Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

UPDATE

JUNE 2014

The Cost of Compromise

Introduction

1. The Cyber Security Operations Centre (CSOC) regularly responds to cyber security compromises involving Australian government networks and other networks of national importance. This publication summarises the common cyber security compromise scenarios observed by the CSOC, and the costs associated with remediating these compromises.

2. The *Strategies to Mitigate Targeted Cyber Intrusions* remain your best defence against the cyber threat. Implementing the Top 4 strategies as a package is at the core of this protection, as they mitigate at least 85% of cyber intrusions responded to by the CSOC. The Top 4 strategies prevent execution of malicious software, and minimise software vulnerabilities and the ability of a cyber adversary to propagate across a network. The remaining 31 strategies form an excellent basis from which to assess further network security initiatives based on a risk assessment. Your risk assessment processes should take into account the specific risks faced by your agency, the information you are protecting, and your current network security posture. See *The Cyber Security Picture 2013* for updated information about threats to Australian government networks as observed by the CSOC during 2013.

3. Although the initial cost of implementing the *Strategies to Mitigate Targeted Cyber Intrusions* can seem high for some agencies, they actually represent an important investment in your organisation, reducing long term costs and risk. If you experience a network compromise, not only will you be faced with the cost of implementing these strategies to prevent further compromise, but you will also incur both higher direct and indirect costs associated with remediating the compromise. These costs include, but are not limited to: investigating the compromise, tactical remediation, reputational costs, opportunity costs from the loss of information, and lost productivity.

Can you afford a compromise?

4. Consider these common compromise scenarios responded to by the CSOC.

Low level: Denial of service attacks or malicious code injection against government websites: Some government websites and portals are attractive to hacktivist groups or individuals looking to cause nuisance, and are targeted repeatedly by denial of service attacks. The CSOC also sees many cases of malicious code being injected into legitimate federal, state and local government websites, for example, tourism websites or websites containing information about council services. Visitors to these websites can become victims via a drive-by download, and consequently the website can be blacklisted by search engines, security and anti-virus products. Such blacklisting can be difficult to reverse, and can result in loss of business and the ability to provide online services to the community.

Medium level: A cyber adversary has gained access to a network, but has not propagated extensively: A socially engineered email may have traversed the gateway and its attachment opened by a user, causing malicious code to execute. Or, a cyber adversary may be in possession of legitimate user credentials. This can still be a damaging compromise, because the adversary may have had enough time to steal valuable data from the network – the CSOC has seen cases where information has been stolen within 10 minutes of compromise. While time and resources will need to be temporarily diverted to investigate and remediate this activity, it is essential that be done to prevent even more damage from occurring.

High level: Major compromise of a network: The typical high-range compromise responded to by the CSOC involving an Australian government victim can usually be traced back to a socially engineered email; where a user has opened an attachment or clicked on a link, causing malware to execute on the workstation. The cyber adversary then established their presence on the network by compromising multiple workstations (in the worst examples, several hundred). The cyber adversary will find ways to mimic legitimate users, escalate privileges and access the most sensitive information on a network, and generally use any means available to make sure they maintain persistent access. Poorly-secured networks are likely to be exploited by multiple adversaries.

These compromises can take months or even years to discover, making them extremely damaging for the Australian Government. Foreign state-sponsored cyber adversaries have stolen intellectual property, information about Australia's negotiating position and government policy, and other information that could diminish the government's ability to achieve desired outcomes.

In the experience of the CSOC, the worst and most serious compromises can drain resources and take years to resolve. It can take at least 12 months to 2 years to fully remediate a compromise once discovered – to both remove the adversary from the network, and then implement the *Strategies to Mitigate Targeted Cyber Intrusions* to prevent further network compromises from occurring. It can also be difficult to fully assess the damage of these compromises when insufficient logs have been retained.

How often do these compromises occur?

5. **Low or medium level compromises are identified by or reported to the CSOC daily.** They can hit the biggest departments, or the smallest agency. Many cyber adversaries are indiscriminate, and are simply looking for the weakest link for opportunities to conduct malicious activities. Since 2012, the number of **known high-level compromises** of Australian government departments responded to by the CSOC **has reduced**, as more departments have implemented at least the Top 4 *Strategies to Mitigate Targeted Cyber Intrusions*, and then selectively implemented the remaining 31 to maximise their network defences. While the nature and impact of some of the activity observed by the CSOC remains unknown, raising your baseline cyber security posture forces cyber adversaries to either pursue easier targets, or become more sophisticated. As the CSOC plays an important role in ensuring that the Australian Government is positioned to defend against sophisticated threats, and update its advice accordingly, improved baseline security across the Australian Government increases the resources available to the CSOC to focus on sophisticated threats.

The cost of compromise

6. There are a number of direct and indirect costs associated with a compromise, including but not limited to:

a. Resources to investigate the extent of the intrusion, and understanding the harm.

b. The immediate remediation of the intrusion (for example by cyber security specialists).

c. Reactive implementation strategies to mitigate further intrusions – this is more expensive to do in response to an incident, as timeframes are more compressed compared to implementing these strategies proactively.

d. Lost productivity, and the costs of diverting staff and resources from other business to deal with a compromise.

e. Opportunity costs associated with the theft of information, such as intellectual property, or information about Australia's negotiating position.

f. Broader costs to the Australian economy where non-government information is stolen from government networks, e.g. patent information, personal information used to conduct fraud.

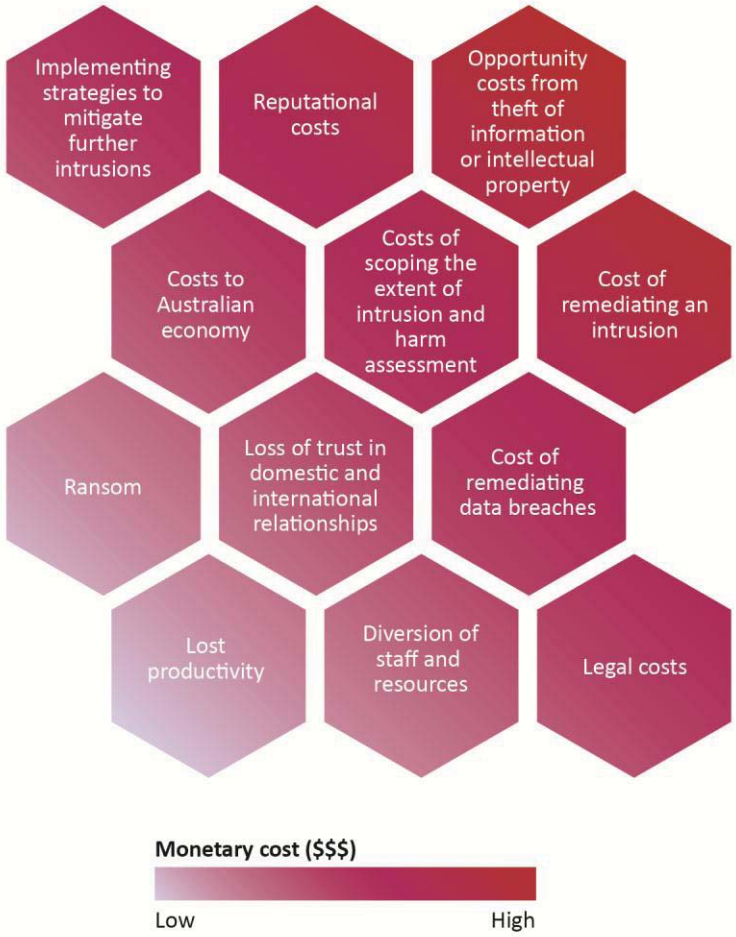
g. Reputational costs, including negative media exposure and the trust of your customers, in the case of disruption to the availability of online services.

h. Costs associated with breaching privacy legislation, or remediating data-breaches of financial information.

i. Legal costs when impacted third-parties may sue for negligence or breach of contract.

j. Loss of trust by government and industry partners, harming domestic and international relationships critical to the department.

k. The cost of paying a ransom, in the case of a ransomware attack.



7. If you do not have the skills and resources in-house to remediate an intrusion, contracting a suitably skilled company to do this work for you can be expensive, especially for smaller agencies. Other factors such as the availability of your logging records, documentation about the structure of your network, and how long the network has been compromised can also impact the costs and time to remediate a compromise. The CSOC commonly finds that poor logging records, or a poor understanding of the layout of a network, can impede the CSOC's ability to assist a victim organisation and result in more time and resources being required to remediate the compromise.

8. No department or agency is immune from the risk of compromise. While the upfront costs of implementing the *Strategies to Mitigate Targeted Cyber Intrusions* may seem high, senior managers should consider the associated costs that could be incurred if a serious compromise occurs on your network.

9. Even if you do not think that your information is particularly interesting, valuable or sensitive, consider the recent emergence of ransomware attacks, which tend to be more indiscriminate and opportunistic. In these cases, your information only needs to be valuable to you!

A final word

10. Your network is not necessarily the only network that holds your agency's information – do not forget about contractors and other service providers, who may be the weaker and therefore more attractive target for a cyber adversary that wants your information. Also consider that you likely hold the information of others, often with contractual provisions around confidentiality or secrecy. While your own information may potentially not be of interest to a cyber adversary, information you hold for third parties may be, and cyber adversaries often target the weakest link.

Further Information

11. The *Australian Government Information Security Manual* (ISM) assists in the protection of official government information that is processed, stored or communicated by Australian government systems, and is available at:

http://www.asd.gov.au/infosec/ism/index.htm

12. ASD's *Strategies to Mitigate Targeted Cyber Intrusions* and its companion ASD products, which complement the advice in the ISM, are available on ASD's website:

http://www.asd.gov.au/top35mitigationstrategies.htm

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.