Attachment G.18

SAPN_PUBLIC_IT Enterprise Information Security Business Case Step Change

03 July, 2015

Table of contents

[redacted]

1 Executive summary

The Enterprise Information Security function of SA Power Networks is responsible for proactively preventing, detecting and responding to security threats across the Information Technology (**IT**), Operational Technology (**OT**) and Telecommunications (**Tel**) networks, leading to safe and available enterprise information systems, and the level of service expected by our customers.

In October 2014, SA Power Networks submitted the 'Information Security Foundation' business case[1] as part of its regulatory proposal to the Australian Energy Regulator (**AER**). The business case recommended a range of measures to improve information security at SA Power Networks, in order to respond to increasing levels of security threats and to close the gap between the information security controls at SA Power Networks as at July 2014 and the level already implemented by SA Power Networks' industry counterparts.

In its Preliminary Decision on SA Power Networks determination 2015-16 to 2019-20[4] (**Preliminary Determination**), the AER has rejected the proposed opex step change for information security improvements due to the following two reasons:

1) The AER expected that the costs of achieving compliance with changed privacy laws "would be reflected in SA Power Networks' base opex" because the privacy law changes "should have taken effect by 12 March 2014"[5].
2) For all other proposed improvements, the AER stated that it considered that "SA Power Networks has not clearly put forward a case as to why it would require an increase in its total opex budget for this program"[6]. In particular, the AER listed seven specific areas in relation to which, in the AER's view, the information was not clearly stated or insufficient[7].

We do not accept the AER's Preliminary Determination to reject the opex step change for information security. In response to the AER's reasons for rejecting our proposed opex step change, we note that:

1) Changes to privacy laws were not the main driver for the increased opex requirements.

[1] *Information Security Foundation Business Case*, Project Ref Number BC26, Supporting Document 20.102, SA Power Networks, October 2014.
[2] Unless otherwise specified, all costs are expressed in June 2015, $ million.
[3] The period between 1 July 2015 to 30 June 2020 $ June 2015.
[4] *Preliminary Decision on SA Power Networks determination 2015-16 to 2019-20*, Australian Energy Regulator, April 2015
[5] *Preliminary Decision SA Power Networks determination 2015-16 to 2019-20, Attachment 7 – Operating Expenditure*, Australian Energy Regulator, April 2015, p. 7-91
[6] *Preliminary Decision SA Power Networks determination 2015-16 to 2019-20, Attachment 7 – Operating Expenditure*, Australian Energy Regulator, April 2015, p. 7-93
[7] *Preliminary Decision SA Power Networks determination 2015-16 to 2019-20, Attachment 7 – Operating Expenditure*, Australian Energy Regulator, April 2015, p. 7-93. The AER considered that "the business case did not identify:
1) the specific information security risks SA Power Networks faces
2) whether those risks have caused incidents for SA Power Networks in the 2010-15 RCP
3) the cost to SA Power Networks from those incidents
4) how those risks are expected to change in the 2015-20 RCP from the risks it faced in the 2010-15 RCP
5) what options SA Power Networks has considered to deal with those specific risks
6) how these options do or do not address the specific risks SA Power Networks has identified
7) why the preferred options need to be funded through an increase in SA power Networks' total opex budget."
[8] This program is described in the *Information Security Foundation Business Case*, Project Ref Number BC26, Supporting Document 20.102, SA Power Networks, October 2014..

[redacted]

2) We disagree with the AER's assessment that the 'Information Security Foundation' business case did not clearly put forward a case for an increase in the total opex budget for information security program. Nevertheless, we have carefully reviewed the AER's assessment of the business case and provided more information in relation to the seven areas identified in the AER's assessment as inadequately covered in the business case. The summary of our answers is provided below and the detailed answers are presented in the main body of this document.

Table 1: SA Power Networks' summary response to the seven areas identified in the AER's Preliminary Determination as inadequately covered in the Information Security Foundation business case

Summary response	Detail
AER question #1: ***[What are] "the specific information security risks SA Power Networks faces"?***	

The specific security risks that were faced by SA Power Networks at the time of the development of the 'Information Security Foundation' business case have been presented in Section 4.1.6 of the business case. These risks have recently been updated to take into account the increased exposure due to the IT/OT/Tel convergence. The key risks currently faced by SA Power Networks can be categorised as follows:
• **Information Technology risks** – the risks related to unauthorised access to the corporate IT environment by an external or internal party resulting in SA Power Networks' corporate systems and data being compromised. The risk analysis has been carried out that shows that if the proposed operational activities are not undertaken, there is [redacted] risk of the following consequences to our customers, staff, contractors and owners:
  ○ interruptions to customer facing services and/or loss of data resulting in non-compliance with our regulatory or legal obligations, financial penalties and potential loss of life[9];
  ○ disclosure of corporate information to unauthorised parties resulting in increased vulnerability to future attacks, potential reputational damage and financial consequences; and
  ○ disclosure of private and sensitive information held by SA Power Networks in relation to our customers, staff and contractors resulting in potential financial or reputational consequences to those parties and financial penalties to SA Power Networks.
• **Operational Technology risks** – the risks related to unauthorised access to the OT environment by an external or internal party resulting in SA Power Networks' electricity distribution system and related data being compromised. The risk analysis has been carried out that shows that if the proposed operational activities are not undertaken, there is [redacted] risk of the following consequences to our customers:
  ○ power outages;
  ○ damage to power networks; and
  ○ potential loss of life.
• **Supply chain risks** – the risks related to unauthorised access to either corporate IT environment or OT environment via a third party supplier[10] whose network or equipment has been compromised, resulting in the consequences described above.
	Our detailed response to this question can be found in Section 4.1 of this document.

[9] SA Power Networks is required to support customers who are on life support systems

[10] Examples include suppliers of development and maintenance services for SA Power Networks core business systems or a supplier of maintenance services for the Supervisory Control and Data Acquisition (**SCADA**) system.

Summary response	Detail
AER question #2: ***[Identify] "whether those risks have caused incidents for SA Power Networks in the 2010-15 RCP".***	
[redacted]	Refer to Section 4.2 of this document for our detailed response.
AER question #3: ***[What was] "the cost to SA Power Networks from those incidents"?***	
[redacted]	Refer to Section 4.2 of this document for our detailed response.

[redacted]

Summary response	Detail
AER question #4: ***"How those risks are expected to change in the 2015-20 RCP from the risks it faced in the 2010-15 RCP"?***	
Those risks are expected to increase in the 2015-2020 RCP due to: • increased terrorist and cyber-criminal activity as evidenced from recent industry and government reports[13]; • convergence between IT, OT and Tel environments [redacted] A cyber security attack in 2015 to a US based utility was enabled by a combination of physical vulnerabilities and network-enabled capability which disabled SCADA and Telecommunication systems. [14]; • greater number of external suppliers [redacted]; and • greater variety of devices and applications used on the network, [redacted]	Refer to Section 4.1 of this document for our detailed response.
AER question #5: ***"What options SA Power Networks has considered to deal with those specific risks"?***	
As described in the 'Information Security Foundation' business case, SA Power Networks has considered three options to deal with those risks: [redacted]	Refer to Section 4.3 of this document for our detailed response.

[13] Refer, for example: *Targeted Attacks Against the Energy Sector*, Symantec, 1 January 2014, June 2013 Status Report, US Department of Homeland Security, 1/6/2013 and The Global State of Information Security® Survey 2015, PwC.

[14] Refer, *Experts warn of escalating grid security issues after PG&E break-in*, June 2015, http://www.utilitydive.com/news/experts-warn-of-escalating-grid-security-issues-after-pge-break-in/400524/

Summary response	Detail
AER question #6: ***"How these options do or do not address the specific risks SA Power Networks has identified"?***	
[redacted]. The Status Quo option was not considered adequate to address the identified risks because not all cyber security risks can be prevented. This has been demonstrated by numerous recent studies and is increasingly recognised by industry experts. For example, in March 2015 the commander of the US Cyber Command and National Security Agency was quoted as saying that business leaders should assume hackers are penetrating their networks: "We must increasingly assume that despite our best efforts, they're going to get in"[16]. Therefore, a more complete security program to not only prevent, but also detect and quickly respond to security breaches is the only appropriate strategy. [redacted]	Refer to Section 4.3 of this document for our detailed response.
AER question #7: ***"Why the preferred options need to be funded through an increase in SA power Networks' total opex budget"?***	
In its Preliminary Determination, the AER indicated that, consistent with the AER Expenditure Assessment Guideline[17], its approach to the opex assessment considers[18]: • "…whether the proposed step changes in opex are already compensated through other elements of our opex forecast. Such as the base efficient opex or the 'rate of change' component…" and also • " …whether each proposed step change is driven by an external obligation (such as new legislation of regulations)…" and • "Step Changes should generally relate to a new obligation or some change in the service providers operating environment beyond its control." The proposed opex step change for information security is required to respond to the changes in operating environment beyond SA Power Networks' control (i.e., increasing levels of terrorist and cyber-criminal activities), to meet our regulatory compliance obligations under changing market requirements, and to prudently prepare to meet the increased expectations of the Federal Government on Critical Infrastructure providers in response to increased cyber security threats. [redacted]	Refer to Section 4.4 of this document for detailed response.

[15] *Information Security Foundation Business Case*, Project Ref Number BC26, Supporting Document 20.102, SA Power Networks, October 2014, p.7.
[16] *US Cyber Chief issues corporate hacking warning*, Australian Financial Review, 5 March 2015.
[17] *Expenditure assessment forecast guideline*, AER, November 2013, p. 11.
[18] Preliminary Decision SA Power Networks determination 2015-16 to 2019-20 Attachment 7 – Operating expenditure April 2015, Section C3.

Summary response	Detail
[redacted]	
The proposed opex step change cannot be compensated through the 'rate of change' allowance, which covers price growth, output growth and productivity growth. The opex step change to mitigate the increasing levels of security threats has not been included in the 'rate of change' allowance as it is not influenced by forecast network growth, price increases for current materials of labour due to Consumer Price Index (CPI) changes, or improvements in productivity or efficiency. The opex step change relates to prudent and efficient costs required to respond to the changes in SA Power Networks operating environment driven by external environment changes that are beyond our control.	

Based on the reasons outlined above, we disagree with the AER's decision to reject our proposed opex step change for information security. However, since the start of the implementation of our security program in 2014, we were able to reduce the associated ongoing operating costs [redacted]

Our revised proposal is outlined in [redacted]

[redacted]

[redacted]

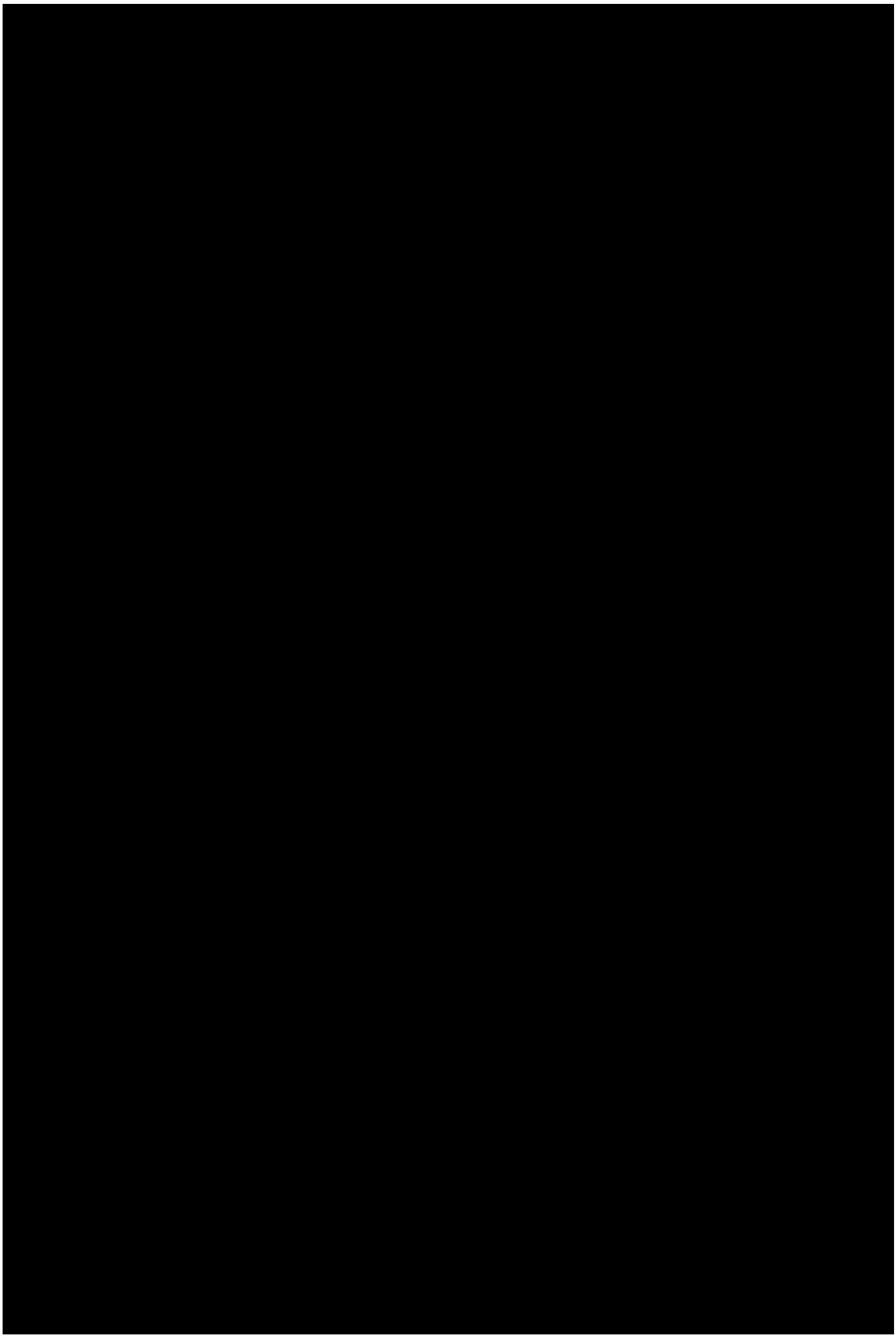
SA Power Networks' approach to increasing the overall IT Security Support FTE is in line with the federal government's focus on cyber security and the need for specialist cyber personnel. The Defence Minister Kevin Andrews said "… the upcoming Defence White Paper [August 2015] would include a multi-pronged approach to cyber warfare including:

- Growing the specialist cyber workforce,
- Increased resources to protect sensitive information, systems and platforms,
- An international rules based approach to cyber issues"[19]

[redacted]

[19] "Australia to spend millions and employ 'cyber warriors' to stop growing threat of cyberttacks" http://www.news.com.au/national/politics/australia-to-spend-millions-and-employ-cyber-warriors-to-stop-growing-threat-of-cyber-attacks/story-fns0jze1-1227402546867

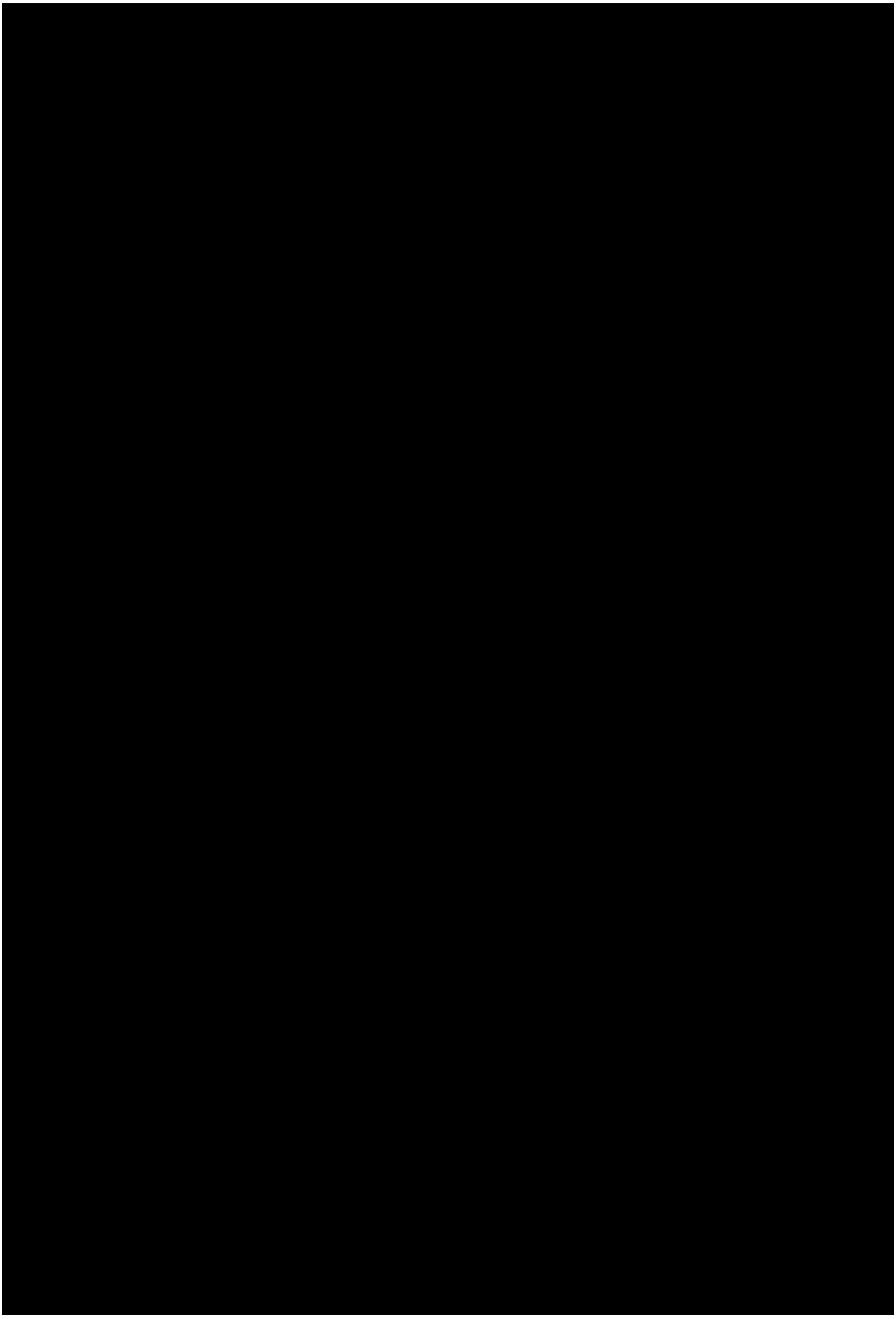
[20] *Gartner IT key metrics data*, Gartner, December 2013. The *Gartner IT key metrics data*, Gartner, December 2014 also shows a continuing increase in FTEs supporting security functions across industries. SA Power Networks was unable to obtain the Utilities specific information.

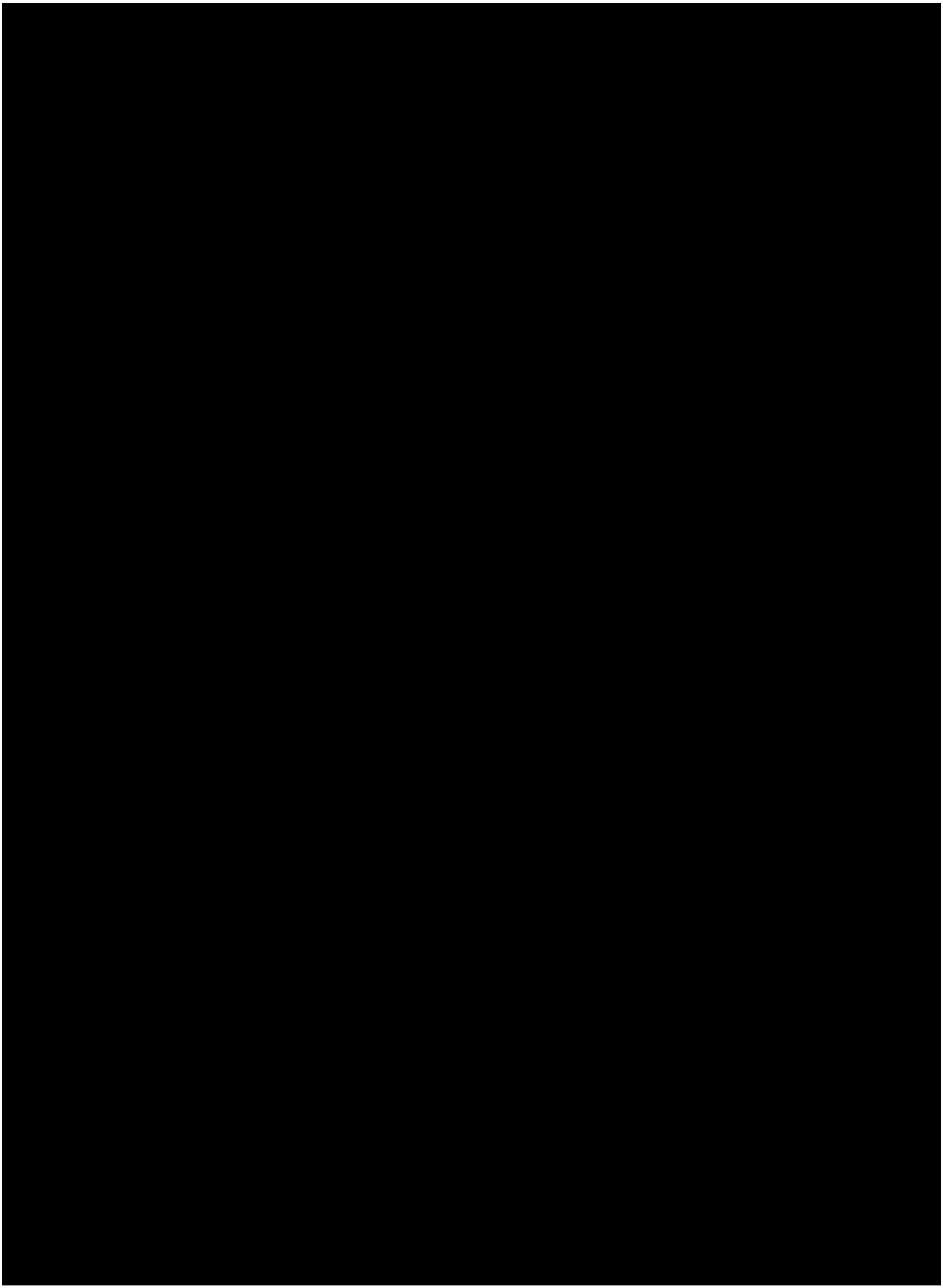


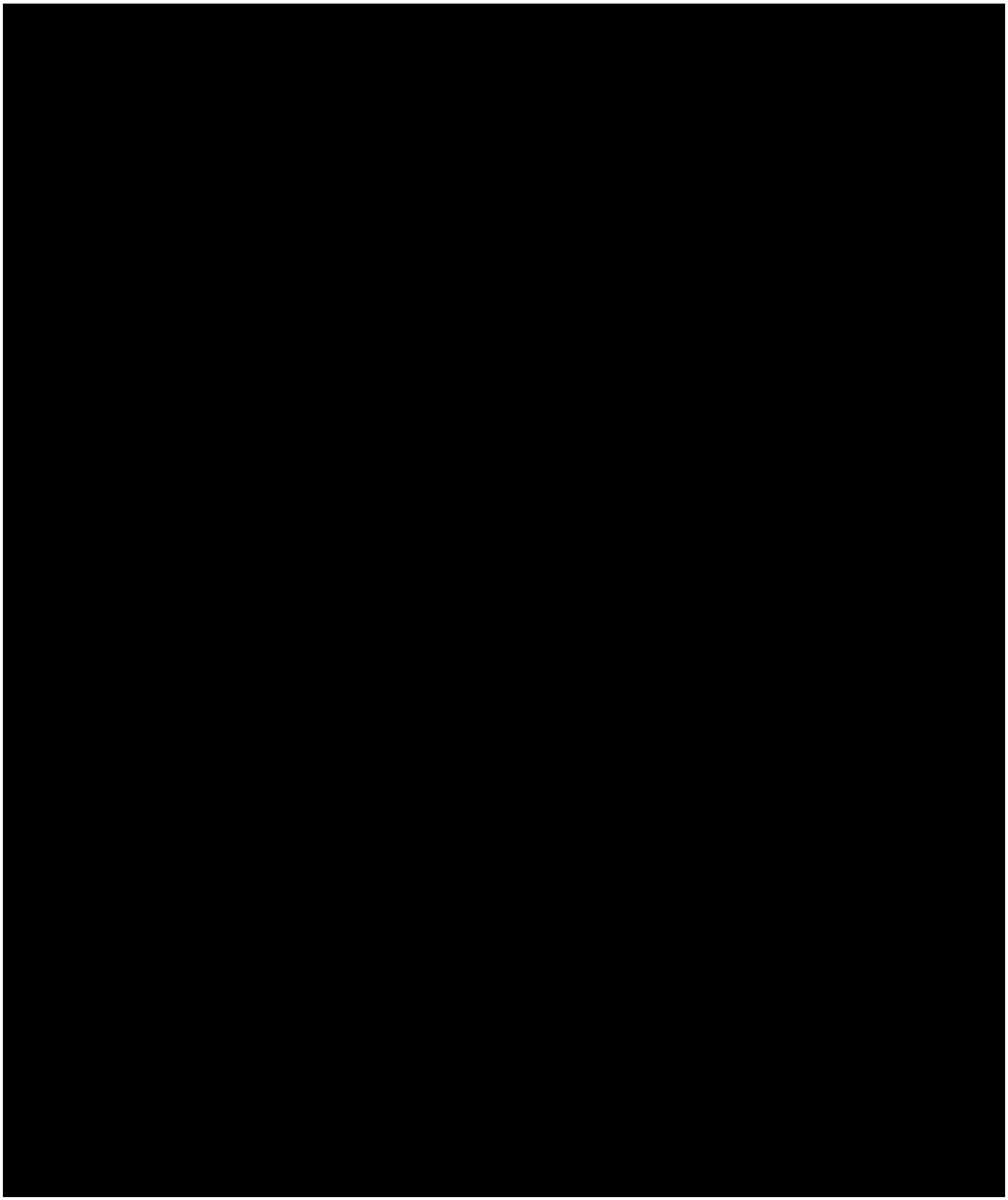
[redacted]

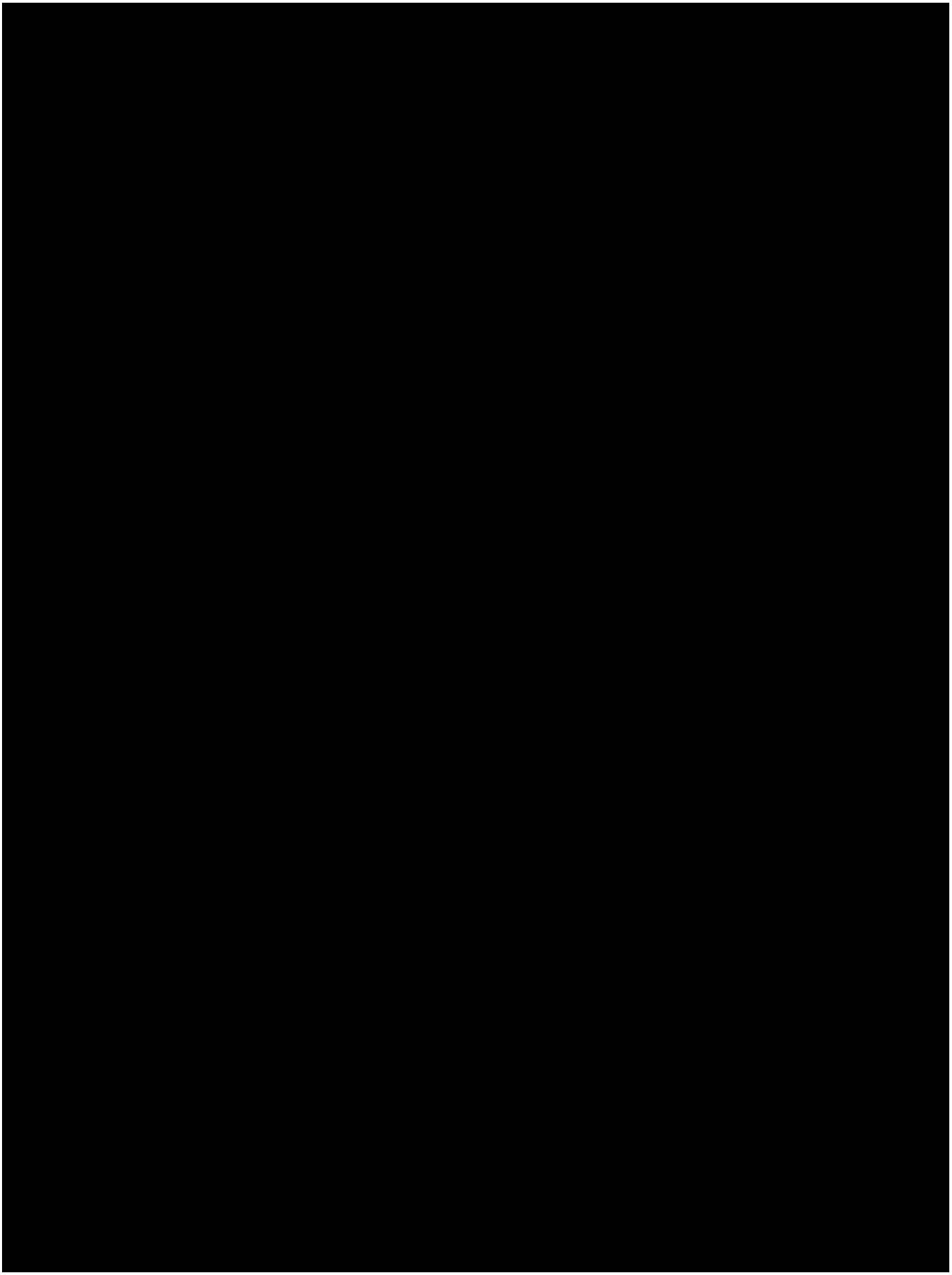
[22] Gartner defines IT Security FTE as: IT Security personnel includes in-house and contract full-time equivalents supporting the following IT security functions: IT infrastructure and application security, general IT risk process management, IT compliance process management, and IT privacy process management Information Technology Security Analysis Framework.

[23] Gartner defines an IT FTE as: An IT FTE represents the logical staff to support functions performed by the physical staff, measured in calendar time. This includes all staffing levels within the organization from managers and project leaders to daily operations personnel. This includes both in-sourced FTEs and contract FTEs. This excludes staff of a third-party vendor, who are not operationally managed by in-house staff, but managed by service-level agreements.









[redacted]

[24] PwC: Global State of Information Security Survey 2015 – Power and Utilities
[25] https://www.pm.gov.au/media/2014-11-27/cyber-security-review-0
[26] http://www.tisn.gov.au/documents/australian+government+s+critical+infrastructure+resilience+strategy.pdf
[27] http://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf
[28] Opening address at the 2015 Australian Cyber Security Centre (ACSC) Conference by Attorney-General for Australia

[redacted]

[29] NER 6.5.6(a) (2) and NER 6.5.6(a) (4) Compliance/Regulatory, NER 6.5.7 (a) (3) and NER 6.5.6 (a) (3) Maintain the quality Reliability and Security of Supply

[30] http://www.asd.gov.au/speeches/20140505_ascs_cebit_cyber_security.htm

[redacted]

[31] Trojan horse that encrypts files on the compromised computer and then prompts the user to purchase a password to decrypt.
[32] http://www.mcafee.com/au/about/news/2014/q3/20140904-01.aspx

[redacted]

[33] http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat
[34] http://www.theage.com.au/it-pro/security-it/what-a-major-data-breach-costs-target-by-the-numbers-20140506-zr5ny.html
[35] Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Monitor (Oct-Dec 2012),* USA, 2012
[36] http://www.businesswire.com/news/home/20150413005064/en/Dell-Annual-Threat-Report-Sheds-Light-Emerging#.VXp3i_4cSB9
[37] Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Monitor (Jan-Apr 2014),* USA, 2014
[38] Refer, *Experts warn of escalating grid security issues after PG&E break-in*, June 2015, http://www.utilitydive.com/news/experts-warn-of-escalating-grid-security-issues-after-pge-break-in/400524/

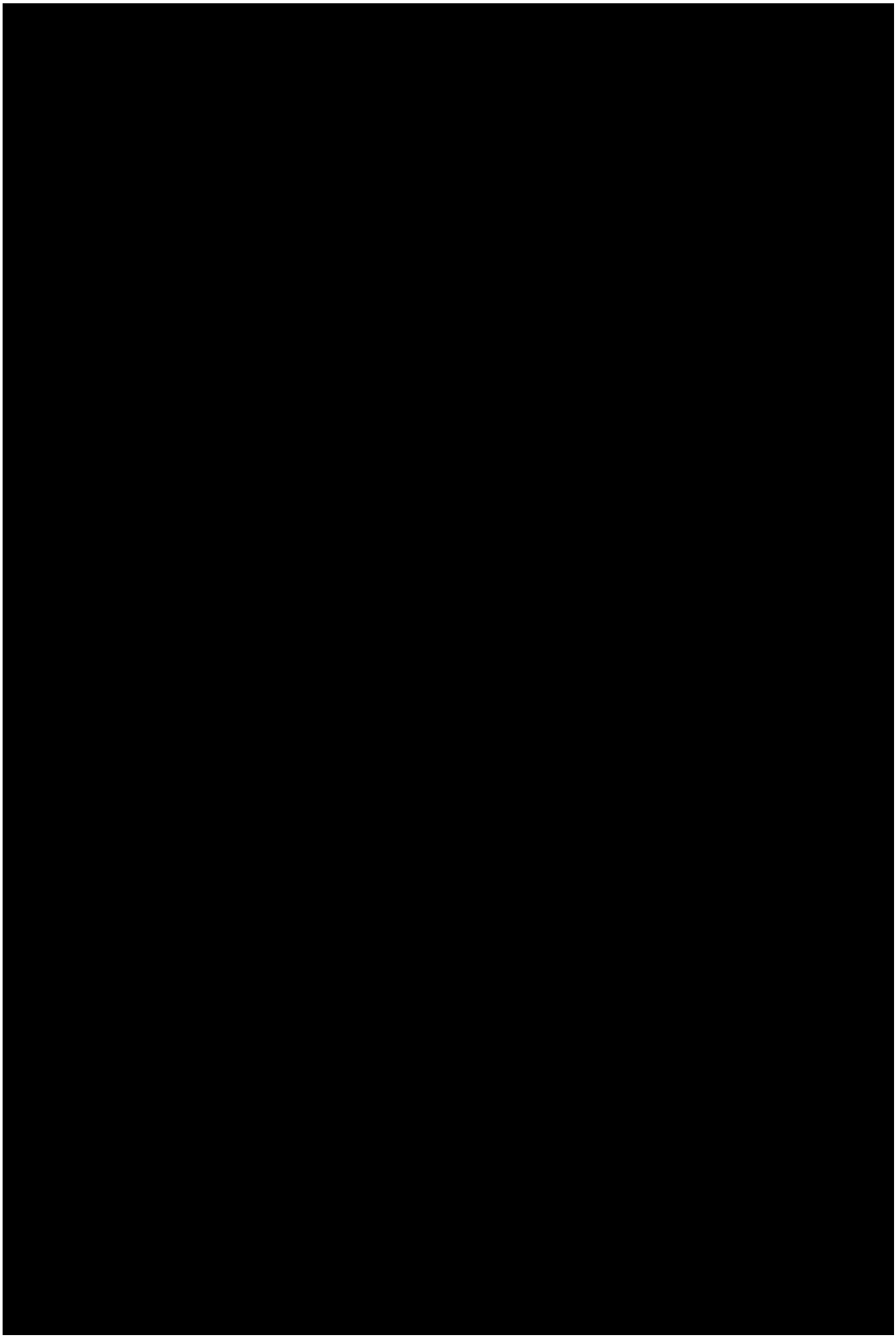
[redacted]

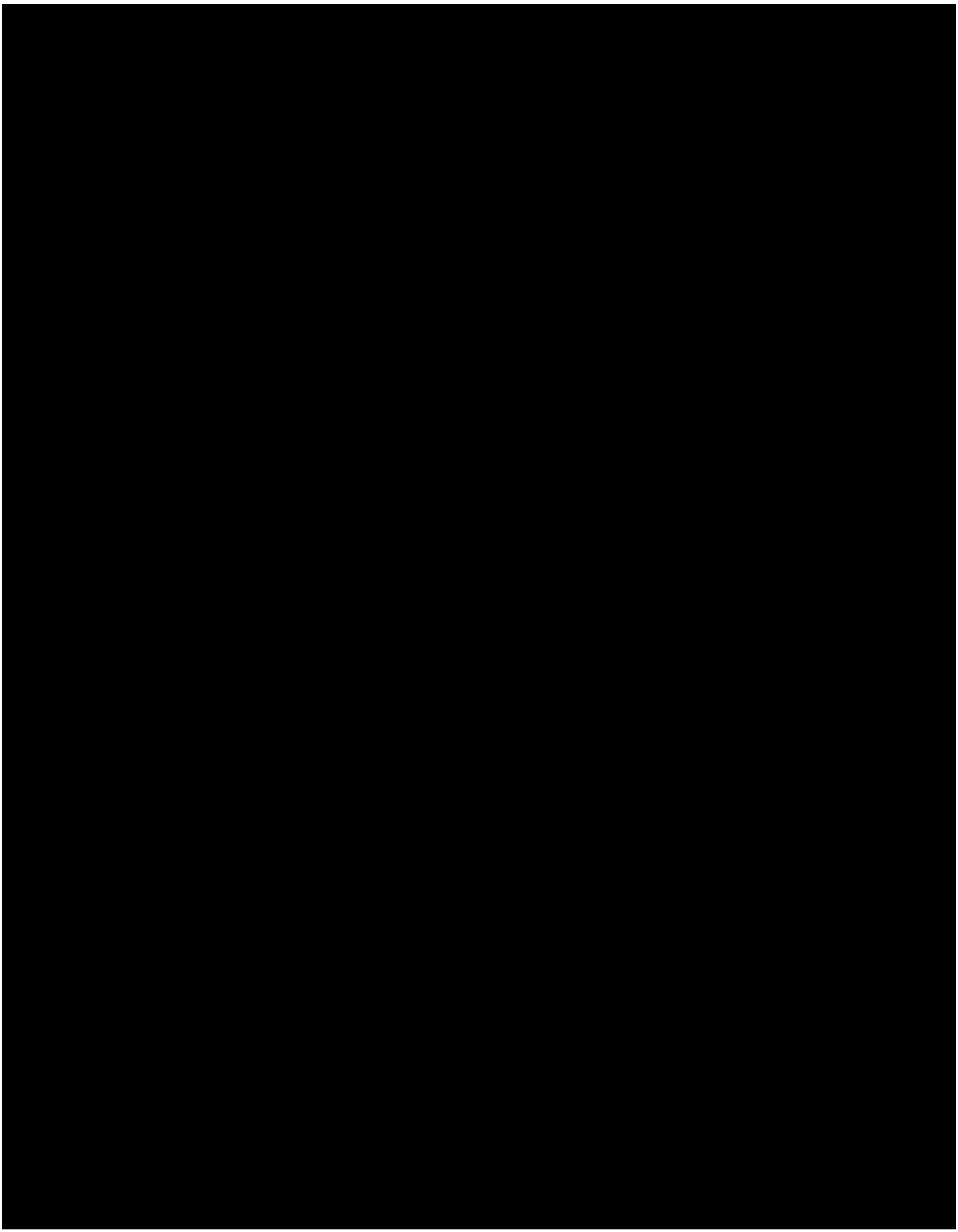
[39] US Cyber Chief issues corporate hacking warning, Australian Financial Review, 5 March 2015

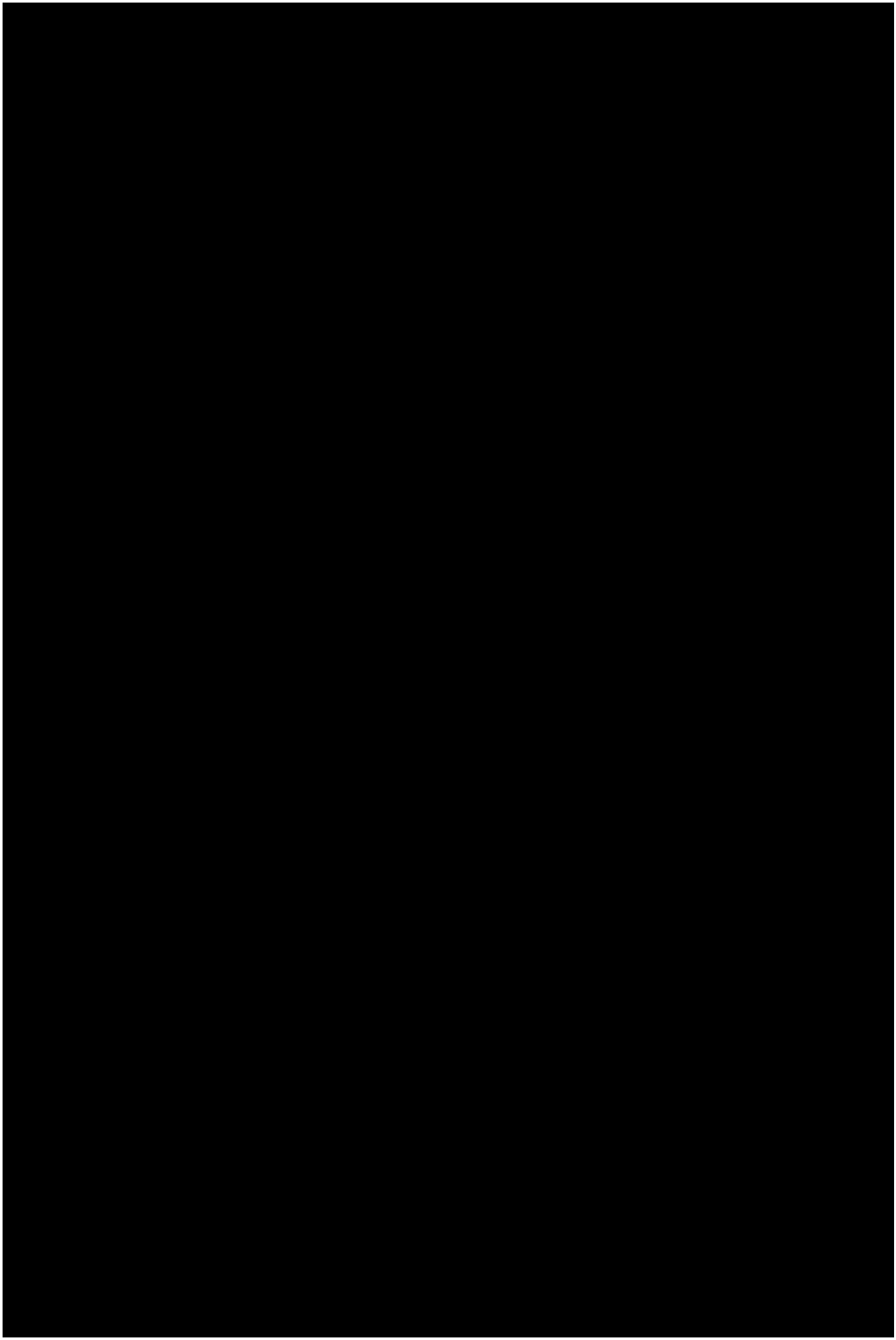
[redacted]

[40] Catastrophic consequences are defined as follows:

- Financial impact of $100m or more OR
- WHS - Multiple Fatalities OR
- Environment - Long term environmental harm. Permanent irreparable damage OR
- Reputation /Customer Service / Legislative and Regulatory - Loss of Distribution Licence OR
- Organisational - Disaster which can cause collapse of the business OR
- Reliability - Adelaide CBD without supply for longer than 24 hours.







[redacted]

[41] Attachment 20:102 Information Security Foundation Business Case

[redacted]

[42] Preliminary Decision SA Power Networks determination 2015-16 to 2019-20 Attachment 7 – Operating expenditure April 2015 Section C3

[43] NER 6.5.6(a) (2) and NER 6.5.6(a) (4) Compliance/Regulatory, NER 6.5.7 (a) (3) and NER 6.5.6 (a) (3) Maintain the quality Reliability and Security of Supply

[redacted]

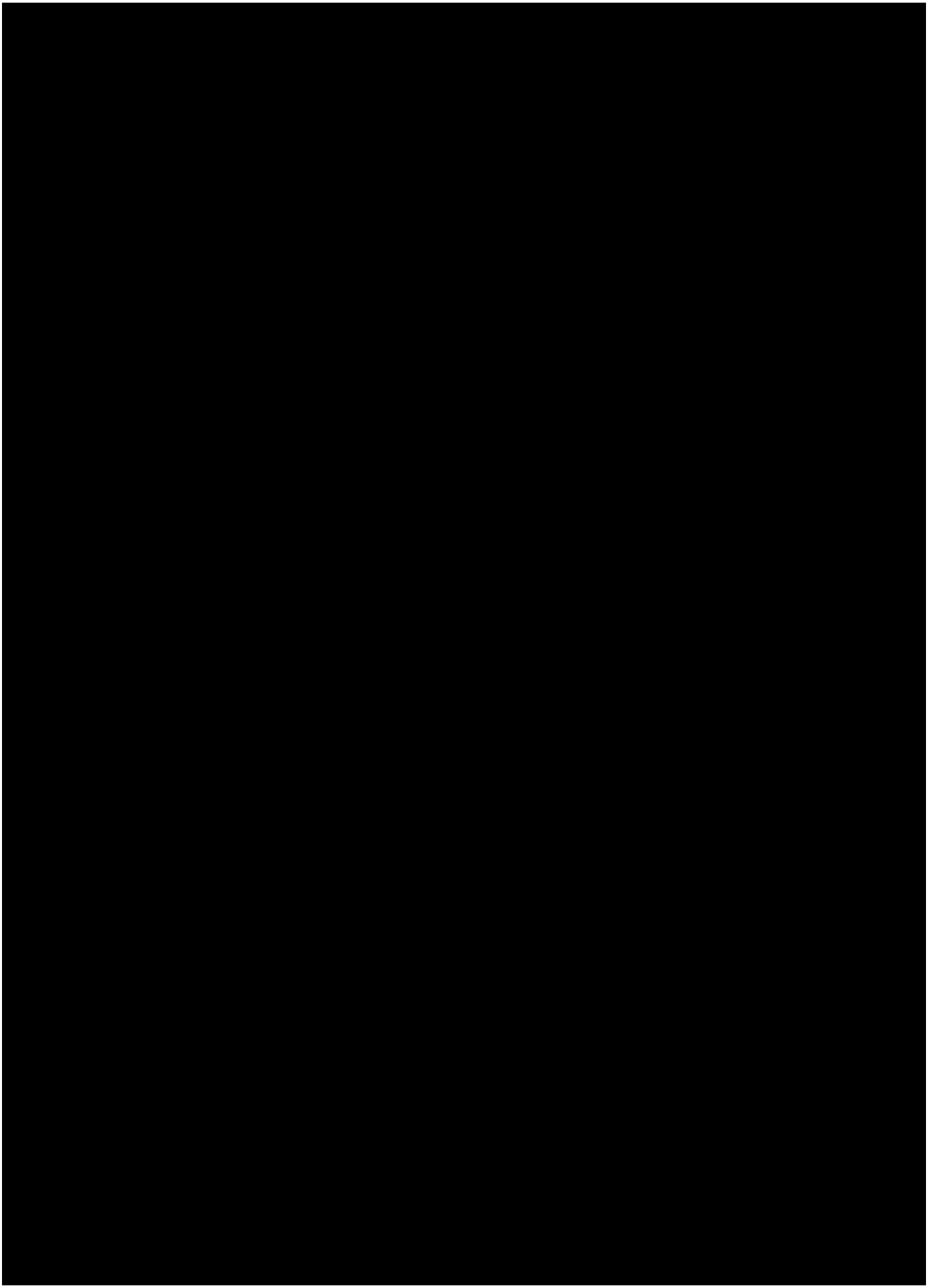
[redacted]

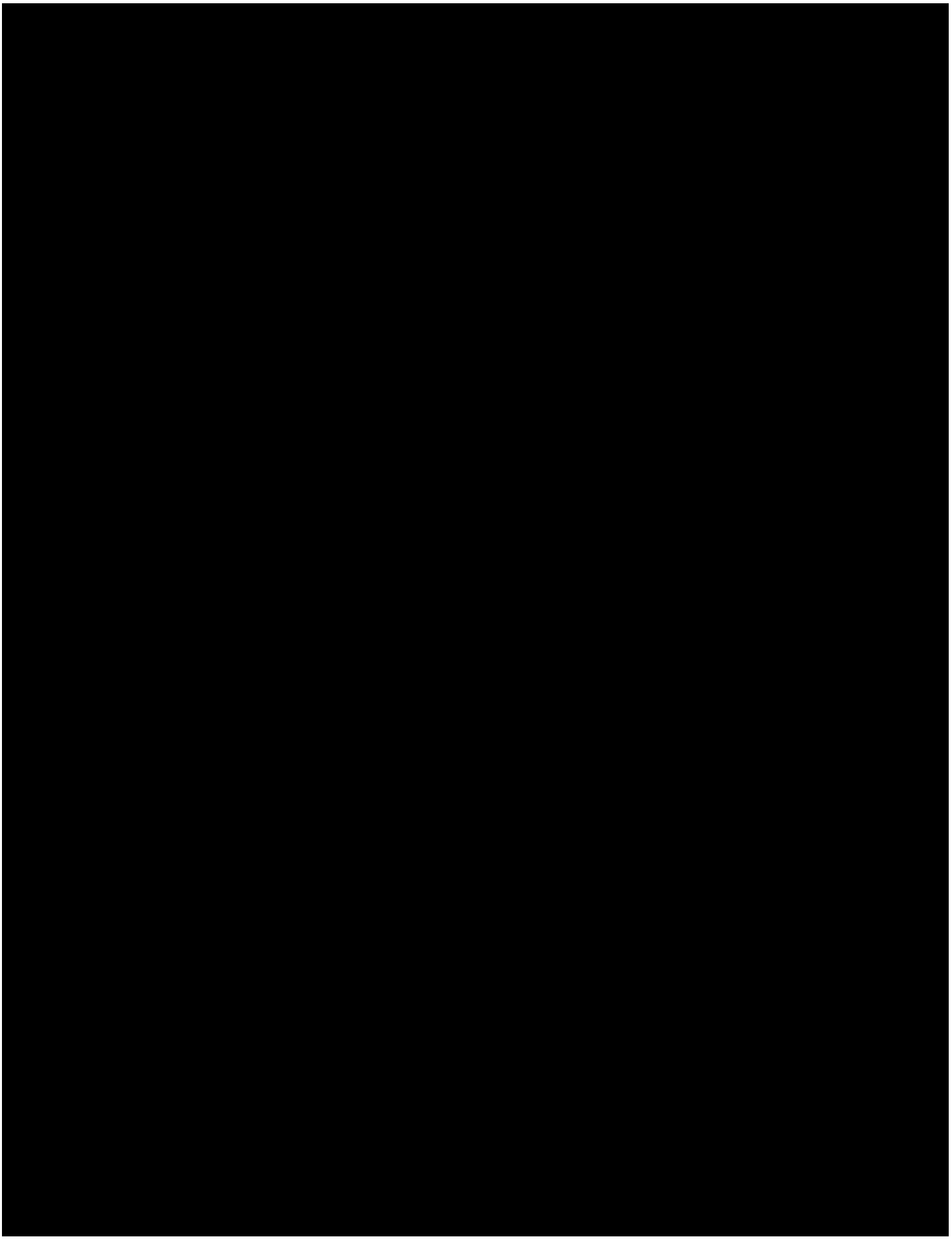
[44] Gartner defines IT Security FTE as: IT Security personnel includes in-house and contract full-time equivalents supporting the following IT security functions: IT infrastructure and application security, general IT risk process management, IT compliance process management, and IT privacy process management Information Technology Security Analysis Framework.

[45] Gartner defines an IT FTE as: An IT FTE represents the logical staff to support functions performed by the physical staff, measured in calendar time. This includes all staffing levels within the organization from managers and project leaders to daily operations personnel. This includes both in-sourced FTEs and contract FTEs. This excludes staff of a third-party vendor, who are not operationally managed by in-house staff, but managed by service-level agreements.

[46] Gartner IT Key Metrics Data 2015: Key IT Security Measures: by Industry Published: 15 December 2014. Report No: G00266084

[47] "Australia to spend millions and employ 'cyber warriors' to stop growing threat of cyberttacks" http://www.news.com.au/national/politics/australia-to-spend-millions-and-employ-cyber-warriors-to-stop-growing-threat-of-cyber-attacks/story-fns0jze1-1227402546867





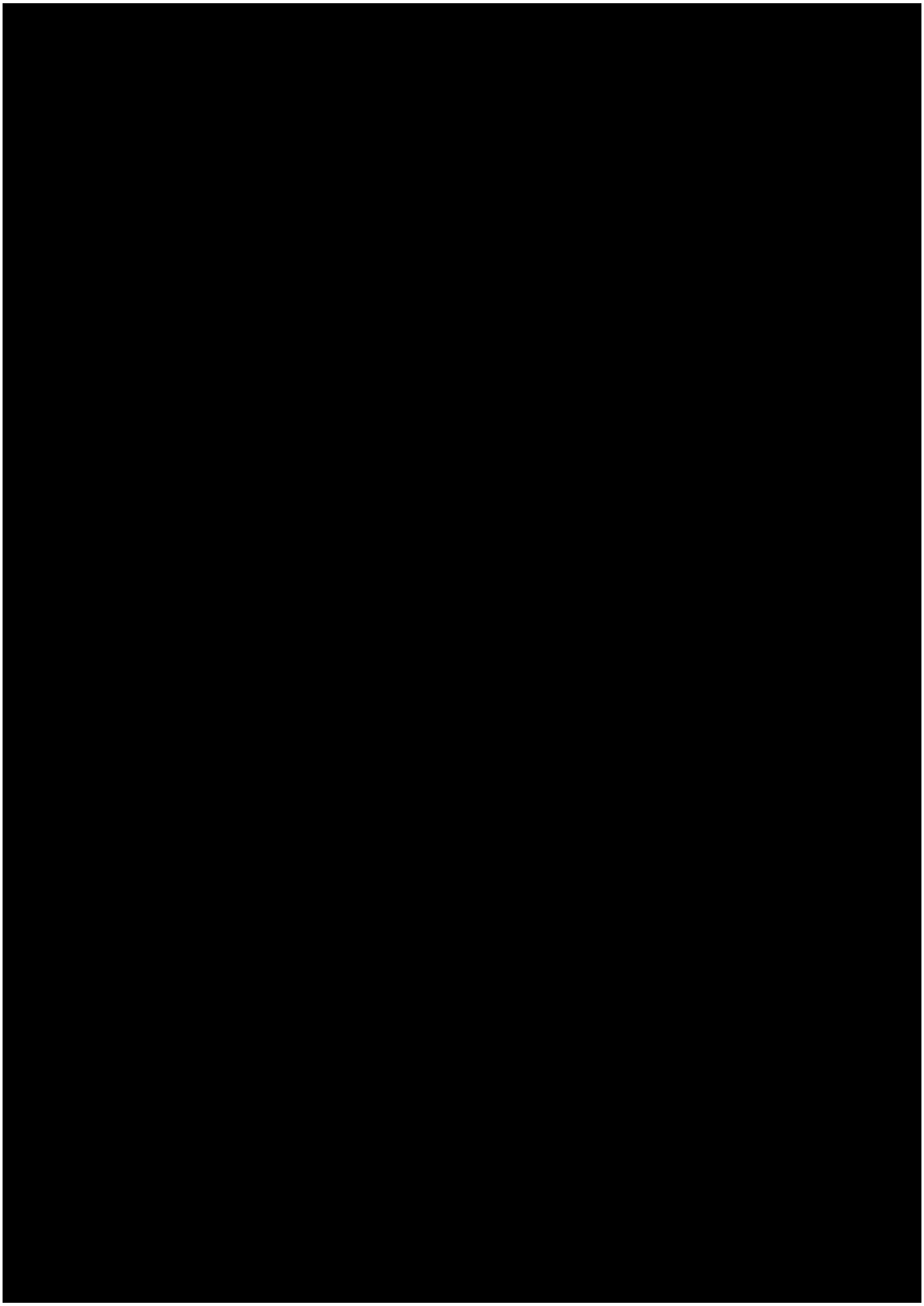
[redacted]

[48] In June 2015 $ terms, the opex step change has reduced from $10.2 million in our Original Proposal is $9.0 million

6 References / supporting documents

Ref	Document Name	Date	Version	Author
1.	Enterprise Information Security Strategy FINAL	25/11/2014	V1.0	SA Power Networks
2.	The Global State of Information Security® Survey 2014 – Power and Utilities	2014	N/A	PwC
3.	The 2015 Global State of Information Security Survey – Power and Utilities	2015	N/A	PwC
4.	Gartner IT Key Metrics Data 2015: Key IT Security Measures	Dec 2014	N/A	Gartner
5.	SA Power Networks Regulatory Proposal 2015-20.	Oct 2014		SA Power Networks
6.	Attachment 21.13. SA Power Networks Opex Step Changes.	30/10/2014		SA Power Networks
7.	Attachment 20:102 Information Security Foundation Business Case	30/10/2014		SA Power Networks
8.	Attachment 20:35 Information technology Strategy 2014-2020	30/10/2014		SA Power Networks
9.	Attachment 20:32 Information Technology Investment Plan 2015-2020	30/10/2014		SA Power Networks
10.	SA Power Networks Risk Management Framework	Sept 2014		SA Power Networks
11.	Targeted Attacks Against the Energy Sector,	Jan 2014		Symantec
12.	June 2013 Status Report	Jun 2013		US Department of Homeland Security
13.	1 US Cyber Chief issues corporate hacking warning	5 March 2015		Australian Financial Review
14.	Expenditure assessment forecast guideline, p. 11	Nov 2013		AER
15.	Ernst & Young 2012 Global Information Security Survey	2012		Ernst and Young
16.	Federal Government Critical Infrastructure Resilience Strategy	May 2015		Australian Federal Government
17.	National Guidelines for protection of critical infrastructure from terrorism	2011		Australian Federal Government
18.	Address on Cyber Security Review	Nov 2014		Prime Minister of Australia
19.	Address at the opening of the Australian Cyber Security Centre	Nov 2014		Attorney General for Australia
20.	Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Monitor (Jan-Apr 2014)*	Jan-Apr 2014		USA
21.	Address to the 2014 CeBIT Cyber Security Conference "Managing Cyber Security in an Increasingly Interconnected World"	May 2014		Australian Assistant Secretary for Cyber Security

Ref	Document Name	Date	Version	Author
22.	Ponemon Institute '2015 Cost of Data Breach Study: Australia'	May 2015		Ponemon Institute LLC



[redacted]