Strategic Security Review
CitiPower and Powercor
June 2019

Important Notice

Inherent Limitations

This report, which has been prepared at the request of CitiPower and Powercor (CitiPower/Powercor) provides a summary of Bellrock Group findings during the work undertaken, consistent with the scope in our engagement contract.

The services provided in connection with this engagement comprise of an advisory engagement, which is not subject to Australian Auditing Standards or Australian Standards on Review or Assurance Engagements, and consequently, no opinions or conclusions intended to convey assurance have been expressed.

Bellrock Group has taken reasonable steps to ensure the accuracy of information provided but cannot warranty completeness, accuracy or reliability in relation to the statements and representations made by, and the information and documentation provided by, CitiPower/Powercor representatives or other personnel consulted as part of the process.

Bellrock Group has indicated within this report the sources of the information provided where appropriate. We have not sought to independently verify those sources, unless otherwise noted within the report. Where we have provided quotes within the report, they are not attributed to persons to preserve anonymity. Where quotes are included from external sources they are attributed accordingly.

This report is prepared solely for the purpose set out in the introduction to this report and is not to be used for any other purpose without Bellrock Groups prior written consent. Other than our responsibility to CitiPower/Powercor, neither Bellrock Group nor its employees undertake responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility.

Bellrock Risk & Special Services | ABN 84 169 225 343
41 – 47 Thomsons Road, Keilor Park, VIC, Australia, 3043
T: 61 1800 273 732 | E: connect@bellrockgroup.com.au | W: bellrockgroup.com.au

Contents

1 EXECUTIVE SUMMARY

Bellrock Group was appointed by CitiPower/Powercor to undertake a Strategic Security Review of their critical assets located across Victoria.

The objective of the Review was to analyse the overall security program (including strategy and delivery methodology) and provide recommendations to improve the program, where appropriate. This encompassed security related threats (internal and external sources), security systems (access control, detection and surveillance), hardware systems, security model, security awareness and stakeholder sessions.

This Review was conducted between January and May 2019 and focused on site reviews, benchmarking, stakeholder interviews, analysis of current strategies and procedural documentation. This was supplemented by consideration of forward-looking analysis of crisis scenarios.

CitiPower/Powercor are focused on improving its security capability through investment into operational elements, development of technology and improving its security model. Currently, CitiPower/Powercor are managing some risks well with good controls in place (for those specific risks) and is recognised as having a strong commitment from the Executive and Board to improve its security program and underlying culture.

However, the Review identified there are some gaps and a lower level of maturity when assessed against the industry and some high security risks across CitiPower/Powercor. This places CitiPower/Powercor at a higher level of risk, potential increased costs, lower operational effectiveness and increased reputation risk, compared to its peers.

The Review determined that CitiPower/Powercor are behind industry benchmarks for a mature and contemporary security level, including:

- Strategy and Delivery Methodology – CitiPower/Powercor have limited security documentation and systems in place (for example, security strategy, standards or security risk methodology); however, it does have some security operating procedures;
- Security Model – CitiPower/Powercor does not have the appropriate capability or resources to develop, implement and maintain a contemporary security program;
- Security Assets – Current security infrastructure is deemed not fully effective due to failures, damaged assets, non-integrated systems and limited detection and response capability; and
- Security Awareness - No formal internal stakeholder plans or sessions are in place and no training and awareness programs were observed.

This Review has identified several areas of focus that will assist CitiPower/Powercor in creating a contemporary and commercially aware security capability, focusing on improving customer and colleague service, reducing costs and risks, increasing stakeholder engagement and enhancing the security program.

Key recommends are detailed in Section2 ‘Recommendations’.

1.1 RISKS

A comprehensive assessment of relevant threats and weaknesses was conducted throughout the facilities. Consistent with progressive risk management practice, these exposures have been prioritised in terms of risk (ranging from Negligible to Extreme). The following risks are deemed to be ‘High - Extreme’ and therefore subject to priority treatment:

- Position and Structure;
- Systems and Procedures;

- Electronic Security;
- Security Resourcing;
- Locking Systems;
- Security Culture;
- Abusive & Threatening Behaviour; and
- Theft.

1.2 Risk Scenarios

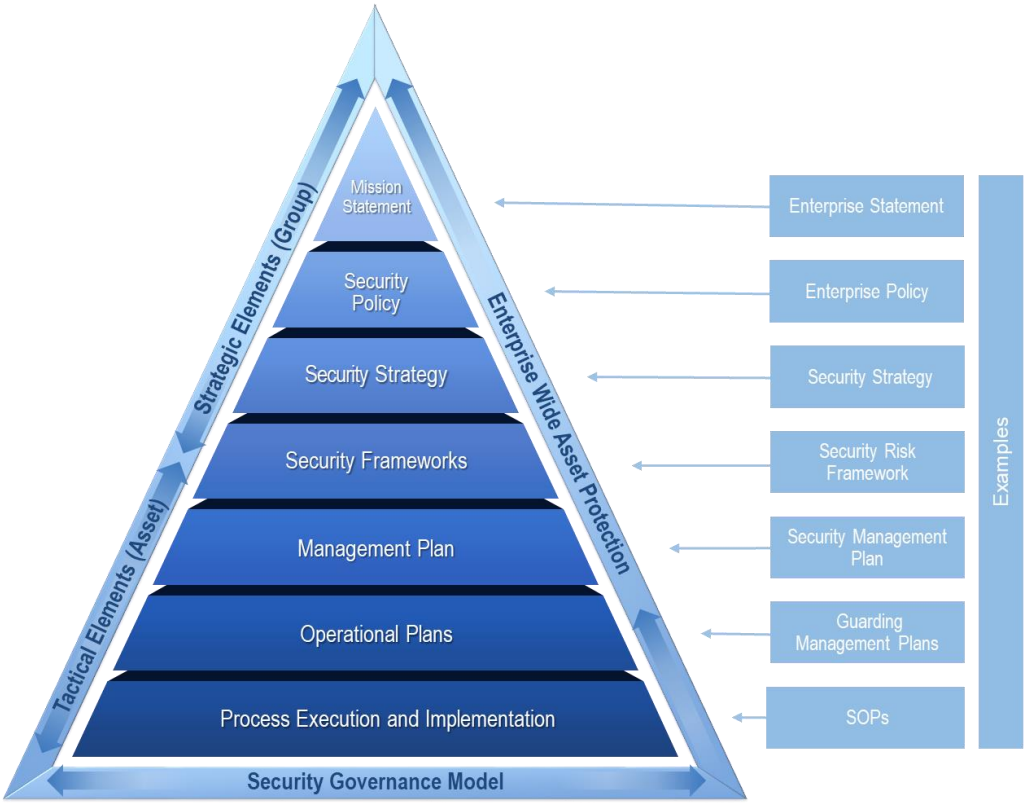
The Scenario Analysis provides an understanding of potentially critical events that could impact upon CitiPower/Powercor and its associated businesses. This is not intended to be a prediction of these events. Instead, it is a forward-looking understanding of the implications of these events to enable CitiPower/Powercor to plan an appropriate response.

The following risk scenarios were identified:

- Suspicious Package Delivered; and
- Asset breach of Zone Substation.

1.3 Approach

It is recommended that CitiPower/Powercor implements a governance model designed to link strategic objectives, frameworks, operational plans and process execution. The governance model is used as a virtual structure to define their approach for strategy, frameworks, management plans and operational procedures. Bellrock Group has designed a model that CitiPower/Powercor can implement to achieve this:



1.4 Risk Dashboard

Bellrock Partners Security Risk Dashboard

Key Risks

Environment Risk	Security Risk	Integrity Risk	Political Risk
			
Prioritised Rating – Extreme Risk	Priority Rating – Extreme Risk	Priority Rating – High Risk	Priority Rating – Moderate Risk
Position, Utilities, Demo-graphics, Ecology	Systems, People, Property, Business Interruption	Internal Theft, External Theft	Anti-Social Behaviour, Civil Disorder, Terrorism
Key Observations:. • Easy access into critical assets. • Significant fencing issues allowing open access to critical assets. • Property neighbours are increasing the vulnerability to CitiPower/Powercor assets. • Asset spread is vast causing limitation for security provider options.	**Key Observations:** • There is no formal security policy, strategy or security risk framework. • No formal security standards or risk methodology for assets and key systems. • No technology standards or specifications. • There is no technology roadmap in place for Security infrastructure.	**Key Observations:** • Significant asset breaches and theft incidents • Over 30 incidents since January 1, 2019. • Average security loss is $1300. • Anecdotal evidence indicates incident numbers are higher than what is being reported.	**Key Observations:** • No material protesting have occurred. • Generally staff and contractor behaviour is appropriate. • Security profile needs to lift across the enterprise.
Key Recommendations: • Develop a strategic plan to address incidents at a macro level. • Deploy / upgrade fencing to all critical assets. • Combine security contracts into one provider. • Implement a dedicated security control room to manage and respond to incidents. • Implement an agreement with a security provider to respond to all assets.	**Key Recommendations:** • Implement a security policy. • Implement a security strategy (DRAFT), focusing on service quality, financials, risks and incident reduction. • Implement a security management plan for CitiPower/Powercor. • Deploy two additional resources focused on security strategy and operational requirements.	**Key Recommendations:.** • Implementation of a theft and security awareness campaign. • Install surveillance systems to deter and detect would be offenders. • Deploy a copper theft / crime prevention plan focused on deterrence using a copper marking product (E.g. DataTrace) and extensive signage. • Deploy intruder detection systems	**Key Recommendations:.** • No immediate treatment is required. • Risks should be placed in a monitor and awareness state. Improvements should be captured within standard business practices.

2 RECOMMENDATIONS

This Review has identified that CitiPower/Powercor have significant opportunities to improve in delivering a security program that achieves best practice outcomes for the industry in which it operates. The Review has identified areas of focus that will assist the enterprise create a contemporary and commercially aware security capability, focusing on improved asset protection, reducing risks, increasing stakeholder engagement and enhancing the security for supply of energy to the community.

A full and extensive list of the observations and recommendation is provided at section 7.5 of the report. Further, the priority attributed to the action has been highlighted.

Several key recommendations have been provided for consideration.

Adoption of these recommendations will result in a safer experience for CitiPower/Powercor and an improvement in the organisational security maturity level.

Key recommendations are:

1. *Implement a strategic approach for CitiPower/Powercor Security.*

   This will include incorporating an overarching framework including security strategy and plans, operational plan, risk methodology, technology roadmap, investment plan and governance model (including executive reporting). The plan should detail return on investment/reduction of risk for capital investments.

   Rationale

   Lack of documented plans, strategies and policies are considered a high-risk factor for the enterprise. Clear and concise frameworks and structures will ensure a robust blueprint and provide direction for security operations going forward.

2. *Implement a structured security management team (2 x FTE) to meet the needs of the CitiPower/Powercor in achieving an effective and proactive security program.*

   Deployment of a Security Director reporting to the Head of Risk to establish and implement the security framework and system (contract for 12 months) and a Security Manager (ongoing role) reporting to the Group Real Estate Manager for all operational security contracts and matters.

   Rationale

   The current security management staffing model is not sufficiently resourced to deliver the security program required for CitiPower/Powercor.

3. *Implement a dedicated security presence / control room.*

   Currently numerous assets and alarms are going unmonitored from the security systems, increasing the risk to CitiPower/Powercor and the community.

   Rationale

   It is expected that numerous alarms and site breaches are being missed, not actioned or responded to. This increases the risk to the supply of electricity to the community and a health and safety risk to staff and the public.

4. *Enhance critical asset protection (fencing)*

   Implement an anti-climb fence to all critical assets; Zone Substations (ZSS) and depots.

   Rationale

   It is expected that individuals will try and breach critical assets for different reasons (theft, disruption, vandalism). Breach of these assets could cause significant harm to individuals, the community or a safety risk to staff.

5. *Address the weaknesses in the current CCTV coverage and systems.*

   Deploy additional surveillance equipment to all ZSS and uplift the coverage on depots to include all entry/exits, high risk and volume areas and the property perimeter. Each system should be aligned to one enterprise solution.

   Rationale

   Currently numerous critical assets are not support by surveillance systems (ZSS). Furthermore, operational areas (depots) have limited coverage.

6. *Deploy a detection capability*

   Deploy a detection capability for critical assets (ZSS) covering perimeter line, external doors to switching room and internal motion detection. Furthermore, enhance current systems at depots to include all sheds and operational areas. All systems should be monitored via the new control room.

   Rationale

   It is expected that individuals will try and breach critical assets for different reasons (theft, disruption, vandalism). The current security program will not detect or have the ability to respond affectively to a breach.

7. *Integrate duress facilities and uniform response processes.*

   Deploy duress facilities to all customer focused areas (for example, reception areas) and develop response procedures.

   Rationale

   Several differing approaches and procedures apply to duress response. A process needs to be developed to ensure all duress alarms and activity is managed consistently and appropriately.

8. *Improve awareness of personal safety for all users.*

   Develop a dedicated security awareness program for all staff/contractors.

   Rationale

   All staff have a role to play in ensuring the facilities are as safe as possible. Engaging with and educating staff/contractors to highlight how they can contribute to enhance the security culture will ensure personal safety is improved for all.

9. *Upgrade lighting in critical areas.*

   Deploy security lighting into ZSS to be active on alarm and across the perimeter areas of depots.

   Rationale

   Enhance the deterrence, detection and response capability to a breach or attempted security incident.

10. *Installation of a new keying system (current key patent expires 2019).*

    Replace all keying systems for electrical assets.

    Rationale

    The system keying that CitiPower/Powercor's has in place has it patent set to expire in 2019. This eliminates the contract of key management and significantly increases the risk to assets.

11. *Implementation of Copper Theft Plan*

    Development and deployment of a specific Copper Theft Plan including key risk indicators, performance factors and improvement security controls.

    Rationale

    Since 2012, there has been more than 400 reported incidences of copper theft across CitiPower/Powercor and more than 30 since January 1, 2019. Additionally, we anticipate this problem to expand, which exposes serious risk to the safety of workers and the communities and increases the supply risk to the community.

3 CONTEXT AND FRAMEWORK

3.1 PROJECT OBJECTIVES

The purpose of this Review was to provide CitiPower/Powercor assistance in strengthening their current security management framework and processes with the aim of reducing the number of security incidents and improve the management of break-ins, theft and unauthorised entry across their network commercial assets.

3.2 PROJECT SCOPE

The scope of the Review is to includes to undertake a review of the physical security of the network and commercial assets as per below

- All depots and offices (approximately 20);
- All zone substations (approximately 134);
- Selected underground / indoor distribution substations in high-risk areas;
- Selected construction project sites in high-risk areas;
- Subsequently, provide detailed advice on the following;
    - Security breaches / gaps across the above assets when compared to best practice;
    - A practical operating model with clear roles and responsibilities to manage physical security efficiently and effectively;
    - A prioritised program of work to close security breaches / gaps as identified through the physical security inspections; and
    - Additional standards, policies and procedures required to improve the management of security.

3.3 REVIEW METHOD

The review method was based on the following elements:

Stage 1: Survey

Stage 2: Data Collection

Stage 3: Data Analysis

Stage 4: Stakeholder Interviews

Stage 5: Risk Assessment and Evaluation

Stage 6: Reporting

3.3.1 Survey Design

This stage of the engagement involved the selection of a group of comparable companies and the design of the survey questions, including numerous infrastructure companies from the 26 participants. Bellrock Group developed a series of Security Risk and Security Management Indicators that drew on the following material:

- Bellrock Group' security risk and security management experience.
- CitiPower and Powercor's criteria that identified relevant areas of focus and examination.

The above factors were used to design a detailed survey to provide insight into the participating organisations' approach to security risk and security management.

3.4 Data Analysis

3.4.1 Data Interrogation

The Review was undertaken by the global network of Bellrock Group' offices and representatives and coordinated and consolidated by the Head Office team in Melbourne. This entailed identifying appropriate sources of data from the selected organisations involved in the Review.

3.5 Reporting

CitiPower and Powercor's security policies and processes were assessed against the participating organisations. This analysis focused on relevant factors contained in the survey. The results of the survey and Bellrock Group' analysis of the data and considerations are presented in this report.

3.6 Review Inclusions

The following criteria form the framework of the assessment:

- Identification, evaluation and treatment recommendations of threats, strengths and critical scenarios related to Environment, Security, Integrity and Political risk factors (refer to Appendix 1 - Risk Taxonomy for further details on risk factors);
- Reference to relevant policies/procedures and applicable risk standards, guidelines and statistics (refer to Section 3.11 - Reference Material for further detail).

3.7 Review Exclusions

The following factors are excluded from the scope of this report:

- Third party contractor security risk standards, practices and exposures; and
- Information Technology risks.

3.8 Stakeholder Input

The following CitiPower/Powercor personnel have provided input to this project:

Stakeholder	Role
Steven Murray	Head of Procurement and Property
Terry Duncan	Strategy, Programs and Change Manager
James Rennick	Manager Network Facilities
Ben Smith	Group Workplace Services Manager
Tanveer Ali	Category Manager - Indirect Products & Services
Amanda Williams	Risk & Internal Audit Manager
Stuart Johnson	Network Facilities Specialist
Nathan Herring	Network Facilities Specialist
Peter Daley	Network Facilities Specialist
Ian Bloomer	Network Facilities Specialist
Cameron Bell	Network Facilities Specialist

3.9 Reference Material

The following documents and data have been used as relevant references for this report:

- Attachment 1 – Break-in Register
- Attachment 2 – Unauthorised Access Statistics
- Attachment 3 – Locations Security Review
- Attachment 4 – ENA Guidelines
- Audit Findings – Asset Inspection and Maintenance
- Business Case Recommendations (UE)
- Critical Infrastructure Business Case
- DRAFT – UE Network Infrastructure Security Guide
- DRAFT – UE Authorised Access AFAP
- Organisational Structure
- Risk Report Summary – Extract for Security Related Risk
- Security Review 2019 Security Assets
- Services Rates
- UE AFAP EN301-16-2018 Sensor Lights ZSS
- UE AFAP EN301-18-2018 Electronic Keys ZSS
- UE AFAP EN301-22-2018 CCTV Zone Construction Sites
- Zone Substations – Security Guidelines
- 2018 ZSS Customers
- Australian Standard AS/NZS ISO 31000:2018 – Risk Management – Principals and Guidelines
- International Standard SO/IEC 31010:2018 Risk Management – Risk Assessment Techniques
- Standards Australia HB 167:2006 – Security Risk Management
- Standards Australia HB 292:2006 – Business Continuity Management
- ISO 22300:2012 Societal Security – Terminology
- Various security and risk industry associations

4 BELLROCK GROUP SECURITY RISK MODEL

The Bellrock Group Security Risk Model incorporates the current leading thinking on risk practices and philosophy. To this end, our model encompasses extensive risks that could impact CitiPower/Powercor and covers the full continuum of threats, ranging from negligible to catastrophic, whilst recognising inherent strengths and opportunities.

4.1 RISK IDENTIFICATION

Bellrock Group identifies Enterprise Security Risk in the following risk classes:

- Environment Risk;
- Security Risk;
- Integrity Risk; and
- Political Risk.

These classes of risk and their accompanying risk factors provide a comprehensive and robust identification of threats and strengths within the environment.

Please refer to Appendix 1 - Risk Taxonomy for a detailed list of all the risk factors.

4.2 RISK EVALUATION

Bellrock Group adopt the criteria of Likelihood and Impact to evaluate relevant threats.

Please refer to Appendix 2 - Risk Matrix for an illustration of risk ratings.

4.2.1 Risk Likelihood

The Likelihood Rating considers the following factors for each threat:

- Internal historical data, based on reported incidents and anecdotal information;
- External historical data from similar industries; and
- The opportunity for the threat to arise, based on internal controls and external circumstances.

Please refer to Appendix 3 - Risk Likelihood Criteria for detailed explanation.

4.2.2 Risk Impact

The Impact Rating considers the potential tangible and intangible effects of threats that can materialise, in the form of:

- Financial Loss;
- Business Disruption;
- Reputational Damage;
- Legal Liability;
- Environment and Community;
- Employees; and
- Health and Safety.

Please refer to Appendix 4 - Risk Impact Criteria for a detailed explanation.

4.1 SCENARIO ANALYSIS

Scenario Analysis is used to complement the evaluation of potential major or extreme risks that are difficult to capture with standard assessment processes that tend to focus on historical incidents and current/prevailing risk circumstances. This can enable CitiPower/Powercor to better foresee highly disruptive events and plan accordingly.

The Scenario Analysis process creates a set of shared expectations for the future and consists of two main phases:

- Identifying criticalities and building alternate scenarios about the future; and
- Understanding the impact of these scenarios and determining a response.

Please refer to Appendix 5, Scenario Analysis & Emerging Threat Matrix for a detailed explanation.

4.2 RISK TREATMENT

The Risk Treatment phase of the process seeks to prioritise the management of the most important threats (Extreme and High), whilst establishing a process to monitor the less imperative exposures (Moderate, Low and Negligible). Extreme and High Risks are managed in the following manner:

Risk Treatment & Accountability:	Detailed recommendations for the comprehensive treatment of the risk in question and nomination of accountable persons.
Key Benefits:	Detailed explanation of how the proposed treatment will reduce the threat level of the risk.
Best Practice Standard:	Description of the external benchmark and best practice standards that may apply to the risk in question.
Timeframe:	Definition of the timing for the treatment (higher the risk, greater the priority), with due consideration to organisational resources/logistics.
Performance Indicators:	Explanation of how the accountable persons should monitor the treatment to ensure appropriate progress and meeting of objectives.

4.3 RISK TERMINOLOGY

The risk related terminology used throughout this report is based on the meanings contained in ISO 22300:2012 Societal Security – Terminology.

Please refer to Appendix 6 - Glossary for detailed list of terms and meanings.

5 BENCHMARKING

The Data Analysis section presents information and insights gathered through the analysis of:

- CitiPower/Powercor documented information;
- The benchmarking survey;
- Research; and
- Stakeholder feedback.

5.1 CITIPOWER/POWERCOR DATA

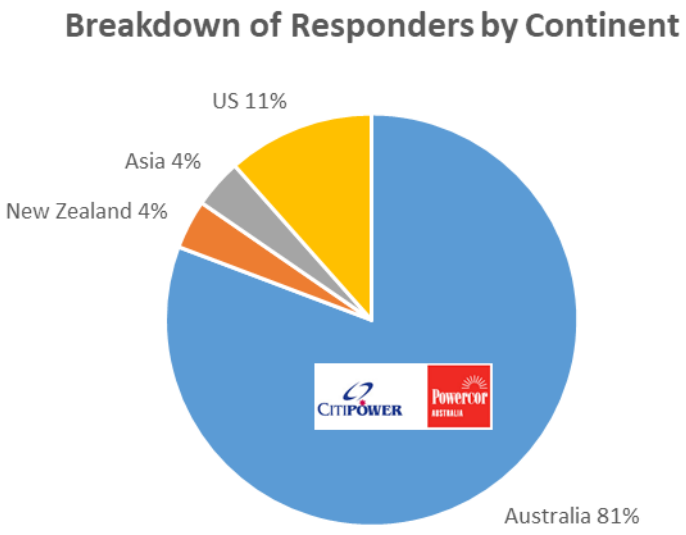
CitiPower/Powercor supplied documentation and stakeholder sessions and identified valuable indicators and factors that were used to develop the survey and data valuation.

5.2 GLOBAL SURVEY

A total of 26 organisations took part in the benchmarking survey. This section presents a profile of those organisations and key information and insights gathered from the survey and interview process.

5.2.1 Demographics of Participating Organisations

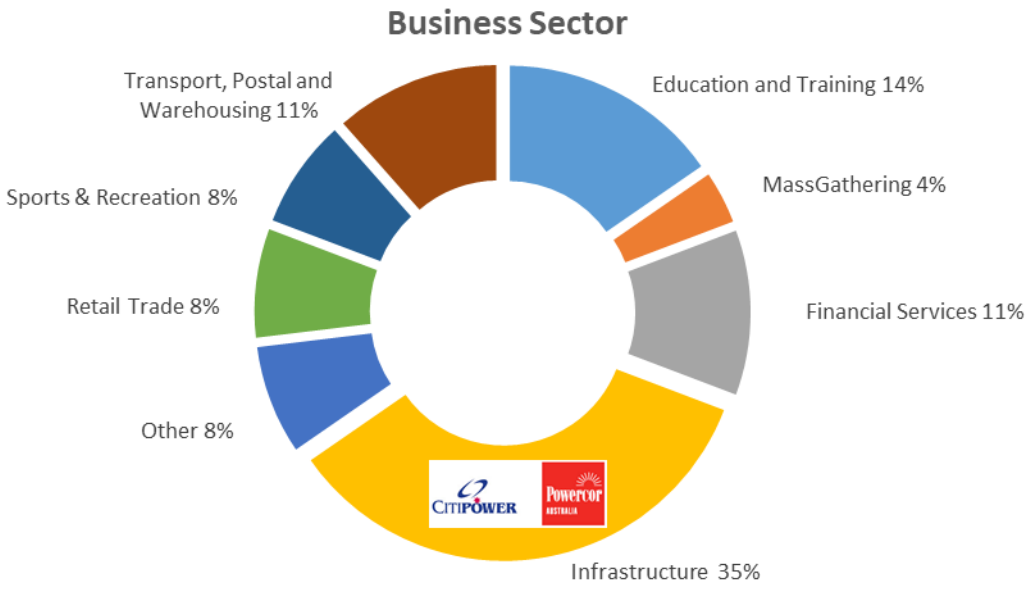
Bellrock Group ensured that the survey included international and Australian organisations. The Head Office for 81% of participating organisations was in Australia, 11% in the United States of America and 4% each in New Zealand and Asia.



5.2.2 Business Sector

Organisations from multiple industries were invited to participate in the survey, with a focus on achieving a broad range of views.

Of the participating organisations, the majority were from the Infrastructure / Services industry (35%), Education and Training (14%), Transport, Postal and Warehousing (11%) and Financial Services (11%) sectors.

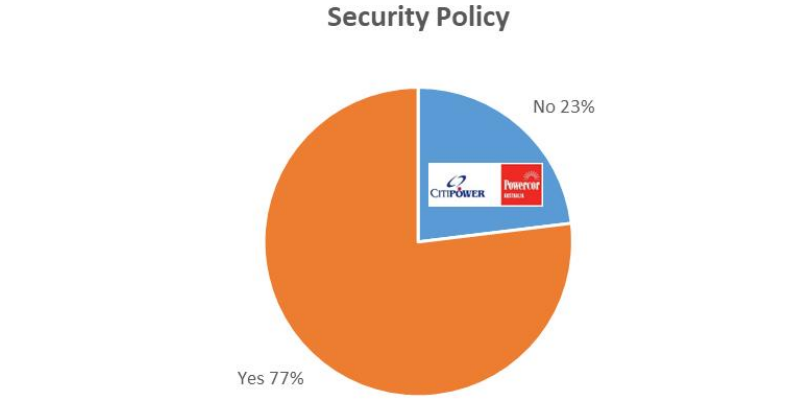


Key Points and Observations

- Participants included several energy / utility providers from across Australia.

5.2.3 Policy Support and Objectives

The vast majority of firms benchmarked have dedicated security policies (77%). Furthermore, analysis indicated that firms evaluated the effectiveness of the policy based on the reduction of threats, risk and critical incidences, rather than cost reduction.



Key Points and Observations	Risk Exposure – High (see section 7.3.2)

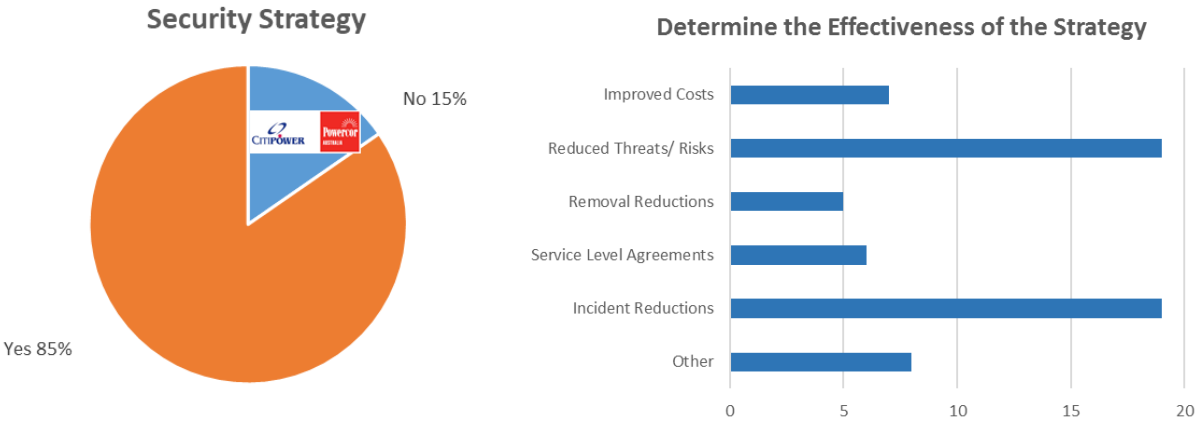
- CitiPower/Powercor doesn't have a specific Security Policy with set principles aligning to the organisation's strategy plan or vision. This is not in line with industry best practice and below current expectations of a mature and integrated security capability.

5.2.4 Security Strategy

From the review, 85% of organisations responded to having a set Security Strategy, encompassing the entire organisation, including people, information and assets.

Majority of these organisations also included Key Performance Indicators (KPIs) to assess the effectiveness of the Strategy. Key factors included:

- Improved costs;
- Reduction in risk and threats;
- Incident processes; and
- Service Level Agreements.



Note – Scale is per respondent and respondents could select multiple options.

Organisations which participated in the survey responded that their Security Strategy is reviewed at least annually, with set objectives for the next 3 years (88%).

The majority of firms which participated in the survey indicated that the structure of their Security Strategy revolved around the management of outsourced providers to:

- Improve costs;
- Increase service quality;
- Reduce risk; and
- Integrate technology to improve processes and security.

Furthermore, data indicated that many organisations had internal emergency management, loss prevention strategies and conducted internal investigations, if necessary. The majority of the security initiatives tended to focus on training and communication programs, compared to capital or staff costs; which is evidence of mature programs.

Key Points and Observations	Risk Exposure – High (see section 7.3.2)

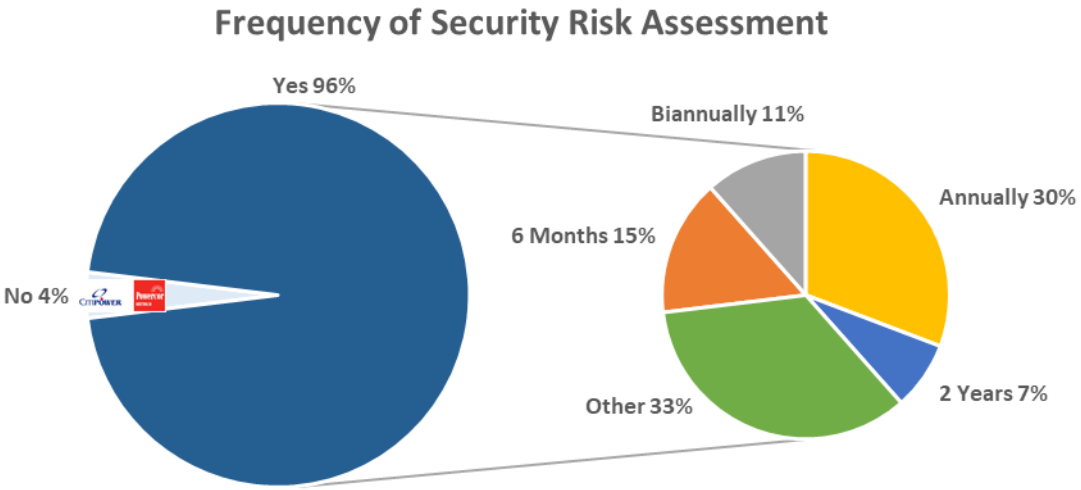
- CitiPower/Powercor doesn't have a set Security Strategy which defines its set objectives, capabilities, risks or opportunities that are aligned to the enterprise plan. This places CitiPower/Powercor at a higher risk of exposure through invalidated metrics, potential increased costs and risks and reduced insight into incidents.
- Benchmarking analysis had 73% of organisations reviewing more frequently than annually, excluding post incident.

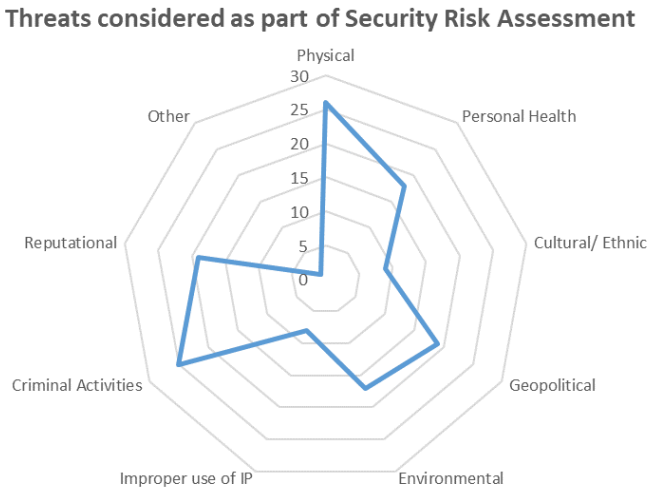
The core themes for the procedures were identified as:

- Improved costs;
- Incident management response;
- Mature processes;
- Integrated processes with emergency and crisis management;
- Outsourced specialist process elements; and
- Insight into support organisation to improve service delivery (e.g. Guarding providers).

5.2.5 Security Risk

Of the organisations that completed the survey, over 96% conducted a formal and scheduled Security Risk Assessment of their facilities. Analysis of this figure indicates that firms vary in their frequency of completing Security Risk Assessments. However, 54% complete annually or more frequently, whereas, CitiPower/Powercor does not have a set program in place.



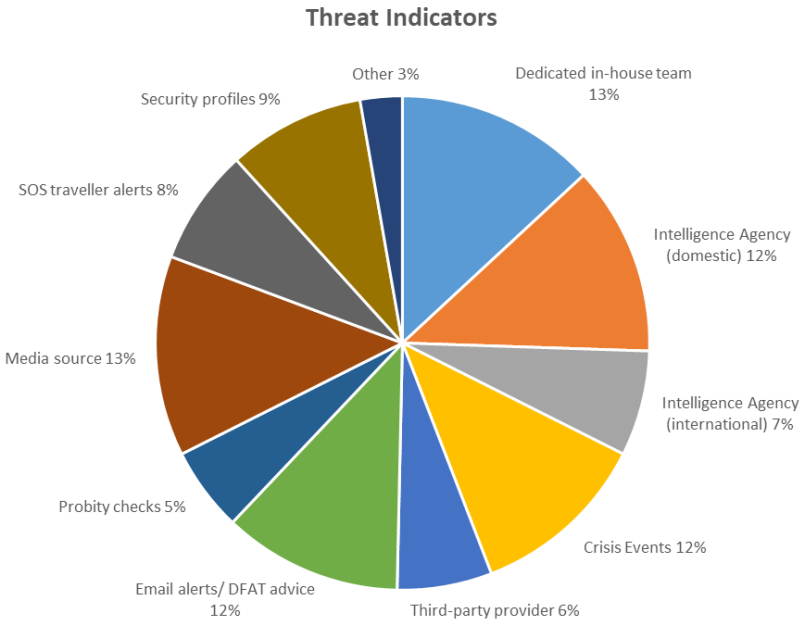


Key Points and Observations | Risk Exposure – High (see section 7.3.2)

- CitiPower/Powercor does not have a uniform and planned Security Risk Assessment process to identify new or emerging risks, instead utilising an informal process.
- CitiPower/Powercor are investing in improving insight into risk and control recommendations.

5.2.6 Threat Indicators

As part of the risk process, the following threat factors were identified and considered by participants:



Key Points and Observations | Risk Exposure – High (see section 7.3.2)

- CitiPower/Powercor are behind the industry in relation to threat and data sources, which could result in missed threats, emerging risk, increased vulnerabilities and potential cost.
- No active monitoring of new or emerging threats.

5.2.7 Industry Insight

Industry insight and threat-based monitoring was one area which provided critical insight into the shift by organisations from a reactive to a proactive process, focusing on people elements and not assets.

Organisations also expressed this as a major area of focus for the next 12 months, based on changes across criminal and terrorism areas.

Initiatives include:

- Active monitoring of external events;
- Maturing and integration of security, emergency management and business continuity programs;
- Improving governance and reporting;
- Incorporating business lead intelligence into security capabilities; and
- Increased CCTV intelligence and systems integration.

5.3 Stakeholder Feedback

As part of the review process, Bellrock Group engaged with numerous key stakeholders who are directly engaged in the operation of the facilities / security department.

Without exception, all conversations were candid, constructive and directed towards the best interests of CitiPower/Powercor (no quotes or comments have been attributed to any individual).

Key themes that were identified through the conversations focused on the following general topics:

Stakeholder Feedback

"CitiPower/Powercor needs to transform our security approach to be more strategic"

"No clear plan around copper theft."

"We do not have the right capabilities, resources and systems in place."

"We are focused on ensuring our staff and the community are safe at all times."

"We need to improve training and awareness."

"Security needs to evolve and focus on being proactive."

"The processes, reporting and insights are limited."

"Our systems are not integrated."

"We need to improve our detection and monitoring capability."

"Fences at regional assets are in need of upgrading."

"Our approach to security is ad-hoc and we are under resourced."

"We should leverage the regulator for capital improvement costs."

The majority of the concerns or issues raised centred on four recurring themes:

- Capability;
- Systems;
- Culture; and
- Relationships.

5.4 Maturity Analysis

Four dimensions were used to measure the maturity of the various aspects related to the Security Department. The ratings are based on survey results and interviews with relevant stakeholders from all participating organisations (including CitiPower and Powercor).

	Indicators of Maturity
Capability	• Extent of involvement of leadership in the Security department • Adequacy of personnel dedicated to the function • Employee involvement and understanding of the objectives • Extent of training and personnel expectations
Systems	• Set a defined Policy and Strategy • Consideration of leading practices • Consistent and contemporary methodologies, including infrastructure • Audited and governed systems
Culture	• Extent to which all staff understand their roles, organisational strategy and how they contribute to the success of CitiPower/Powercor • Division takes ownership and accountability for their objectives, in line with the enterprise • Consistent approach to enterprise processes • Stakeholder engagement, feedback and culture surveys
Relationships	• Trusting relationships are held with key internal stakeholders • Strong relationships are held with external stakeholders • Stakeholders understand Security's function and services

Ratings are defined with the value aligned with maturity, as shown below.

Rating	1	2	3	4	5
Name	Ineffective	Rudimentary	Adequate	Capable	Proficient

Please refer to Appendix 4 – Risk Impact Criteria for a detailed explanation of the maturity ratings.

5.5 MATURITY RATINGS

	Maturity Ratings Comparison	
Dimensions	**CitiPower/Powercor**	**Industry Benchmark**
People	2	3.75
Systems	2.5	3.5
Culture	2.75	4.0
Relationships	2.75	3.75

5.5.1 People

	Maturity Ratings	
Dimensions	**CitiPower/Powercor**	**Industry Benchmark**
People	2	3.75

Key Points and Observations

Currently, CitiPower/Powercor does not have a dedicated security department or lead. The function defaults to the Manager, Network Facilities. Although this is an appropriate business unit for security, it is not adequately resourced to effectively manage security operations (contracts, incidents, issues, stakeholder queries or improvements).

Additionally, CitiPower/Powercor has not established its security program or framework, strategically. This should be established within the overall risk environment and department.

5.5.2 Systems

	Maturity Ratings	
Dimensions	**CitiPower/Powercor**	**Industry Benchmark**
Systems	2.5	3.5

Key Points and Observations

Currently there are no dedicated Security Policy, Strategy, uniformed procedures, security risk framework, governed processes or incident management processes for Security.

CitiPower/Powercor has not established a convergent approach for physical, personnel or information security.

This is not a best practice approach and increases compliance and regulatory concerns for CitiPower/Powercor.

5.5.3 Culture

	Maturity Ratings	
Dimensions	**CitiPower/Powercor**	**Industry Benchmark**
Culture	2.25	4.0

Key Points and Observations

Culture and service delivery is key to organisational performance. Security has an immature process for stakeholder engagement (internal and external), incident advice and a limited approach to continued improvement focus, which should include Risk, Financial and Service Quality factors.

During the stakeholder sessions, negative feedback was received in relation to the culture and focus for Security.

Key insights included:

- Tactical approach;
- Very reactive, rather than proactive;
- No strategic approach to security or risk;
- No dedicated security awareness plan or training; and
- Concerns with the resourcing and funding.

5.5.4 Relationships

	Maturity Ratings	
Dimensions	**CitiPower/Powercor**	**Industry Benchmark**
Relationships	2.5	3.75

Key Points and Observations

Throughout discussions, Security presented a low level of engagement with internal working relationships across the organisation; which is a direct reflection on the current resources and capability. However, it should be noted that the Facilities team is focused on provided the best level of service it can with current resources.

Implementing a formal approach to stakeholder management, aligned to CitiPower/Powercor's values, missions and critical business function, is essential.

6 RISK IDENTIFICATION

6.1 ENVIRONMENT RISK

6.1.1 Position

(a) Position (ZSS)

Due to the nature of operations for CitiPower/Powercor, critical ZSS assets are located far and wide across the state; including in metro inner and rural assets. Each asset is identified as unique in its own way, but characteristics are similar:

- External boundary fence (varying styles);
- Switching room;
- Utilities; and
- Major electrical infrastructure.

Due to the nature and location of the assets; the external areas are against unique; including:

- Bushland;
- Industry or commercial assets;
- Part of a larger property;
- Street front or bushland; and
- Residential.

(b) Position (DSS)

As the ZSS breakdown into Distribution Substations (DSS), the assets structure is consistent, but locations are extremely varied. The assets are located in isolation, as part of non-owned CitiPower/Powercor assets, basements of old building, next to a ZSS or within commercial operations.

These varied locations make it extremely difficult for CitiPower/Powercor to secure the assets or know when an asset is breached.

(c) Depots

In comparison to ZSS, depots are located in major areas across the state to support the operational requirements of the enterprise. Similar to ZSS, each asset is unique, but has similar features:

- Office space;
- Sheds and storage areas;
- Trucks and vehicles; and
- Major electrical infrastructure.

Again, due to the varied locations of CitiPower/Powercor ’s assets depots; the external areas are unique; including:

- Commercial or residential assets;
- Uninhabited land;
- Major infrastructure; and
- ZSS.

Key Points and Observations	Rated High Risk (see section 7.4.1)

- Asset variance for location and surroundings is significant.
- Some assets are secured via physical controls only.
- It's expected that some asset breaches will go unnoticed for a period of time.
- Asset security is not fully effective.
- Breach of assets could cause significant OH&S concerns or los of supply of energy to the consumer.
- Remove unneeded equipment / stock from ZSS.
- Secure high value items in depots out of site.

6.1.2 Perimeter Security

(a) Perimeter (ZSS)

Although each asset is varied, majority of the assets (>85) are secured by a chain link fence between 1.8m to 2.4 meters high with 300mm of barbed wired to the top. Of these asset, majority of the fences are ageing and require significant upgrades and some in need of immediate repairs.

Of the remaining assets, CitiPower/Powercor has invested in upgrading to a weldmesh style or Colourbond to a minimum of 2.1 meters plus additional protection. These assets are significantly more secure than the chainlink format (and aligned to ENA Guidelines).

Furthermore, some inner assets are secured via brick fence with additional wire. In the similar vain to the chainlink fences, these assets need further strengthening.

Across all ZSS, there is limited security signage to deter an offender and limited detection or response capability for breach.

(b) Perimeter (DSS)

The perimeter structure of the DSS varies significantly between assets; however due to the design methods it is difficult for CitiPower/Powercor to imply standards to older assets. Based on this, CitiPower/Powercor needs to focus on detection and response capabilities for these assets and implement rigorous standards for new assets.

(c) Perimeter (Depots)

CitiPower/Powercor has commenced an upgrade program for fences for depots and including perimeter protection for some assets. This program needs to be uniformed to newly formed security guidelines. Response to the alarm activation should be removed from the Facilities Management department and embedded in the proposed security control room.

All systems should be interfaced with lighting and camera surveillance on activation.

Key Points and Observations — Rated Extreme Risk (see section 7.4.1)

- Ageing perimeter security, including holes in fences and breach methods.
- Easy access and scalability for offenders.
- CitiPower/Powercor has commenced upgrading perimeter security across inner and metro assets.
- Limited perimeter detection or response capability is in place for ZSS or DSS.
- Fencing is being damaged by nearby trees and bushland.
- Implement consistent design standards for all assets (based on ENA guidelines), with integrated detection and response capability.
- All detection systems should be interfaced with lighting and camera surveillance on activation.
- No strategic approach to security or incident management.

6.1.3 Utilities and Services

(a) Electrical

There have been no reported material issues with supply of electricity to security systems at CitiPower/Powercor assets.

(b) Communications

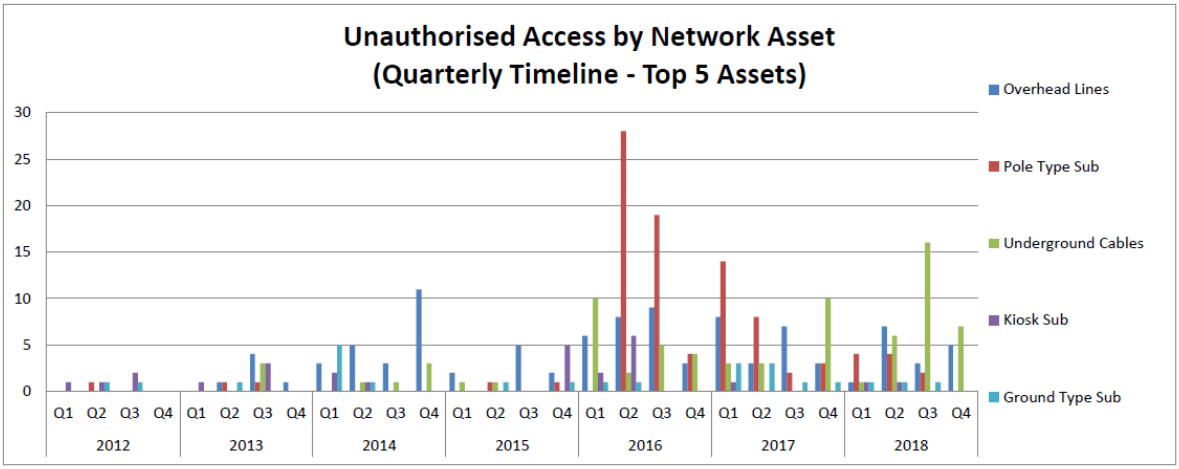
There are communication lines running in and out of the depots, major assets and most ZSS. Whereas, DSS; currently have no communications. This needs to be taken into account when deploying security assets to DSS.

6.1.4 Incidents

Since 2012, there has been more than 400 reported incidences of copper theft and asset breach across CitiPower/Powercor and more than 30 since January 1, 2019. Additionally, we anticipate this problem to expand, which exposes serious risk to the safety of our workers and the communities.

Currently, the recorded average incident is costing CitiPower/Powercor $1,314 in losses; with some incidents incurring losses of over $50,000. These numbers do not include the loss of operational time, investigations or repairs; which could see this number increase by three-fold.

	2012				2013				2014				2015				2016				2017				2018												
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	2012	2013	2014	2014	2016	2017	2018	2019	Total
Overhead Lines						1	4	1	3	5	3	11	2		5	2	6	8	9	3	8	3	7	3	1	7	3	5		6	22	9	26	21	16		100
Pole Type Sub		1				1	1							1		1		28	19	4	14	8	2	3	4	4	2		1	2		2	51	27	10		93
Under Cables							3			1	1	3	1	1			10	2	5	4	3	3		10	1	6	16	7		3	5	2	21	16	30		77
Kiosk Sub	1	1	2		1		3		2	1						5	2	6			1				1	1			4	4	3	5	8	1	2		27
Ground Type Sub		1	1			1			5	1				1		1	1	1			3	3	1	1	1	1	1		2	1	6	2	2	8	3		24
Indoor Sub		1				2			1	2		1				3	2		1		1		2		1	5	1		1	2	4	3	3	3	7		23
Installation								1		1		1						1	3			1	2		1	1	1			1	2		4	3	3		13
Customer asset									1									1	2		1	1									1		3	2			6
Non Network Item									5			1														1					6				1		7
Zone / Terminal		2	1				1									1			1									1	3	1		1	1		1		7
Lighting									1			1																			2						2



Key Points and Observations

- Potential inaccuracy of incident numbers and underreporting.
- Outdated security operating procedures.
- No enterprise security awareness program.
- CitiPower/Powercor will continue to be a target of theft due to copper prices.

6.1.5 Ecology

Due to the varied locations, CitiPower/Powercor could be impacted by major environmental threats (floods, cyclones, fires, earthquakes or landslides).

These threats are taken into consideration as part of the emergency management process.

6.2 Security Risk

6.2.1 Systems & Procedures

Currently, CitiPower/Powercor has numerous disparate documents and processes in place, however, it was noted that several were outdated. Additionally, third party contractors would be improved with key service level agreements.

Key Points and Observations Rated Extreme Risk (see section 7.4.2)

- There is no formal Security Policy, Strategy, Security Management Plan, Risk Program or framework.
- No Security Governance Model is in place (refer to 7.2 – Security Governance Model).
- Limited Service Level Agreements in contracts.
- No formal security standards or risk methodology for assets and key systems.
- No technology standards or specifications.
- There is no technology roadmap in place for physical security systems.

6.2.2 Electronic Security Systems

CitiPower/Powercor utilises the Gallagher platform across its core assets / sites; whereas United Energy use the Integriti platform. Currently, there is a mix of electronic and mechanical keys across the enterprise. Both are solid and reliable platforms but means that users need to use multiple cards across assets.

Within the surveillance areas, CitiPower/Powercor utilise trusted products from the Milestone and AXIS brands across its corporate and depot assets. Whereas, no surveillance capability is deployed across ZSS or DSS assets.

Additionally, across some key assets, security infrastructure is ageing and not operational (for example, PE Beams at Ballarat).

Key Points and Observations | Rated High Risk (see section 7.4.3)

- CitiPower/Powercor manage several platforms for security, which are not integrated.
- CitiPower/Powercor does not have an established technology strategy.
- No preventative maintenance program is in place.
- No security standards are in place for systems or design guidelines.
- Conduct a review of additional product, Pelco, Panasonic and Sony cameras.
- All systems should be interfaced into the new proposed control room, minimum 30 days storage.
- Installation standards are not uniformly enforced and reviewed for all electronic security work.
- Security does not have established SLAs and KPIs to enable realistic and agreed expectations for network-dependant users.
- Asset and performance registers not current or maintained.
- Duress facilities are not installed in all customer facing locations and response processes are fragmented.

6.2.3 Physical Security Measures

CitiPower/Powercor contract Wilson Security to support their corporate assets and alarm responses. During the stakeholder sessions, the following concerns were raised:

- Process accuracy;
- Ability to cover all assets;
- Limited Key Performance Indicators (KPIs);
- Limited operational reporting in place from Wilson; and
- Limited management engagement (Wilson Security).
- Performance levels.

6.2.4 Security Resources

The current security management staffing model is not effective or sufficiently resourced to deliver the program required for CitiPower/Powercor.

The model is currently unstructured and has the Manager Network Facilities, operating in their current role, while trying to manage all operational tasks. This approach is assessed reactive, not strategic and operate in an ad-hoc manner.

Additional resources required should be funded to cover two key areas:

- Strategy, governance, standards and frameworks;
- Operational requirements, including:
  - Contract management;
  - Project support and management;
  - Incident management;
  - Stakeholder engagement; and
  - Reporting.

Key Points and Observations	Rated High Risk – (see section 7.4.4)

- Current model is under resourced and ineffective.
- Deployment of a Security Director reporting to the Head of Risk to establish and implement the security framework and system (contract circa 12 months)
- Deploy a Security Manager reporting to the Group Real Estate Manager for all operational security contracts and matters.
- Implement key performance indicators for the strategy role.

6.2.5 Locking System

A restricted profile master keying system is in place at CitiPower/Powercor, however multiple keys are unaccounted for and its ageing. Additionally, the patent will expire in 2019. This eliminates the contract of key management and significantly increases the risk to assets.

In addition, Bellrock Group were advised that some of the key records are potentially inaccurate.

Key Points and Observations	Rated High Risk – (see section 7.4.5)

- CitiPower/Powercor is currently rolling out access control to replace mechanical locks across some assets.
- Unknown key access profiles and keys unaccounted for.
- The key systems is outdated with numerous gaps, requiring a full upgrade.
- No security audit of keys.

6.2.6 Security Culture

The security culture at CitiPower/Powercor was assessed as rudimentary. This was evident through the current lack of systems, engagement and education programs. This could be improved through an enterprise approach, incorporating security programs, asset management, information security and incident response.

Key Points and Observations	Rated High Risk – (see section 7.4.6)

- No enterprise security awareness training plan.
- High level of opportunistic thefts.
- CitiPower/Powercor approach to security education and awareness can improve.

6.2.7 People | Sexual Harassment & Assault

CitiPower/Powercor has had previous significant customer threats, including at depots in reception areas that could have resulted in harm to staff or contractors. In addition, field staff have received abuse during their work.

Key Points and Observations	Rated High Risk – (see section 7.4.7)

- Potential underreporting of incidents.
- No enterprise security awareness training plan.
- No formal duress facility for reception staff in all customer facing locations.
- No anti-jump barrier protection in place.

6.2.8 Property

There have been no reports of ongoing material property damage. Minor evidence of vandalism and graffiti occur on a regular basis and one incident of a vehicle driving into an asset.

6.2.9 Business Interruption

There have been no reports of activities that result in Business Interruption (Bomb Hoax, Bomb Detonation, Release of Noxious Chemicals, Discharge of Firearms, Denial of Building Access or Building Evacuation Obstacles) over the past 24 months.

6.3 Integrity Risk

6.3.1 Internal Theft |Theft of Physical Assets

Since 2012, there has been more than 400 reported incidences of copper theft across CitiPower/Powercor and more than 30 since January 1, 2019. Additionally, we anticipate this problem to expand, which exposes serious risk to the safety of the workers and the communities.

Key Points and Observations	Rated High Risk – (see section 7.4.8)

- Continual thefts occurring across the network, causing risk to the supply of electricity and OH&S concerns.
- No enterprise security awareness training plan.
- No plan to address incidents at a macro level.
- CitiPower/Powercor has engaged with Victoria Police regarding thefts.

6.4 Political Risk

6.4.1 Anti-Social Behaviour

There have been minor instances of antisocial behaviour at CitiPower/Powercor.

6.4.2 Civil Disorder

There have been no instances of significant mass civil disorder at CitiPower/Powercor.

6.4.3 Terrorism

There is no history of terrorism or terrorist threats at CitiPower/Powercor, however, terrorism threats from external and internal sources to Australia are present. CitiPower/Powercor represents a potential threat due to the critical services it operates.

Australia's current National Terrorism Threat Level is Probable. This is based on Australia's Intelligence, assessed by security agencies, and indicates that individuals or groups continue to possess the intent and capability to conduct a terrorist attack in Australia.

7 RISK EVALUATION & TREATMENT

Bellrock Group has conducted a comprehensive evaluation of risks associated with CitiPower/Powercor's facilities and operations.

The following section describes the prevailing and emerging threats that should be prioritised for treatment.

7.1 RISK PRIORITISATION

Consistent with progressive risk management practices, the proceeding risk evaluation section prioritises the higher risks, based on the likelihood of their occurrence and their potential impact.

To this end, the prevailing higher risks are itemised and dissected in detail, whilst the lower risks are summarised for information, monitoring and appropriate review.

This approach enables the client to focus its resources on the key risks whilst remaining aware of the subsidiary risks (cognisant of the fact that risk profiles change over time and can therefore not be ignored on an ongoing basis).

Based on our evaluation, the higher risk at the sites are as follows:

Risk Class	Risk Factor
Environment Risk	Position & Structure
Security Risk	Systems & Procedures
	Electronic Security Systems
	Security Resourcing
	Locking Systems
	Security Culture
	Abusive & Threatening Behaviour
Integrity Risk	Theft

7.2 Operating Model

As part of the Review, Bellrock Group identified the need to invest in additional (two) resources to both develop the strategic security model and program, including:

Strategic (Security Director) factors:

- Strategy;
- Policy;
- Frameworks;
- Development of Standards and Procedures;
- Governance model (refer to 7.3 Security Governance Model); and
- Executive engagement.

As this role is focused on establishment of key strategy and risk items, we recommend this role is set for a fixed contract of 12 months and reports to the Head of Risk and Financial Control. We anticipate an investment of $200,000 for the right candidate.

Operational (Security Manager) factors;

- Contract management and performance;
- Security projects;
- System design and reporting;
- Incident management and advice
- Stakeholder engagement;
- Implementation of strategy and standards;
- All operational matters; and
- Law enforcement engagement.

This role will be focused on operations and delivering the set strategic elements. Based on this, we recommend implementation of a Security Manager (ongoing role), reporting to the Group Real Estate Manager, we anticipate an investment of $130,000 per annum for the right candidate.

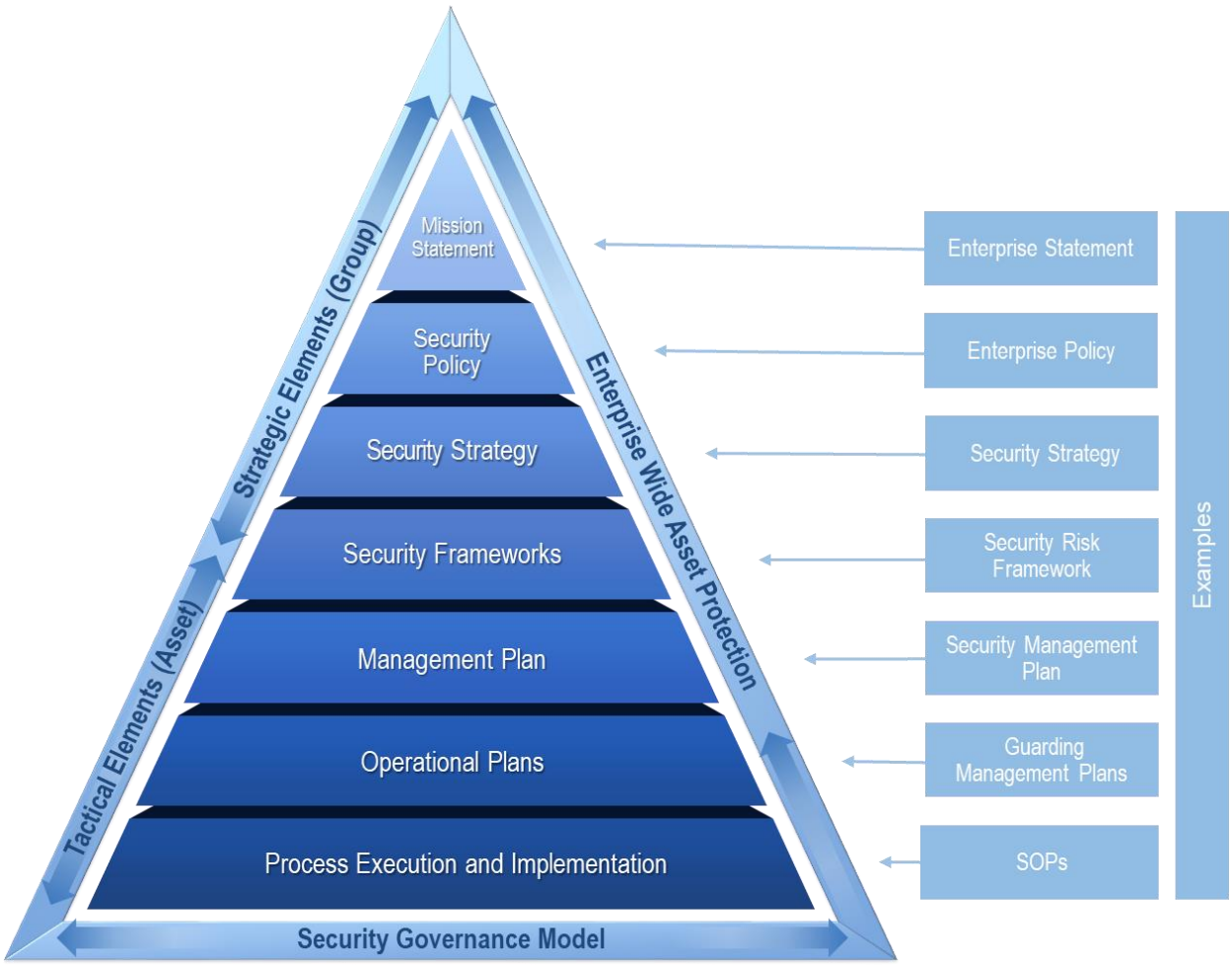
The focus of these two roles is to implement an affective security programs to ensure the protection of staff, contractors, assets and the supply of electricity to the community.

7.3 Security Governance Model

It is recommended that CitiPower/Powercor implements a governance model designed to link strategic objectives, frameworks, operational plans and process execution. The governance model is used as a virtual structure to achieve the following:

- Integrated Security Management: and
- Enterprise-Wide Security.

Bellrock Group has designed a model that CitiPower/Powercor can implement to achieve a full end-to-end governance structure for security risk. The value of the model lies in the integrated and interdependent nature of its elements to provide a genuine enterprise wide outcome for CitiPower/Powercor.


Mission Statement
Security Policy
Security Strategy
Security Frameworks
Management Plan
Operational Plans
Process Execution and Implementation
Strategic Elements (Group)
Tactical Elements (Asset)
Enterprise Wide Asset Protection
Security Governance Model
Enterprise Statement
Enterprise Policy
Security Strategy
Security Risk Framework
Security Management Plan
Guarding Management Plans
SOPs
Examples

7.4 HIGH RISKS

7.4.1 Position & Structure

Risk Class	Risk Factor	Primary Rating	Residual Rating
Environment Risk	Position & Structure	Extreme Risk	Moderate Risk

Likelihood

The threat is **Expected** to occur due to:

- Easy access to the facility.
- Specific incident identified as an ongoing concern.
- Exposed vulnerabilities in place.

Impact

The impact is expected to be **Major** for the following reasons

- OH&S concern.
- Potential compromise of operations.
- Supply failure.

Treatment

The risk of 'Position & Structure' can be reduced through an improvement in electronic and operational controls. Treatment should include:

- Replacing all chain-wire fences with ENA recommended fencing.
- Deploy new security signs to all sites.
- Deploy additional sensor lights to all ZSS and depots.
- Develop and deploy an enterprise security awareness program or include a module in the safety training program.
- Develop a sharing of information program with local law enforcement and emergency services.
- Implement a dedicated security control room to manage and respond to incidents (24/7).
- Implement an agreement with a security provider to respond to all assets.
- Conduct a training session on incident reporting (Security Officers).
- Remove trees and bushes in or near assets; increasing natural surveillance.
- Apply rigorous security construction standards to all new DSS.
- Implement consistent design standards for all assets (based on ENA guidelines), with integrated detection and response capability.
- Integrate security systems with lighting and camera surveillance on activation.
- Remove unneeded equipment / stock from ZSS.
- Secure high value items in depots out of site.

Accountability: Facility Management

7.4.2 Systems & Procedures

Risk Class	Risk Factor	Primary Rating	Residual Rating
Security Risk	Systems & Procedures	Extreme Risk	Moderate Risk

Likelihood

The threat is **Expected** to occur due to:

- No set policy or plan.
- Strong prevailing opportunity or threat indicators for incident to occur.
- Specific incidents identified.
- No specific security processes in place.

Impact

The impact is expected to be **Major** for the following reasons:

- Financial loss.
- Reputation damage.
- OH&S issues.
- Property damage.

Treatment and Accountability

The risk of 'Systems & Procedures' can be reduced through an improvement in operational controls. Treatment should include:

- Implement a Security Policy.
- Implement a Security Strategy for CitiPower/Powercor (currently in DRAFT format), focusing on service quality, financials, risks and incident reduction.
- Implement a Security Risk Framework.
- Implement an enterprise wide Security Management Plan.
- Implement a Security Operation Plan for each depot and overall for the ZSS, aligned to the Security Management Plan.
- Conduct an annual Threat Assessment of critical assets
- Deploy a Stakeholder Management Plan, including stakeholder details, priority, frequency and purpose.
- Increase industry relationships (locally & internationally).
- Deploy an internal capability to implement and maintain a contemporary security program.
- Improve incident reporting, categorization and reporting to stakeholders.
- Develop a strategic plan to address copper theft
- Improve processes between Security and Crisis Management.

Accountability: Risk and Facility Management

7.4.3 Electronic Systems

Risk Class	Risk Factor	Primary Rating	Residual Rating
Security Risk	Electronic Security	High Risk	Moderate Risk

Likelihood

The threat is **Expected** to occur due to:

- No technology standards or specifications.
- There is no technology roadmap in place.
- No maintenance agreements in place.

Impact

The impact is expected to be **Medium** for the following reasons:

- Personal injury.
- Opportunity theft.
- Financial loss.
- Reputation damage.

Treatment and Accountability

The risk of 'Electronic Security' can be reduced through an improvement in electronic and operational controls. Treatment should include:

- Remediate current outages and implement processes to actively manage faults.
- Implement standards for security systems and products, including design guidelines.
- Implement a 7-10-year Technology Roadmap for security systems to;
  - Integrate systems;
  - Improve disaster recovery;
  - Improve performance;
  - Define capital and operational costs;
  - Increase detection; and
  - Develop redundancy capability.
- Implement a dedicated security control room to manage and respond to incidents (24/7).
- Uniform all access control systems under the Gallagher platform.
- Deploy new CCTV (30 days recording) and intruder detection systems (perimeter, internal and external doors) to all ZSS and enhance both systems at depots (all internal areas, sheds and operational areas).
- Outsource all security system design specification and assurance with new capital projects and capitalize the costs to the project.
- Install monitored intrusion detection systems in high risk locations, for example, DSS.
- Establish an asset register for security systems.
- Deploy wireless duress buttons for frontline staff, with incident response to be performed by Security. Each site should have a blue warning light in the back of house notifying staff of an incident.
- Review the Incident Response Process and implement a consistent approach with Security.
- Refresh all alarm / disarm procedures and uniform across all sites.

Accountability: Facility Management

7.4.4 Security Resourcing

Risk Class	Risk Factor	Primary Rating	Residual Rating
Security Risk	Security Resourcing	High Risk	Moderate Risk

Likelihood

The threat is **Likely** to occur due to:

- Adhoc approach to security.
- Resource levels and capabilities are not adequate.
- Limited policy and governance document and planning.

Impact

The impact is expected to be **Major** for the following reasons:

- Personal injury.
- Opportunity theft.
- Financial loss.
- Reputation damage.

Treatment and Accountability

The risk of 'Security Resourcing' can be reduced through an improvement in operational controls. Treatment should include:

- Deployment of a Security Director reporting to the Head of Risk to establish and implement the security framework and system (contract 12 months) and a Security Manager (Ongoing) reporting to the Group Real Estate Manager for all operational security contracts and matters.
- Deploy a 24/7 security officer into the new security control room.
- Combine all security providers into one consistent agreement with SLAs.
- Improve focus of Security Officers on core services.
- Update all Security Operating Procedures, aligned to security plans.
- Improve third party vendors reporting
- Improve contract KPIs and issue Contract Breach Notice when failures occur (within new contract).
- Implement performance-based outcomes to contractor's criteria, build in awareness and continuing improvement in delivery/performance assessment.
- Ensure CitiPower/Powercor 's culture and values are consistently reinforced in the delivery of contractor-based services.

Accountability: Facility Management

7.4.5 Locking Systems

Risk Class	Risk Factor	Primary Rating	Residual Rating
Security Risk	Locking Systems	High Risk	Moderate Risk

Likelihood

The threat is **Expected** to occur due to:

- Lost or unaccounted keys.
- Doors left unlocked/open.
- Concerns with key register.
- Patent expiry.

Impact

The impact is expected to be **Medium** for the following reasons:

- Opportunity theft.
- Financial loss.
- Reputation damage.
- Property damage.

Treatment and Accountability

The risk of 'Locking Systems' can be reduced through an improvement in operational and physical controls. Treatment should include:

- Conduct a full audit of keys.
- Audit the Key Register to manage all keys, including a hierarchy based on operational requirements.
- Replace all keying systems for electrical assets.
- Continue to replace perimeter and higher risk mechanical locks with access control.
- Undertake an annual audit of all keys.
- Install anti-tamper strike plate over locks (mechanical and electronic).

Accountability: Facility Management

7.4.6 Security Culture

Risk Class	Risk Factor	Primary Rating	Residual Rating
Security Risk	Security Culture	High Risk	Moderate Risk

Likelihood

The threat is **Likely** to occur due to:

- Incidents of theft and valuables left unattended.
- No formal security awareness program.
- Assets not secured.

Impact

The impact is expected to be **Major** for the following reasons:

- Personal injury.
- Opportunity theft.
- Financial loss.
- Reputation damage.
- Property damage.

Treatment and Accountability

The risk of 'Security Culture' can be reduced through an improvement of operational controls. Treatment should include:

- Define what Security Mandate and Vision is and share with colleagues.
- Develop a Training and Awareness Plan, including Performance Metrics.
- Align the Security Awareness Program to safety strategies.
- Leverage Safety Champions, to include security elements.
- Improve communication to stakeholders, post an incident, including regular Stakeholder Incident Reporting (e.g. monthly).
- Implement security awareness campaigns for higher risk periods (e.g. Christmas).

Accountability: Executive and Risk

7.4.7 Abusive & Threatening Behaviour

Risk Class	Risk Factor	Primary Rating	Residual Rating
Security Risk	Abusive & Threatening Behaviour	High Risk	Moderate Risk

Likelihood

The threat is **Expected** to occur due to:

- Reported reoccurring incidents.
- Extensive external examples of similar risks in similar environments.
- Reported incidents in nearby properties.

Impact

The impact is expected to be **Medium** for the following reasons:

- Noticeable influence on staff morale/productivity.
- Realistic potential for loss of commercial standing and reputation.

Treatment and Accountability

The risk of 'Abusive & Threatening Behaviour' can be reduced through an improvement in electronic and operational controls. Treatment should include:

- Deploy wireless duress buttons for frontline staff, with incident response to be performed by Security. Each site should have a blue warning light in the back of house notifying staff of an incident.
- Provide frontline staff with security awareness training to deal with abusive/threatening behaviour.
- Leverage safety champions to include Security elements.
- Engagement with key stakeholders to identify emerging or changed risks (e.g. projects, reception, Call Centres) as part of the stakeholder management plan.
- Implement a zero-tolerance process for significant incidents.
- Conduct regular testing of incident response process for duress button activation.
- Deploy anti-jump barriers in each reception area.

Accountability: Risk

7.4.8 Theft

Risk Class	Risk Factor	Primary Rating	Residual Rating
Integrity Risk	Theft	High Risk	Moderate Risk

Likelihood

The threat is **Expected** to occur due to:

- High incidents.
- Ongoing incidents.
- Open environment.
- Limited policy and governance document and planning.

Impact

The impact is expected to be **Medium** for the following reasons

- Opportunity theft.
- Property damage.
- Financial loss.
- Reputation damage.

Treatment and Accountability

The risk of 'Theft' can be reduced through an improvement in electronic and operational controls. Treatment should include:

- Increased awareness regarding theft and securing of sensitive information and personal items.
- Deploy a copper theft / crime prevention plan focused on deterrence based on market copper (E.g. DataTrace) and extensive signage.
- Extend training and awareness of theft issues to Floor Warden, Emergency Management Officers and project staff.
- Implement a zero-tolerance process for incidents.
- Restrict access and after-hours access to necessary staff and contractors.
- Implement a clean desk process for sensitive information (e.g. contracts).
- Increase incident reporting to stakeholders re theft incidents and recommended mitigation strategies.
- Deploy new CCTV (30 days recording) and intruder detection systems (perimeter, internal and external doors) to all ZSS and enhance both systems at depots.
- Deploy additional sensor lights to all ZSS and depots.
- Replacing all chain-wire fences with ENA recommended fencing.
- Deploy new security signs to all sites.
- Install lids on copper bin at depots and lock overnight.
- Deploy CCTV cameras and motion senor lighting over high risk areas (tool, bins and copper).

Accountability: Risk and Facility Management

7.5 LOWER RISKS

The following risks were evaluated as Negligible, Low or Moderate. The response to these risks should mainly entail awareness and ongoing monitoring and review rather than immediate prioritisation for treatment.

Risk Factor	Likelihood	Impact	Rating
Environment Risks			
Power Failure	Expected	Minor	Moderate
Water Failure	Expected	Minor	Moderate
Telecommunications Failure	Expected	Minor	Moderate
Flooding	Possible	Major	Moderate
Earthquake	Possible	Major	Moderate
Fire (not Arson)	Possible	Major	Moderate
Cyclone	Possible	Major	Moderate
Landslides	Rare	Major	Low
Demographics	Unlikely	Minor	Negligible
Security Risks			
Abduction/Kidnap	Unlikely	Major	Moderate
Bomb Hoax	Possible	Minor	Low
Bomb Detonation	Unlikely	Major	Moderate
Release of Noxious Chemicals	Possible	Major	Moderate
Discharge of Firearms	Unlikely	Major	Moderate
Arson	Unlikely	Medium	Low
Malicious Damage	Unlikely	Minor	Negligible
Sabotage	Unlikely	Medium	Low
Denial of Building Access	Likely	Medium	Low
Unauthorised Site Entry	Possible	Major	Moderate
Vandalism	Expected	Minor	Moderate

Integrity Risks			
Theft of Information	Possible	Major	Moderate
Burglary	Likely	Medium	Moderate
Theft from Vehicles	Likely	Minor	Moderate
Theft of Vehicle	Possible	Minor	Low
Eavesdropping	Unlikely	Minor	Negligible
Telephone Tapping	Unlikely	Minor	Negligible
Political Risks			
Terrorism	Rare	Catastrophic	Moderate
Civil Disorder	Possible	Minor	Low
Anti-Social Behaviour	Possible	Minor	Low

Please refer to Appendix 6 - Risk Treatment Monitoring, for Negligible, Low and Moderate risks, which should be monitored on an ongoing basis.

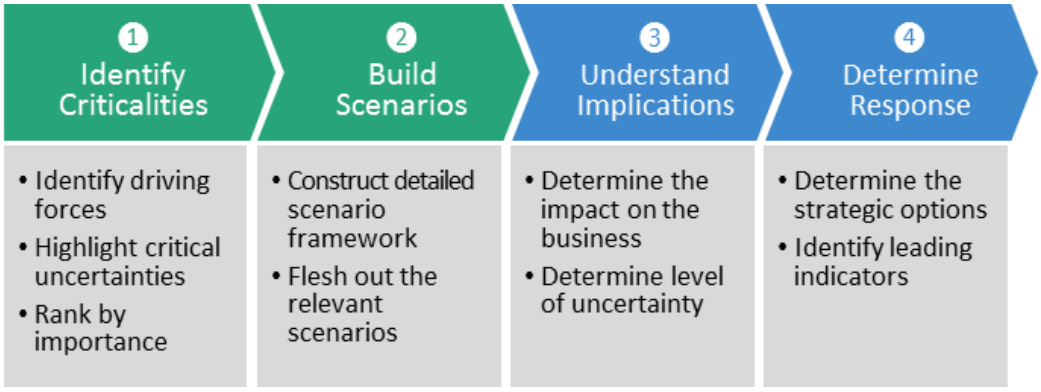
7.6 Scenario Analysis

The Scenario Analysis tool provides an understanding of potentially catastrophic events that could impact upon the building and its associated businesses. This is not intended to be a prediction of these events. Instead, it is a forward-looking understanding of the implications of these events in order to enable the organisation to plan an appropriate response.

The Scenario Analysis process consists of two main phases,

- Developing alternate 'stories' or scenarios for the future; and
- Understanding the implications of these scenarios and determining the response.

The chart below illustrates the Scenario Analysis process:



Based on this initial review, a preliminary scope of relevant scenarios comprises of the following:

- Suspicious Package Delivered; and
- Asset breach of Zone Substation.

These scenarios are examined in the following section in terms of criticalities and implications. A response has not been developed at this stage as an effective and comprehensive plan for critical and catastrophic scenarios requires the participation of a range of operational and business stakeholders. The response stage of the scenario analysis process will therefore need to be developed in consultation with relevant organisational stakeholders.

7.6.1 Suspicious Package Delivered

Suspicious Package Delivered		
Risk Class: Terrorism	Risk Factor: Bomb Identification/Detonation	Scenario Priority: Prioritise
Identify Criticalities	Couriered mail can be delivered straight to the facility. As CitiPower/Powercor is a major brand, it is not outside the realm of possibility that extremists' groups or vengeful individuals could affect CitiPower/Powercor the brand.	
Build Scenarios	At approximately 3:00pm, a courier arrives at the facility (head office) to deliver a package to the CEO. Reception tell the courier to wait, but he advised he is running late and needs to depart, leaving the package at reception. The package is heavy, and when unwrapped, the inner box is coated with white powder. Security then call Police. The facility is placed in lockdown as a precaution. Nearing 7pm, staff have not been informed of any new developments. Employees are irate and want to return home. The media are trying to contact the receiver of the package, who is distraught over the situation. Some of the staff members turn to social media to vent their frustration and keep their relatives updated. The media pick up on some of the messages and broadcast them. The media attempt to lure staffers to help them contact the receiver of the package. At 10pm, the facility is advised the package is non-suspicious and the lockdown is lifted.	
Understand Implications	This scenario can result in the loss of operational efficiency and inaccessibility for several hours. There is some negative media attention focused on the site security and CitiPower/Powercor regarding staff comments on social media. The package receiver may experience trauma from the events.	
Determine Response	Response to be developed in conjunction with relevant stakeholders.	

7.6.2 Asset Breach at Zone Substation

Asset Breach at Zone Substation		
Risk Class: Security	Risk Factor: Asset Breach	Scenario Priority: Prioritise
Identify Criticalities	The facilities are easily accessible due to fence type and locations.	
Build Scenarios	Staff are sent to Geelong ZSS due to a reported fault on the line. As staff arrive, they find 4 – 6 kids (around 10 – 14 years of age) playing ball sports inside the ZSS against the switching building. When staff enter the ZSS the kids try to depart via a hole in the fence. However, staff manage to get to one kid to discuss what they are doing inside and how dangerous it is. The child explains they play down-ball in the ZSS everyday afterschool and sometime use slingshots to hit the wires. Later that day, CitiPower/Powercor is contacted by the child's mother accusing staff of harassment to her child and a lack of security and safety controls. She will contract the regulator.	
Understand Implications	This scenario can result in the loss of operational of critical equipment and a significant danger to the children of harm. There is negative media attention focused on the incident regarding how secure the site is and bullying of children.	
Determine Response	Response to be developed in conjunction with relevant stakeholders.	

7.7 Summary of Recommendations (Higher Risk)

7.7.1 Position & Structure

Risk Class	Element	Key Recommendations	Action Immediately	Comment	Status/Owner
Environment Risk	Position & Structure	Replacing all chain-wire fences with ENA recommended fencing.			
		Deploy new security signs to all sites.			
		Deploy additional sensor lights to all ZSS and depots.			
		Develop and deploy an enterprise security awareness program or include a module in the safety training program.			
		Develop a sharing of information program with local law enforcement			
		Implement a dedicated security control room to manage and respond to incidents			
		Implement an agreement with a security provider to respond to all assets.			
		Conduct a training session on incident reporting (Security Officers).			
		Remove trees and bushes in or near assets; increasing natural surveillance.			
		Apply rigorous security construction standards to all new DSS.			
		Implement consistent design standards for all assets (based on ENA guidelines), with integrated detection and response capability.			
		Integrate security systems with lighting and camera surveillance on activation.			
		Remove unneeded equipment / stock from ZSS.			
		Secure high value items in depots out of site.			

7.7.2 Systems & Procedures

Risk Class	Element	Key Recommendations	Action Immediately	Comment	Status/Owner
Security Risk	Systems & Procedures	Implement a Security Policy.			
		Implement a Security Strategy for CitiPower/Powercor (DRAFT), focusing on service quality, financials, risks and incident reduction.			
		Implement a Security Risk Framework.			
		Implement an enterprise wide Security Management Plan.			
		Implement a Security Operation Plan for each depot and overall for the ZSS, aligned to the Security Management Plan.			
		Conduct an annual Threat Assessment of critical assets			
		Deploy a Stakeholder Management Plan, including stakeholder details, priority, frequency and purpose.			
		Increase industry relationships (locally & internationally).			
		Deploy an internal capability to implement and maintain a contemporary security program.			
		Improve incident reporting, categorization and reporting to stakeholders.			
		Develop a strategic plan to address copper theft			

7.7.3 Electronic Security

Risk Class	Element	Key Recommendations	Action as a Priority	Comment	Status/Owner
Security Risk	Electronic Security	Remediate current outages and implement processes to identify and remediate faults.			
		Implement standards for security systems and products.			
		Implement a 7-10-year Technology Roadmap for security systems to; • Integrate systems; • Improve disaster recovery; • Improve performance; • Define capital and operational costs; • Increase detection; and • Develop redundancy capability.			
		Implement a dedicated security control room to manage and respond to incidents			
		Uniform all access control systems under the Gallagher platform.			
		Deploy new CCTV (30 days recording) and intruder detection systems (perimeter, internal and external doors) to all ZSS and enhance both systems at depots (all internal areas, sheds and operational areas).			
		Outsource all security system design specification and assurance with new capital projects and capitalize the costs to the project.			
		Install monitored intrusion detection systems in high risk locations, for example, DSS.			
		Establish an asset register for security systems.			
		Deploy wireless duress buttons for frontline staff, with incident response to be performed by Security. Each site should have a blue warning light in the back of house notifying staff of an incident.			

		Review the Incident Response Process and implement a consistent approach with Security.		
		Refresh all alarm / disarm procedures and uniform across all sites.		

7.7.4 Security Resourcing

Risk Class	Element	Key Recommendations	Action as a Priority	Comment	Status/Owner
Security Risk	Security Resourcing	Deployment of a Security Director reporting to the Head of Risk to establish and implement the security framework and system (contract 12 months) and a Security Manager (Ongoing) reporting to the Group Real Estate Manager for all operational security contracts and matters.			
		Deploy a 24/7 security officer into the new security control room.			
		Combine all security providers into one consistent agreement with SLAs.			
		Improve focus of Security Officers on core services.			
		Update all Security Operating Procedures, aligned to security plans.			
		Improve third party vendors reporting			
		Improve contract KPIs and issue Contract Breach Notice when failures occur (within new contract).			
		Implement performance-based outcomes to contractor's criteria, build in awareness and continuing improvement in delivery/performance assessment.			
		Ensure CitiPower and Powercor 's culture and values are consistently reinforced in the delivery of contractor-based services.			

7.7.5 Locking System

Risk Class	Element	Key Recommendations	Action as a Priority	Comment	Status/Owner
Security Risk	Locking Systems	Conduct a full audit of keys.			
		Audit the Key Register to manage all keys, including a hierarchy based on operational requirements.			
		Replace all keying systems for electrical assets.			
		Continue to replace perimeter and higher risk mechanical locks with access control.			
		Undertake an annual audit of all keys.			
		Install anti-tamper strike plate over locks (mechanical and electronic).			

7.7.6 Security Culture

Risk Class	Element	Key Recommendations	Action as a Priority	Comment	Status/Owner
Security Risk	Security Culture	Define what Security Mandate and Vision is, and share with colleagues.			
		Develop a Training and Awareness Plan, including Performance Metrics.			
		Align the Security Awareness Program to safety strategies.			
		Leverage Safety Champions, to include security elements.			
		Improve communication to stakeholders, post an incident, including regular Stakeholder Incident Reporting (e.g. monthly).			
		Implement security awareness campaigns for higher risk periods (e.g. Christmas).			

7.7.7 Abusive & Threatening Behaviour

Risk Class	Element	Key Recommendations	Action as a Priority	Comment	Status/Owner
Security Risk	Abusive & Threatening Behaviour	Deploy wireless duress buttons for frontline staff, with incident response to be performed by Security. Each site should have a blue warning light in the back of house notifying staff of an incident.			
		Provide frontline staff with security awareness training to deal with abusive/threatening behaviour.			
		Leverage safety champions to include Security elements.			
		Engagement with key stakeholders to identify emerging or changed risks (e.g. projects, reception, Call Centres) as part of the stakeholder management plan.			
		Implement a zero-tolerance process for significant incidents.			
		Conduct regular testing of incident response process for duress button activation.			
		Deploy anti-jump barriers in each reception area.			

7.7.8 Theft

Risk Class	Element	Key Recommendations	Action as a Priority	Comment	Status/Owner
'Integrity Risk	Theft	Increased awareness regarding theft and securing of sensitive information and personal items.			
		Deploy a copper theft / crime prevention plan focused on deterrence based on market copper (E.g. DataTrace) and extensive signage.			
		Extend training and awareness of theft issues to Floor Warden, Emergency Management Officers and project staff.			
		Implement a zero-tolerance process for incidents.			
		Restrict access and after-hours access to necessary staff and contractors.			
		Implement a clean desk process for sensitive information (e.g. contracts, assignments).			
		Increase incident reporting to stakeholders re theft incidents and recommended mitigation strategies.			
		Deploy new CCTV (30 days recording) and intruder detection systems (perimeter, internal and external doors) to all ZSS and enhance both systems at depots.			
		Deploy additional sensor lights to all ZSS and depots.			
		Replacing all chain-wire fences with ENA recommended fencing.			
		Deploy new security signs to all sites.			
		Install lids on copper bin at depots and lock overnight.			
		Deploy CCTV cameras and motion senor lighting over high risk areas (tool, bins and copper).			

APPENDICES

Appendix 1 – Risk Taxonomy

Risk Class	Risk Factor	
Environment Risk	Position and Structure	Building structure and facilities
		Proximity to public transport and amenities
		Proximity to and accessibility of emergency services
		Proximity to other buildings and businesses
		Proximity to chemical, manufacturing or hazardous goods
		Proximity to criminal or threatening organisations
	Utilities and Services	Power
		Water
		Telecommunications
		Transportation
		Critical Vendors
	Demographics	Crime statistics (property and person)
		Unemployment statistics
		Population profile
	Ecology	Flood
		Cyclone
		Earthquake
		Fire (not Arson)
		Landslide
Security Risk	Systems and Procedures	Security Policies and Procedures
		Electronic Security Systems
		Physical Security Measures
	People	Physical Assault
		Sexual Harassment & Assault
		Abduction/Kidnap
		Aggressive Behaviour
	Property	Arson
		Malicious Damage
		Vandalism
		Sabotage
	Business Interruption	Bomb Hoax
		Bomb Detonation
		Release of Noxious Chemicals
		Discharge of Firearms
		Denial of Building Access
		Building Evacuation Obstacles
Integrity Risk	Internal Theft	Theft of Physical Assets
		Theft of Information
	External Theft	Burglary
		Theft from Building
		Theft from Vehicles
		Theft of Vehicles
	Surveillance	Eavesdropping
		Telephone Tapping
Political Risk	Anti – Social Behaviour	
	Civil Disorder	
	Terrorism	

Appendix 2 –Risk Matrix

RISK MATRIX	IMPACT				
LIKELIHOOD	Insignificant 1	Minor 2	Medium 3	Major 4	Catastrophic 5
Expected A	Low	Moderate	High	Extreme	Extreme
Likely B	Low	Low	Moderate	High	Extreme
Possible C	Negligible	Low	Low	Moderate	High
Unlikely D	Negligible	Negligible	Low	Moderate	High
Rare E	Negligible	Negligible	Low	Low	Moderate

Appendix 3 – Risk Likelihood Criteria

Rating	Details
Expected A	The threat is expected to occur within the next 1 year due to: (a) Continued reported incidents highlighting an ongoing concern (b) Compelling anecdotal evidence from a variety of relevant sources (c) Extensive external examples of a similar risk nature in corresponding industry or operating environment (d) Strong prevailing opportunity and threat indicators for incident to occur
Likely B	The threat is likely to occur within the next 5 years due to: (a) Specific incidents identified or a recognised trend (b) Strong anecdotal evidence at similar facilities or organisations (c) Various external examples of a similar risk nature in corresponding industry or operating environment (d) Significant opportunity or threat indicators for incident to occur
Possible C	The threat may occur within the next 5 years due to: (a) Incidents have been recorded over a two-three-year period (b) Intermittent or sporadic anecdotal evidence at similar facilities or organisations (c) Sporadic external examples of a similar risk nature in corresponding industry or operating environment (d) Moderate opportunity or threat indicators for incident to occur
Unlikely D	The threat is unlikely to occur due to: (a) Incidents have occurred at similar facilities or organisations (b) Unconfirmed anecdotal evidence of occurrence at similar facilities or organisations (c) Unsubstantiated external examples of a similar risk nature in corresponding industry or operating environment (d) Low level of opportunity for the incident to occur
Rare E	The threat could only occur in exceptional circumstances due to: (a) No recorded incidents at similar facilities or organisations (b) No anecdotal evidence of incident occurrence (c) No external examples of a similar risk nature in corresponding industry or operating environment (d) Minimal opportunity for the incident to occur

Appendix 4 – Risk Impact Criteria

Rating	Details
Insignificant 1	(a) Total financial loss to a maximum of $10,000 (b) Business disruption contained to within half a day (c) No compromise of intellectual property (d) No chemical or toxic release (e) No physical injuries or psychological trauma (f) No harm to reputation or brand (g) No impact on staff engagement or efficiency (h) Fundamental IT systems remain available (i) No impact to client or counterparties (j) Minor legal issue or breach of regulations
Minor 2	(a) Total financial loss to a maximum of $50,000 (b) Business disruption contained to within 0.5 – 2 days (c) Small and temporary compromise of intellectual property (d) Chemical spill or toxic release with minor impact (e) First aid treatment required (f) Small and temporary brand reputational issues (g) Minor impact on staff engagement or efficiency (h) Minor restriction to fundamental IT systems (i) Minor impact to operations affecting clients or counterparties (j) Minor fine or legal concern
Medium 3	(a) Total financial loss to a maximum of $250,000; (b) Business disruption contained to within 2 – 7 days (c) Moderate compromise of intellectual property (d) Chemical spill or toxic release with moderate impact (e) Offsite medical treatment required (f) Realistic potential for loss of commercial standing and reputation (g) Noticeable impact on staff engagement or efficiency (h) Moderate restriction to fundamental IT systems (i) Moderate impact to operations affecting clients or counterparties (j) Breach of regulation with investigation by authority
Major 4	(a) Total financial loss to a maximum of $1,000,000 (b) Major business disruption exceeding 7 days but less than 1 month (c) Significant compromise of intellectual property (d) Chemical spill or toxic release with major impact (e) Major physical/psychological injury requiring extensive treatment (f) Enterprise-wide damage to brand and reputation (g) Major impact on staff engagement or efficiency (h) Major restriction to fundamental IT systems

	(i) Major impact to operations affecting clients or counterparties (j) Major breach of regulation with punitive fine
Catastrophic 5	(a) Total financial loss of over $5,000,000 (b) Material business disruption of greater than 1 month (c) Material compromise of intellectual property (d) Chemical spill or toxic release with material impact (e) Injury resulting in fatality (f) Enterprise-wide and protracted damage to brand and reputation (g) Critical impact on staff engagement or efficiency (h) Fundamental IT systems not operational (i) Unable to service clients or counterparties (j) Investigation by regulatory body resulting in business interruption or possibility of custodial sentence

Appendix 5 –Scenario & Emerging Threat Analysis Matrix

Scenario & Emerging Analysis Matrix
The chart below illustrates the evaluation of scenario implications and their priority. Scenarios/Emerging Threats are evaluated based on Uncertainty and Impact.

SCENARIO MATRIX	IMPACT				
UNCERTAINTY	Insignificant	Minor	Medium	Major	Catastrophic
Complete Uncertainty	Monitor Occasionally	Monitor Regularly	Prioritise Action	Initiate Action	Initiate Action
Indeterminate Uncertainty	Monitor Occasionally	Monitor Occasionally	Monitor Regularly	Prioritise Action	Initiate Action
Variable Uncertainty	Monitor Impromptu	Monitor Occasionally	Monitor Occasionally	Monitor Regularly	Prioritise Action
Low Uncertainty	Monitor Impromptu	Monitor Impromptu	Monitor Occasionally	Monitor Regularly	Prioritise Action
No Uncertainty	Monitor Impromptu	Monitor Impromptu	Monitor Occasionally	Monitor Occasionally	Monitor Regularly

Uncertainty is used instead of 'Likelihood' because it is futile and counterproductive to attempt to predict catastrophic future events. Instead, the focus should be on understanding the impact of these events by considering how clear or not (i.e. uncertain) the outcomes may be.

In Scenario Analysis, 'Uncertainty' is defined as follows:

- No Uncertainty: Distinct view of the future. Certain outcome.
- Low Uncertainty: Clear view of the future. Dependable outcome.
- Variable Uncertainty: Limited set of possible future outcomes, one of which may occur.
- Indeterminate Uncertainty: Indeterminate outcomes but bounded within a definable range.
- Complete Uncertainty: Limitless range of possible outcomes. Unknowable outcome.

Appendix 6 – Glossary

Term	Definition
Activation	The implementation of response and recovery procedures, activities and plans in response to an incident declaration.
Alternate Site	A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of an incident.
Business Continuity	A pro-active process, which identifies the key functions of an organisation and the likely threats to those functions. From this information, plans and procedures can be developed thus ensuring key functions continue whatever the circumstances.
Business Impact Analysis (BIA)	The process of analysing all business functions and the effect that a specific incident may have upon them.
Consequence	The outcome of an event affecting objectives. A consequence can be certain or uncertain and can have positive or negative effects on objectives
Emergency Management	The discipline which ensures an organisation, or community's readiness to respond to an emergency in a coordinated, timely, and effective manner.
Event	Occurrence or change of a set of circumstances. An event can also be referred to as an "incident" and may have several causes and can consist of something not happening.
Fast Recovery Site (FRS)	Where hardware and software are stored and run to enable functional continuity.
Mitigation	Measures taken to prevent, limit and reduce impact of the negative consequences of incidents, emergencies and disasters.
Risk	The effect of uncertainty on objectives. The effect can be positive and/or negative.
Risk Source	An element which alone, or in combination, has the potential to give rise to risk. A risk source can be tangible or intangible. A "hazard" or "threat" is also a risk source
Resilience	The adaptive capacity of an organisation in a complex and changing environment.
Scenario	Pre-planned storyline that drives an exercise; the stimuli used to achieve exercise objectives.
Stakeholder	Person that holds a view that can affect the organisation.
Threat	Potential cause of an unwanted incident, which can result in harm to individuals, a system or organisation, the environment or the community.
Vulnerability	The intrinsic properties of something, resulting in susceptibility to a risk source that can lead to an event with a consequence.

Appendix 6 – Risk Treatment Monitoring

The following section describes the current Negligible, Low and Moderate risks that should be monitored.

Risk Factor & Rating	Risk Treatment and Accountability
Environment Risks	
Power Failure Water Failure Telecoms Flooding Earthquake Fire Landslides Demographics	• Regular testing of emergency management system • Maintenance and audit program for systems • BCP/Disaster Recovery Plan (annual testing) • Crisis Management Plan (bi-annual testing) • Incident Management Plan (bi-annual testing) • Develop and update escalation model • Establish formal Stakeholder Relationship Plan • Implement enterprise security incident reporting system • Site specific security procedures • Liaison with utility providers as part of annual BCP Testing • Liaison with Telco providers as part of annual BCP Testing
Security Risks	
Physical Security	• Escalate reporting of identified issues to appropriate stakeholders • Action identified issues on an immediate basis • Maintain site specific security procedures and processes • Enterprise/site security incident reporting and awareness program • Maintain enterprise Counselling Plan • Maintain enterprise wide education, awareness program and Code of Conduct • Develop site specific security incident capability and awareness program • Zero tolerance for offenders • Provide portable duress system for key staff • Identify higher risk areas and ensure fixed and maintained CCTV cameras in these areas • Regular testing of Incident Management Plan and processes • Formal relationship with local and national authorities
Abduction/ Kidnap	• Establish Kidnap and Ransom Plan • Regular testing of Incident Management Plan and processes • Formal relationship with local and national authorities • Establish Formal relationship with international advisor

Bomb Hoax	• Test and review policies and systems on a regular basis • Escalate reporting of identified issues to appropriate stakeholders • Action identified issues on an immediate basis
Bomb Detonation Noxious Chemicals Discharge of Firearm	• Site specific security procedures and processes • Enterprise/site security incident awareness and reporting program • Fixed CCTV cameras in higher risk areas • Zero tolerance for offenders • Incident Management Plan and processes • Incident Management Plan formal relationship with local and national authorities, maintenance and audit program for systems • Tested emergency management system (fire detection) • BCP/Disaster Recovery Plan (annual testing) • Develop Incident Management Plan for Arson and/or Bomb Threats • Formal relationships with agencies, e.g. CFA/Police/AFP/ASIO
Arson Malicious Damage Sabotage Denial of Access	• Site specific security procedures and processes • Enterprise/site security incident awareness and reporting program • Fixed CCTV cameras in higher risk areas • Zero tolerance for offenders • Incident Management Plan and processes • Incident Management Plan formal relationship with local and national authorities • Maintenance and audit program for systems • Tested emergency management system (fire detection) • BCP/Disaster Recovery Plan (annual testing) • Develop Incident Management Plan for Arson and or Bomb threats • Formal relationships with agencies, e.g. MFB/CFA/Police/AFP/ASIO
Vandalism	• Ensure systems maintenance program is adequate and appropriate • Ensure maintenance program is conducted per the required schedule and standards • Test and review systems on a regular basis • Escalate reporting of identified issues to appropriate stakeholders • Action identified issues on an immediate basis • Remove vandalism as soon as possible • Photograph and report vandalism to police

Integrity Risks	
Theft of Information Burglary Theft from Vehicles Theft of Vehicle	• Maintain site specific security procedures and processes • Enterprise/site security incident reporting and awareness program • Ensure fixed CCTV cameras in strategic risk areas • Formal relationships with local agencies • Portable duress system for front line staff • Fixed CCTV cameras in higher risk areas • Maintenance and audit program for systems • Crisis/Incident Management Plans • Formal relationship with local authorities e.g. Police
Theft of Physical Asset Theft from Building	• Maintain site specific security procedures and processes • Enterprise/site security incident reporting and awareness program • Ensure fixed CCTV cameras in strategic risk areas • Formal relationships with local agencies • Portable duress system for front line staff • Fixed CCTV cameras in higher risk areas • Maintenance and audit program for systems • Crisis/incident management plans • Implement a clear desk policy • Secure high-risk areas when not being used • Formal relationship with local authorities e.g. Police
Eavesdropping Telephone Tapping	• Implementation of anti-eavesdropping equipment in sensitive areas • Implement security sweeps prior to sensitive meetings; inclusive of Security Guard until meeting concludes • Embedded event response process to identify eavesdropping equipment • Implement an awareness program with senior management in sensitive positions • Implement an 'external surveillance' procedure, framework and managerial processes • Complete a review of higher risk applications that users can download onto their phones; higher risk applications should be banned within policies • Review the policy surrounding wireless connections from phones • Engagement with Information Technology to encrypt devices • Implement an awareness program with senior management, executives and staff
Political Risks	
Terrorism Civil Disorder Anti-Social Behaviour	• Develop and maintain site specific security procedures and processes • Enterprise/site security incident reporting and awareness program • Ensure fixed CCTV cameras in strategic risk areas • Emergency management system tested and up to date • Provision of portable duress system for front line staff • Maintenance and audit program for systems • BCP/Disaster Recovery Plan (annual testing) • Up to date Crisis/Incident Management Plans • Formal relationship management program with local and national authorities • Establish enterprise counselling plan including access for families

Bellrock Risk & Special Services | ABN 84 169 225 343
41 – 47 Thomsons Road, Keilor Park, VIC, Australia, 3043
T: 61 1800 273 732 | E: connect@bellrockgroup.com.au | W: bellrockgroup.com.au