Global Information Assurance Certification Paper

Mitigating Teleworking Risks

1. The Arrival of Teleworking

Across the globe, many Corporate Networks now extend into their workers' homes. The nature of these extended networks is changing rapidly and dramatically. In its earliest years, remote access was generally restricted to systems support staff for emergency support access. But the growing importance of information and information systems in doing business has created a need for access to information quickly and at all times of the day or night. And anyone might need that information - business end users are just as likely to need access as technical support staff.

The introduction of the infrastructure to facilitate these new business needs has also opened the door to telecommuting. Uptake was relatively slow in the early years as companies and workers considered the viability of the concept and awaited the broadband access required to make it efficient. Now that broadband has reached the home (in the shape of digital subscriber line [DSL], in its various guises, and cable modems) teleworking is finally taking off, and in a big way. In the US, recent surveys vary in their estimates of the number of teleworkers but one (Cahners In-Stat Group) finds that there are 32 million teleworkers currently, up from around 19 million in 2000. This is hardly surprising, given the possible benefits to the employee - flexible working location, improved work/life balance, reductions in commuting times, and even the prospect of reduced city-centre congestion when you do have to go to the office. The company also wins - there can be expense savings on city-centre desk space, there is evidence that teleworkers take less sick leave as they continue to work from home, and even that teleworkers work more hours and more days in general. Teleworking has clearly arrived and it looks set to be a permanent feature of the work environment.

2. Teleworking - the threats

With the increased freedom afforded us by teleworking there also comes increased information risk. The risk may be considered in two layers - the risk at the remote PC and the risk at the corporate network.

2.1. Exposure of remote PC on Internet

The teleworker's PC cannot be protected by the company at all times. When not connected to the office network, the teleworker's PC will be used for Web surfing, new software will be installed, old software reconfigured, e-mail attachments opened and Internet files downloaded. Hence, the system build is clearly not compliant with the corporate standard, which raises questions on the effectiveness of any security software running on the remote PC, and the risk of virus infection is increased.

There is also the risk of physical access to corporate information stored on the remote PC. A corporate PC is situated within the office premises, where it is generally protected by multiple layers of building access controls, 24 hour on-site security personnel and surveillance equipment (for larger companies, at least.) On the other hand, the remote PC is likely to have only one layer of physical access control (ie., the front door) and is unlikely to have 24 hour on-site protection or surveillance. The risk of the PC and/or the information it contains being stolen or otherwise exposed is hence increased.

All of this activity is generally restricted by the company security policy but this cannot be enforced on a private PC. Hence, when the user next logs in to the office, the damage may already have been done - information may already have been accessed directly from the remote PC, and/or a compromised/infected PC becomes part of the office network.

2.2. Exposure of corporate resources on Internet

Consider the nature of the access required by a teleworker. The aim is to allow them to work from home as effectively as they might in the office. Hence, they need access to the data available in the office environment. This may require mapping network drives to the remote PC, access to confidential databases, intranet web servers, or corporate applications. Ordinarily, these services would never be made available outside the corporate network. In fact, the teleworker's remote PC effectively becomes part of the corporate network but it sits outside the traditional network perimeter and information defences.

Hence, by extending the network to the teleworker's home via the Internet, the risk of these services being exposed on the Internet is increased. The exposure may be direct or indirect - direct to the Internet by presenting service interfaces at the corporate network perimeter and transmission of corporate information over public lines; or indirect by use of the remote PC to bridge between the Internet and the corporate network. Direct exposure can be mitigated by strong identification, authentication and authorisation at the corporate firewall or DMZ and the use of encryption technology to protect data integrity and confidentiality. (Typically, a virtual private network [VPN] is employed to provide aspects of all of the above.) Indirect exposure can be mitigated by protecting the remote PC by deploying standard security measures on the PC but, as discussed above, the security status of the remote PC cannot be guaranteed and hence the corporate network must be protected against a compromised remote PC.

3. Always-on connections - the threats

Effectively, the teleworker's PC becomes no-man's-land in the battle between corporate information security and the inquisitive and destructive forces at work on the Internet. This has been the case since telecommuting began, but the introduction of always-on connections is bringing its own threats.

3.1. Dial-up modem v always-on - inherent threats

Until recently, the teleworker, whether permanently stationed at home or simply accessing corporate e-mail in the evening, had little choice other than to connect via a standard 56k analogue modem over POTS (Plain Old Telephone System) or relatively expensive ISDN. Performance can be painfully slow, particularly via POTS. The introduction of broadband, always-on connections has radically improved the situation. However, the analogue modem has some inherent advantages over DSL/cable when it comes to security due to the nature of the connection technology.

Since the analogue modem uses a standard phone line to connect to the ISP, long-duration connections are not financially viable, generally speaking. Hence, the connection to the Internet tends to be relatively short lived (no more than a few

hours at the maximum.) Also, the ISP will allocate your IP address dynamically when you log in. This combination of short connection periods and variable IP address makes it more difficult (though not impossible) for a potential cracker to find your system since they must look in the right place at the right time to spot you online. It also limits the amount of time which the cracker has to penetrate your system once you have been found.

Analogue modems also provide the option of dialling direct into the corporate network via a modem pool. There are advantages to this approach -

- **Obscurity** : the network gateway will not generally be made public knowledge and, hence, the number of unauthorised connection attempts is minimised.
- **Segregation** : the remote PC is not connected to both the Internet and the corporate network simultaneously. Hence, there is no risk of acting as a bridge between the Internet and the office.

DSL/cable modem connections are almost the diametric opposite of dial-up connections. Connection speeds are comparatively high bandwidth. The service is generally paid for at a fixed price per month and hence the connection can be long-lived or even semi-permanent. The ISP can allocate a permanent IP address (though dynamic addressing is still possible.) As a result, the home PC is now a viable target on the Internet, facing essentially the same scans, probes and attacks as any permanent Internet presence. Also, the technology does not allow direct connection from the home to the office, thus requiring that connection is made via an ISP. Hence, the telecommuter's PC is connected to both the Internet and the corporate network, and risks acting as a bridge between the two.

The possibility of utilising the telecommuter's PC as a bridge into the corporate network must be a great temptation to a cracker. Would they prefer to

1. break into the company network via an enterprise level firewall/DMZ which is configured and maintained by security professionals, with IDS, hardened operating systems and 24 hour monitoring

OR

2. break into a Windows PC, with a (probably) unmaintained, ill-configured firewall, minimal IDS, minimal monitoring and a VPN tunnel into the heart of the corporate network which has already been authenticated and authorised?

Clearly, the second option is likely to be simpler and quicker. Hence, it will be important to protect the remote PC from the Internet when the teleworker is connected to the corporate network. However, the teleworker's PC is not only at risk when connected to the office.

3.2. Teleworkers' behavioural threats

With the massive increase in useable bandwidth, always-on connections are likely to lead to online behavioural changes in the user. Evidence from a recent SBC/Southwestern Bell survey in the US suggests that DSL subscribers spend almost four times longer on the Internet than dial-up customers. Even if the subscriber always breaks the Internet connection after use, the risk of being located and attacked is clearly greater the longer he or she spends online.

The same survey also indicates that almost twice as many subscribers will

download files such as MP3 or video using DSL compared to dial-up modem. Downloading a 1MB file on a 56k analogue modem is a daunting task, easily taking 30 minutes or more and often requiring multiple attempts. But with DSL, the download will often take less than a minute. The user's options are now much wider - any size download can be considered, even just out of mild interest. Hence, downloads become more common and, with it, the risk of virus infection grows. Once the virus is on the teleworker's PC, it is effectively on the corporate network.

3.3. Bridging networks - an example scenario : Zombies and Sub7

As mentioned above, the typical home broadband connection will connect the teleworker to both the Internet and the corporate network. Hence, the possibility exists for a hacker to access corporate resources via the remote PC. Malicious IRC Bots, commonly known as Zombies, are a particularly dangerous example of how a hacker might create such a bridge. Steve Gibson, of Gibson Research Corporation, gives a detailed description on the GRC web site of his investigation into the use of Zombies to compromise machines for DDoS attacks and more.

To summarise Gibson's findings, Zombies are modified Trojan horse viruses which act as IRC (Internet Relay Chat) agents. The machine is typically infected by opening a file posted to a chat room or via an e-mail attachment. Once the infected PC is booted, the Zombie will attempt to "phone home" to an IRC server, announcing its availability to the hacker who distributed it. It will provide details of the IP address and port on which it can be contacted. The hacker can then contact the Zombie via the IRC channel and tell it to launch denial of service attacks on any given IP address. With hundreds or possibly thousands of these Zombies available to a hacker, massive distributed DoS attacks are possible, which is exactly what happened to the Gibson Research site. It is worth noting that broadband, always-on connections are particularly sought after by the Zombie hacker community and hence are more likely to be targeted for further investigation if the machine becomes infected.

However, Gibson also discovered that the hacker will often use the Zombie to download the Sub7 Server Trojan. Once installed, Sub7 will also attempt to connect to the Internet and post its connection details to an IRC server or via e-mail. If successful, the hacker now has access to watch everything that is happening on the infected PC and can even take control of the machine, run applications, download and upload files, restart Windows, and so on. The complete list of Sub7's functionality is impressive but frightening - just about anything is possible. (For details see the description of the Sub7 Trojan on the BWeb site - see References.)

Obviously, if a telecommuter's PC was to be infected by such a Zombie, the hacker may have direct access to the corporate network every time the user logs in. Even if the PC is default configured to prevent simultaneous Internet and corporate access (as discussed later regarding the use of VPN's) the power of Sub7 could allow the hacker to reconfigure or to install software to workaround that protection. Sub7 is also capable of logging keystrokes even while the hacker is not connected to the compromised PC. The keystroke log can then be downloaded at the hacker's leisure. Hence, the teleworker's activity could be monitored even if the hacker is locked out of the system while it is connected to the corporate network.

4. Mitigating the threats

As demonstrated in the discussion above, there are some very real security issues to be considered around teleworking. These issues are wide-ranging - the accidental introduction of viruses to the office environment; increased exposure to Internet attacks; even acting as a backdoor into the heart of the corporate network.

To protect against these issues, security must be taken seriously by the teleworker and his or her company. The remote PC must be protected against the Internet and the corporate network should be protected from the remote PC. This final section discusses the vital areas which must be tackled in protecting the teleworker and the company.

4.1. Security Policy

As ever, good security begins with the security policy. Security policy must cover telecommuting/teleworking. In particular it should consider -

- who may telework - identify the roles/jobs which may be considered for teleworking
- services available to teleworkers - the types of network and application services which may be provided to teleworkers
- information restrictions - are there classified information types which should not be made available to teleworkers?
- Identification/authentication/authorisation - how should teleworkers be identified, authenticated and authorised before accessing corporate resources
- Equipment and software specifications - are there any specific equipment or software products which must be deployed on the teleworker's PC? (eg., firewall or encryption software)
- Integrity and confidentiality - consider how the connection to the remote PC should be protected (ie., VPN) and how data on the machine should be protected
- Maintenance guidelines - how should the teleworker's PC configuration be protected, updated and monitored?
- User guidelines - clarify the user's role in protecting corporate resources - eg., appropriate use of resources; user should not modify security configurations; use of anti-virus software; storage of corporate data on local drives; use of encryption tools
- User education - ensure that users understand the possible information risks associated with teleworking, how those risks are addressed, and the user's role in minimising the risks

4.2. User Education

To repeat the statement above, user education is essential. Users must understand that teleworking does entail genuine security risks and that they have a role to play in protecting corporate resources from attack, damage or loss. It is also to their own benefit that they understand the risks to their own PC and private data of their

behaviour while accessing the web in their own time, and how to mitigate those risks.

4.3. Protect the remote PC

The remote PC must be protected from the Internet and corporate information stored locally should be protected from prying eyes. (Note, however, that ideally corporate information should not be stored on the teleworker's own PC - this should be considered in the security policy.)

4.3.1. Firewalls

The corporate perimeter defences need to be extended to bring the remote PC within the perimeter - ie., firewall software should be installed on the remote PC. However, there are several issues around the effectiveness of the firewall.

The firewall software must be properly maintained - this means software patches must be implemented as appropriate and the firewall must be correctly configured. Bear in mind that the remote PC probably belongs to the user and hence he or she has full administrator access to the machine - the system configuration may change regularly which could leave the firewall disabled. Hence, you should consider implementing an automated audit process when the user logs into the corporate network. This audit should check that the software is operational, correctly configured and that patches have been applied. If necessary, patches should be applied before allowing the user to continue.

There is also the question of the choice of firewall product. There are certainly home firewall products which are effective in blocking uninvited inbound traffic. However, there are also products which will allow most or all outbound connections, opening the PC up to the Zombie attack discussed earlier, for example. Hence the firewall product should preferably be capable of monitoring and blocking all network traffic from applications which have not been specifically authorised to access the network/Internet.

The user's education should include an understanding of the role played by the firewall and how important it is that the firewall is running correctly. The user should be encouraged to have the firewall running whenever they are connected to the Internet, even when not connected to the corporate network. This will help to protect the user's own files and ultimately protects corporate resources.

A home firewall is an essential precaution on the remote PC. However, designing a standard configuration which is maximally effective for every home PC is essentially impossible. Manual configuration could be considered but this could prove time-consuming and expensive if it is to be handled by qualified personnel, while most end users do not have the experience to handle this unaided. Hence, it should not be assumed that the remote firewall is fireproof. Multiple layers of security will be required - strength in depth is the key.

4.3.2. Virus protection

Anti-virus software is an essential measure on any web user's PC, whether or not they telework.

As per the firewall, the anti-virus product must be properly maintained - the software

must be patched as and when necessary, the virus definition files must be regularly updated, and the software must be configured correctly. It should be configured for automatic scanning of e-mails and files opened. Entire system scans should be performed at regular intervals.

Again, it is possible that the software could be disabled as a result of user action. Hence, consider performing an automatic audit of the virus software at login, ensuring that the software is running, that definition files are up to date and that patches have been applied. If possible, check the time of the last system scan. New definition files or patches should be applied and the last system scan should be confirmed as recent before the user is allowed to continue.

The user's education should include an understanding of the importance of the anti-virus software and the correct operation of the product. Teach good practice in the handling of downloads and attachments. The user should be encouraged to keep the product operational at all times, whether connected to the Internet or not.

However, it is always possible that a virus will be missed by the software and the remote PC will be infected anyway, spreading to the corporate network at the next login. To counter this possibility, consider running anti-virus software in the DMZ back at the office.

4.3.3. Data protection

If corporate data will be stored on the remote PC, then it should be protected by encryption software. There are packages which will encrypt disk partitions or individual files as required.

If the data will be stored on removable media then not only should it be encrypted but it should also be removed from the PC and locked away when not in use.

Also, bear in mind that information security does not only refer to protection from deliberate attack or theft. Information can be lost due to hardware or media failures and hence backups should be kept. Since the typical home PC is unlikely to have an automated backup network attached, the teleworker should be careful to make backups as required. Also, information security is about availability. Information stored on the remote PC is not likely to be available from the office.

For these reasons, it is preferable that corporate information should be stored on the corporate network and not at home.

4.4. Protect corporate resources from the Internet

If the remote PC is compromised by a hacker and/or infected by a virus, then the corporate network is at risk. Alternatively, the link between the remote PC and the office could be compromised directly. Hence, precautions should be taken to control the PC's access to corporate resources and to monitor the contents of the traffic.

4.4.1. Identify, authenticate and authorise remote connections

It is vital that only authorised personnel are able to access corporate resources remotely. All attempts to connect to corporate services should be captured within the DMZ until the source of the connection has been identified and authenticated.

Strong authentication technology should be employed. At the least, this should be strong passwords - ie., of appropriate length, not easily guessed, and containing non-alphanumeric characters. These requirements should be enforced automatically. Given that Trojans such as Sub7 can provide a hacker with your userID and password, you should also require that passwords are changed frequently. One-time password technologies make it almost impossible for the hacker to steal a usable password, and hence these technologies are far preferable. Typical one-time password technologies involve the use of a password combined with a passcode. The passcode is generated using an electronic token, and is based on a hash generated from the current time or from a randomly generated challenge provided by the corporate authentication server. Since the hacker does not have access to the token he or she cannot reply with the correct passcode and hence cannot be authenticated.

Once identified and authenticated the user should be permitted access only to services and resources for which they have been authorised. This is particularly important in order to protect against the possibility of a hacker compromising the remote PC and posing as the authenticated user. Ideally, each individual service/resource request will be authorised separately, rather than simply allowing access to an area of the corporate network. It is only if the user's access rights are understood at this level of detail that the inappropriate behaviour of a hacker might be effectively identified.

4.4.2. Protect the remote link

The remote link should be protected against surveillance and interference by the use of VPN tunnel technology. VPN creates a secure link (known as a tunnel) between the remote host and corporate DMZ. Data confidentiality is protected by encrypting the payload of the TCP/IP packets in transit. Data integrity is ensured by including a hash of the payload in the header. Source and target IP addresses on the private networks are also protected. Since no unauthorised party can read or interfere with the payload, we effectively have a secure tunnel through the public network.

The use of VPN's is becoming very popular as a solution for secure teleworking communications. However, it should be remembered that the VPN only protects the data in transit and is not an entire solution in its own right. It is essential to protect against unauthorised VPN connections to the corporate network, and to monitor/authorise remote behaviour via the VPN connection in case it has been hijacked.

The configuration of the VPN client on the remote PC is also essential. In particular, the risk of bridging between the Internet and the corporate network can be minimised by configuring the VPN to disable access to the Internet while connected to the corporate network. In this mode, while VPN is active, the PC's default route is to the VPN server at the office and the Internet is not visible. Similarly, communications services on the PC are not made available on the Internet.

4.5. Protect corporate resources from the remote PC

4.5.1. Monitor traffic and behaviour

VPN technology is a powerful tool to ensure integrity and confidentiality of data on the remote link. However, if the user's PC is compromised, then the VPN tunnel allows the cracker, posing as the authenticated user, direct access to the corporate information network, and may actually be effective in disguising the cracker's behaviour.

Hence, it is important that the VPN is terminated within a DMZ. The external firewall, facing the Internet, will authenticate and authorise the connection to the telecommuter's machine. However, data packets are encrypted within the VPN and hence the cracker's activities are disguised at this firewall.

Beyond the end of the VPN, network-based IDS should be deployed before the internal firewall in order to monitor the user's activity. This should watch for unusual or inappropriate behaviour, such as network activity outwith the user's typical working hours, uploading or downloading of large amounts of data, or the use of network scanning tools.

The use of SSL to access the corporate intranet over VPN should also be considered carefully. Since SSL is encrypted "end-to-end", it may be used to hide a cracker's activity. Hence, the use of web proxies should be considered. The proxy should be located within the DMZ, and the IDS should monitor the intranet traffic.

Also, the teleworker's network traffic should be scanned for viruses within the DMZ. This will help to protect the office network from any virus which may have slipped past the scanners on the remote PC.

4.5.2. Restrict remote service functionality at source

In some cases there is no better protection than to prevent access to a service or resource altogether.

For example, some corporate databases or internal applications may be considered too sensitive to risk any form of external access. Any such application or information should be carefully segregated from the remote access systems by appropriate use of access control and authorisation systems, network firewalls and IDS.

Some degree of control over the movement of data to and from the corporate network can also be provided by thin client technology such as Citrix WinFrame/Meta Frame or Microsoft Windows Terminal Server. Thin client technology allows the remote PC to act as an interactive "window" onto the corporate network, without providing direct access to the network. For example, applications such as word processors, spreadsheets, databases, and so on, can be run on the corporate server while making their user interface (text or GUI) available on the remote PC. The teleworker can see and interact with the application but all processing is performed on the office server, and the data files remain on the corporate network. In this way, the teleworker can access information and even create/update information without having access to download large amounts of data or upload malware. (Note that the thin client server must be configured correctly to ensure that files cannot be downloaded to the remote PC or uploaded to the server. Thin client servers generally provide the capacity for file transfer if required.) The protection provided is limited - files can be updated or contents entirely deleted, while macro viruses could be cut and pasted into a document. However, it does limit the damage that can be done in a given time.

4.5.3. Refuse remote access if necessary

Bear in mind that it may be necessary to completely refuse remote access. This may a blanket ban across the entire firm. Or simply a restriction on the job roles which may request remote access - eg., individuals handling cash transfers cannot use remote access, and so on. The key to making this decision, as ever, is to weigh the benefits of remote access against the perceived risks and impact.

References :

Survey on growth of telecommuting :

Langhoff, June. "Telecommuting surveys." 2001. URL :

http://www.langhoff.com/surveys.html (21 Aug. 2001)

SBC/Southwestern Bell survey on behavioural changes induced by always-on, high bandwidth connections :

Alfano, Pete. "Quicker Internet access with DSL becoming more popular." Foster's Daily Democratic Online. URL : http://www.fosters.com/special_sections/online/articles2001/0412c.htm (21 Aug. 2001)

Pastore, Michael. "DSL Users Diving into the Net." CyberAtlas online. 03 Apr 2001. URL : http://cyberatlas.internet.com/markets/broadband/article/0,,10099_732381,00.htm (22 Aug. 2001)

Zombies/IRC Bots :

Gibson, Steve. "Attacks Against GRC.COM." . Gibson Research Corporation web site. 04 Jul 2001. URL : http://grc.com/dos/grcdos.htm (21 Aug. 2001)

Sub7 Server Trojan :

Mobman. "Sub7." BWeb web site. URL - http://www.bsoft.swinternet.co.uk/trojans/sub7.htm#Functionality

Small Office/Home Office security :

Hirsch, Jessica L. "Telecommuting: Security Policies and Procedures for the "Work-From-Anywhere" Workforce." 13 Dec 2000. URL : http://www.sans.org/infosecFAQ/homeoffice/telecom.htm (17 Aug. 2001)

Zimmer, Kevin. "Protecting Your Company from the Small Office or Networked Home Office." 12 Feb 2001. URL : http://www.sans.org/infosecFAQ/homeoffice/protecting.htm (17 Aug. 2001)