Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security for a CRM environment

Customer Relationship Management software has been a buzzword in the Information Technology industry for quite a few years now. Many companies are looking at how CRM can help make them more successful by providing an extensive customer information database in which Sales, Marketing, Service, and other departments can use a variety of ways to better serve the customer. In today's competitive marketplace, good customer service is extremely important. There are many software vendors selling CRM software packages that offe...

Copyright SANS Institute
Author Retains Full Rights

AD

Streamline IT security environments and compliance processes.

Transforming IT Management.

Security for a CRM environment

Jason LaFrance

01/13/2003
GSEC Practical v1.4b

Abstract:

Customer **R**elationship **M**anagement software has been a buzzword in the Information Technology industry for quite a few years now. Many companies are looking at how CRM can help make them more successful by providing an extensive customer information database in which Sales, Marketing, Service, and other departments can use a variety of ways to better serve the customer. In today's competitive marketplace, good customer service is extremely important. There are many software vendors selling CRM software packages that offer a one-stop solution for gaining marketplace share, manage, and retain customer loyalty to their product. It is note worthy for companies to keep in mind that CRM deals with handling a company's most important resource: Customer Data.

This paper is designed to help the security professional determine the considerations that are involved with a secure CRM rollout. It will cover:

- Company procedure considerations for CRM.
- Policies that need to be in place: Privacy and Security.
- Security questions and answers for a CRM vendor and integrator.
- Technology that will to be secured in many CRM implementations.

What is CRM?:

There is no one definition that describes, "What is CRM?". This is because CRM has a different definition for every company. I would best explain CRM as a combination of processes, polices, and technology that is driven by business philosophy centered on the customer. A company that wants to implement CRM is attempting to fully satisfy, understand its current customer base, and attract more customers. By optimizing the business model the company hopes to make its relationship with the customer satisfying. This helps the company save money, and generate more revenue by understanding the customer demographic better. [16]

When you think about it you may realize that CRM has been around since the beginning of commerce. This could be compared to many years ago when the local butcher knew your name, what you might want when you walked in the door, and began using a new meat slice to cut the meat faster and to the thickness you want. [16] In the present we are interfacing with implementations of CRM technology when we go to buy merchandise off the Internet from companies like Amazon.com where they recommend items you might like based on past purchases. This may also be in the form of a sales agent that is able to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

know who is calling before they answer the phone. The agent would also know your order history because it is already on their screen.

CRM is a Process, not a Technology:

Stephen Horne from DMNews stated: "CRM is a process, not a Technology" [9] but this was only one of many quotes I found that made this statement during my research for this topic. I agree with this statement to some degree, but I also have observed that the process is now being driven by the Technology that makes CRM a combination of the two. The first step to successfully implement and secure a CRM environment is to look at the processes your company currently uses to manage and collect customer data.

When a company first decides to set aside a budget to start a CRM implementation, the first resources that should be allocated are key people within the company to investigate how current business processes are performed. The duty of these investigators is to look for inefficient and insecure ways that current processes are done. Also they look at present methods that could be enhanced or improved upon. Investigators should look for procedures and polices that users currently follow to perform their job. If the company is certified by a corporate standards organization such as International Organization for Standardization (ISO), there should already be policies and procedures in place. As a new CRM process is implemented, revision of these ISO documents is important to consider. Properly documenting the procedures is critical to marinating ISO certification.

It is possible that current processes put in place by the company can be insecure, and leave customer data exposed. Here are some common process related mistakes to exposing customer data.

- Not shredding customer documents with sensitive information.
- Insecure filing of customer data. (If hard copy is needed)
- Seizing of customer data from terminated employees.
- Unmonitored access to customer files within the company where many users may have access, or the general public are allowed.
    - Unlocked filing cabinets.
- Current customer database insecure.

Many companies have failed at CRM due to customer data being exposed, or profits not realized as expected. This is because the CRM implementation was modified to use their current processes instead of analyzing and improving the processes to work with CRM. [8] Here is an example of a process that is insecure and inefficient that CRM could help with if the process was optimized:

The customer leads come into the company via many different sources such as a Fax, phone, E-mail, Internet Web form, or postal mail. The current procedure is to print out all the contacts, and have an intern or part time employee enter them

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

into the current customer contact database. After the data entry is competed, and then the printed contacts are discarded in the recycling bin. There are several ways that this process could be changed so there is less exposure of customer data:

- All printed customer data shredded once entered.
- Reduce the number of possible customer data sources.
- Do not print out e-mails and web forms.

CRM could further help with securing these processes by allowing technology to help file this information:

- Automate web form collection directly into CRM.
- Build customized insertion of E-mail information into CRM.
- Integrate faxing with CRM to send and receive faxes.

During the deployment of the technology, it will not matter how much security is put in place to implement CRM, if like in the example the process is not investigated and planned out before CRM is rolled out to the company.

Policies:

Security Policy:
It is important that a company, regardless of the need for CRM, have a security policy in place to protect the business. If this security policy is not already in place, then steps should be taken to create a security policy before CRM is fully functional. If security policies are already in place for the company then it is important to review them to see if they are up to date. [11] This is also the time to evaluate how polices will change due to the CRM implementation. Investigate what levels of policy the CRM program affects, and modify those policies. New issue-specific and procedural policies should be created to cover the CRM application and its data.

An example of where there's a needed security policy is in the recent Identity Theft ring at Teledata Communications. A Helpdesk employee was given access to user's accounts and passwords that he used to distribute to a third-party for money. It was stated that policies were in place to prevent unauthorized employees from getting this access, but polices do not matter if they are not followed. [1]

Customer Privacy Policy:
Current policies regarding customer data, and privacy should be reviewed (assuming that there are policies in place). If there are no policies in place to protect customer data, then it is critical that a policy be created. These policies should not only be available to customers, but to every person that is employed in the company. [18] The privacy policy that is generated should accurately and honestly represent the way that the company handles its customer data. It is important to understand that a policy should protect the customer from undesired

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

invasion of privacy. It is also important that the company keeps in mind its intended customers and the privacy policy should reflect what that customer base is. For example, customers of a bank expect to have a very stringent privacy policy about what data the bank shares. A company such as an online job search firm might have fewer restrictions to their privacy policy. [12]

No matter how the privacy policy reads the customers that read it should be able to easily understand it. The company's privacy statement may be perfectly legal, but if the customers cannot not easily find it, or read it, then they may not understand what the agreement means. This may protect the company in court but will lose customers in the process. October 2002 the Federal Trade Commission listed some guidelines to writing an effective privacy policy [6]:

Notice language should be:

- Concise - simple and straightforward, not "jargoned up" or "dumbed down."
- Direct - using the word "you" to engage your reader.
- Affirmative - telling customers what is, rather than what isn't; what they should do, rather than what they shouldn't do.
- Active rather than passive.
- Respectful.
- If you must use technical terms, you can still help your reader understand them.
- Define the term in a text box close to its use.
  Include a glossary in the notice.
- On your website, hyperlink the term to a definition or use a simpler term or phrase in the text and link to the technical term.
- Highlight your company's contact information clearly and conspicuously.

In addition to the suggestions above I feel that a privacy policy…

- Be made widely available, and easy to find to every customer and employee.
- Provide methods the company uses to protect customer information.
- Provide a provision to protect data if the company is sold or goes bankrupt, or clearly explain what does happen to customer data.

A company that does not follow its privacy policy risks losing those customers who are affected by the violation. If a violation of customer privacy happens a lot, or to a large number of people, then the company will run the risk of being publicly known for this violation. Which in turn they loose credibility, and damage their reputation. Legal action against the company could very likely result from a violation of customer privacy.

The now closed Toysmart is one company that was sued and blocked from selling its customer list when it wanted to sell off the company. Its privacy policy

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

had a statement that promised users no customer data that was collected would ever be transferred, or reveled for any reason. Due to this provision Toysmart was only able to sell it's data to a company willing to hold the same policy as Toysmart had. Because of this, many online retailers changed their policy to include statements that would allow customer data to be transferred if acquired or sold. [4]

An example of the privacy policy listed on the Federal Trade Commissions website is listed at the end. This example provides an excellent illustration of their suggestions for an effective privacy policy.

Technology and Security related to CRM:

CRM packages that are developed by software companies are designed to be one-stop solutions to managing all the customer data for a company, and present the data back to the employee or customer that needs it. These products generally have a base product for CRM, and then provide add-on features that can be incorporated into other parts of the business. For example, a company may purchase a CRM package initially for Marketing and Sales to handle collecting customer contact data, literature distribution, and customer leads. Later they can add on functionality for a customer to access extranet sites to view order information, invoices, and sales history. Some packages even have Helpdesk packages for customers and employees to track product problems, provide knowledge base, and online support.

These are the types of technologies that go into supporting CRM Packages:

- Database Servers to store customer data.
- Web Servers to present data to internal employees, Sales representatives, Field Service Technicians, and customers.
- CRM Application.
- Web Browsers
- Wireless devices such as Cell phones, Laptops and PDA's.

As can be seen from the technologies listed above there are many different fronts to secure on a CRM package. The reason this is such a big issue is because many of the businesses that are now looking into CRM are small to medium businesses. These size businesses may not have the technologies in place, and will need them to work with CRM. They will quickly have to implement the technology, and learn how to secure it. This may cause the implementation of security to be an afterthought to getting the system up and running. Small to medium size companies usually have a smaller IT department that might not have the time to properly install and monitor these new services. Small businesses also have to keep in mind which technology the vendors they are looking to implement fits with their current environment. If a company were mainly using Microsoft Windows as their desktop and server operating system it would be more advantageous for them to pick a vendor that fully supports this

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

environment. The reason behind this is the current IT staff will hopefully have a good understanding on how the Microsoft environment works, and will have default security practices in place. Bringing in a Unix server to run an Oracle database or Apache web services might force a strained IT department to learn how to secure an unfamiliar technology. This could cause important security issues to be missed.

Microsoft Software:
In my research of smaller CRM companies that target small to medium businesses tend to use a limited number of platforms to run the Web, Database, and other systems. Every vendor in the small and medium business range support Microsoft; Windows 2000 for the operating system, Internet Information Server for the web server, SQL 7.0 or 2000 for the database, and Outlook for the e-mail client to drive their CRM package. For many companies this may not be an issue, because they are already working to protect these systems. It's the companies that have standardized on non Microsoft products such as Eudora mail client or Apache web servers that are going to be forced to switch over to these programs, and are going to need to learn about how to secure them.

The reason for this issue is because each of these products that are required to run CRM has major security vulnerabilities that need to be patched, and setup properly so they are secure. Here are a few reasons why for each product:

Windows 2000 – It is important to secure the CRM program by first securing the operating system the CRM application will be installed on. Administrators should consult the Microsoft security checklist for Windows 2000 server and SANS best practices for securing a Windows 2000 Server before CRM should be installed. [13] The Administrator should evaluate any risk that is introduced due to settings that cannot be applied due to the CRM requirements.

Outlook – Almost every new virus that has been released in the past few years take advantage of vulnerabilities in the Outlook code that allows the virus to automatically send out messages and access. Outlook relies heavily on Internet Explorer, and can affect Outlook security such as Microsoft Security Patch MS01-020. [14]

Internet **I**nformation **S**erver 5 (IIS5) – This web server application installed by default is considered very insecure. Viruses such as Code Red and Nimda have targeted this software. CRM administrators should have the time to learn how to administer, backup, and restore IIS. Following security best practices for IIS5 from Microsoft's website [11] and SANS Internet Information Server course are key to limiting vulnerabilities in IIS. [17] Administrators should also keep up to date on all new Microsoft vulnerabilities that are released for IIS.

Microsoft SQL Server - Has been the target of viruses such as SQLworm and JS/SQLSpida.a.worm that take advantage of open 1433 ports to the Internet.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[15] Also at the time of this writing the SQL port 1433 was the third most scanned port world wide as reported by Dshield.org. [5]

For all Microsoft products it is important to keep up to date on all new security patches and Service Pack that are released. It is also important to consider a non-production server to test patches and Service Packs before installing them to a production server to determine if there might be issues. A known good backup is also critical incase there are problems requiring a restore.

Wireless:
Many CRM companies are offering wireless solutions to access customer data out of their CRM package. These offerings come in the form of accessing data from a Laptop, PDA, and cell phones. Since wireless has been under fire about providing secure access to data, it's important for a company to carefully weigh the cost of using wireless vs. security. Since every company may have different requirements about what type of data their remote sales reps., and customers may want to view. It's important to answer these questions when considering the use of wireless devices in the CRM environment:

- What type of data is being transferred?
- What security protocols can be used to wirelessly access the data in the CRM software?
- Who is the intended audience?

Every CRM implementation now allows for Web and wireless access portals for both customers and employees. If a direct wireless access into a CRM package is preferred, then a company may want to only allow very little data fields that can be transferred. Only using a **W**ired **E**quivalent **P**rivacy security implementation the company would only want to limit transferred data that they would not care if others saw or knew about. Credit card numbers, possible lead information, and quotes could be vulnerable to theft or unwanted modification. Use of VPN with to access the network, or SSL via a web portal would be a more secure way to access the data.

Personal Firewall:
Another important security measure to consider for the remote user is a personal firewall to protect their computer and connection into the corporate network. Many remote users now work out of their Home/home office, and subscribe to a broadband service. Remote users are also quite often allowed to connect to client's networks. Whether it is for a field service tech attempting to access CRM, or other Internet resources, or for sales reps. to submit quotes, then without a personal firewall these mobile devices are constantly open for attack. It is also just as important that the user understands what the firewall does, and how to use it to protect the data on their devices.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Vendor Research:

When completing the **R**equest **F**or **P**roposal (RFP) to evaluate different vendors for CRM, it is important to include some or all of these questions below. This will help a company wanting CRM to plan any changes, and get training for any of the network infrastructure changes that are needed. Answers to these questions will help define how vendors consider security.

What to research in CRM vendors for security:
Question: Is there supporting technology requirements of the database, Web and other products diversified?
Reason: Try to select a vendor that uses the technology you currently use to support their software, or select one your current staff has knowledge of. Otherwise make sure at least one member is qualified to maintain, backup, and secure this technology.
Question: How closely does the company work with supporting vendors?
Reason: If the CRM vendor you choose does not have good support from the underlying technology you could lead to vendors debating on a "Who is to blame situation". This could affect the reliability and availability of the CRM package while the IT department is sorting out who, or what is at fault.
Question: How quickly do they qualify patches to underlying systems?
Reason: There are frequent patches to Database and Web Servers. It is important to find out how quickly a CRM vendor will test to see if the CRM package works with these new patches. It is also important to test patches on a test server before installing them in the production environment.
Question: How often do they release Service Packs and fixes?
Reason: Does the vendor release Service Packs or patches quickly after a known venerability is released for their product? Find out if they offer Service Level Agreements (SLA) for producing patches and releasing them.
Question: What vulnerabilities have been found in the past? How many have been found?
Reason: It would be good to know if one vendor has reported a lot of vulnerabilities in their code. This may indicate that their product may not have been developed as well as others products. This can be misleading though. Market share may also plays a factor in this since Hackers usually go after the biggest install base to exploit a larger number of installations if venerability is found. A recommended practice is to search through sites that report on security vulnerabilities such as Carnegie-Mellon's Computer Emergency Response Team (CERT), and Securityfocus.com BUGTRAQ forum. [3]
Question: What are the support options, and what type of support does it handle?
Reason: Depending on your Risk assessment, it is recommended to find out what levels of support your CRM package allows. Do any of these support levels help with security incident handling and response? How quickly can they help is the system has been compromised? This is especially important in the initial

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

implementation and function since the vendor will have a lot more knowledge about the software than the IT staff.
Question: Do they publish security recommendations (Checklists) for their products?
Reason: This is a good indication if the vendor is considering security in the software. Find out if recommendations are also provided for the underlying software products as well.
Question: What kind of training is offered?
Reason: Training will help IT staff get up to speed on the new software and reduce the learning curve of supporting the software. This will allow more time for staff to audit the system for problems and intrusions.
Question: Is there Local Support?
Reason: Even with the growing popularity of remote access software like PCAnywhere, it still advantageous to identify if one vendor has a local support person to help in emergencies. If the vendor does not have a local source, then look for other local support centers that have knowledge to support the CRM package.
Question: What are their references?
Reason: This could be important in finding out how other companies are satisfied with their CRM package. Ask about how their security implementation went, and was there a focus on security. If they did not focus on security, then this could mean that the vendor does not take security seriously in their implementations. Question the vendor about its security focus. The vendor should be just as serious about security as the company implementing CRM.

CRM Integrators:
Vendors that sell CRM solutions are not necessarily the same company that will implement the software on-site. While many CRM vendors do have staff that will help implement their product, they may not have staff available in the time frame the company wants to implement the software. What happens then is the vendor provides a list of CRM integrators to do the deployment and configuration of the product. Many of the same questions posed for the vendor itself should be applied to the choices of integrators to see which one fit the best. In addition to the list above these considerations should be investigated also.

- Will the vendor of your CRM provide at least one member from it staff? This will help ensure that solutions define in the Request for Proposal while choosing a vendor is implemented.
- Is the Integrator prone to do the work quickly in lieu of implementing the product correctly? This can cause problems and leave security and operational issues. Talk to references to find out how satisfied customers were with the Integrators. Suggest that the references come from the CRM vendor and not the Integrator.
- Look for an integrator that has done installations similar to the nature of your business. Since different industries have different business and security models an integrator that mainly does implementations for manufacturing firms, may not be familiar with a Medical industry

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

implementation, and may miss important steps to implement the product securely. [2]

The ASP option:
Another option to implement CRM (And other services) is having an outside vendor host the CRM package called an **A**pplication **S**ervice **P**rovider. (ASP) This generally involves a high-speed WAN link, such as a T1, to link between you and the third party site. Users access, and update the data on the ASP's site. The ASP is responsible for taking care of the security, reliability, availability, and backup of the data. It is likely that security of the data on the ASP will be better than the company that needs hosting can provide. This is because the ASP will be hosting other sites as well, and making sure that the data from various companies are kept separate is essential to keep the clients trust. The ASP allows a quick and lower initial up front cost to implementing a CRM package. The ASP already has the infrastructure in place and usually gives Service Level Agreements to guarantee uptime of their systems.

There are drawbacks to this environment however.

- Even though ASP's may have very good SLA, the hosted site is still at the mercy of the facility that manages the connection between the two sites. Make sure that there are SLA or redundant diverse data paths to the ASP for failover. This may add quite a bit to the cost of the implementation.
- The link between the two companies is also venerable to Distributed Denial of Service attacks. If a Hacker knows this connection is critical to business function it may be easy to block data going between the two sites.
- An ASP is a business, is subject to hard times, and might go out of business. It is important to understand what might happen to data in the event the ASP is no longer host of your data. There should be a plan to continue working with that CRM system. The hosted company should make sure the contract says that all data remains the property of the hosted site.
- Integration between the CRM and other business applications may be harder, or impossible to integrate due to the location of the data. Flexibility or policy of the ASP can also hinder integration.

Finally if an ASP is going to be a choice for setting up the CRM environment, then suggest that the company give a tour of their facilities. The ASP should be able to prove to you that they are securing your data. They might not be able to show the whole plant to you for security reasons, but if they were not willing to allow tours on-site, it would be a warning sign of possible issues.

Summary:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

With all the potential customers a company has to reach it is easy to see that CRM allows a better way to manage, reach a companies desired customers, and provide the customer with the products and information they need. Making sure the company secures that data is very important. A company that allows entrusted customer data to be exposed or stolen, or the customer to be misleading, endangers the company by losing the customer they rely on. CRM can help secure this data as long as policies and processes are solidified, and data that is handled is transferred security to every employee, customer and device. At the time of this writing there were not many reports about security vulnerabilities about the specific CRM packages themselves. This may be due to the infancy the software is still in. Attackers may find it easier to exploit the vulnerabilities already known about in the widely distributed database and web server software, rather than the CRM software. If the CRM install base continues to grow, attackers may find it worthwhile to find security vulnerabilities in the CRM code.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References:

[1] Berger, Matt. "Feds crack huge identity theft ring." 26 Nov 2002. URL: http://computerworld.com/securitytopics/security/story/0,10801,76227,00.html (26 Nov 2002).

[2] Clark, Sam. "How good is your CRM systems Integrator?" 09 Jan 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2833576-2,00.html (23 Nov 2002).

[3] Davidson, Mary Ann. "With Security, you get what you pay for." 14 March 2002. URL: http://zdnet.com.com/2100-1107-859767.html (17 Nov 2002).

[4] Dillion, James, Mary Hilderand and Jacqueline Klosek. "Minimize the Risks of Privacy Violations When Operating E-Commerce Web Sites." New Jersey Journal. 16 Sept 2002. URL: http://www.goodwinprocter.com/publications/dillon_hildebrand_klosek_09_16_02.pdf (23 Nov 2002).

[5] Dshield. "Distributed Intrusion Detection System." URL: http://www.dshield.org (16 Nov 2002).

[6] "GETTING NOTICED: Writing Effective Financial Privacy Notices." Oct 2002. URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/getnoticed.htm (16 Nov 2002).

[7] Greenberg, Paul. CRM at the Speed of Light, Second Edition. Berkeley: McGraw-Hill/Osborne, 2002. 333-349.

[8] Hershey, Linda. "Why CRM Implementations Fail. What Part Don't You Understand?" http://www.realmarket.com/required/lghcons1.pdf (23 Nov 2002).

[9] Horne, Stephen. "CRM is a Process, not a Technology." 19 Nov 2001. URL: http://www.analytici.com/images/pdf/DMNews.pdf (11 Nov 2002).

[10] Howard, Michael. "Microsoft Internet Information Services 5 Checklist." 29 June 2000. URL: www.microsoft.com/technet/prodtechnol/iis/tips/iis5chk.asp (26 Nov 2002).

[11] Hunter, Glenn. "Essential CRM Knowledge: understanding security issues." 06 Feb 2001. URL: http://searchsecurity.techtarget.com/webcastsTranscript/0,289691,sid14_gci516630,00.html (15 Nov 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[12] Mello, Adrian. "Dangerous games with customer data." 24 July 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2875371,00.html (15 Nov 2002).

[13] Microsoft. "Window 2000 Server Baseline Security Checklist." 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp (7 Dec 2002).

[14] Microsoft Security Bulletin (MS01-020). "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment." 29 Mar 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp (7 Dec 2002).

[15] Network Associates. "Virus Information Library." 22 May 2002. URL: http://vil.nai.com/vil/content/v_99500.htm (7 Dec 2002).

[16] Pantazopoulos, Aris. "What's Really CRM." URL: www.crm2day.com/what_is_crm (15 Nov 2002).

[17] SANS Security Essentials IV. "Internet Information Server (IIS5) Security." Sans Institute. 2001. Section 10.5.7.

[18] Scheier, Robert. "CRM Privacy Management: How you can help." 16 April 2002. URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci817322,00.html (15 Nov 2002).

Additional References:

Privacy Council: http://www.privacycouncil.com
SearchCRM: http://searchcrm.techtarget.com
CRMcommunity: http://www.crmcommunity.com
Destinationcrm: http://www.destinationcrm.com
ITWorld: http://www.itworld.com
Frontrange: www.frontrange.com
Saleslogix: www.saleslogix.com
Peoplesoft: www.peoplesoft.com
Amazon: www.Amazon.com
Dshield: www.dshield.org
Network Associates: www.nai.com
Microsoft Security Homepage: http://www.microsoft.com/security/

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Example privacy policy from the Federal Trade Commission
(http://www.ftc.gov/ftc/privacy.htm)

Privacy Policy

This is how we handle information we learn about you from your visit to our website. The information we receive depends on what you do when you visit our site.

If you visit our site to browse, or to read or download information like consumer brochures or press releases:

> We collect and store: the name of the domain and host from which you access the Internet (for example, aol.com or princeton.edu); the Internet protocol (IP) address of the computer you are using; the browser software you use and your operating system; the date and time you access our site; and the Internet address of the website from which you linked directly to our site.
>
> We use this information to measure the number of visitors to the different sections of our site, and to help us make our site more useful. Generally, we delete this information after one year.
>
> We do *not* use "**cookies**" on this site.

If you choose to identify yourself by sending us an email or when using our secure online forms (e.g., Bureau of Consumer Protection, Project Know Fraud, or Identity Theft complaint forms, or our FOIA Request Form):

> We use personally-identifying information from consumers in various ways to further our consumer protection and competition activities. We collect this information under the authority of the Federal Trade Commission Act and other laws we enforce or administer. We may enter the information you send into our database to make it available to our attorneys and investigators involved in law enforcement. We also may share it with a wide variety of other government agencies enforcing consumer protection, competition, and other laws. If you contact us because you have been the victim of ***Identity Theft***, we also may share some information you provide with certain private entities, such as credit bureaus and any companies you may have complained about, if we believe that doing so might help resolve identify theft-related problems. In addition, when you submit a complaint, you may be contacted by the FTC or any of the agencies or private entities to whom your complaint has been referred.
> If you contact us to order publications, we will use your information only to fulfill

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

your order or to contact you about your order.

In other limited circumstances, including requests from Congress, **Freedom of Information Act** **(FOIA)** requests from private individuals, or in accordance with **our public record rules**, we may be required by law to disclose the information you submit. If you use one of our online forms, the information you provide is up to you. If you don't provide your name or other information, it may be impossible for us to refer, respond to, or investigate your complaint or request.

If you want to get information about you that may be in our records:

The Freedom of Information Act and the Privacy Act of 1974 provide you certain rights to get information about you that is in our records. To learn more about the circumstances under which you can get and correct this information, visit our **Freedom of Information Act** page.

Here's what you should know about the security of the information you provide to us:

We use secure socket layer (SSL) encryption to protect the transmission of information you submit to us when you use our secure online forms. All the information you provide us through these forms is stored securely offline.

If you send us an email, you should know that email is not necessarily secure against interception. So, if your communication includes sensitive information like your bank account, charge card, or social security number, and you prefer not to use one of our secure online complaint forms, contact us by **postal mail** or **telephone** rather than email.

Here's how to contact us about:

- **consumer fraud, misleading advertising, credit cards, or other consumer protection matters**
- **identity theft**
- **antitrust or competition matters**

You also may contact us by **postal mail** or **telephone**. If you do so, we may use the information you provide in the ways we have described in this privacy policy.

If you experience technical problems with the operation of this website, contact our **Webmaster**.

This website links to documents located on websites maintained by various federal agencies or other organizations. Once you access an individual document that links you to another website, you are subject to the privacy policy of the website containing that document

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Cookie

A "cookie"is a small text file that a website can place on your computer's hard drive in order, for example, to collect information about your activities on the site or to make it possible for you to use an online "shopping cart" to keep track of items you wish to purchase. The cookie transmits this information back to the Web site's computer which, generally speaking, is the only computer that can read it. Most consumers do not know that "cookies" are being placed on their computers when they visit websites. If you want to know when this happens, or to prevent it from happening, you can set your browser to warn you when a website attempts to place a "cookie" on your computer. [Back to Privacy Policy]

:

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**