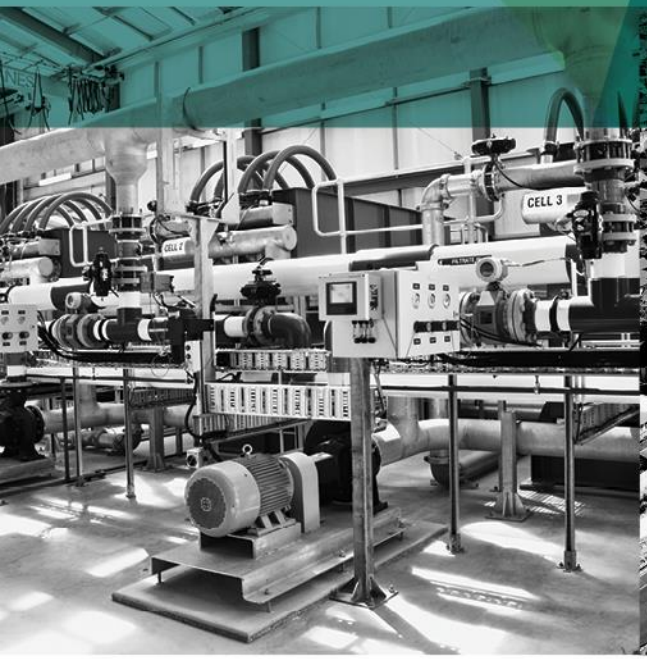
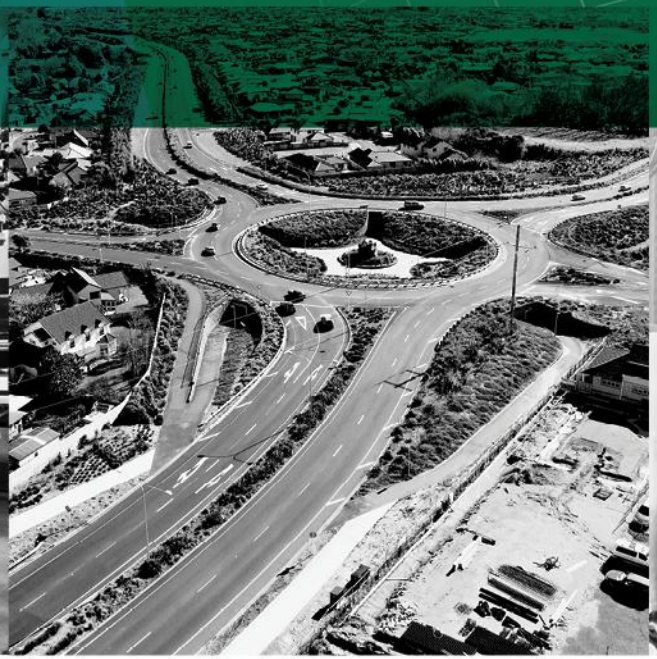
LGFA

NEW ZEALAND
LOCAL GOVERNMENT
FUNDING AGENCY

LGFA Cyber Risk review





July 2018

LGFA Cyber Risk Review

NEW ZEALAND LOCAL GOVERNMENT FUNDING AGENCY

Why complete a cyber risk review of LGFA?

- **Six years since LGFA commenced operations, three years since implementation of the treasury management system.**
- **Significant rise in the number and complexity of cyber attacks in recent years.**
- **In a 2017 NZ Institute of Directors survey, technological disruption was rated by members as the second biggest risk facing their organisations.**

Cyber risk management at LGFA

- **Nov 2016. Cyber risk classified as standalone business risk within the risk management framework.**
- **Jun 2017. Board paper outlining industry best practice for mitigating cyber risk.**
- **Nov 2017. FIS presentation to Board on their control environment for LGFA's treasury management system.**
- **Feb 2018. Independent controls report on FIS host environment.**
- **Mar 2018. Deloitte and PWC short-listed for independent review.**

PWC Review Scope

Review Scope

- **An overall assessment of LGFA's vulnerability to third party cyber attacks.**
- **'Deep dive' into the security of the VPN to LGFA's outsourced service provider of Treasury Management System.**
- **Review of suitability of Service Level Agreements with LGFA's outsourced IT providers.**
- **Evaluation of systems administration and access controls, including around the use of laptops and mobile devices.**
- **Education session for all staff.**

LGFA NEW ZEALAND LOCAL GOVERNMENT FUNDING AGENCY

Key findings

Limited risk of compromise to LGFA's key financial markets systems.

10 risk events that could lead to the following three possible impacts:

1. **Significant reputational damage.**
2. **Loss of shareholder or investor confidence.**
3. **Financial loss (in event that banking system security for overhead processing was compromised).**

10 identified risk events

NEW ZEALAND LOCAL GOVERNMENT FUNDING AGENCY

1. An LGFA laptop is stolen and attacker gains access to key systems and information.
2. A user inadvertently installs malware on a laptop.
3. Weak password management gives an attacker access to key systems.
4. Phishing or social engineering attacks compromise key systems.
5. Log on credentials for banking systems are compromised.
6. Employees accidentally expose sensitive information through email, cloud or other uncontrolled channels.
7. An attacker impersonates an engineer from LGFA's IT service providers.
8. Risk of interception on a shared wireless network.
9. Access to confidential information as a result of poor physical security controls.
10. Theft of paper copies of sensitive information.

PWC recommendations

NEW ZEALAND LOCAL GOVERNMENT FUNDING AGENCY

1. Ongoing security awareness training programme for all staff.
2. Incident response and communications plans for cyber incidents.
3. Multi-factor authentication for access to key systems.
4. Hard drive encryption on LGFA laptops.
5. 'Application whitelisting'
6. Formal procedures for software patching.
7. Implement detailed recommendations from VPN 'deep dive'
8. Regular review and reporting on VPN system logs.
9. Use of VPN for all public shared networks (or use mobile data).
10. Password management software to all staff.
11. Change name of LGFA wireless network.

In conclusion

NEW ZEALAND LOCAL GOVERNMENT FUNDING AGENCY

Given the increased frequency and severity of global attacks, cyber risk is a core business risk that requires ongoing monitoring and management.

From: Mark Butcher <mark.butcher@lgfa.co.nz>
Sent: Thursday, May 25, 2017 8:29:22 PM
To: Neil Bain
Subject: Re: Enquires

Are you available at the moment ? i have some payments i need you to process today

Regards

Mark Butcher

Sent From Mobile Outlook...