Why companies are exposed to social engineering

Date: Oct 2012
Doc Ref: SOS-WP-SE-1210A

Author: Neville Gollan & Nathaniel Carew
# Table of Contents

Introduction................................................................................................................................. 1  
Relevance – the extent of exposure ............................................................................................ 2  
Challenge – making the case...................................................................................................... 4  
Protection – testing for vulnerabilities ...................................................................................... 5  
Conclusion.................................................................................................................................... 7  
About Sense of Security............................................................................................................. 8
Introduction

Who presents the most dangerous threat inside your business? Most organisations would be surprised to know that overly helpful employees can be far more dangerous than the stereotypical "disgruntled employee".

This whitepaper explores the vulnerability of enterprises to social engineering, an attack that manipulates well-meaning or curious employees into unwittingly abetting the theft of corporate secrets.

Three aspects of social engineering will be discussed:

1. Relevance – the extent of exposure;
2. Challenge – making the case;
3. Protection – testing and procedures.

While most CTOs and IT managers focus on the technical aspects of information security, highly publicised episodes overseas have shown that social engineering can sidestep the most advanced technological defences. Hardware solutions, with their reassuring rows of blinking lights, can be rendered ineffective once a social engineer has tricked an employee into giving privileged access to the internal network.

A cyber-security audit used a social engineering technique through placement of baited USB devices to penetrate the networks of eight state government agencies in Western Australia last year¹.

Social engineering is a type of insider threat. Insider threats are typically associated with the disgruntled employee who uses legitimate access to internal systems to steal, delete or manipulate information assets, or to disrupt operational systems dependent on IT such as SCADA control systems.

By comparison, a social engineering attack is carried out by an external assailant who deliberately manipulates an employee's good intention (i.e. their willingness to assist) or their general curiosity, such as enticing them to click on a link in an email to a malicious website. While social engineering and the disgruntled employee are both insider threats, defending against these respective attacks requires very different approaches.

The consequences of not protecting against social engineering can be disastrous, as recent breaches at security vendor RSA and security contractor HBGary have demonstrated. The viability of launching a social engineering attack has risen with the advent of social networking sites with a wealth of personal information that can greatly aid a social engineer.

One of the greatest challenges to enterprises defending against social engineering is coordinating a response from different departments, especially Human Resource

Management. The answer to social engineering is not to buy another security appliance or software product. The best protection is ongoing security awareness training and a robust set of policies and procedures that reminds all employees of their role in safeguarding their company’s integrity and property.

Relevance – the extent of exposure

2011 will be remembered for one of the biggest security breaches ever. Hackers broke into security company RSA’s systems and stole very sensitive data relating to the operation of its security tokens which are used globally by financial institutions, enterprises and governments to authenticate network access and commercial transactions².

The hackers’ first step in embarrassing one of the IT world’s most impregnable companies was a phishing email targeting RSA staff with the subject line “2011 Recruitment Plan”. The malicious spreadsheet it contained helped attackers record passwords remotely and penetrate the corporate network.

This was social engineering at work.

Advances in IT security have made it increasingly difficult to hack into a well-guarded enterprise. Network defences, encryption and smarter detection have forced cyber-attacks to look for easier targets which increasingly mean the soft underbelly represented by employees.

Social engineering has emerged as one of the most successful attack vectors in the past two years. International “hacktivist” group Anonymous claimed the scalp of HBGary, a US IT security contractor, in part by impersonating the CEO and asking for a password reset.

The damage to reputation for RSA and HBGary was enormous. Anonymous hackers posted offensive messages under the Twitter names of various HBGary executives and deleted the backups from their servers³.

The financial costs of the attacks were also measured in the millions. RSA’s affected customers included 80 percent of banks in the US which were predicted to spend US$50 million to US$100 million replacing compromised tokens⁴.

Social engineering is often employed in the theft of data such as intellectual property, personal information or credit-card numbers. This is a growing problem globally although the extent to which it exists in Australia is unknown because Australian businesses are not required to notify customers when a breach occurs.

Six years ago the Australian Law Reform Commission recommended mandatory notifications of data breaches which would bring federal privacy laws in line with the US and UK.

² [http://online.wsj.com/article/SB10001424052702304906004576369990616694366.html](http://online.wsj.com/article/SB10001424052702304906004576369990616694366.html)
However, the Australian federal government has been reluctant to enact legislation due to resistance from telecommunications and other IT companies which claimed voluntary reporting was sufficient protection of consumers' privacy.

IT security companies have said privately that “the scale of data theft dwarfed that known by the government and reported in the media”.

Unfortunately, many businesses may not even know they have been the victim of social engineering. It can take several months to know that an incident has occurred, how it happened and what was stolen.

The Risk of Insider Fraud: U.S. Study of IT and Business Practitioners report found that it took three months on average to recognise insider fraud had occurred and another three months to determine the root cause of the insider fraud incident and the consequences to the organisation.

Common tactics used by social engineers include “tailgating” employees into secure areas by following them through a guarded entrance before the door has closed. Another is pretexting where the social engineer convinces an employee, in person or by phone or email, to hand over confidential information by impersonating someone else.

One of the most widely used tactics is sending “phishing” emails such as the one in the RSA breach. The email is disguised to appear as though it comes from a legitimate source and encourages the target to activate the attached malicious file or click on a link that directs the victim to a website hosting malicious code or requesting personal details.

One practice with a high success rate is baiting. A social engineer leaves infected USB keys or other media in common areas such as lunch rooms, parking lots or foyers for employees to pick up and insert in their computers.

A USB key could contain a keylogger that grabs passwords and keystrokes from the employee’s computer and relays the data back to the hacker’s server on an external network. Connections could also be established out to the attacker, handing over control of the employee’s computer.

A hacker could use a compromised computer to move around the internal network using the access permissions of the user.

None of the methods above requires sophisticated technology or skills and yet they can be extremely effective against many organisations, regardless of the number and complexity of their electronic defences.

Social engineering is not considered in many organisations as a serious threat to corporate information, and the threat consequently is often left unaddressed. This mismatch between the effectiveness of a social engineering attack and the low perception of risk by enterprises.

---

7 The Risk of Insider Fraud: U.S. Study of IT and Business Practitioners by Ponemon Institute LLC, October 2011
The security community typically faces resistance from senior management because they fail to understand neither the need for social engineering assessments nor the advantage in strengthening their policies against them.

**Challenge – making the case**

Enterprises are not doing enough to protect themselves against social engineering despite its potential to cause serious damage. While there is growing recognition that the human factor cannot be ignored, there is still a reluctance to extend traditional, technology-based penetration testing to include human elements.

Social engineering audits can face opposition from senior management. They may decide to confine a penetration test to a technology review rather than one that includes human factor tests, which may be perceived as too complicated or expensive.

The categorisation of social engineering as an insider threat can also cause confusion.

A business may think it has done enough by installing anti-virus, firewalls, permission controls and patching to defend against the typical disgruntled-employee scenario but it would still be vulnerable to social engineering.

Today’s strong focus on customer service can assist social engineers to take advantage of over-helpful receptionists who have access to sensitive information such as the home address of the CEO.

Social engineering has become easier thanks to the popularity of social networks which can give an attacker personal details such as maiden names, school history and favourite pastimes which can be used to construct a fake persona, or the perfect recipe for a password recovery attack that requires answers to “secret” questions. Instead of searching through rubbish bins or “dumpster diving”, a hacker can profile a target within a few hours without leaving the desk.

Common difficulties in fighting social engineering include assigning responsibility for countermeasures, assessing vulnerability and admitting to the size of the threat. The solution is not a simple technical one. It requires co-operation among senior management, leadership in setting examples and development of policies and procedures from within the HR department.

Testing is the first step to analysing opportunities for social engineering, but this can create potential staff related issues when carried out against unknowing staff. An audit must be conducted covertly in a real-world environment but without embarrassing employees or damaging the organisation’s productivity.

Social engineering is almost guaranteed to succeed against an unprepared organisation because it is a human issue, but despite this a breach will not look good for the CIO or the CSO regardless.

While managing people is not the sole responsibility of the CIO or CSO, the consequences of a duped employee surrendering access to the internal network is.
Although the cost of assessment and preventative measures against social engineering are relatively low, the economic climate makes it difficult for companies to spend money on training they may consider “non-essential” rather than spending it on technology which has a clearer return on investment.

An organisation must be open to the results of an audit which can reveal vulnerabilities businesses do not want to admit to. The truth can often be uncomfortable and may stoke political opposition from managers who would rather ignore the problem.

**Protection – testing for vulnerabilities**

Ideally security reviews are scoped to be comprehensive and include testing the people, process and technology elements. Unfortunately most reviews are limited and only assess technology, avoiding to address the human element even though it is potentially a greater threat.

Defending against social engineering is counter-intuitive in some senses. The classic insider threat of a disgruntled employee can be addressed with technology and permission controls. But the greatest threats in social engineering are helpful and naive staff.

Security organisations often discuss the “M&M approach” where an organisation has a hardened outer perimeter but a soft and vulnerable inside. Appropriate defences against social engineering involve “hardening” the attitudes of employees as well.

When defining the scope for a social engineering assessment, management need to consider the risk of not conducting a comprehensive review. A decision needs to be made on how thorough the review should be. Is baiting with USB sticks sufficient? Should other types of test methods be considered?

In most instances a review encompassing social engineering should be undertaken during a normal workday when employees, customers, suppliers and related parties are going about their business as usual. For the review to be effective it must be covert and carried out in a realistic setting. The following methods should be considered as legitimate tests when defining the review scope.
<table>
<thead>
<tr>
<th>Test Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pretexiting</td>
<td>Pretexiting is the act of creating and using an invented scenario (the pretext) to engage a target victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.</td>
</tr>
<tr>
<td>Diversion</td>
<td>Diversion theft, also known as the &quot;Corner Game&quot; or &quot;Round the Corner Game&quot;, is a technique used by malicious parties to persuade a person responsible for a legitimate delivery or materials or information, that the content is requested elsewhere.</td>
</tr>
<tr>
<td>Phishing</td>
<td>Phishing is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate source requesting &quot;verification&quot; of information and warning of some dire consequence if it is not provided.</td>
</tr>
<tr>
<td>Baiting</td>
<td>Baiting is essentially a Trojan Horse that uses physical media. In this instance, an attacker leaves a malware infected media (e.g. USB drive) in a location which is likely to be found by employees and waits for the victim to use the device, activating the attack.</td>
</tr>
<tr>
<td>Quid Pro Quo</td>
<td>In a quid pro quo attack, an external party calls random numbers at a company claiming to be calling back from technical support. Eventually they will hit someone with a legitimate problem, grateful that someone is calling back to help them. The attacker will &quot;help&quot; solve the problem and in the process have the user type commands that give the attacker access or launch malware.</td>
</tr>
<tr>
<td>Tailgating</td>
<td>An attacker, seeking entry to a restricted area where access is by unattended, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access. Following common courtesy, the legitimate person will usually hold the door open for the attacker. The attacker may also fake the action of presenting an identity token.</td>
</tr>
<tr>
<td>Soft Target</td>
<td>A soft target attack often focusses on the more likely weak links in an organisations security. This could be a manager’s mobile device or personal email account on Yahoo!, Gmail, or Hotmail etc; anywhere that an attacker might be able to harvest information for use in breaching the organisation that they work for.</td>
</tr>
</tbody>
</table>

Although a review needs to operate in a live environment it should not interrupt operations, cause loss of productivity or be performed in a manner disrespectful to the organisation or its employees. The review also should use repeatable methodologies and log all actions during the test. The resulting report should include meaningful and actionable findings and recommendations.
When an organisation moves to set up defences against social engineering it is important to consider that these will require regular attention; set-and-forget approaches will not work. Security awareness education is absolutely critical and needs to be frequently addressed. It should be part of the induction process and repeated on a 12-month basis for all staff.

Policies and frameworks help govern behaviour and explain responsibilities to all employees from the top down. If staff do not believe that management are adhering to the same rules and regulations then they are certainly less inclined to follow them themselves. Reactive processes also need to be addressed such as writing an incident response program that triggers an internal procedure after a social engineering attack.

The key to a successful and sustained defence against social engineering is enforcing behaviour throughout the company. CSOs may find positive reinforcement more effective than upbraiding lapses in behaviour.

A company which understands the importance of security at every level will present a much harder target to the social engineer.

**Conclusion**

Social engineering is a very serious threat that can quickly undo large investments in IT security and cause extreme damage to reputation, customer data and corporate IP.

The extent of data theft in Australia may be under-reported and underestimated, but reports from the US and the UK show that failing to defend against social engineering can have severe ramifications on reputation and revenue.

Despite the evidence that social engineering can be more effective than external network attacks, many organisations are excluding reviews from the scope of their security test programme. This inadvertently presents their organisation with residual exposure.

Technology-based defences against internal threats are not effective in stopping social engineering, and the human factor may sit outside the usual considerations before CIOs and IT managers in reviewing security.

Executive leadership and co-operation between departments are essential to winning approval for social engineering reviews and helping ensure a company-wide change in behaviour.

Effective countermeasures to social engineering must be backed by policies, procedures and regular training, and have buy-in from senior management.

Human Resource Management must drive adoption of policies through induction processes and staff retraining, and positively reinforce behaviour through corporate culture.
About Sense of Security

Sense of Security Pty Ltd is an Australian based information security and risk management consulting practice delivering industry leading services and research to organisations throughout Australia and abroad. Our strategic approach to security provides you with a capability to assess your risk and deliver qualified guidance on how to protect your information assets. We provide expertise in governance & compliance, strategy & architecture through to risk assessment, assurance & technical security testing.

For more information please contact us:
Web: www.senseofsecurity.com.au
Email: info@senseofsecurity.com.au
Phone: 1300 922 923

Sense of Security - Compliance, Protection and Business Confidence