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.

Using Security To Protect The Privacy of Customer Information

Advancements in information technology have driven the information security discipline to the forefront in the quest to protect customer data. Protecting this customer data is one of the many aspects of privacy addressed in the SANS Security Essentials curriculum. Although the concepts of governmental privacy regulation and an organization's privacy policy were discussed in that curriculum, this document will tie these together. In addition, it will focus on how these influence the design of an organization's informati...

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia
Stay Secure

Alan Pacocha
SANS Security Essentials GSEC Practical Assignment
Version 1.2f

Using Security To Protect The Privacy of Customer Information

Advancements in information technology have driven the information security discipline to the forefront in the quest to protect customer data. Protecting this customer data is one of the many aspects of privacy addressed in the SANS Security Essentials curriculum. Although the concepts of governmental privacy regulation and an organization's privacy policy were discussed in this curriculum, this document will tie these together. In addition, it will focus on how these influence the design of an organization's information security, as well as organizational infrastructure. Sound privacy policy for an organization must be supported by the appropriate information security infrastructure. It is obvious, that as the Internet has blossomed into a means to offer products or services, it has also increased the various risks to organizations collecting and storing confidential customer data. There is also increased pressure to ensure security infrastructures, both technical and organizational, are equipped to protect this customer data once collected. Currently, one of the highest priorities among organizations is customer data confidentiality, due to government regulations and customer demand. An organization's reputation could be ruined if violations are found which contradict government regulation or its own privacy policy. Information security is the discipline which enables organizations to operate responsibly under these and future privacy requirements.

Why Security & Privacy?

Although the Internet provides convenience to millions of people each day, it is also one of the easiest ways for organizations to collect personal data about their customers. In addition to the Internet, organizations continue to collect this customer data through conventional methods such as using software applications or mailings.

Customers have spoken out, and governments have listened, regarding how organizations hold this information, or in some cases not hold this information. In response, federal and state governments have passed privacy laws protecting personal information from disclosure, transfer, sale, or other means of transmission not authorized by the customer to third parties. Third parties can include other organizations, persons, or other entities.

To comply with these laws, organizations must have information security (IS) and organizational infrastructures in place to protect customer information. In addition, customers must be able to clearly understand an organization's position in regards to protecting this information. As a result, privacy policy has recently been adopted as the standard tool to communicate this intent to customers.

To be effective, a privacy policy must ultimately create trust and confidence with the customer while ensuring their data is protected. The policy must be clear, concise, and lawful, yet limit legal jargon and express the best interest of its customers. Furthermore, it must be easy for the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

customer to obtain and clearly state the customer's choice in how their information is shared or not shared. It must also clearly explain those situations in which the sharing of information is necessary for the product or service. Examples of these situations would be legitimate analysis or research either internally or via prior agreement with a third party.

Generally speaking, customers are not confident organizations consider their best interests in regards to protecting their personal and sensitive information. Customers are afraid of the fact they do not know what organizations know about them. Meanwhile, organizations spanning across various industries, continue to share information about their customers. This sharing decreases customer confidence in areas such as shopping on the Internet and increases the risk of litigation to an organization.[38] It also raises the debate over which pieces of information are public and which are personal. The important point is identifying all personally identifiable information, and then limiting access on a need-to-know basis.[16]

Safely and responsibly protecting customer data, whether collected via an on-line method (Internet) or off-line method (paper applications) can be a competitive edge for an organization by increasing customer trust.[24] However, organizations must appropriately associate and integrate the level of privacy of its customers with the products or services it offers. In general, organizations must place a high priority on bolstering customer confidence by providing the customer with the policies and tools to protect their privacy. IS couples policy and technology to protect customer data.

The Legal Environment

Before an IS solution can be implemented, an organization must understand the legal environment and its connection with its privacy policy. The terms opt-in and opt-out have significant importance with this environment. Opt-in is the authorization a customer gives to allow the sharing of their data.[3] Conversely, opt-out is the instruction from a customer to not share their data.[3] Currently, there are two pieces of federal legislation which affect the transmission and storage of electronic data and its relation to customer privacy, the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

GLBA regulates almost all financial institutions including banking, insurance, and securities firms and covers four main aspects. First, organizations must maintain policies to protect the security and confidentiality of nonpublic information. Second, organizations are prohibited from sharing account information with non-affiliated third parties for marketing purposes. Third, it allows customers to opt-out of sharing personal information. Fourth, it requires organizations to disclose their privacy policy annually to customers.[40] Simplistically, GLBA makes organizations look at their data, the internal handling of it, how they were protecting it, and establish monitoring of it.[12]

HIPAA regulates the electronic storage and transmission of health-care related data. It is estimated HIPAA will be not only be financially exhausting, but time consuming for organizations to implement due to its breadth of restrictions.[31] However, it is expected HIPAA will provide a technical blueprint for the healthcare industry which has been needed for some

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

time. Legislators have only delivered a proposed draft of the security portion of HIPAA, therefore final details will be forthcoming.

Will organizations continue to wait for federal and state governments to dictate privacy policy and the technical details with which to implement it? The answer for now appears to be yes. However, some industries wish to self-regulate themselves.[24] In doing so, they feel they will have more latitude in applying technical solutions as regulation to date primarily speaks in general terms on what kinds of protection to place on it.[16] Another growing movement is for governments to set privacy policy for all industries.[23] Critics of this movement think it would be impossible, but agree some high-level policy may work.

There is pending federal legislation, backed by customer demand, which will have broader implications to organizations focusing on online as well offline practices.[34] This will affect an increased number of organizations. Some organizations are actually welcoming this new regulation because it will set detailed privacy and security standards rather than current regulation which is primarily interpreted. Additionally, it will attempt to prevent state privacy differences, but still allow customers to specifically reject their information from being shared.[32]

Other aspects to the legal environment include the fact state governments have and will continue to pass legislation which can be equal to or exceed the restrictions set forth in federal legislation. Where this is the case, the stronger regulation will take precedence. Organizations have asked governments to limit their privacy regulation primarily because it doesn't address details such as how to protect it. These regulations vary drastically from state-to-state and are allowed under existing regulation such as GLBA.[12,26] If state regulations are allowed to pass and continue, it is expected a chaotic situation will be created. Furthermore, these additional state regulations will force organizations to spend more money and in some cases, be forced to change their business model to comply.[26] To date, over a dozen states are in the process of writing their own privacy regulations.

U.S.–based organizations, not affected by GLBA or HIPAA, operating in Europe and Canada need to assess the impact of broader and stricter regulations than those in the United States. The European Union's privacy regulations are considered the most demanding. However, because of the high trade volume between the U.S. and Canada, Canada has the opportunity to affect more organizations.[28] U.S. organizations are known to be still trying to comply with these various sets of requirements.[28] In contrast, Canadian and European organizations have adapted some what faster due to looking at the concept earlier.

Implementation of the Canadian law is in two parts. The first part, effective January 2002, affects certain industries within Canada such as financial institutions, telephone companies, airlines, and railways. The second part, effective 2004, will cover any organization doing commercial business where personally identifiable information is collected.[22,28] Controversial issues have already surfaced such as protection of customers depending where they transacting business, whether Canadian organizations will now have a competitive edge over U.S. organizations, and the vagueness on the definition of a privacy violation.[22]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Organizational Infrastructure

Once an organization has the legal framework and a privacy policy established, it should review its organizational infrastructure. Organizational infrastructure encompasses personnel, their responsibilities, and their authority. Often this infrastructure is as important as the IS infrastructure because the two complement each other. Competent persons must be in the appropriate positions to guide sound privacy policy for an organization to mitigate risk.

Recently, an increased number of organizations have named Chief Privacy Officers (CPO) to head their privacy efforts. Sometimes they are also referred to as a Privacy Officer, Privacy Director, or Privacy Manager. This position is the focal point of the organization in regards to privacy and may have high to low duties assigned to it.[7] This focal point gives the customer the perception an organization takes privacy very seriously and reinforces the confidence sensitive data will be protected.[15] It also shows commitment from senior management and a further willingness to make privacy a part of the organization. In addition, it is recommended this position not have other responsibilities which would distract and draw attention away from the privacy effort.[15]

A CPO, or other type position, has been found to be a creative mix of talents. This individual usually works with several areas, and depending on organization size will have reporting responsibility to several people but must be tightly integrated with information technology.[15] This position should have the authority to make decisions regarding an organization's privacy effort. Another aspect of the position provides guidance to various areas in the organization regarding the privacy policy and the affects on their data. Establishing this relationship promotes the customer focus component of privacy between areas of the organization. Unfortunately, in some organizations this customer focus is diminished because the CPO is viewed negatively as it does not directly produce income.[15]

An organization's culture should be sensitive to and follow its privacy policy.[5] Educating an organization's employees about privacy and its affects are one of the most important steps to creating this sensitivity.[17] This education can be provided via electronic or paper methods, but must be consistent and focused to ensure all employees are compliant with an organization's privacy policy. As with any IS awareness program, sound privacy policy for an organization must be effectively communicated to its employees.[24] This awareness, as previously mentioned, extends to an organization's customers as well, usually through the delivery of the privacy policy.

An organization could create privacy policy, including finding credible business reasons why, and make organizational infrastructure changes, but not have the most important aspect of information technology to support it, information security. Privacy is dependent on sound IS principles and methods. Consequently, in order to have strong privacy you must have IS. IS should therefore be tightly integrated with the rest of the organization. IS departments should provide the highest level of service to gain the trust of the organization. Furthermore, executive support is crucial for the overall support of an organization's IS program.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Information Security Infrastructure

When considering an organization's IS infrastructure and it's enabling of a privacy policy, there are several issues to address. First, an organization's security policy should outline hardware, software, and other protective measures. Second, this policy should also ultimately support the core organizational functions. Third, security policy should be reviewed periodically to ensure it still supports the organization and the organization's security strategy.

Technology has made access to data easier than ever before. Mapping data flow through an organization is one quick way to identify the major components such as how the data is collected, transported, at what point it will be accessed and how it is stored. Its sensitivity level should also be defined through a formal data classification methodology.[13] An organization may choose to address certain aspects of this data flow specifically in their privacy policy such as databases and online transactions. It is important this data flow be accurately documented for later reference. From the data flow documentation, additional security issues should be identified. These aspects should also be reviewed against existing security policy for compliance. In addition, internal data may flow to third party points.[14] Consequently, third party access to data should also be addressed in the security policy giving detailed instruction.

Data mapping involves identifying who has access to the data and establishing role-based security. For organizations who have yet to identify roles, this can be a huge task to undertake. However, the organization should take it seriously to limit users on a need-to-know basis. The organization and IS should work together to develop a process to identify users. This process can then be used in a centralized security administration environment.[16]

An organization should analyze current technologies being employed to protect their sensitive data as newer technologies may need to be implemented. For example, whether a legacy system could be retrofitted or not. If not, the decision to implement a newer technology would need to be made. Another example surrounds the debate with wireless technologies and their impact to customer privacy. An organization needs to research wireless and its affects on privacy thoroughly as there are currently several IS issues surrounding its use. If a technology will have a significant IS impact to an organization, the privacy policy may want to address it specifically. Investment in newer technologies, such as going to a common platform, will payoff in the long run supporting the organization's privacy policy more effectively. These IS technology changes should be identified early so they are built into the design phase of any existing or future projects.[14]

The IS technologies used in the infrastructure may be dependent upon the industry with which an organization is associated. Consequently, an organization must have IS technologies which are adaptable to policy change, regulation change, or new privacy vulnerabilities. In addition, an organization may closely track direct customer feedback and make changes to the IS infrastructure.

For organizations in multiple states, their information security infrastructures must be equipped to handle these state-to-state variances in requirements. Organizations must establish on-going dialogue between their legal/business areas and IS to stay abreast of these ever changing state

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

requirements. Organizations with large and diverse data repositories must be flexible enough to adapt to this change. The key to this flexibility is to what degree their systems are integrated together.[26]

As mentioned, the customer is the focus of any privacy policy and the IS infrastructure should reflect this. Customer conveniences need to be considered in conjunction with privacy policy within the IS infrastructure such as the opportunity to update or delete their sensitive information.[20,21] The infrastructure should also be able to support policy regarding customer privacy disputes. Some organizations also use cookies to collect information about customers when surfing their own or others web sites on the Internet. As a result, organizations should disclose their policy regarding the use of cookies within their IS infrastructure. Another way to strengthen privacy, is for organizations to consider other methods of customer identification such as id numbers to offer anonymity. For example, issue identification numbers rather than use Social Security numbers to reference an account.

Organizations can promote new tools on the market to protect customer privacy such as the Platform for Privacy Preferences (P3P) framework. P3P is relatively new and is a step towards increased communication between customers and web site operators.[10] It essentially gives the customers a chance to communicate their intent on how they want their information treated.[9] When the customer goes to a web site, the web site reads and abides by the customer preferences set. Although it appears to be an effective tool, both the customer preferences must be set and the organization's web site must be equipped to handle P3P. The intent of this technology is to give the customer the opportunity to select their own level of privacy.

Other IS methods should also be addressed such as implementing or revising audit processes and policy. Auditing is closely related to data flow and the monitoring of compliance within the IS infrastructure enforcing privacy policy and reporting upon any violations. Using data encryption methods for safe transmission and storage along with firewall technology to restrict access to networks must also be considered. Furthermore, reviewing authorization to systems in which the sensitive customer data resides is important as well.

Regulation Enforcement

With all these regulations to account for, one of the concerns organizations face is enforcement. Currently, federal and state governments are using existing laws on unfair and deceptive business practices to take organizations to court for not following their own privacy policies.[18,27] Ironically, some organizations have argued not displaying a privacy policy limits their liability.[10] Essentially, you can't be liable if you don't have a policy.[18] However, this approach is counterproductive to the fact presented earlier stating organizations who show privacy policies may gain a competitive advantage. Ethical organizations are voluntarily displaying policies because customers demand them.[18] By doing this, is enforcement really driving the need for privacy?[27]

The security and privacy communities have also noticed the Presidential administration's impact on enforcement. One arm of the federal government, The Federal Trade Commission (FTC) is active, but is only really going after organizations on an as-needed-basis and staying clear of any

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

state legislation. To illustrate, the Clinton administration was focused on how organizations collected data, versus the Bush administration which is focusing on the misuse of data.[27] With this said, some question whether the lawmakers will work on pending privacy legislation which is weak in financial or criminal punishment.[18,25] Also, the trend is to include all types of data whether collected online or offline and to span across all industries, not just financial and health care.[29] The events of September 11th have also shifted priorities away from privacy to now high priority critical infrastructure efforts.[33] As a result, some argue enforcement of current regulations may have a larger affect on organizations than new legislation.[27]

If an organization were to be investigated, the FTC has indicated it understands breaches will occur.[37] However, they will ask if there was a system with procedures in place for the data and if the procedures were followed.[27] Some have argued privacy regulation is too vague, opening it up to interpretation which leads to unknown risks.[27] Lawsuits have had a difficult time so far showing damages from privacy violations.[27] One reason is customers may not remember what they agreed to under privacy policies from numerous organizations.[18] In those cases where settlements were reached, changes to privacy practices and organizational practices seem very common. However, more governmental and private litigation is to come with health care and financial regulation leading the way.[27]

The Outlook On Security & Privacy

The events of September 11th have changed views of how privacy should be dealt with. Privacy is not and cannot be an absolute right.[37] Freedom can suffer in the name of safety. Consequently, there has been a shift towards security recently, rather than privacy which has worried some. Organizations have become more receptive in sharing security issues with government and one another. An example of this would be corporate security incident where data is voluntarily shared with the government.[33]

Protecting sensitive customer data once collected is critical to the success of an organization. A sound privacy policy enforced using information security technologies and a complementing organizational infrastructure not only supports customer focus and governmental compliance, but possibly a competitive edge. Education of an organization's employees is also a contributing factor to success. Furthermore, as new information security technologies are created, organizations need to assess their impact on privacy policy. Information security enables organizations to operate responsibly with sensitive customer data. However, it is the responsibility of an organization to embrace it as part of their business and infrastructure. Likewise, it is the responsibility of the customer to make organizations responsible for their posted privacy policies.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References

[1] Berman, Jerry & Mulligan, Deirdre. "Privacy In The Digital Age: Work In Progress." Nova Law Review. 1999 Winter. URL: http://www.cdt.org/publications/lawreview/1999nova.shtml

[2] Dash, Julekha & Thibodeau, Patrick. "Medical Privacy Rules Take Effect, But Changes Could Follow." Computerworld. 16 Apr 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59642,00.html

[3] Gillmor, Dan. "Gramm-Leach's Privacy Problem." Computerworld. 23 Jul 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO62385,00.html

[4] Hamblen, Matt. "Ensuring Portable Privacy." Computerworld. 11 Dec 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO54794,00.html

[5] Harrison, Ann. "Privacy Officers At The Table." Computerworld. 12 Mar 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57893,00.html

[6] Hayes, Frank. "Mum On Privacy." Computerworld. 02 Apr 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59137,00.html

[7] Johnson, Maryfran. "Securing Privacy." Computerworld. 05 Mar 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58242,00.html

[8] Johnston, Margret. "Study: Privacy Proposals Could Cost Billions." CNN.COM. 14 May 2001. URL: http://www.cnn.com/2001/TECH/industry/05/14/costly.privacy.proposals.idg/index.html

[9] Lemos, Robert. "P3P Privacy Technology Slammed." ZDNet News. 21 Jun 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2591856,00.html

[10] Markey, Edward J. "Congress Must Act Soon On Privacy Rights." Computerworld. 02 Apr 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59088,00.html

[11] May, Thornton A. "Building A Security , Privacy 'Brand'." Computerworld. 23 Jul 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO62382,00.html

[12] Mearian, Lucas. "Financial Services: Customer Control Is Costly." Computerworld.13 Aug 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO62934,00.html

[13] Mearian, Lucas. "Insurance Industry Urged To Take More IT Risks." Computerworld. 06 Sep 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO63586,00.html

[14] Melymuka, Kathleen. "Panel: Better Privacy And Security Require 'Cultural Evolution'." Computerworld. 20 Jul 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO62411,00.html

[15] Nash, Kim S. "Chief Privacy Officers: Forces? Or Figureheads?." Computerworld. 13 Nov 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO53899,00.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[16] Radcliff, Deborah. "Guarding The Data Warehouse Gate." Computerworld. 01 Oct 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO64307,00.html

[17] Radcliff, Deborah. "Keeping Secrets." Computerworld. 13 Nov 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO53882,00.html

[18] Radcliff, Deborah. "Privacy: The Liability Link." Computerworld. 27 Aug 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO63289,00.html

[19] Rodger, Will. "FTC: Industry Has Work To Do On Internet Privacy." Inter@ctive Week. 01 Aug 1997. URL: http://www4.zdnet.com/intweek/daily/970801a.html

[20] Rosencrance, Linda. "Group Proposes Online Privacy Guidelines." Computerworld. 05 Feb 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57373,00.html

[21] Rosencrance, Linda. "Personalization Trade Group Proposes Privacy Guidelines." Computerworld. 31 Jan 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57176,00.html

[22] Sullivan, Brian. "Canada's Privacy Law Changing Some Privacy Policies." Computerworld. 17 Aug 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO63149,00.html

[23] Thibodeau, Patrick. "Big Companies Urge Congress To Show Restraint On Privacy Matters." Computerworld. 30 Jul 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO62662,00.html

[24] Thibodeau, Patrick. "Chief Privacy Officers Emerging In Response To Data-Privacy Concerns." Computerworld. 14 Sep 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO50228,00.html

[25] Thibodeau, Patrick. "Corporate Privacy Policies Scrutinized." Computerworld. 03 May 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60170,00.html

[26] Thibodeau, Patrick. "Financial Firms Fret Over Costs Of State Privacy Rules." Computerworld. 30 Jul 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO62654,00.html

[27] Thibodeau, Patrick. "Firms Held to Privacy Pledges." Computerworld. 04 Feb 2002. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO67997,00.html

[28] Thibodeau, Patrick. "Foreign Laws Alter IT Privacy Policies." Computerworld. 08 Oct 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO64563,00.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[29] Thibodeau, Patrick. "FTC Privacy Panel Considers Security, Too." Computerworld. 14 Feb 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO41281,00.html

[30] Thibodeau, Patrick. "Government Privacy Concerns Extend To Wireless Technology And Databases." Computerworld. 09 Oct 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO52128,00.html

[31] Thibodeau, Patrick. "HIPAA Privacy Rules Under Fire In Washington." Computerworld. 22 Mar 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58856,00.html

[32] Thibodeau, Patrick. "House Panel Debates Usefulness Of One Privacy Law vs. Many." Computerworld. 04 Apr 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59219,00.html

[33] Thibodeau, Patrick. "Information Security Will Be Key With Lawmakers." Computerworld. 17 Sep 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO63937,00.html

[34] Thibodeau, Patrick. "New FTC Head Wants 'Pause' in Push For Privacy Laws." Computerworld. 04 Oct 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO64453,00.html

[35] Thibodeau, Patrick. "New Vermont 'Opt-In' Privacy Law Faces Legal Challenge." Computerworld. 07 Feb 2002. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO68104,00.html

[36] Thibodeau, Patrick. "Privacy Concerns Extend Beyond Online Transactions." Computerworld. 03 Oct 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO51830,00.html

[37] Thibodeau, Patrick. "Privacy Issues a Growing Concern For Business." Computerworld. 31 Jan 2002. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO67883,00.html

[38] Thibodeau, Patrick. "Proposed Federal Privacy Law Would Override States." Computerworld. 22 Oct 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO64963,00.html

[39] Thibodeau, Patrick. "This Could Be The Year For Privacy." Computerworld. 29 Jan 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57014,00.html

[40] Whitney, Sally. "The Great Privacy Debate." Best's Reviews. Jun 2000. URL: http://www.bestreview.com/2000-06/privacy.html

[41] "Browser Technology Promises To Encourage Better Online Privacy Policies." SiliconValley.com. 12 May 2001. URL: http://www.siliconvalley.com/docs/news/svfront/083976.htm

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[42] "Consumer Privacy: The Critical First Step Toward Meeting The Potential Of The Internet." @Once Whitepaper. Dec 2000. URL: http://once.com/web/about/news/press_releases/dec_white_paper.html

[43] "The Trouble With Technology." Infoworld.com. URL: http://www.infoworld.com/suppsad/ISS/t_issprt2.html

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 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
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	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
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 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