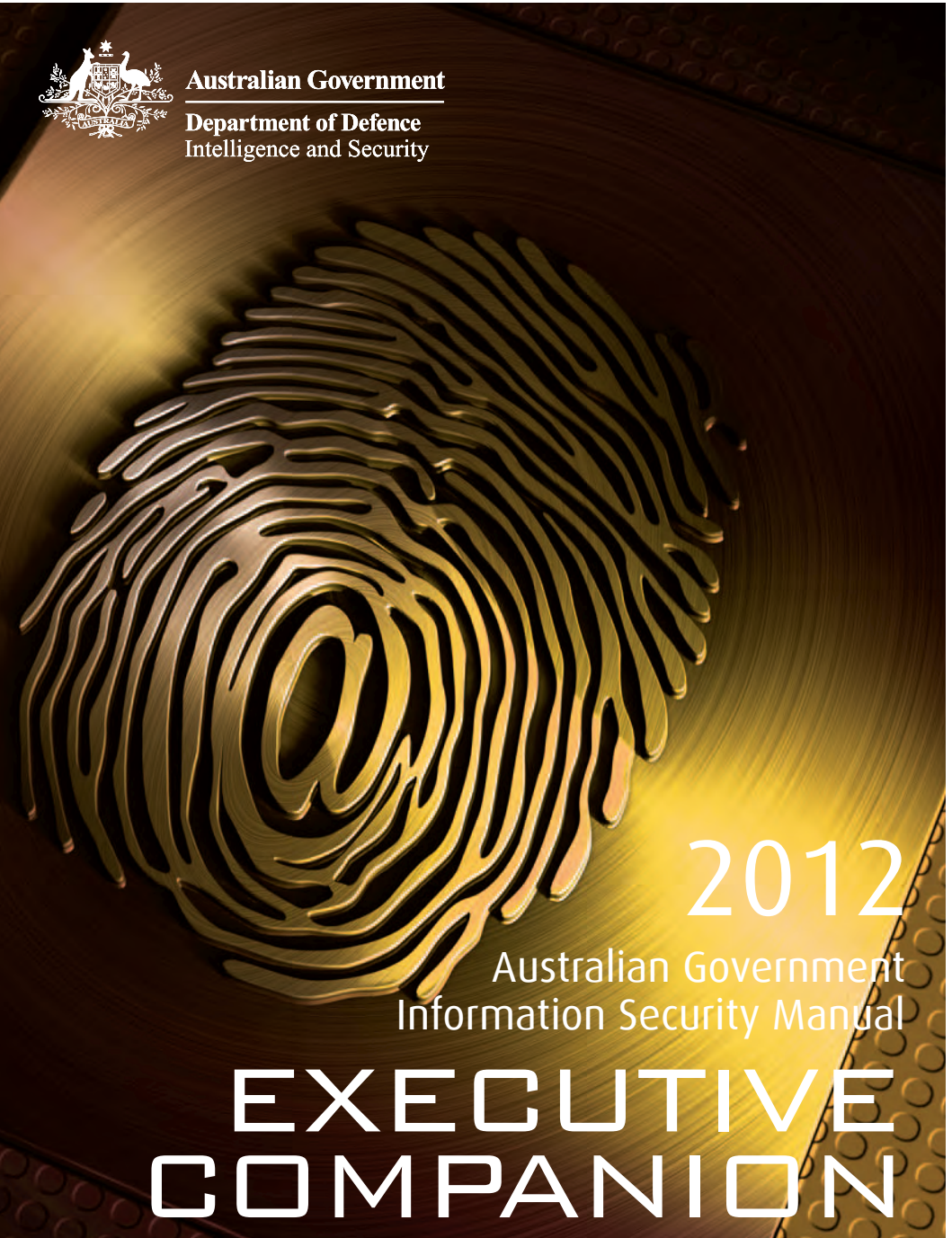




Australian Government

Department of Defence
Intelligence and Security



2012

Australian Government
Information Security Manual

EXECUTIVE COMPANION



2012

Australian Government
Information Security Manual

EXECUTIVE COMPANION



© Commonwealth of Australia 2011

All material presented in this publication is provided under a Creative Commons Attribution 3.0 Australia licence. For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 3.0 AU licence.

<http://creativecommons.org/licenses/by/3.0/au/deed.en>

<http://creativecommons.org/licenses/by/3.0/legalcode>

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet's website.

<http://www.dpmc.gov.au/guidelines/index.cfm>

Contact us

Inquiries regarding the licence and any use of this document are welcome at:

Defence Signals Directorate

PO Box 5076

Kingston ACT 2604

1300 CYBER1 (1300 292 371)

assist@dsd.gov.au.

Foreword

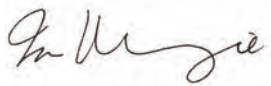
Advances in information technology have greatly benefited the conduct of government and commercial business, and have become essential to everyday communication. Information technology is providing greater accessibility, mobility, convenience and, importantly, efficiency and productivity. Australia's prosperity is dependent on taking full advantage of the digital revolution and all it offers.

But advances in information technology can be a double-edged sword. Australian networks, whether government, commercial or personal, are facing an unprecedented level of intrusion activities. Threats to information can come from a wide range of sources, including individuals, issue motivated groups, organised criminal syndicates and nation states.

It is important to know that things can be done to mitigate the security risks presented by this evolving threat environment. DSD supports agencies in embracing the latest technology by providing the information and tools which enable them to minimise the risks involved. Ultimately, technology will change faster than people's behaviour around it. Helping people make better decisions about new technology will allow us to stay ahead of the curve.

The Australian Government Information Security Manual forms an important part of the Government's strategy to enhance its information security capability. The 2012 release of the Manual comprises, for the first time, three complementary documents designed to provide greater accessibility and understanding at all levels of government. This Executive Companion details the cyber security threat and introduces considerations for those most senior in an organisation in mitigating the risks presented by this threat environment.

I encourage you to consider the key information security issues raised here and to ensure you have effective security governance arrangements in place. Doing so will provide assurance that the information entrusted to you is properly protected.

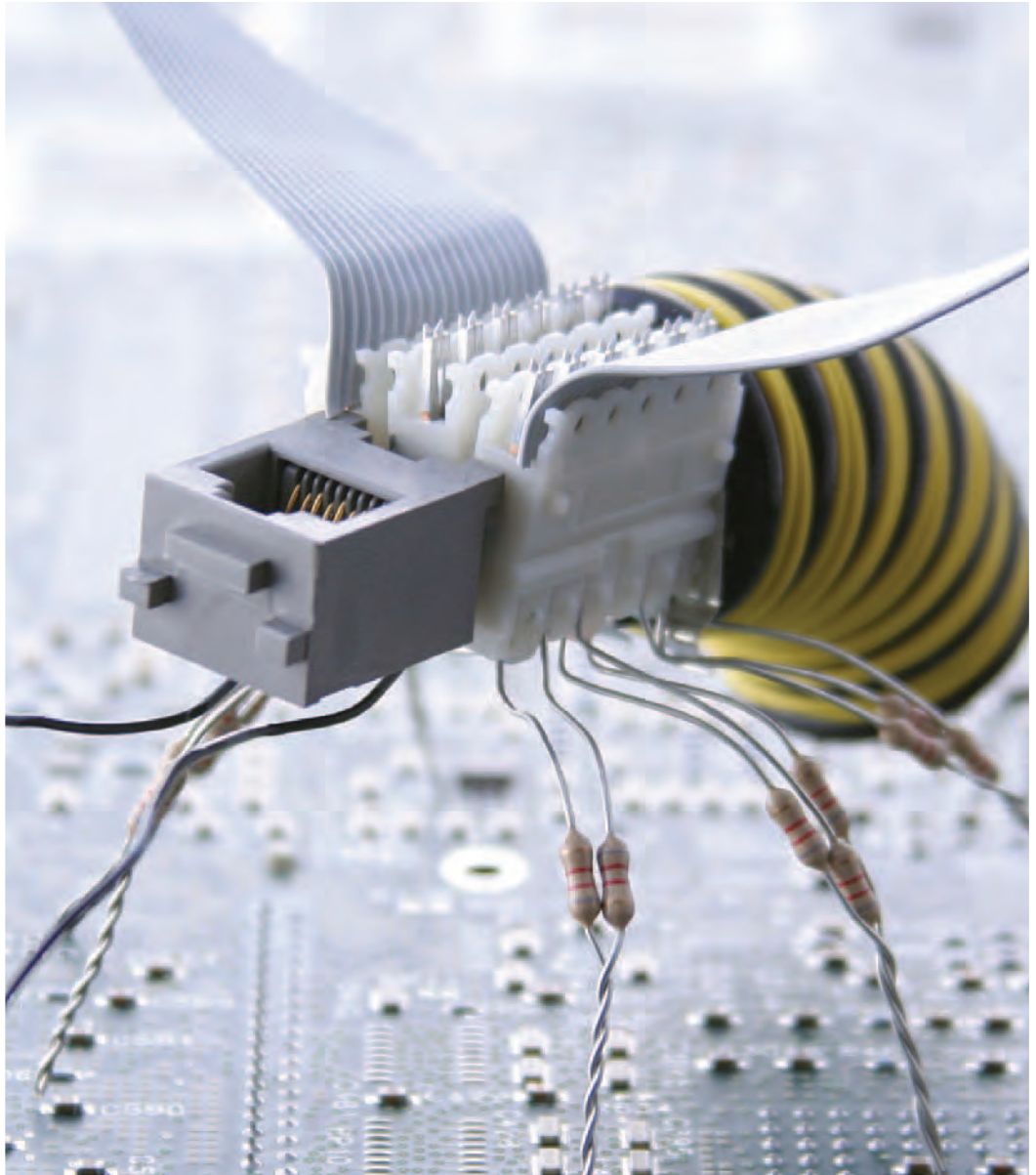


Ian McKenzie Director
Defence Signals Directorate



Contents

THE THREAT ENVIRONMENT	1
TOOLS AND TECHNIQUES	2
ACTORS	3
CONCLUSION	5
COUNTERING THE CYBER THREAT	7
QUESTIONS SENIOR MANAGEMENT NEED TO CONSIDER	8
CASE STUDY	9
THE AUSTRALIAN GOVERNMENT INFORMATION SECURITY MANUAL	13
FORMAT	14
COMPLIANCE	15
DSD'S ROLE	17
WHAT DSD CAN DO FOR YOU	18
WHAT YOU CAN DO FOR DSD	18
CONTACT	18



THE THREAT ENVIRONMENT





The Threat Environment

Advances in information and communications technology (ICT) are allowing for greater accessibility, mobility, convenience, efficiency and productivity across almost all aspects of Australian life. Australia's national security, economic prosperity and social wellbeing now depend on ICT, and the Internet in particular. The security of sensitive government and commercial information, the security of our digital infrastructure, and public and international confidence in Australia as a safe place to do business online are critical to our future. Because any Internet-connected device or computer system is highly susceptible to malicious cyber activity, our dependence on ICT also brings greater exposure to threats. The threat is not limited to classified systems and information. A wide range of institutions, both public and private, have been subjected to malicious cyber activities.

Tools and Techniques

The primary cyber threat to Australia is cyber exploitation, a malicious activity to covertly collect information from ICT systems. Cyber attack – offensive activity designed to deny, degrade, disrupt or destroy information or ICT systems – is also a possible threat to Australia. The vulnerabilities that malicious actors exploit to conduct both cyber exploitation and attack are often the same.

DID YOU KNOW?

A new piece of malware is created every 1.5 seconds.¹

Malicious software (malware) is the main tool used to gain unauthorised access to computers, steal information and disrupt or disable networks. Since malware—along with instructions and guidance for its use—is readily available on the Internet, anyone with intent is able to access the tools and information needed to undertake malicious cyber activity. Examples of malware include *trojans*—programs which seem legitimate but provide malicious actors with a backdoor into systems—as well as *spyware*, a general term for programs that covertly monitor and collect information from a system. Information stolen can be used to craft targeted cyber intrusions, create false identities, or even facilitate access into potentially more valuable commercial or government systems.

Any computer compromised by malware can potentially be invisibly conscripted into networks of compromised Internet-connected computers, known as **botnets**, to send spam, steal information, distribute malware and conduct attacks on a larger scale.

A commonly used technique to spread malware is **social engineering**, in which malicious emails are tailored to entice the reader to open them. Unaware users may be tempted to open malicious email attachments or follow embedded links to malicious websites—either action could lead to a compromise. These campaigns are becoming increasingly tailored and credible. Malicious emails often appear to be from someone the reader knows, such as their employer, colleague or friend. Some even have convincing-looking commercial logos and signatures and target a specific personal interest or a subject matter relevant to their work. Some malicious websites can be equally convincing. They can masquerade as a legitimate site used by an individual, such as their personal banking website, in order to mislead them into revealing personal information.

¹ Trend Micro, *Trend Micro Annual Report: The Future of Threats and Threat Technologies*, 2009.

Over 2010–2011, the number of mass, indiscriminate email-based attacks declined by more than half, but highly-personalised targeted attacks tripled. Cost-benefit decision-making is driving this trend, as although targeted attacks are estimated to cost five times more than mass attacks, the average value per victim can be forty times higher.²

Actors

The Defence Signals Directorate (DSD), through the Cyber Security Operations Centre (CSOC), communicates key assessments to government regarding the actors and trends observed in the Australian cyber threat environment.

Users

Cyber exploitation and cyber crime are unintentionally enabled by everyday users at home, at work or on mobile computing devices. Many users still assume that responsibility for information security rests with the organisations with which they interact, such as banks and online retailers. However, even the best technical security measures can be defeated by inappropriate user behaviour. Some users, in particular individuals and small businesses, are more vulnerable due to a general lack of awareness of cyber threats and relatively low resources devoted to information security.

In 2010, 88% of Fortune 500 companies had botnet activity connected to their Internet domains, and 60% had business email addresses compromised by malware.³

Users are targets in themselves for cyber crimes such as fraud and identity theft. When compromised, users can also become unintentional enablers of malicious cyber activity. The increasingly interconnected nature of our private, public and work ICT means that malware accidentally downloaded on one system can quickly lead to the infection of other devices across different environments. Inadvertently visiting the wrong website or opening the wrong email

attachment can have wider consequences, including the conscription of the device into a botnet – which can then be used to facilitate large-scale cyber crime or cyber attacks—or establish an access point into a connected personal, commercial or government system.

² CISCO White Paper, *Email Attacks: This Time it's Personal*, 2011.

³ RSA, *Cybercrime Trends Report—The Current State of Cybercrime and What to Expect in 2011*, 2011.



Malicious Actors

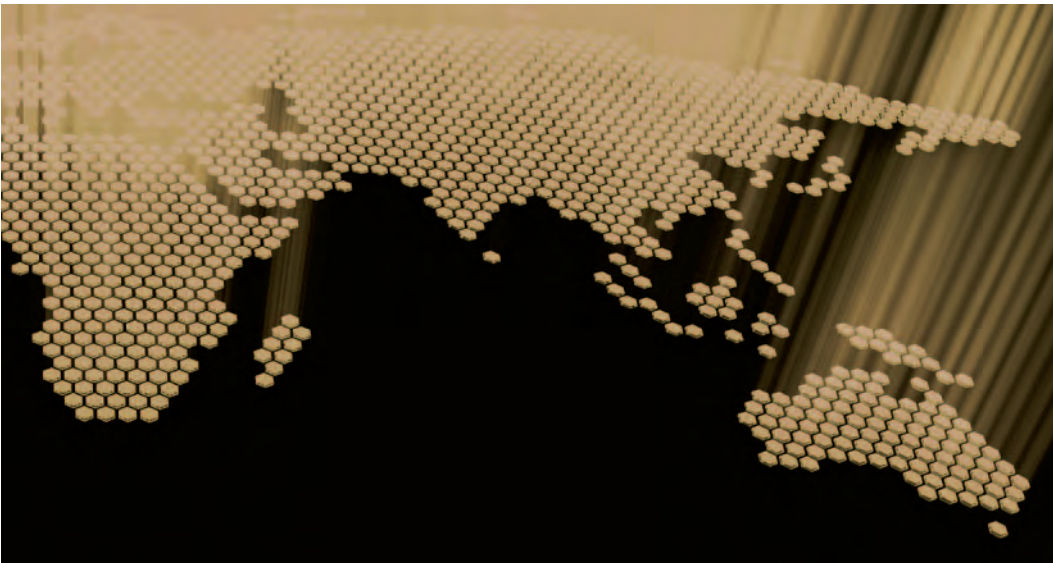
Australia is an attractive target for cyber exploitation due to its prominent role in the Asia-Pacific region and major international organisations, and its strong diplomatic, defence and intelligence relationship with the United States. Australia’s wealth, resource industries and niche expertise in some research and development fields also motivate actors to target Australia. Information collected through cyber exploitation could be used to gain a relative economic, diplomatic or political advantage against Australia. It can also be used to bridge a technological gap, for instance, by stealing intellectual property malicious actors are able to access new technologies while circumventing costly and lengthy research and development programs. Personal information gathered, such as financial or medical records, could also be used to enable malicious activities through techniques such as social engineering.

DID YOU KNOW?

After Wikileaks released a large amount of classified US State Department cables in November 2010, online payment service provider PayPal terminated WikiLeaks’ account, thereby closing its principal method for receiving financial donations from supporters. Claiming to support transparency and counter-censorship, Anonymous organised a Distributed Denial of Service attack that shut down PayPal’s website, as well as those for Mastercard and Visa.

Issue-motivated groups may see value in disrupting systems of national interest as a form of protest or propaganda. Loosely coordinated international hacker groups, such as Anonymous and LulzSec, have gained notoriety and demonstrated their intent and capability to conduct cyber attacks and data theft against a wide variety of high profile targets, including the US Central Intelligence Agency, UK Serious Organised Crime Agency, online gaming services, and Australian federal and local government networks. Citing a range of idealistic motivations, such as fighting for individual freedoms, government transparency and

opposing censorship, as well as simply for malicious ‘fun’, the groups often exploit common and relatively unsophisticated techniques to achieve their aims. For the most part, these attacks have been embarrassing and inconvenient. However, the disclosure of sensitive commercial or government information can threaten national interests, for example through the loss of consumer confidence in Australia’s digital economy.



The Australian Competition and Consumer Commission reported a loss of around \$63 million from cyber crime and scams in 2010.⁴

Cyber criminals are following legitimate businesses online to create new opportunities for profit. The nature of the Internet—borderless, anonymous, easily accessible and holding high volumes of financial, commercial and personal information—has boosted the incentives for committing cyber crime and allowed its organisation to become more audacious, efficient and effective.

A prolific and increasingly professional underground market of malicious cyber tools and services exists on the Internet. This market includes the sale or hire of criminal malware and botnets, guidance, recruitment and trading stolen information such as credit card details and intellectual property.

Criminals are becoming less content with simple, indiscriminate spam and fraud attempts, and are developing sophisticated, customised malware that targets emerging technologies, social media and mobile computing devices. The last few years have also seen a proliferation of target-specific malware aimed at, for example, particular banks, types of ATMs and financial exchanges.

Conclusion

The incentives for, and capability to conduct, malicious activity in cyberspace will be enhanced by a combination of observed trends.

Motivation is increasing. Australia's increasing reliance on the Internet is leading to more high-value information being stored and communicated on Australian government and commercial networks. This is boosting the incentive to undertake cyber crime or exploitation for direct monetary profit or indirect economic and political advantage.

There was a 46% surge in malicious software targeting mobile devices between late 2009 and late 2010.⁵

Capability is easier to acquire. Acquiring a cyber capability is becoming easier with increasingly sophisticated tools, information, and guidance readily available online.

New technologies will generate new vulnerabilities. The proliferation of new technologies will increase the number of potential vulnerabilities. Of note, the growth in cloud computing and expanding use of mobile computing devices, such as smartphones, laptops and tablet computers, will generate more platforms—with distinct software, settings and applications—and more users to exploit.

The spectrum of malicious actors is expanding. The ease of acquiring a cyber capability coupled with the potential high gains—whether financial, economic, diplomatic or political—is enticing more actors into malicious cyber activity.

4 Australian Competition and Consumer Commission, *Targeting Scams—Report of the ACCC on scam activity 2010*, 2011.

5 McAfee Labs, *McAfee Threats Report: First Quarter 2011*, 2011



COUNTERING THE CYBER THREAT





Countering the Cyber Threat

Malicious cyber activity will continue to challenge Australia's national security, economic prosperity and social wellbeing. As cyber threats become increasingly sophisticated and targeted, cyber security incidents can have significant and direct impacts on organisations. However, properly assessing the security risks specific to your organisation can help to minimise your vulnerability to cyber threats.

Questions Senior Management Need to Consider

Are you confident that your networks are not currently compromised? Is the security culture of your organisation a strength or a weakness? Here are five questions you should discuss with your information security team to review your organisation's security measures.

"What would a serious cyber security incident cost our organisation?"

Good information security is like an insurance policy. Good security can avoid direct costs of cleanup and also indirect costs such as downtime, lost productivity and loss of reputation and confidence in your organisation. If customer records, financial data or intellectual property were stolen, could you quickly and accurately determine what was lost? What if you had to take a system offline to conduct a forensic or legal investigation?

"Who would benefit from having access to our information?"

Your information is valuable. There are many state and non-state actors who would benefit from having access to your agency's information. Identify critical information, the confidentiality, integrity and the availability of which is essential to the ongoing function of your organisation. It is important to consider the aggregated value of your information, not only the value of individual records. Every organisation faces different threats and security risks, and needs to deal with them in different ways.

"What makes us secure against threats?"

Security is an ongoing process, not a product. As cyber intrusions become more sophisticated and targeted, so do information security techniques and processes. To secure your organisation against threats, make sure appropriate security governance, clearly defined policy, user education and third party assessments are in place, as they are all vital parts of information security. There is no silver bullet for information security and security products alone are not a solution.

"Is the behaviour of my staff enabling a strong security culture?"

Staff education is key. It only takes one malicious email attachment to be opened or one malicious website to be accessed to potentially compromise your whole business. Effectively trained staff enable a strong security culture. Responsibility for information is shared amongst all members of your organisation, so all staff should be aware of the threat to reduce the security risk of valued information being stolen.

"Are we ready to respond to a cyber security incident?"

Will a compromise affect your continuity? Sadly, many organisations generally do not take information security seriously until they have been compromised. Your systems could be taken offline by an attack, for example through a Denial of Service attack, affecting the availability and resilience of your network. Having access to current threat information, including the likelihood and consequences, will enable informed risk assessments.

Most organisations conduct fire drills—perhaps it's also time to test your resilience against a serious cyber security incident.



CASE STUDY



Case Study

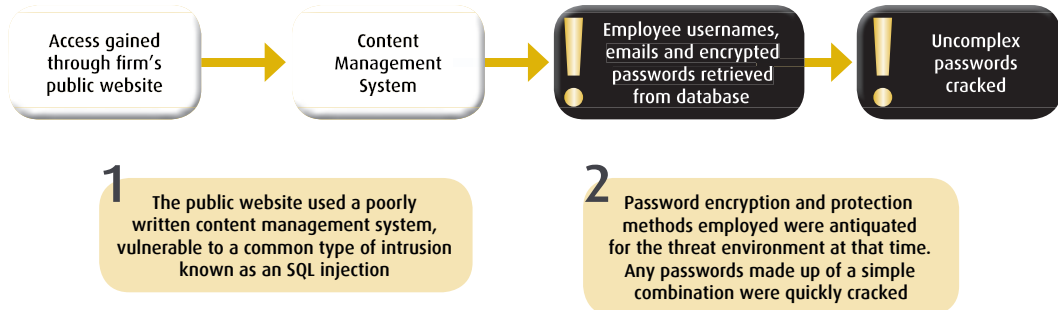
The information contained in the following case study has been derived from a range of open source materials. It has been included for demonstration purposes and is not intended as a commentary of those involved.

This case study examines events of early 2011 involving a firm affiliated with a technology security company that sells its products to a large western government. This company is recognised as an expert in information security best practices. Of particular note, the affiliated firm provides sensitive and classified information security services to foreign intelligence communities and other government agencies, including those relating to defence.

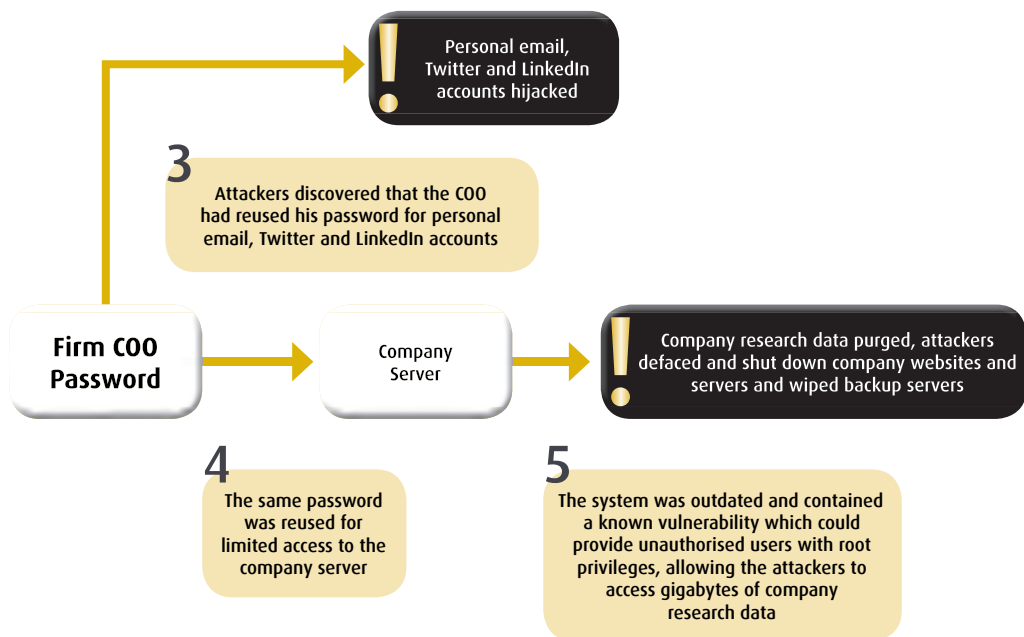
The affiliated firm's Chief Executive Officer had been personally researching an online group associated with collaborative, international activism through hacking, and in February 2011 revealed his intention to publicise its leaders' identities. In retaliation, over the following two days this online group managed to download the affiliated firm's entire corporate email archive and post it online, deface and shut-down its websites and servers and publish the usernames and passwords of anyone who had ever registered with associated websites.

Incredibly, this was achieved through unexceptional and widely known techniques, and was successful because—although considered an expert in information security—this security company and its affiliates didn't follow basic security practices themselves.

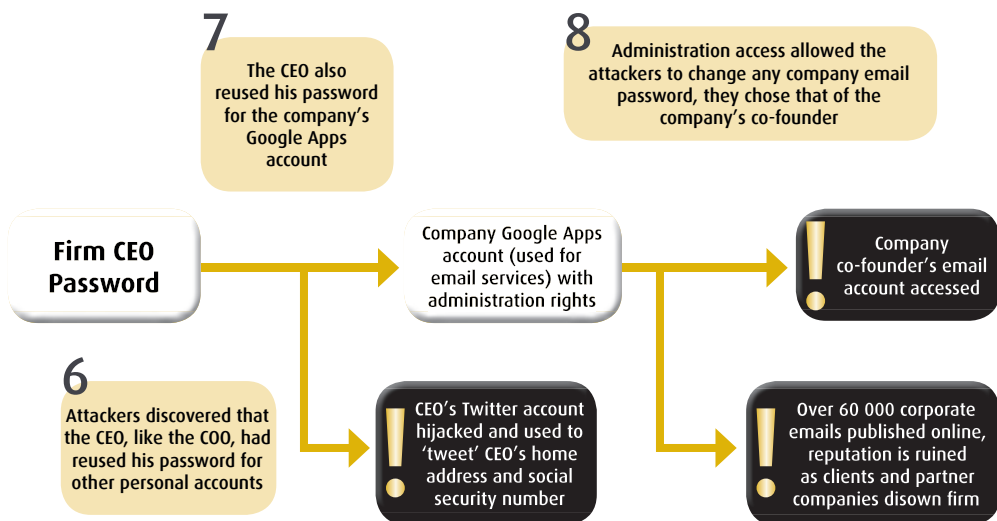
Here's how the attack was allegedly carried out.



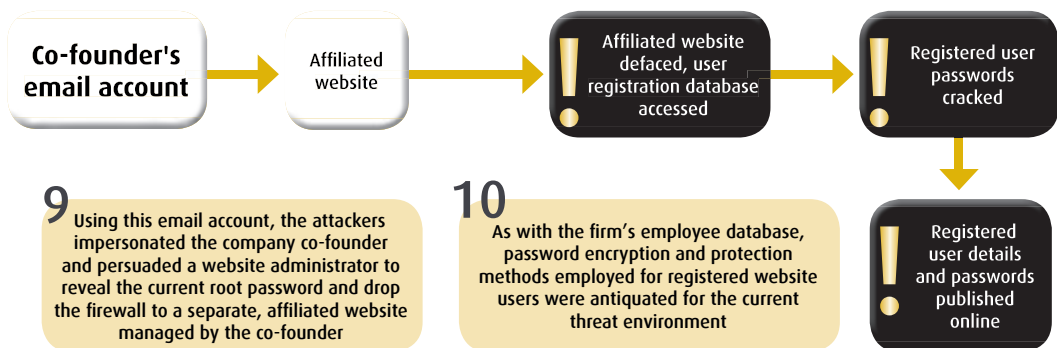
Regrettably, the uncomplex passwords cracked included those of the firm's Chief Operating Officer (COO) and Chief Executive Officer (CEO)—both of which were comprised of 6 lower case letters and 2 numbers. The attackers then discovered that the COO had reused the same password for other personal and business applications.



More significantly, the CEO had also reused the same password for a number of other accounts.



Access to the company co-founder's email account then allowed the attackers to undertake a social engineering campaign.



Had this technology security company and its affiliate properly understood their threat environment and the value of their information, as outlined in the *Questions Senior Management Need to Consider*, the significant operational and reputational damage outlined above could have been avoided.

What would a serious cyber security incident cost our organisation? Good information security is like an insurance policy. Had stronger information security practices been implemented from the start, this company may have prevented the substantial loss of information, reputation and confidence that ensued. Of particular note, the incident may have been mostly averted had the company invested in a well-written content management system, not susceptible to an SQL injection attack, for its public website.

Who would benefit from having access to our data? As a firm that provides services to government, there would already be many state and non-state actors who would find its information valuable. However, when the CEO publicised his intention to reveal the identities of the online group's leadership, his firm's security risk profile—and consequently that of the entire company—changed. The CEO did not acknowledge the increased value of the company's information to a potential attacker, and therefore did not re-assess the adequacy of information security practices.

What makes us secure against threats? Security is an ongoing process, not a product. In this case, for example, although password encryption and protections had been put in place at the start, their adequacy had degraded over time as technology evolved and attackers uncovered ways to exploit them. Because the company did not re-evaluate the threat environment, this security weakness remained unaddressed.

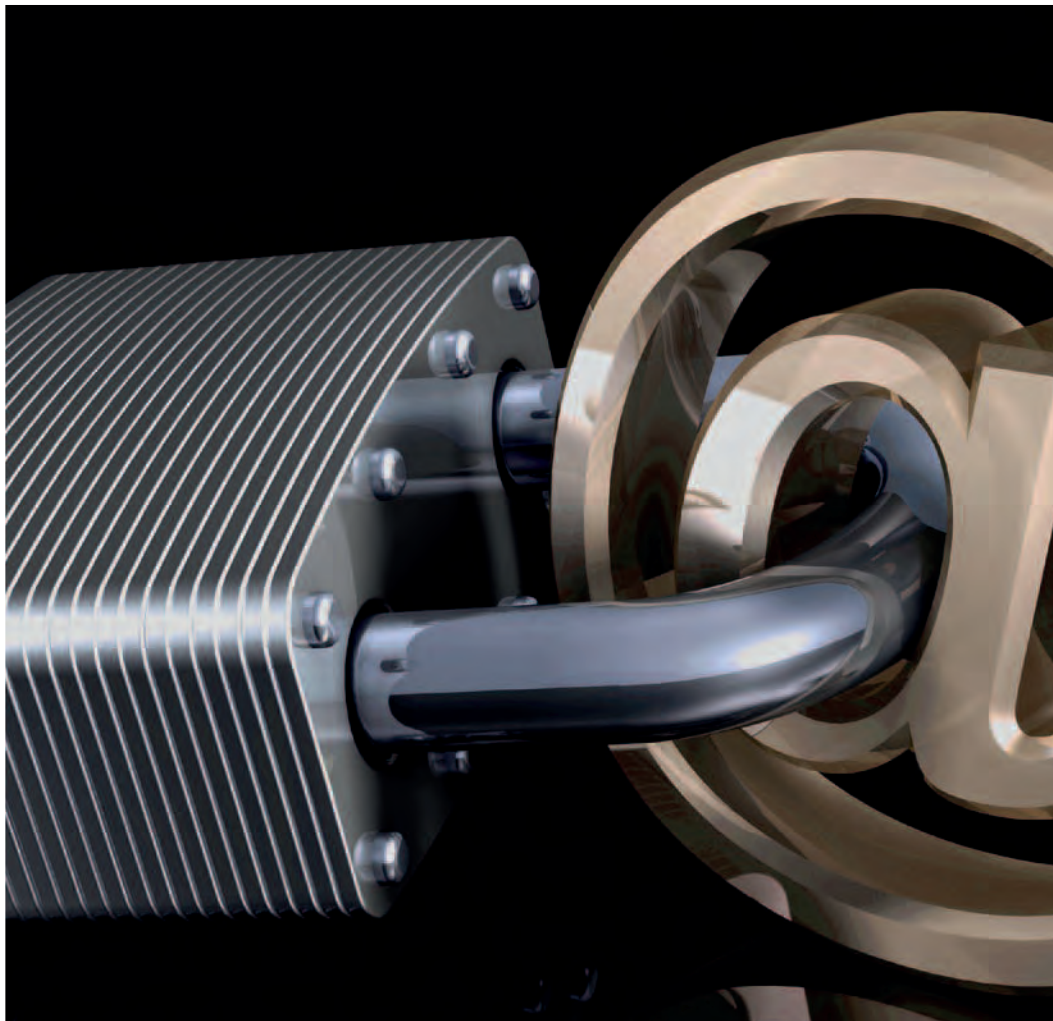
DID YOU KNOW?

41% of employees use the same password for multiple accounts.⁶

Is the behaviour of my staff enabling a strong security culture? Senior executives re-using passwords, and a website administrator susceptible to social engineering, demonstrate behaviour detrimental to the development of a sound security culture and a lack of security risk awareness.

Are we ready to respond to a cyber security incident? In this case, the company did not understand its threat environment and, as is commonly the case, only started taking its information security seriously once compromised.

⁶ RSA, 2011, *Workplace Security Survey*.



THE AUSTRALIAN GOVERNMENT INFORMATION SECURITY MANUAL



The Australian Government Information Security Manual

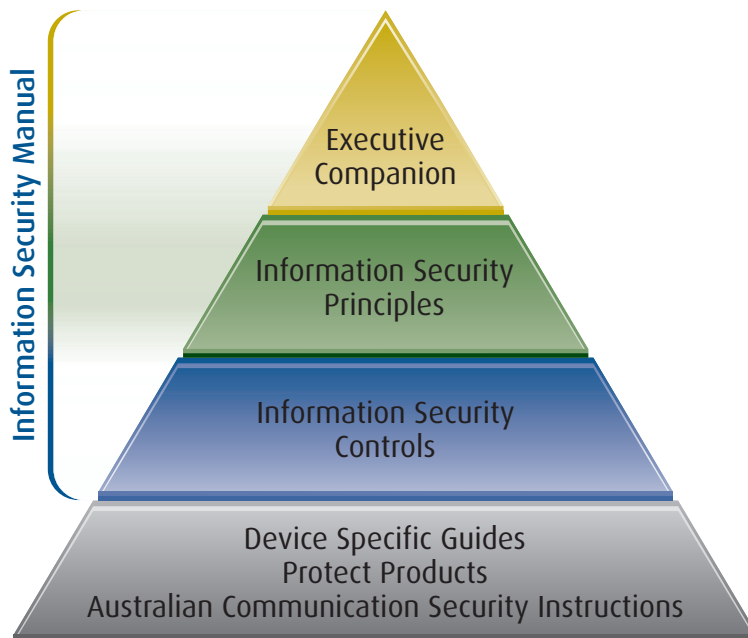
The *Australian Government Information Security Manual* (ISM), issued by DSD, is the Government's flagship document designed to assist Australian government agencies in applying a risk-based approach to protecting their information and ICT systems. This manual supports the guiding principles and strategic priorities outlined in the *Australian Government Cyber Security Strategy* by providing detailed information about the cyber security threat, as well as assisting agencies in determining appropriate controls to protect their information and systems.


While there are other standards and guidelines designed to protect information systems, the advice in the ISM is specifically based on activity observed by DSD on Australian government networks.

Format

This release of the ISM comprises a high level 'principles based' document and a detailed controls manual, further complemented by this 'Executive Companion'. This new format is designed to be more accessible to a wider audience across all levels of government to improve awareness of information security issues.

This product suite targets different areas of your agency to ensure that key decision makers across government are made aware of and involved in countering threats to their information and ICT systems. These products are designed to complement each other and provide agencies with the necessary information to conduct informed risk-based decisions based on their own business requirements, specific circumstances and risk appetite.





The **Executive Companion** is targeted towards the most senior executives in each agency, such as Deputy Secretaries, Secretaries and Chief Executive Officers, and comprises broader strategic messaging about key information security issues.

The new **Principles document** is aimed at Security Executives, Chief Information Security Officers, Chief Information Officers and senior decision makers across government and focuses on providing agencies with a better understanding of the cyber threat environment and rationale to assist agencies in developing informed information security policies within their organisations.

The **Controls manual** is aimed at IT Security Advisors, IT Security Managers and security practitioners across government. This manual provides a set of detailed controls that, when implemented, will help agencies adhere to the higher level principles document.

DID YOU KNOW?

If implemented as a package, DSD's top 4 mitigation strategies would have prevented at least 85% of intrusions analysed and responded to by DSD in 2010.

DSD provides further information security advice in the form of device specific guides, Australian Communications Security Instructions and *Protect* products—such as *Strategies to Mitigate Targeted Cyber Intrusions*. While these products reflect the policy specified in the ISM, not all ISM requirements can be implemented on all devices or in all environments. In these cases, device specific advice may take precedence over the non-platform specific advice in the ISM.

Compliance

The ISM provides agencies with a set of detailed controls that can be implemented to mitigate risks to their information and systems. Agencies are encouraged to make informed, risk-based decisions specific to their unique environments, circumstances and risk appetite.

There are two categories of compliance associated with the controls in the ISM—'must' and 'should'. These compliance requirements are determined according to the degree of security risk an agency will be accepting by not implementing the associated control. While the majority of ISM controls can be risk managed within an agency, the compliance requirements provide an indication of the appropriate level within your agency where any residual security risks must be accepted in order to grant non-compliance.

Non-compliance with 'must' controls is likely to represent a high security risk to agency information and systems. Therefore, the agency head is required to consider the justification for non-compliance and accept the associated security risks. It is important to note that non-compliance for some controls with a 'must' compliance requirement relating to the use of cryptographic material can only be granted by the Director DSD. These controls are marked accordingly in the ISM.

Non-compliance with 'should' controls is likely to represent a medium-to-low security risk to agency information and systems. Therefore, the accreditation authority (a senior executive delegated to accept security risks to information systems on behalf of an agency) can consider the justification for non-compliance and accept the associated security risks.



DSD'S ROLE





DSD's Role

What DSD can do for you

As directed by the *Intelligence Services Act (2001)*, DSD provides foreign signals intelligence as well as advice and assistance on matters relating to the security and integrity of electronic information. These twin missions complement each other, with the skillsets and capabilities required to be an expert at one being precisely those required to master the other. It is the same reasoning why Australia's signals intelligence and information security functions were co-located in the Defence Signals Bureau—the forerunner of DSD—more than 60 years ago.

While communications technology has changed fundamentally since that time, the integral link between the two missions remains unchanged. DSD understands the vulnerabilities in communications networks—it exploits them in foreign networks and so it is best placed to defend them in Australian government networks.

As the Commonwealth authority on information security, and informed by its signals intelligence expertise and capabilities, DSD can provide agencies with advice and assistance as well as further information on the cyber threat. DSD conducts a number of workshops and forums with IT Security Advisors throughout the year to facilitate open discussion on countering the cyber threat. These discussions focus on the challenges faced by Australian government agencies in protecting their information and systems.

The CSOC, located in DSD, provides coordinated operational responses to cyber security incidents of national importance. The CSOC is a resource designed to serve all government agencies and has embedded representation from the Australian Defence Force, Defence Intelligence Organisation, Australian Security Intelligence Organisation, Australian Federal Police and CERT Australia.

What you can do for DSD

Successfully protecting Australian networks from an increasingly sophisticated and persistent cyber threat requires strong collaboration. While DSD can provide technical advice and assistance, we can not tackle this challenge alone. Reporting of cyber security incidents provides DSD with greater visibility of the threat environment and assists in the prevention of cyber intrusions on Australian government networks.

While the information in the ISM is extensive, it represents advice at a point in time as technology and the threat environment continue to evolve. Please keep us informed on how we can continue to provide tailored advice that best meets the needs and requirements of your agency. DSD will focus on providing advice according to where it is most needed.



Contact

For all urgent and operational enquiries:

- Phone 1300 CYBER1 (1300 292 371) and select 1 at any time.
- Fill out a cyber security incident report form on the OnSecure website (<http://www.onsecure.gov.au/>).

For all non-urgent and general enquiries:

- Phone 1300 CYBER1 (1300 292 371) and select 2 at any time.
- Use the Advice and Assistance form on the OnSecure website. Australian Government-sponsored customers who do not have one should apply for an OnSecure account.
- Email: assist@dsd.gov.au
- Fax: (02) 6265 0760

