

## New Zealand Defence Force improves efficiency of response to network attacks

### Case study

**Industry sector**  
*Defence*

**Challenge**  
*Poor visibility of computer security response handling information across numerous databases made it difficult to track progress effectively.*

**Solution**  
*Blackthorn GRC provides a centralised response management solution. State-of-the-art encoding technology within the Blackthorn GRC Z-Crypto module ensures that information stays secure.*

**Benefits**  
*Advanced reporting features offer comprehensive status reporting and enable detailed proactive risk analysis. Collaborative tools support information-sharing with other departments.*

With numerous disparate systems for recording computer security incidents, it was difficult for staff within the New Zealand Defence Force (NZDF) to get a status overview. To address this, the organisation implemented Blackthorn GRC and significantly increased the efficiency of its incident management activities – improving situational awareness, ensuring that approved processes are followed, and cutting response time.

Comprising army, navy and air services, NZDF is responsible for safeguarding New Zealand's borders and interests, as well as participating in UN peacekeeping operations and humanitarian aid missions worldwide. Headquartered in Wellington, the organisation has 14,766 staff, including regular and reserve forces as well as civilian personnel.

#### Multiple databases

Along with other large organisations in both the commercial and public sectors, NZDF is subject to frequent attacks on its network. To combat these threats, its computer information security branch has established a range of software tools and protocols. However, with information held on multiple databases and spreadsheets, situational awareness was poor.

"We were looking for a better way to coordinate incidents," comments Chris Ward, Strategic Information Assurance Manager at NZDF. "To improve the efficiency of our response, we needed better visibility of investigations across the organisation."

#### Flexible and secure solution

To address this, NZDF decided to implement an incident management solution and selected Blackthorn GRC. As Ward explains, the flexibility of the solution was key to this decision.

"We were attracted by the fact that the software can be deployed to support different processes across numerous business areas, while drawing on a single data depository," he comments. "As well as allowing us to make cost savings because it reduces the number of solutions we must support and maintain, this also provides the opportunity to introduce leaner, more collaborative processes."

Security was also an important consideration for NZDF. "Blackthorn GRC's Z-Crypto module incorporates advanced encoding technology to ensure that information stays secure," says Ward. "With NZDF handling classified and sensitive data, this was a critical requirement for our chosen solution."

#### 24-hour support

With the help of the QCC team, the implementation of the software went smoothly. "Blackthorn GRC offers numerous pre-configured dashboards and standard workflows," remarks Ward. "This meant we could get the solution up and running quickly without having to start from scratch."

According to Ward, the customer support provided by QCC was also an important factor in the successful implementation. "Even though we're on the other side of the world, the QCC team offered 24-hour support," he says. "The service we've received has been absolutely fantastic. They met all our expectations – and more!"



*“Blackthorn GRC’s support for collaborative working helps to ensure that all necessary notifications take place and no process steps are missed.”*

Chris Ward, Strategic Information Assurance Manager, NZDF

*“If we have prior warning of the types of attack that other organisations are suffering, we can be better prepared to combat future threats.”*

Chris Ward, Strategic Information Assurance Manager, NZDF



### Supporting collaborative working

Now, when responding to a computer security attack, the NZDF teams follow a pre-approved process workflow within Blackthorn GRC. “There are different types of workflow for each incident so we can be sure that appropriate actions are taken at each stage,” comments Ward.

As part of the workflows, staff can also communicate with colleagues based in other locations, exchanging key information and sending notifications within the solution instead of using email or telephone calls. “Blackthorn GRC’s support for collaborative working helps to ensure that all necessary notifications take place and no process steps are missed,” highlights Ward. “It also saves a considerable amount of time, enabling us to respond faster to deal more effectively with computer security incidents.”

### Improved situational awareness

With a single, centralised point for all response tracking, it is now much easier for senior staff to obtain a full situation overview of all ongoing incidents. This helps them to monitor the team’s progress and act quickly to resolve any issues.

Analytical functionality within Blackthorn GRC is also providing managers with more detailed information about the number and type of attack, as well as response-handling time and cost per incident. “Previously, it took a significant amount of time to calculate the resources required to manage the incident response process – and even then, it could be an incomplete picture,” comments Ward. “Now, thanks to Blackthorn GRC, we can access comprehensive and accurate statistics, quickly and easily.”

### Proactive risk management

As well as being able to monitor activities that follow an incident more effectively, risk management tools within the solution also allow staff to identify key risk areas. This then enables them to take proactive steps to avoid a repeat of certain types of incident.

“By helping us to identify potential risks and gaps in our defences, Blackthorn GRC enables us to rework our processes accordingly,” remarks Ward.

### Extending the solution

As well as using Blackthorn GRC to help it manage its response to computer security incidents, NZDF is also looking at implementing the software to support its physical security incident and logistics teams, as well as its military police force.

Information-sharing with other government departments is also a prospect. Using collaboration tools within Blackthorn GRC, NZDF could set up and receive automatic notifications of attacks on other networks. “If we have prior warning of the types of attack that other organisations are suffering, we can be better prepared to combat future threats,” concludes Ward. “Ultimately, I believe that this integrated approach will help us to protect our networks more effectively.”



QCC Information Security Ltd • Buchanan House  
24-30 Holborn • London EC1N 2LX • UK

Tel: +44 (0)20 7353 9000  
Email: [contact@qccis.com](mailto:contact@qccis.com)  
Web: [www.qccis.com](http://www.qccis.com)

‘Blackthorn’, is a registered trademark of QCC Information Security Limited in the United Kingdom. Information on ‘Blackthorn’ can be found at [www.qccis.com](http://www.qccis.com). Other company, product and service names may be trademarks, or service marks of others.

This case study illustrates how one QCC customer uses the ‘Blackthorn’ technology. Many factors have contributed to the results and benefits described in this case study. QCC does not guarantee comparable results. All information contained herein was provided by the featured customer. QCC does not attest to its accuracy.

This publication is for general guidance only. Information is subject to change without notice. Please contact QCC Information Security Ltd. or its authorised ‘Blackthorn’ reseller for latest information on ‘Blackthorn’ or other QCC products and services. No part of this publication may be reproduced or transmitted, in any form or by any means, or stored in any retrieval system of any nature, without prior written permission of QCC Information Security Ltd, except for fair dealing under the Copyright, Designs and Patents Act.

© Copyright QCC Information Security Ltd. 2011. All Rights Reserved.  
Front cover image © UK MOD Crown Copyright 2011.

QCC-MKTG091211a-MS-Case Study NZDF-v1.1

#### About Blackthorn

*Blackthorn is an out-of-the-box solution for managing all activities related to sensitive operations and issues.*

*It’s a straightforward and highly secure approach to integrating key functions within your business into a single, coherent database of information that can give true clarity on operational risk.*

#### Further information

To find out more about Blackthorn, contact us now on [blackthornmail@qccis.com](mailto:blackthornmail@qccis.com) or +44 (0)20 7353 9000.