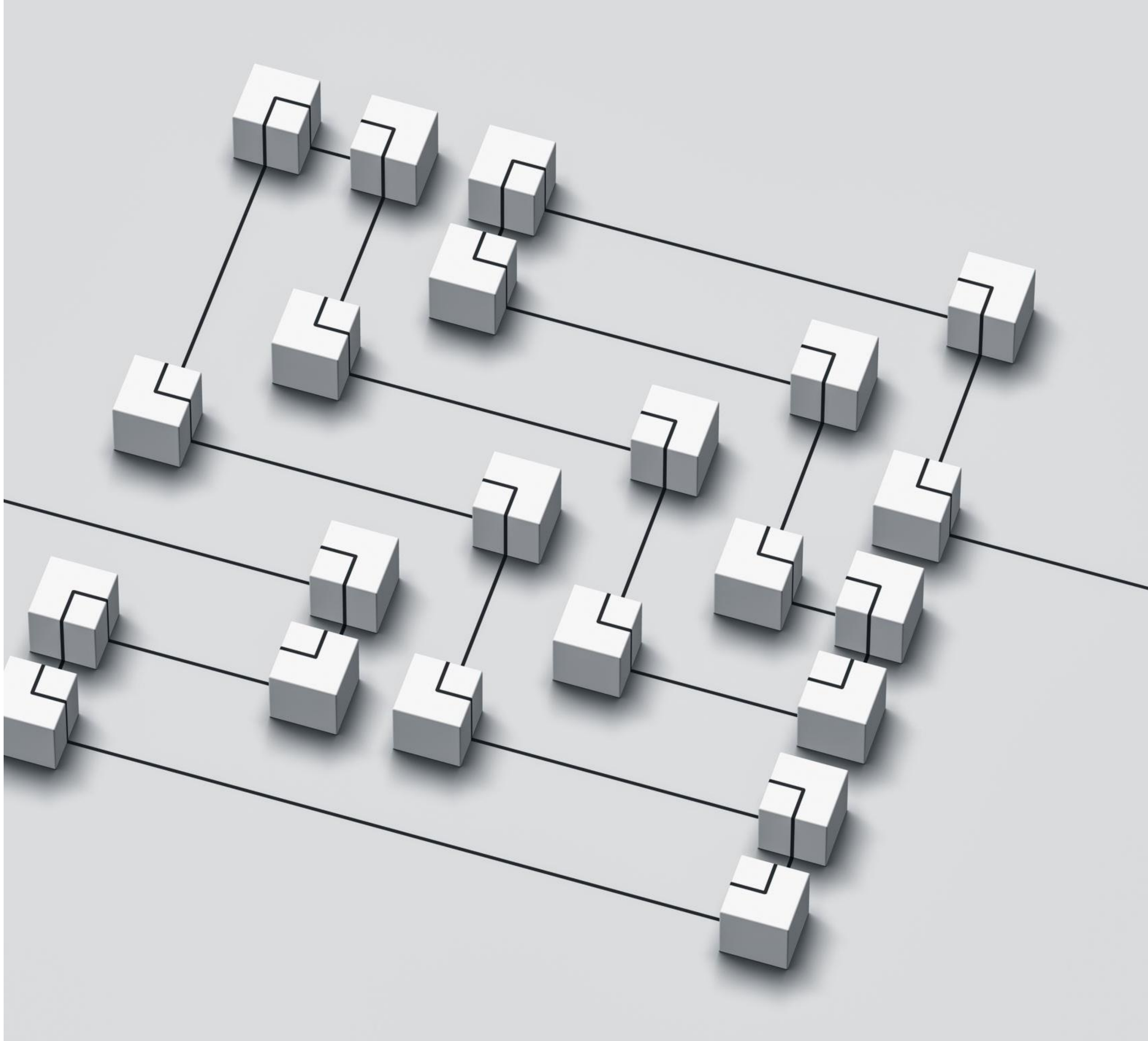
OPTUS DATA BREACH (2022)

MEDIBANK DATA BREACH (2022)

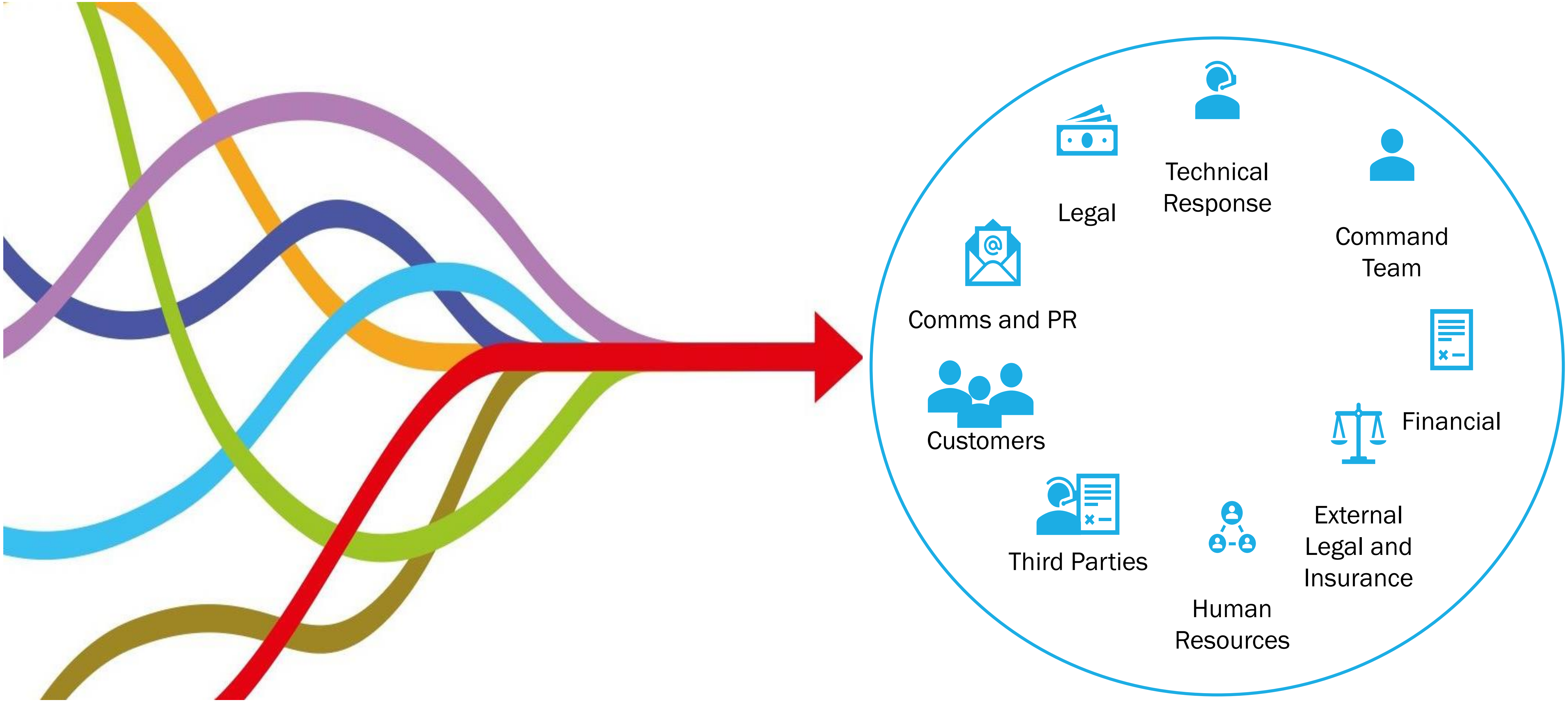
AUSTRALIA POST DATA BREACH (2023)

INTEGRATED FRAMEWORK FOR INCIDENT MANAGEMENT

- **Stream Integration:** Ensure coordination between all streams of work.
- **Comprehensive Planning:** Develop detailed plans for each stream.
- **Regular Drills:** Conduct regular exercises to test preparedness and coordination.



INTEGRATED FRAMEWORK FOR INCIDENT MANAGEMENT



Technical Response

Legal

Command Team

Comms and PR

Financial

Customers

External Legal and Insurance

Third Parties

Human Resources

SIMONA DIMOVSKI: www.linkedin.com/in/simona-dimovski-100/
SKYGRID INDUSTRIES: www.skygridindustries.com.au

INTEGRATED FRAMEWORK OVERVIEW

Develop Comprehensive Plans: Establish detailed plans for each stream, ensuring all components are addressed.

Coordinate Across Streams: Appoint a central coordinator to manage the incident. Ensure seamless coordination between all streams

Regular Training and Testing: Conduct regular drills and training for all teams to ensure preparedness and effective response.

Timely Communication: Implement clear and timely communication strategies for all stakeholders, including internal teams, customers and the public.

Continuous Improvement: Regularly review and update plans and procedures based on lessons learned from incidents and emerging threats.

SIMONA DIMOVSKI: www.linkedin.com/in/simona-dimovski-100/
SKYGRID INDUSTRIES: www.skygridindustries.com.au

PREPARATION STREAM

01

Policies and Procedures: Develop comprehensive incident response policies and procedures.

02

Incident Response Team: Establish a dedicated response team with defined roles and responsibilities.

03

Training and Drills: Conduct regular training and simulation exercises to prepare for various types of incidents.

04

Communication Protocols: Set up clear internal and external communication plans.

TECHNICAL RESPONSE TEAM

01

Detection Tools: Deploy advanced monitoring and detection tools to identify breaches early.

02

Containment Strategies: Develop and test strategies for immediate and long-term containment of incidents.

03

Eradication Procedures: Implement processes for removing threats and applying necessary updates.

04

Recovery Plans: Establish procedures for restoring normal operations and verifying system integrity.

LEGAL STREAM

01

Compliance: Ensure adherence to legal and regulatory requirements (e.g., GDPR, APRA CPS234, etc).

02

Documentation: Prepare templates for breach notifications and evidence handling.

03

Liaison: Maintain relationships with legal authorities and law enforcement.

04

Training: Regularly train legal teams on data protection laws and incident management.

HR STREAM

01

Internal Communication: Develop guidelines for informing and supporting employees during an incident.

02

Support Services: Provide counseling and support resources for affected employees.

03

Insider Threats: Implement measures to address potential insider threats and manage employee-related issues.

04

Training: Ensure employees are aware of their roles and responsibilities in incident response.

CUSTOMER STREAM

01

Analysis: Who are your customers and what do they need from you in a time of crisis. What customer data do you hold?

02

Notification: Inform affected customers promptly and transparently about the incident.

03

Support: Provide assistance, such as credit monitoring or identity theft protection, as needed.

04

Communication and Feedback Maintain clear channels for customer inquiries and feedback to improve response and recovery efforts.

COMMS AND PR STREAM

01

Communication Plans: Create templates and strategies for internal and external communication.

02

Spokesperson: Designate a trained spokesperson for handling media inquiries and public relations.

03

Social Media Monitoring: Implement procedures for monitoring and responding to social media activity related to the incident.

04

Regular Updates: Provide timely and transparent updates to stakeholders and the public.

THIRD PARTIES

01

Vendor Communication: Notify third-party vendors and partners who may be affected or involved in the incident.

02

Coordination: Work with third parties to manage and resolve the incident.

03

Security Review: Assess and enhance the security measures of third-party vendors**.**

04

Contractual Obligations: Ensure compliance with contractual obligations and review third-party agreements

COMMAND TEAM

01

Coordination: Set up a command center or incident management team for overseeing response efforts.

02

Decision-Making: Develop a decision-making framework for allocating resources and making high-level decisions.

03

Reporting: Create protocols for reporting to the executive team and board.

04

Regular Reviews: Conduct regular reviews and updates of the incident management plan

FINANCIAL STREAM

01

Coordination: Set up a command center or incident management team for overseeing response efforts.

02

Decision-Making: Develop a decision-making framework for allocating resources and making high-level decisions.

03

Reporting: Create protocols for reporting to the executive team and board.

04

Regular Reviews: Conduct regular reviews and updates of the incident management plan

EXTERNAL LEGAL AND INSURANCE STREAM

01

Engagement: Establish relationships with external legal advisors and insurance providers.

02

Coverage Review: Regularly review and understand insurance coverage and limits.

03

Claims Management: Develop processes for filing and managing insurance claims.

04

Compliance: Ensure compliance with external legal requirements and industry standards

HOW DO YOU DO ALL OF THIS?

- Assess what you need to uplift first
- Don’t’ try and do it all at once, chunk it down – focus on one stream at a time
- Figure out what you can do inhouse and what you need to bring in external help
- Establish a working group to support you, you will need people power with the right skills to do this right
- Tackle the highest gaps / most burning needs first
- Consider bringing in a third party to do the heavy lifting and accelerate the uplift
- Reach out to me after this presentation if you have specific questions about how I can assist your organisation

Questions