Folks

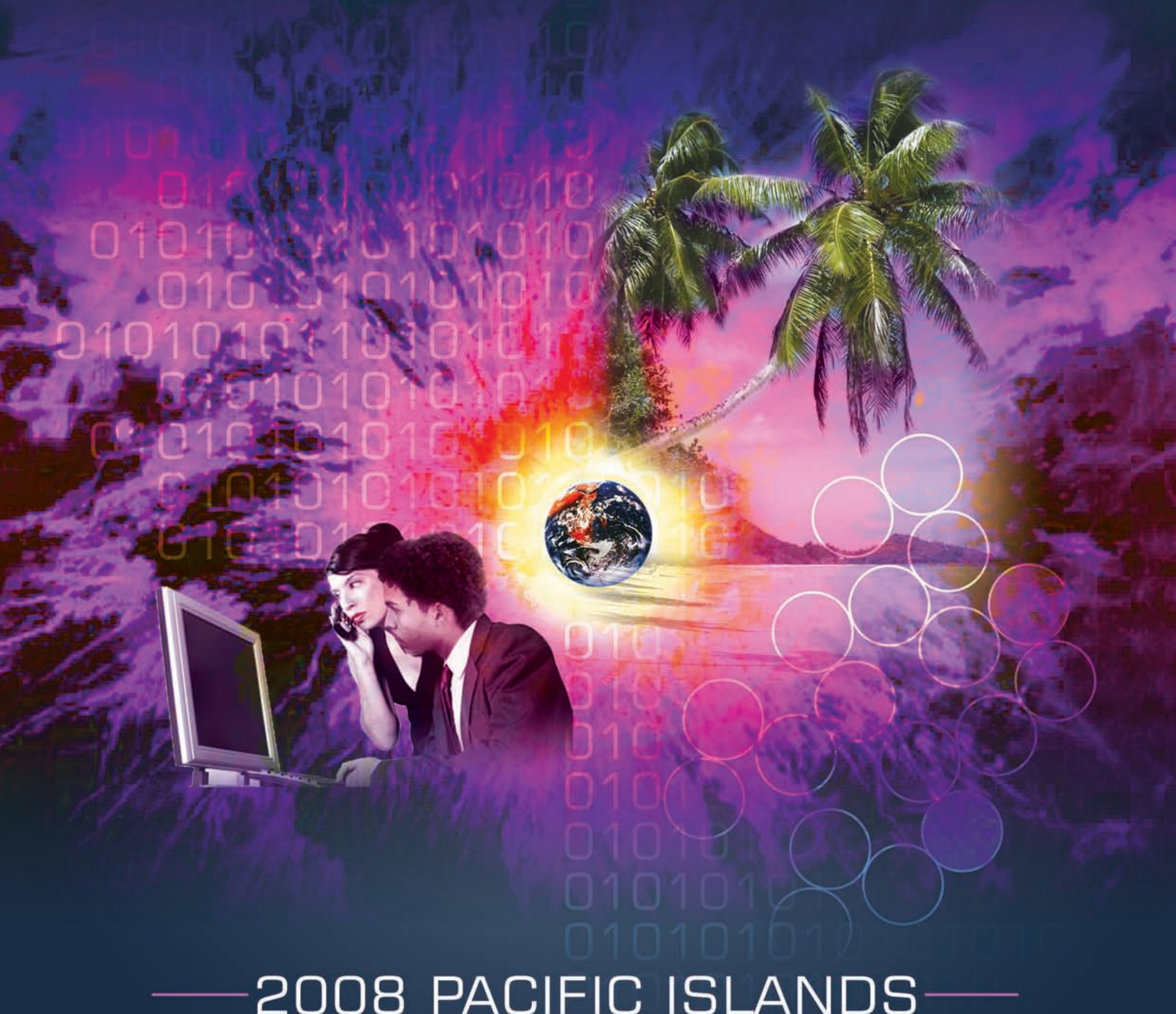
I refer to your current Senate Standing Committee inquiring into the major economic and security challenges facing PNG and the island states of the southwest Pacific. Earlier this year I completed the 2008 Pacific Islands Computer Crime and Security Survey which as a submission may be of interest and assistance to your inquiry. The survey can be located at my website www.esecurity.net.au and is the thumbnail on the lower RHS.

Please contact me if I can be of any assistance regarding this matter.

regards

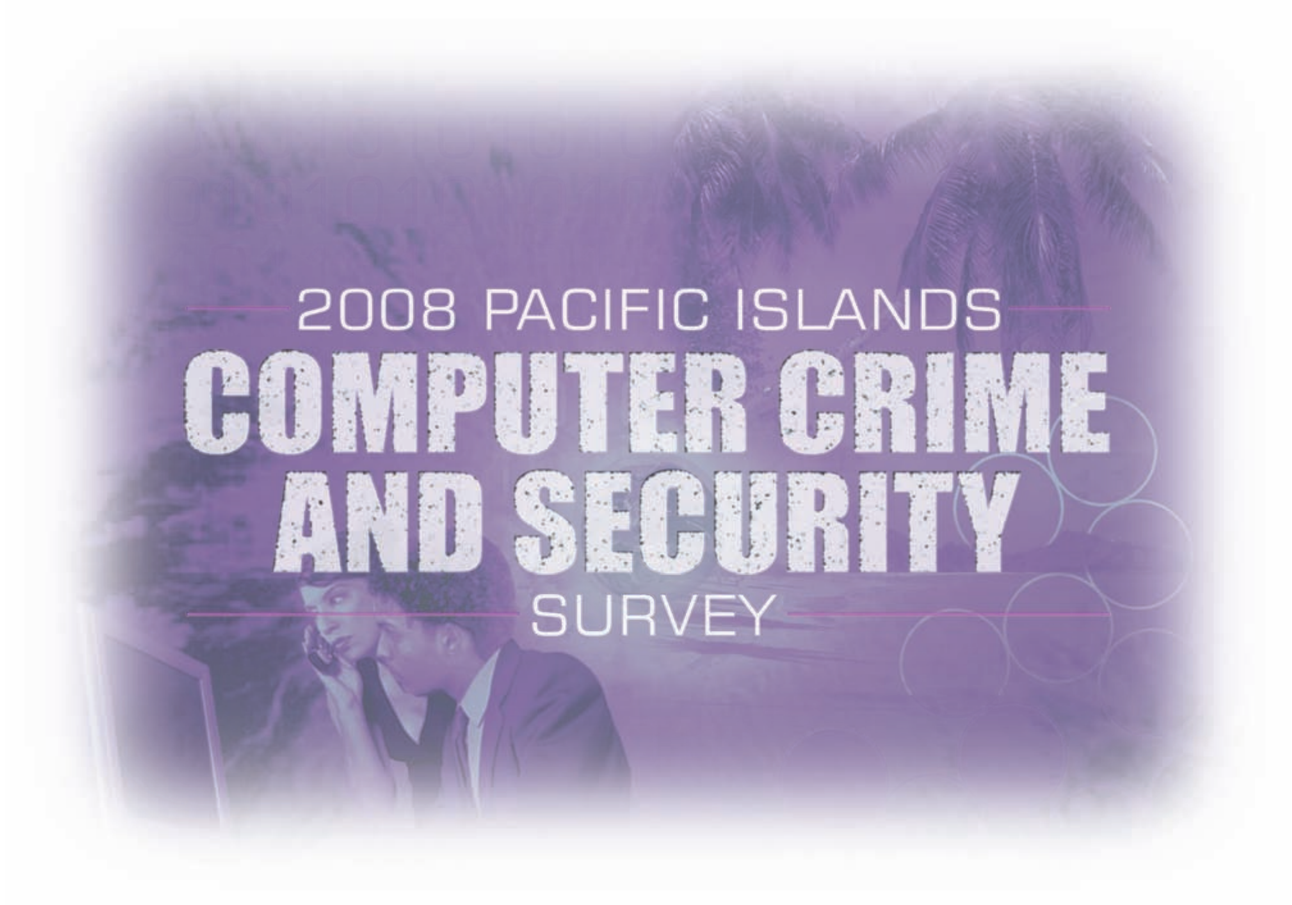
Nigel Phair

NIGEL PHAIR



2008 PACIFIC ISLANDS COMPUTER CRIME AND SECURITY SURVEY

SPONSORED BY Microsoft



National Library of Australia Cataloguing-in-Publication entry

Author: Phair, Nigel

Title: 2008 Pacific Islands computer crime & security survey [electronic resource] / Nigel Phair

Publisher: Kambah, A.C.T. : esecurity publishing, 2008

ISBN: 9780980342123 (pdf)

Notes: Includes index. Bibliography.

Subjects: Computer crimes – Pacific Islands.

Dewey Number: 364.1680961

ESECURITY PUBLISHING

publishing@esecurity.net.au

CONTENTS

Executive Summary

The key findings for 2008 are:

Almost one third of organisations experienced an electronic attack which harmed the confidentiality, integrity or availability of their systems. Of these organisations, 15% experienced more than 10 attacks.

Nearly two thirds of respondents thought their organisation needed to do more to ensure an appropriate level of IT security qualification, training, experience or awareness among staff and management.

Half of respondents used, or followed as a guide, IT security related standards.

One third or organisations thought their current level of IT security funding was adequate.

Over half of respondents were victim to Nigerian-style internet scams.

Nearly half of the respondents which experienced an electronic attack chose not to report the incident to any external organisation.

Introduction

The 2008 Pacific Islands Computer Crime and Security Survey is adapted from other survey tools and provides the opportunity to discover the trends and issues of IT security and cyber crime within the Pacific Islands. This survey seeks to examine the nature and scope of electronic crime and information security.

Information technology is improving the way organisations within the Pacific Islands are conducting business and interacting with stakeholders and clients. But these opportunities regularly come attached with threats, many of which may cause damage to the economy where these organisations operate.

Whilst respondents were small in number they cover a broad spectrum of Pacific Islands and industry sectors. It is anticipated future surveys will increase in respondent numbers allowing for a comparison of findings.

The support and cooperation of all organisations who took part in this survey is sincerely appreciated.

Cyber Crime and the Pacific Islands

Transnational crime represents a challenge for all Pacific Island nations. Reducing the exposure to technology enabled crime and having strong information security is critical to strengthening the economic and societal characteristic of the Pacific Islands. Organised criminal networks which focus on the use of technology to conduct criminal activity target areas of least resistance. The Pacific Islands are vulnerable as they are culturally, educationally and socially diverse, geographically isolated and sparsely populated.

The survey response indicates a degree of victimisation, which is made more important by the fact that over half of respondents stated they were part of their Islands critical infrastructure. Critical infrastructure includes information technology and communication systems which, if disrupted or destroyed, would significantly impact on the social or economic wellbeing of a nation and affect its ability to ensure national security. This survey concerns itself with the national information infrastructure of the Pacific Islands which like elsewhere in the world is susceptible to attack by criminals.

It is generally accepted that the Pacific Islands is already used to some degree as the target, facilitator or both of transnational crime. This is no different for technology enabled crime. The biggest risk in the future for Pacific Island internet users is the threat of personal, business and potentially some government computers being compromised by remote hackers. Once controlled by overseas based criminals they can be used for a variety of activity, including the hosting of illegal content, as spam relays, routing of unlawful communications and anonymous malicious attacks against other computer networks both within the Pacific Islands and globally.

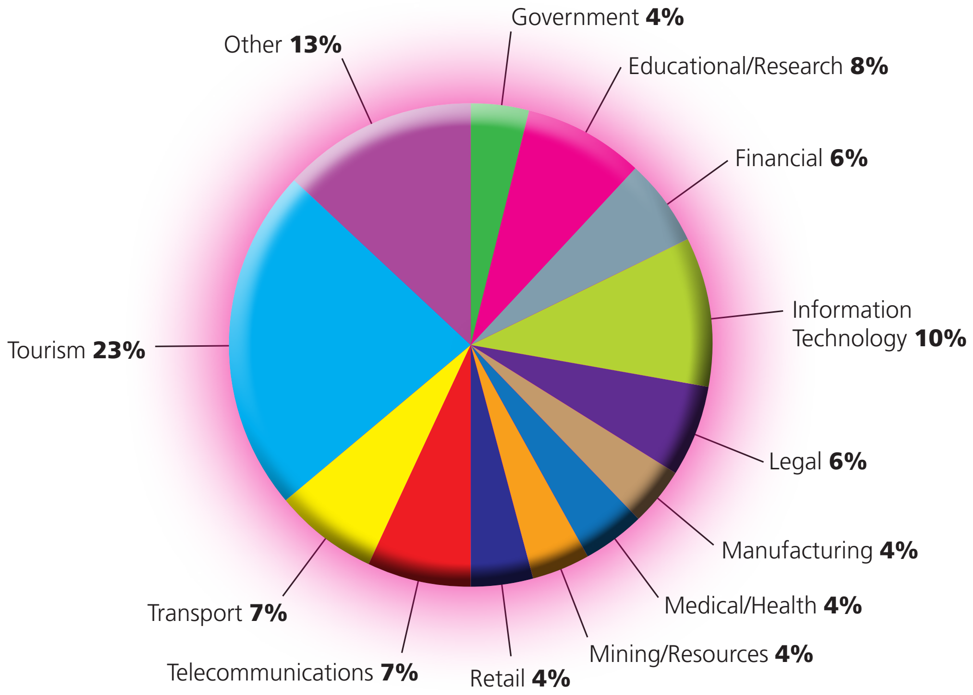
The internet and related technologies is already allowing the Pacific Islands to trade goods and services with other economies, including the advertising of tourist destinations in an efficient and professional manner. However the borderless nature of the internet allows cyber criminals based in any part of the world to target Pacific Island people, businesses and governments for financial gain. Future surveys will determine the speed and impact of electronic crime within the Pacific Islands.

Coupled with this is the general lack of law enforcement capability in dealing with electronic crime across the Pacific Islands. Law enforcement agencies are focused on the delivery of essential community policing functions and not equipped or trained to respond to and investigate this emerging crime type. Added to this is the general lack of specific computer crime related legislation within Pacific Island economies.

Who We Asked

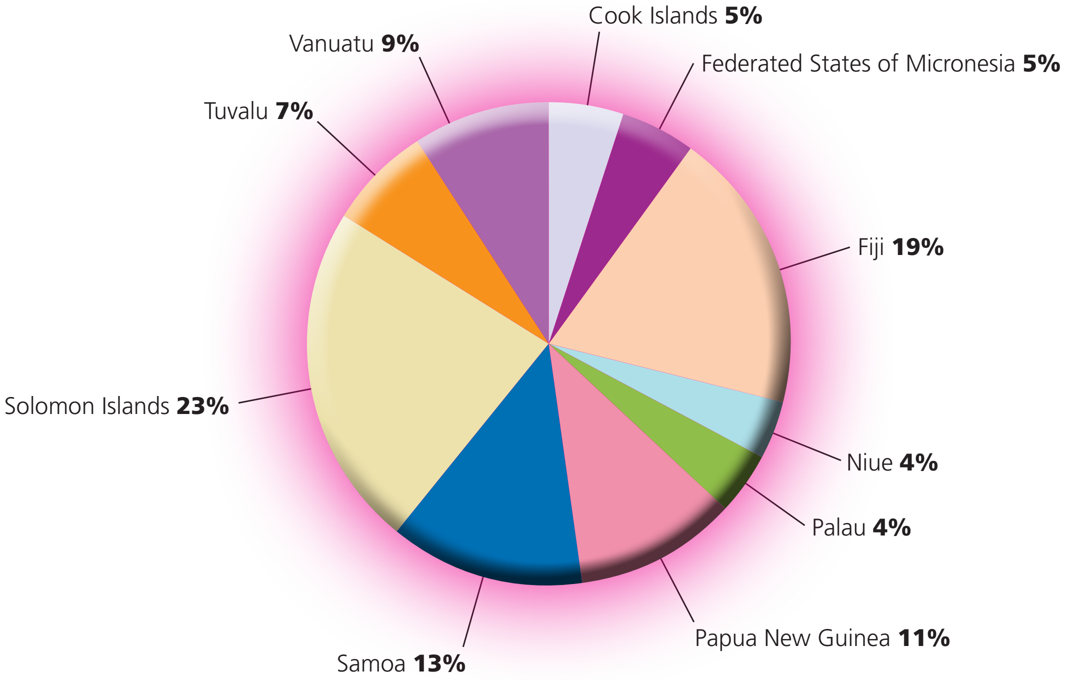
Survey respondents represented a broad range of industry sectors, however not surprisingly the greatest number originated from tourism.

Location Of Respondents



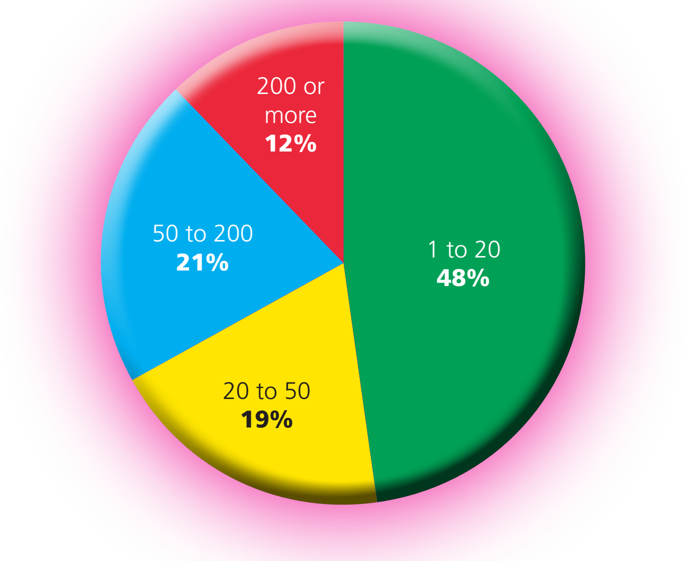
The location of the respondents also shows a broad representation across the Pacific Islands with the bigger number of respondents from those Islands with the biggest population.

Location Of Respondents



Nearly half of respondent organisations were small sized organisations which contained less than 20 employees. This feature is inline with the economic consistency of the majority of Pacific Island commerce.

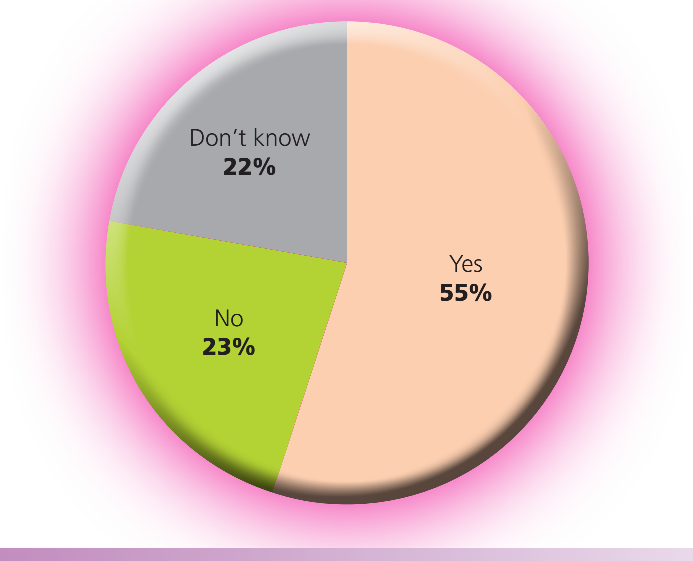
Respondents by Number of Employees



Over half of respondents identified themselves as forming part of their Islands' critical infrastructure. This statistic is important, not just the protection of computer networks but also from an incident response perspective. Cyber threats against critical infrastructure seek to disrupt the confidentiality, integrity and availability of its information systems.

It is these networks which are vital for the functioning of society. The private sector represents 96% of survey respondents which means Pacific Island Governments need to rely on solid public/private partnerships for protecting such facilities and operations.

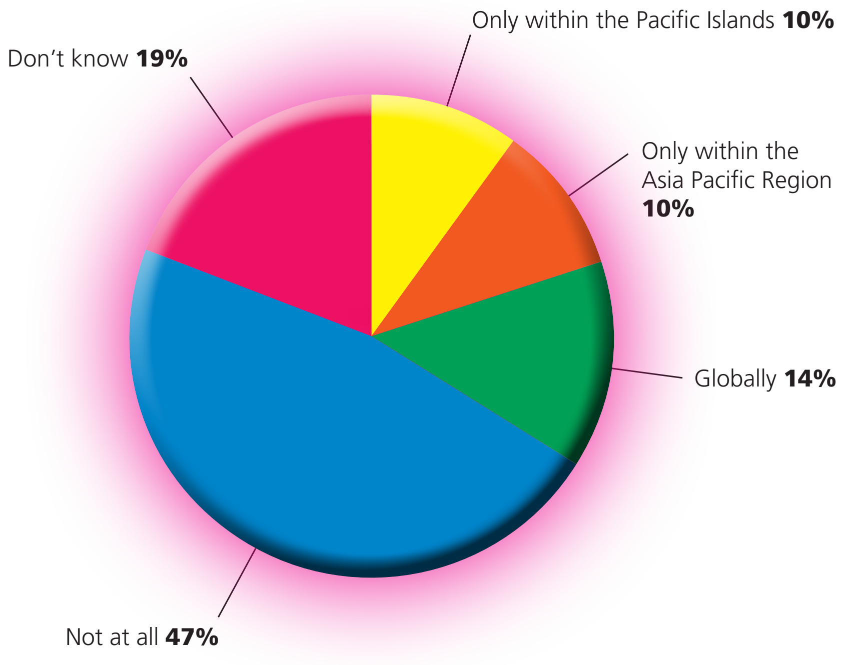
Do You Believe Your Organisation is Part of Your Island Critical Infrastructure?



Nearly half of respondents don't offer any electronic commerce facilities and of those who do, only 14% offer this on a global basis. This should greatly reduce the impact of crimes against an organisations financial systems such as online payments systems as this is a significant vector for fraudulent activity resulting in financial losses.

This reduction in global e-commerce will not necessarily result in the exposure to phishing scams and other social engineering attacks which are designed to steal consumers' personal identity data and financial account credentials. Phishing attacks and similar schemes use bogus emails to lead recipients to counterfeit websites designed to trick them into divulging personal financial data. As phishing evolves, particularly through technical deception and known Pacific Island brands are hijacked more recipients will fall victim.

Do You Offer E-Commerce Facilities Trans-nationally?

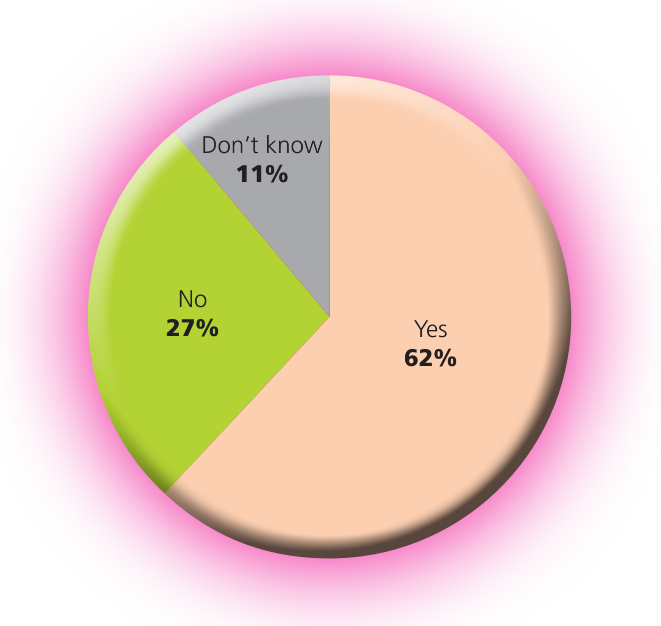


Readiness to Protect IT Systems

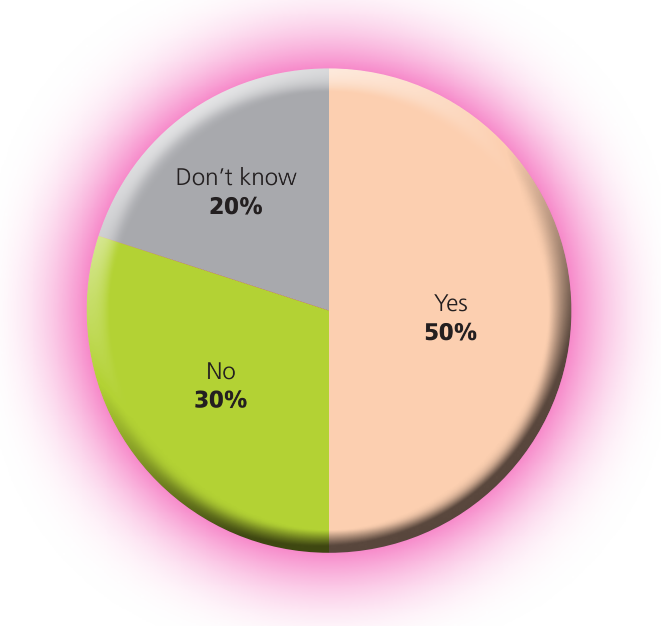
This component of the survey attempts to gauge the level of readiness amongst respondent organisations to react to electronic attacks and safeguard critical systems and information.

Over half of respondents considered they need to do more to be ready to protect their IT systems with only half following any IT standards or guides.

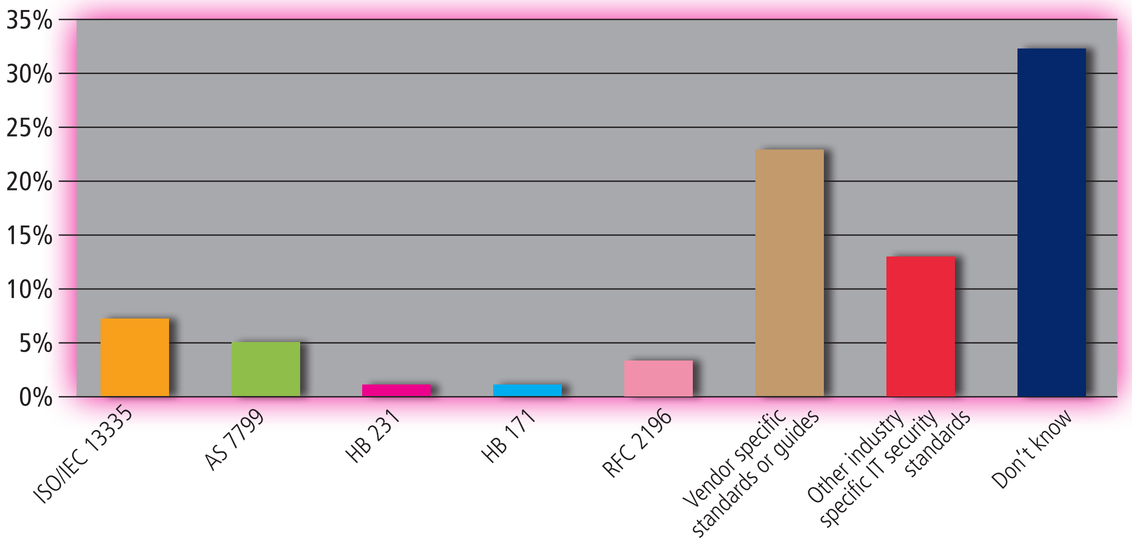
Do You Think Your Organisation Needs to do More to Ensure an Appropriate Level of IT Security Qualification, Training, Experience or Awareness Among Staff and Management?



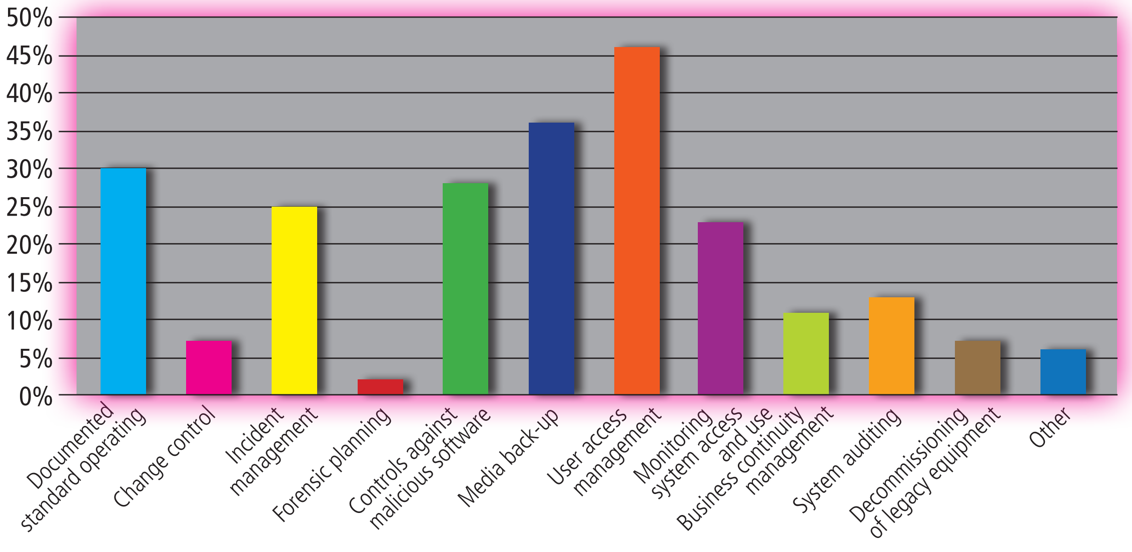
Does Your Organisation Follow, or use as a Guide, any IT Security Related Standards?



IT Security Related Standards Used

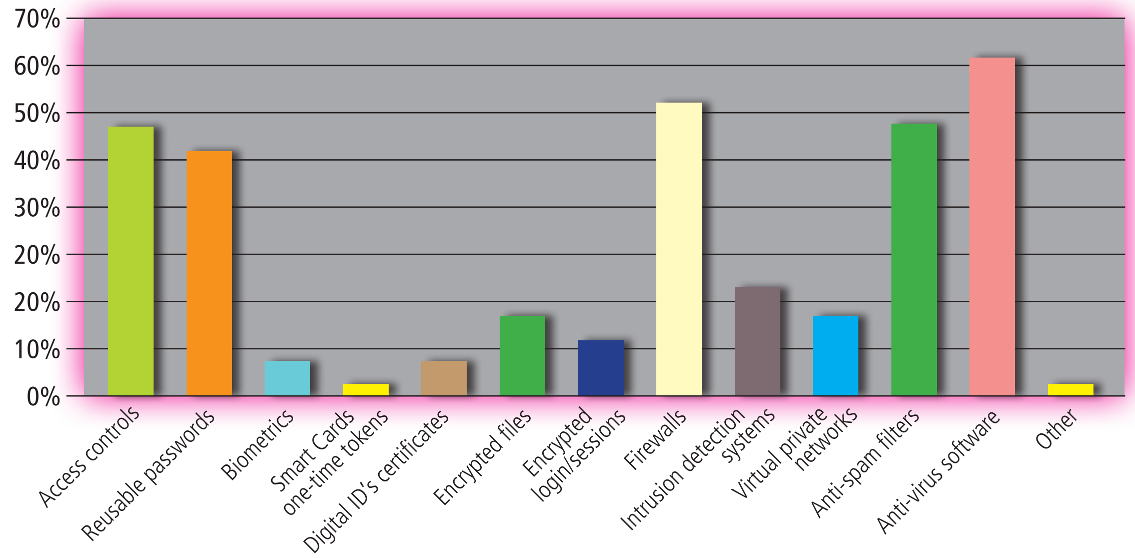


Computer Security Policies and/or Procedures Followed



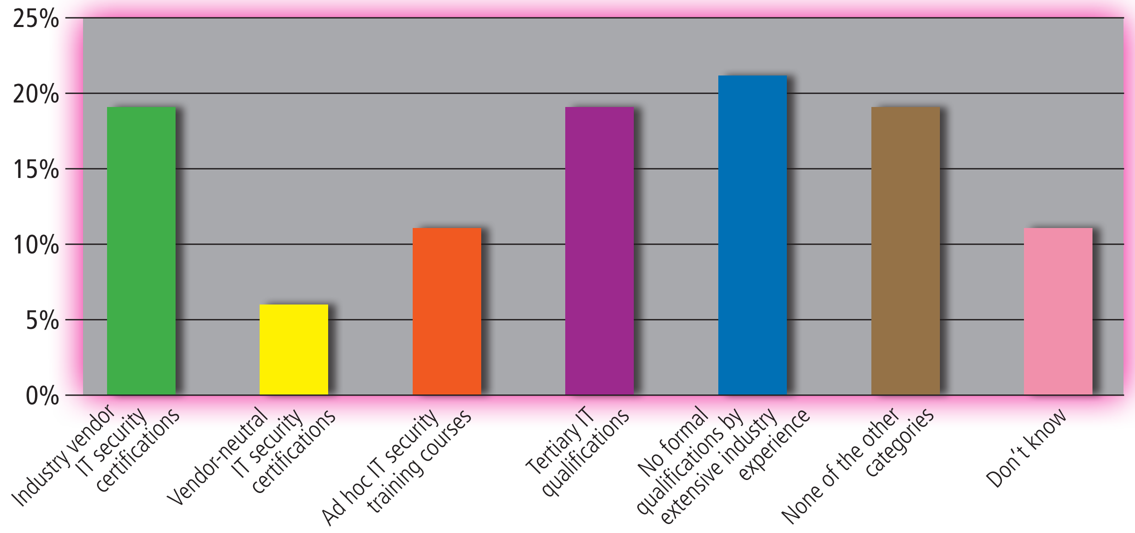
User access management is used by more respondent organisations than other policies and procedures. In the majority of cases this is coupled with firewalls, anti-spam filters and anti-virus software to form the backbone of online defences.

What Type of Computer Security Technologies do You Use?

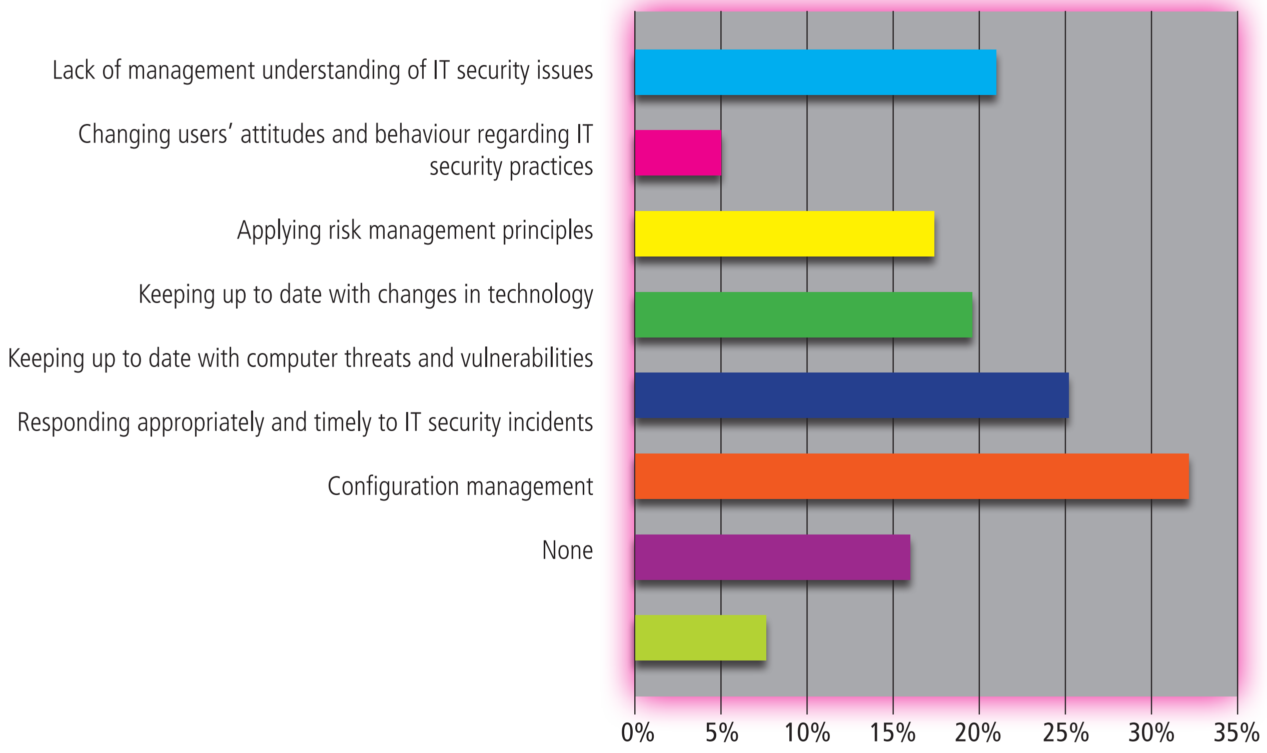


There is a broad range of qualifications and staff training identified which when added together demonstrates some level of training for staff performing an IT security role.

IT Security Qualifications and/or Training of Staff

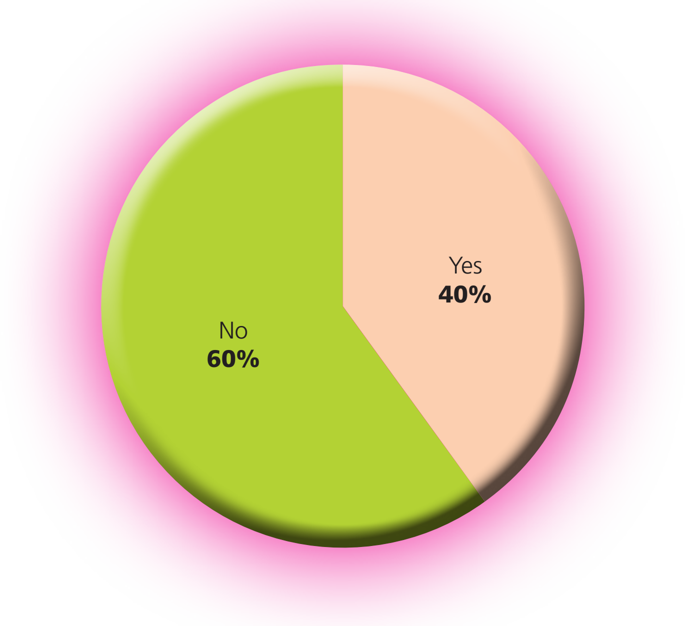


What Aspects of IT Security Management Does Your Organisation Find Most Challenging of Problematic?



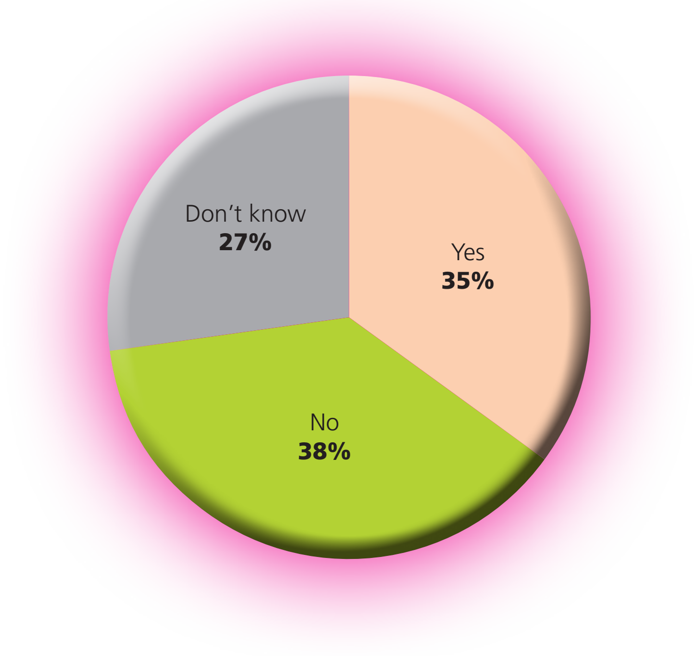
Changing user attitudes and keeping up to date with changes in technology are the greatest concern for managers. This is coupled with 60% of respondents not having increased expenditure on IT security in the past 12 months

Has Your Organisation Increased Expenditure on IT Security Over the Past 12 Months?



Over a third of organisations thought their current level of spending on IT security was adequate. However it was essentially even with those respondents who thought they were not spending enough and those organisations who didn't know.

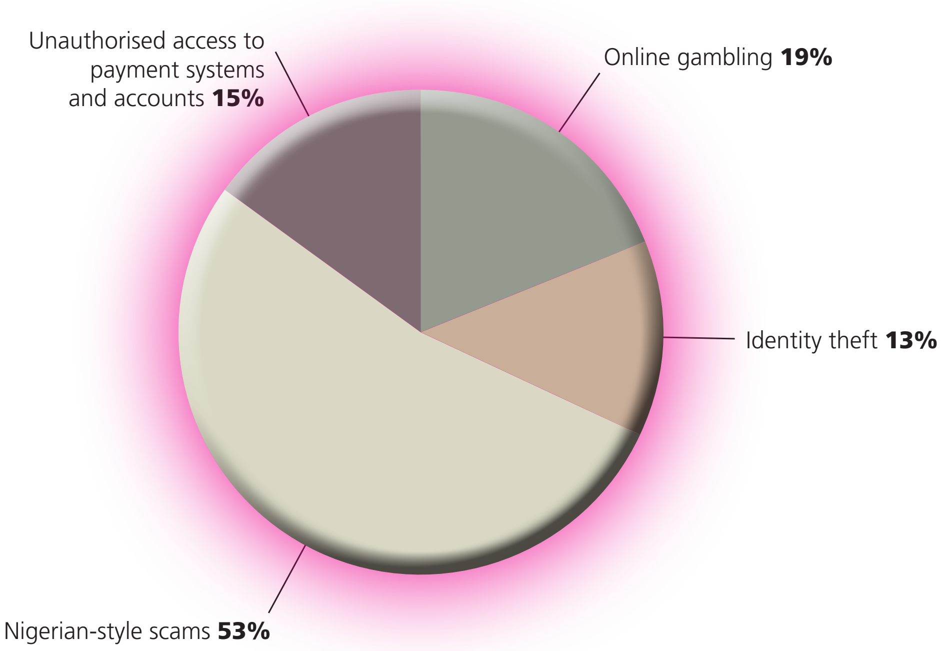
Do You Think Your Level of IT Spending is Adequate?



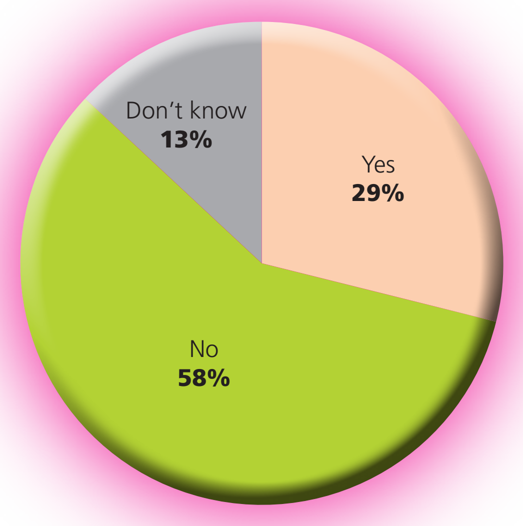
Cyber Crime Trends

This component of the survey seeks to identify the number of electronic attacks experienced by respondent organisations as well as the type of online criminal activity endured. Respondents encountered a range of cyber crimes with over half having suffered from Nigerian-style scams. Nigeria has become famous for the '419' scams otherwise known as 'Nigerian Letters'. These letters were once posted via traditional mail to victims promising the recipient large sums of money in return for assisting (often by paying bank fees) the perpetrator to transfer money from Africa. This activity is now executed via email where it is both cheaper to send and able to be delivered to many more recipients.

Has Your Organisation Suffered From any of the Following Cyber Crimes?

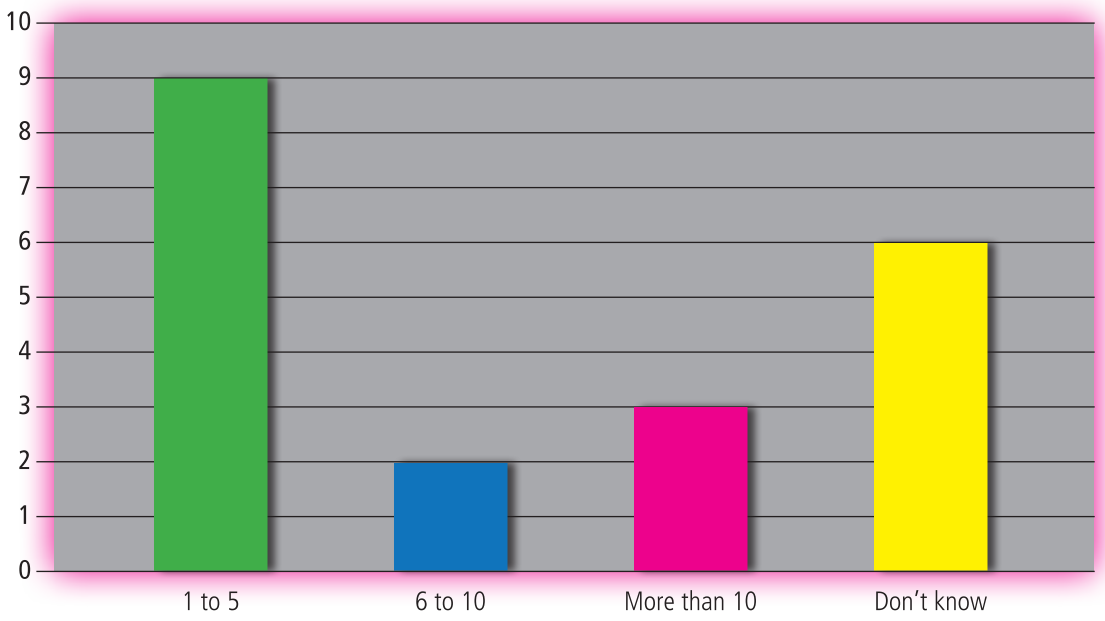


In the Last 12 Months Did Your Organisation Experience One or More Electronic Attacks?

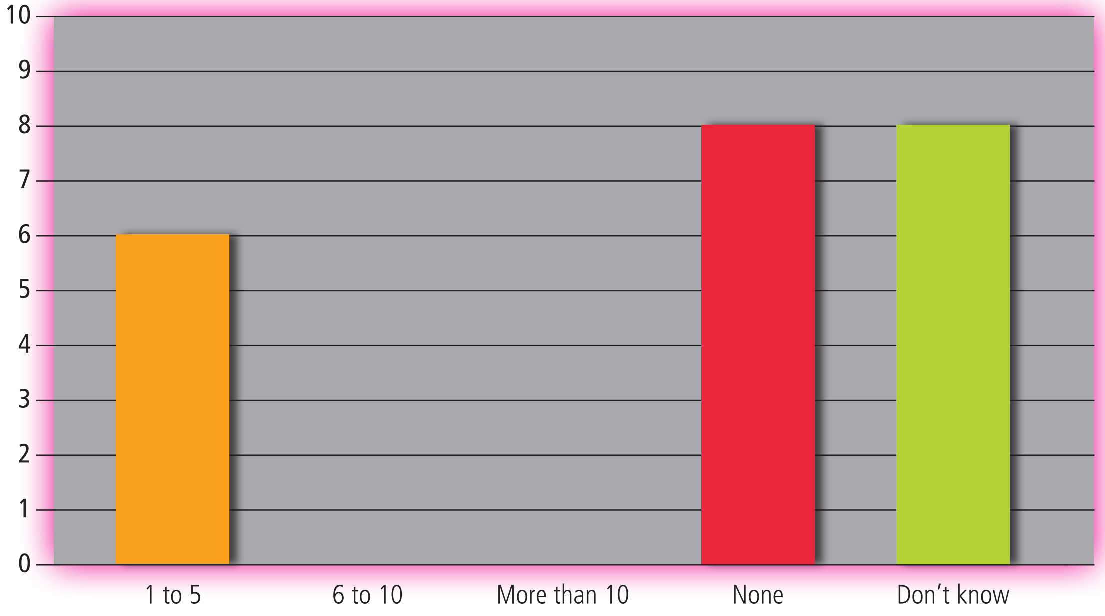


Almost one third of organisations experienced an electronic attack which harmed the confidentiality, integrity or availability of their systems. Of these organisations, 15% experienced more than 10 attacks.

If Yes, How Many Attacks Occured in the Last 12 Months?

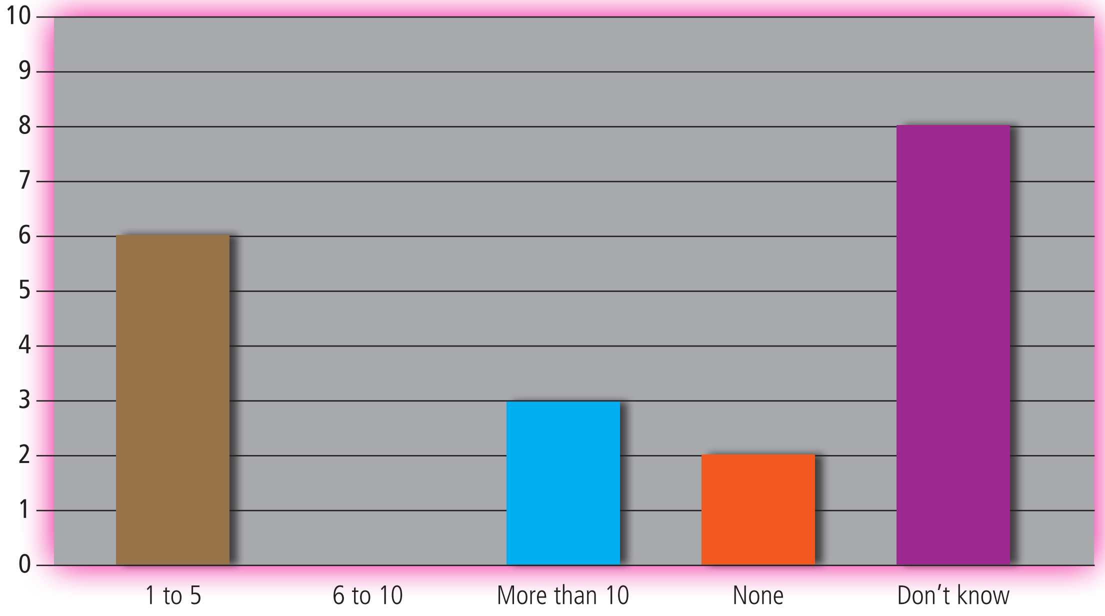


How Many Attacks Were From Inside the Organisation?

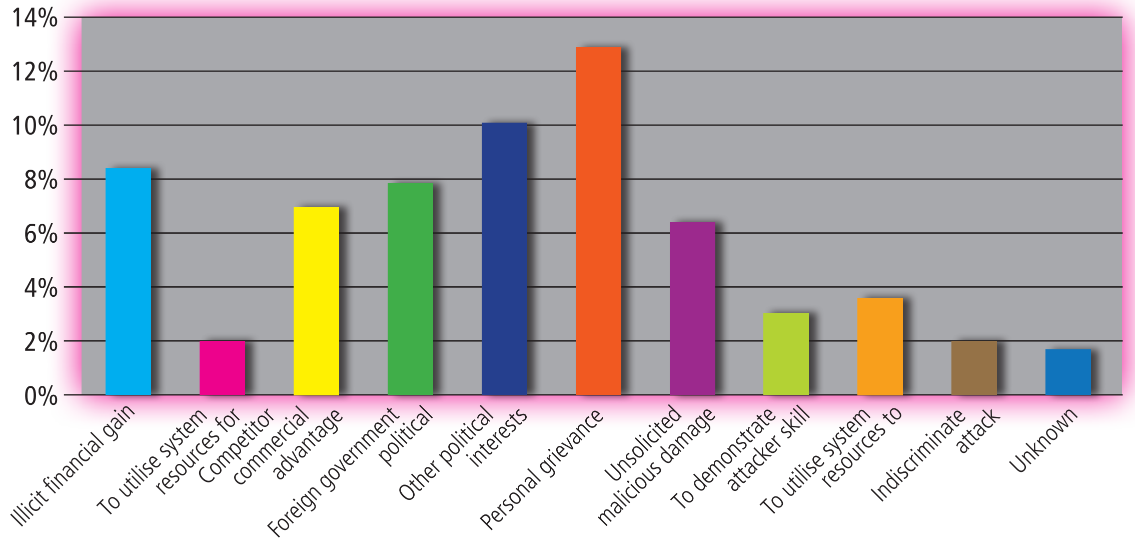


More attacks were reported by organisations to have originated from outside the organisation as opposed to internally.

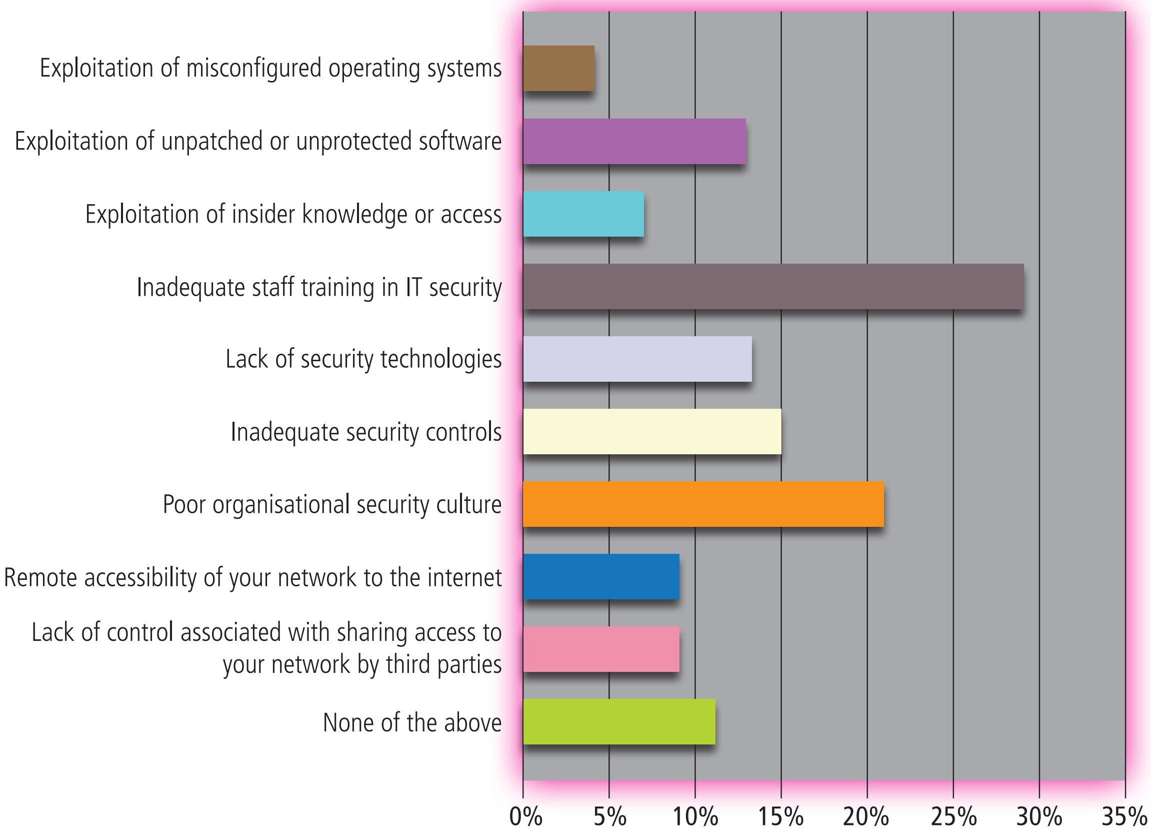
How Many Attacks Were From Outside the Organisation?



In Your Opinion What was the Motive for the Electronic Attacks?

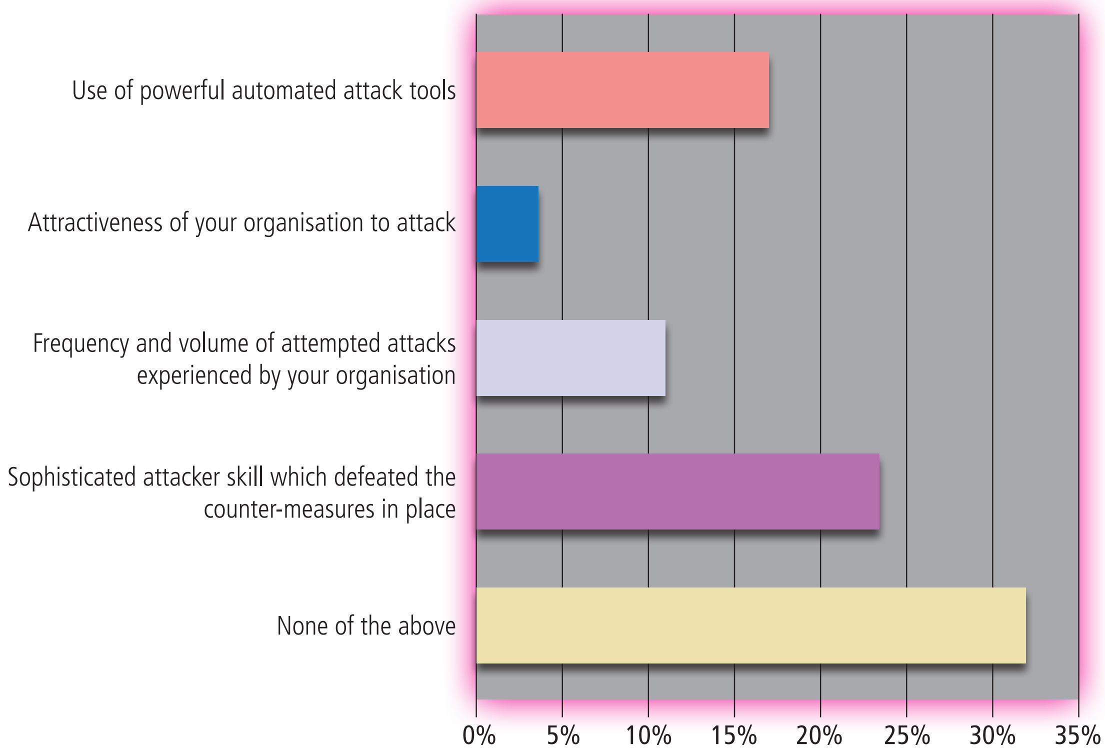


In Terms of Your Organisation Vulnerabilities, What Factors do you Believe Contributed to Those Electronic Attacks?



Over two thirds of respondents gave a reason as to why they had suffered an attack which impaired the confidentiality, integrity or availability of their systems.

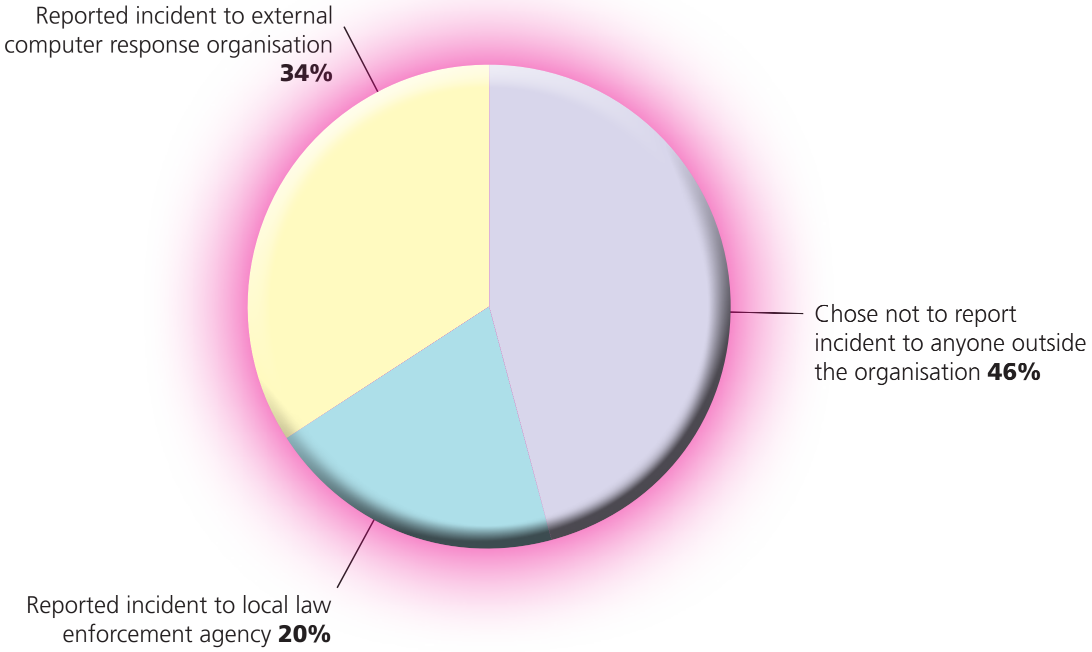
In Terms of the Threat Faced by Your Organisation, What Factors do you Believe Contributed to Those Attacks?



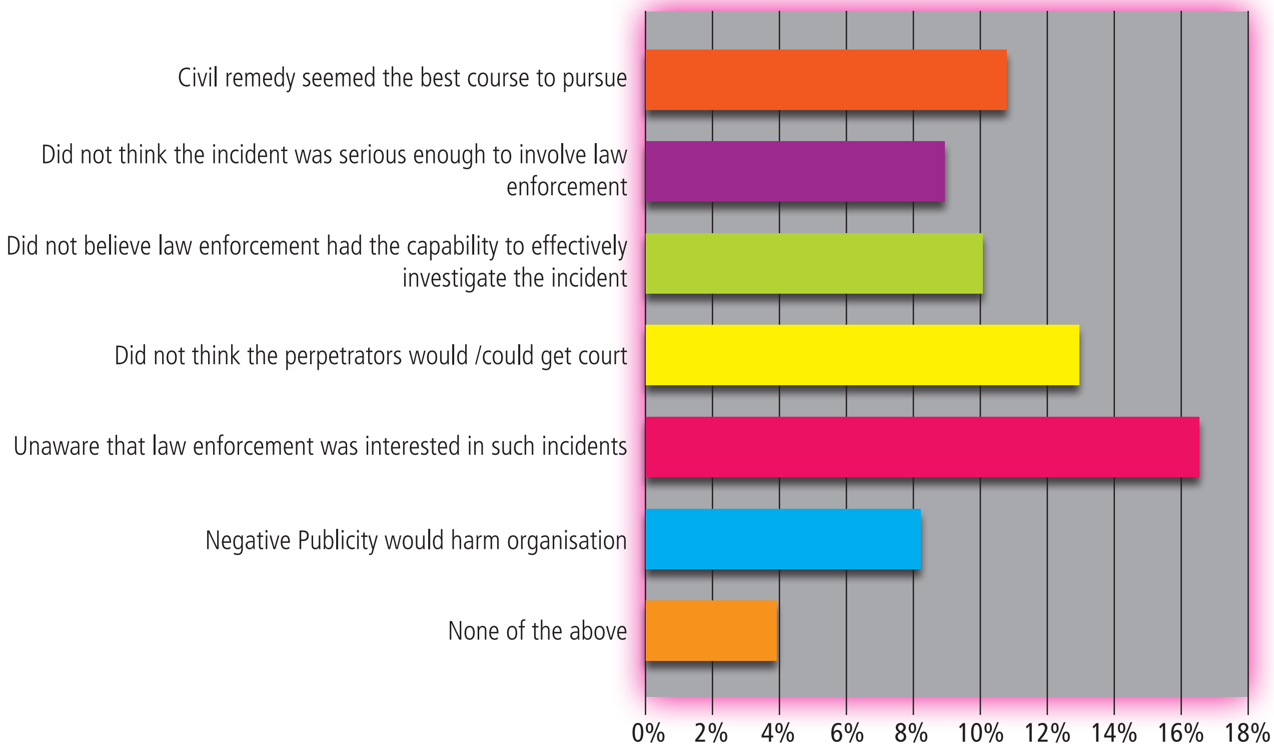
Incident Response

This component of the survey seeks to discover how organisations responded after experiencing an electronic attack. A tested incident response plan can save an organisation from ongoing attack and/or financial loss along with the potential embarrassment from suffering damage against the confidentiality, integrity or availability of IT systems. Nearly half of such organisations chose not to report the incident to any external organisation.

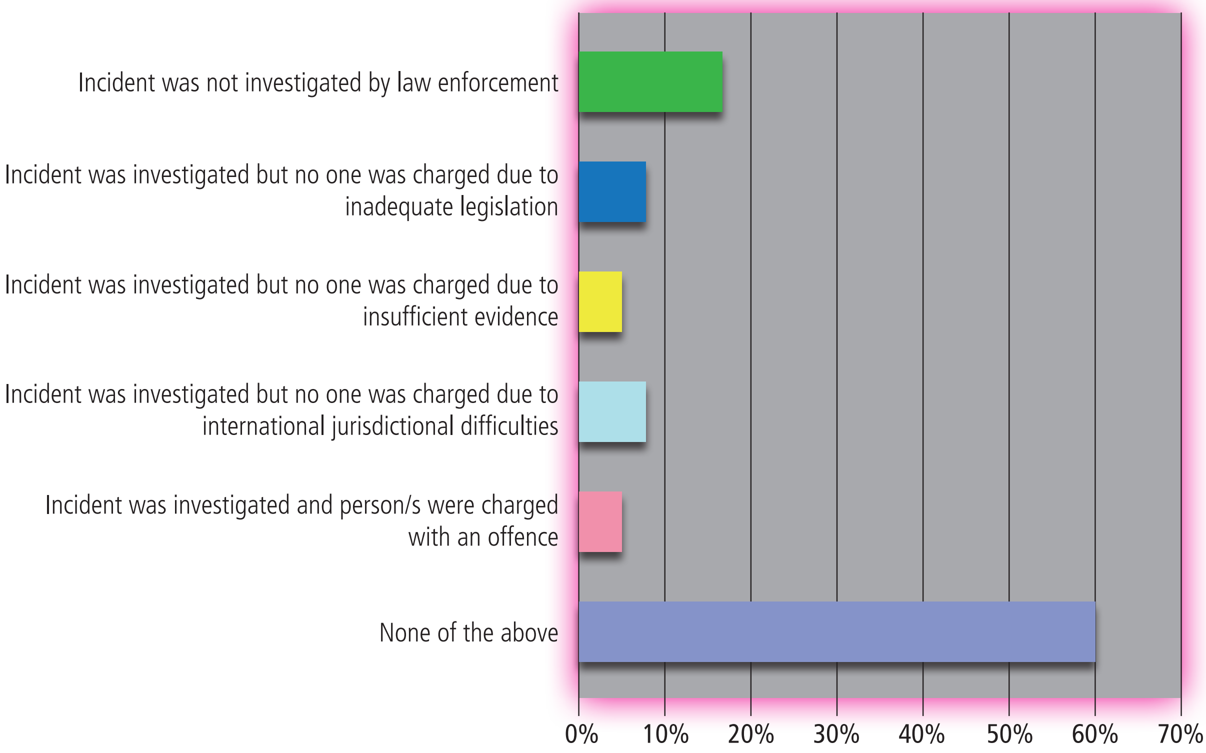
If Your Organisation Experienced Electronic Attacks, to Whom did you Report the Incidents?



In Instances Where Your Organisation did not Report Electronic Attacks, What Were the Reasons for not Informing Law Enforcement?



If Your Organisation Reported Incident/s to a Law Enforcement Agency, What was the Outcome?



Methodology

Electronic survey questionnaires were emailed to over 700 organisations, including individual businesses, trade groups and government departments across the Pacific Islands.

During January and February 2008, recipients were invited to complete the online survey gaining a response rate of about 7% (52). The small sample size makes it difficult to draw accurate conclusions, however some general insights can be gained into the state of computer crime and security within the Pacific Islands. All responses are anonymous.

It is anticipated future surveys will contain a greater sample and allow for the analysis of trends and issues within the region.

References

Attorney-General's Department (Australia). Trusted Information Sharing Network
www.tisn.gov.au

AusCERT. 2006 Australian Computer Crime and Security Survey University of Queensland 2006

McCusker, R. Transnational Crime in the Pacific Islands: Real of Apparent Danger?
Australian Institute of Criminology 2006

Phair, N. Cybercrime: The Reality of the Threat eSecurity Publishing 2007

Pacific Islands ICT Best Practises.
http://www.picisoc.org/tiki-index.php?page=Pacific+Islands+ICT+best+practices

2008 PACIFIC ISLANDS

COMPUTER CRIME AND SECURITY

SURVEY

Cover design: www.robcrispe.com