;login:

THE MAGAZINE OF USENIX & SAGE

October 2001 • Volume 26 • Number 6

inside:

THE WORKPLACE

The Corporate Policy Web

By John Nicholson

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

the corporate policy web

Summary

Every company has policies and procedures designed to reduce mistakes, increase the likelihood of consistent behavior and generally minimize risk. The goal of this column is to list some of the policies that you and your general counsel should work together to develop and maintain. In general, your company should probably have the following policies: an Acceptable Use Policy for internal users, a Terms of Service for any external users/customers, a Monitoring Policy, a Data Retention Policy, an IT Risk Management Policy, an Incident Response Policy, and a Privacy Policy. Each policy should be tested/audited on a regular basis.[1]

by John Nicholson

John Nicholson is an attorney in the Technology Group of the firm of Shaw Pittman in Washington, D.C. He focuses on technology outsourcing, application development and system implementation,

John.Nicholson@ShawPittman.com

Introduction

Corporate policies and procedures serve a number of functions – they are educational, they increase the likelihood that processes will be performed consistently, they minimize the number of mistakes made or steps skipped, and they provide the company with a document that it can show the world to say "This is how we do 'x'." Developing corporate policies also allows your company to figure out potential responses to situations ahead of time, decreasing the number of decisions that are made in the heat of the moment.

In several other columns, I've discussed some of the policies that your company ought to have in place: a Harassment Policy, an Acceptable Use Policy, a Monitoring Policy, and a Security/Risk Evaluation Policy. The purpose of this column is to add to that list and explain why this collection of policies is necessary and what they should look like.

Policies Your Company Should Have

As far as your company's use of technology is concerned, your company should probably have, in some form or another, at least the following policies in place and under regular testing and compliance review:

- Acceptable Use Policy for internal users
- Terms of Service for any external customers/users
- Monitoring Policy
- Data Retention Policy
- Risk Management Policy
- Incident Response Policy
- Privacy Policy

Acceptable Use Policy

The Acceptable Use Policy (AUP) is the terms of service by which all employees, contractors, etc. (including executives and administrators) access and use your network and internal systems. Your AUP should govern all of the systems that an internal user might use, including corporate systems, email, intranets, corporate databases, peer-to-peer applications such as Napster and Gnutella, PDAs, personal ISP accounts, instant messaging software, and anything else they might be able to use or access via your network.

An AUP educates users about what they can and cannot do, and informs them of any penalties that may be associated with doing things they are not allowed to do (e.g., account termination, disciplinary action, termination of employment). An AUP should include at least the following:

From a legal perspective, an AUP can help limit the company's exposure to harassment or breach of confidentiality claims

- It should specify that your network and systems are for business purposes and that personal use of the system is not permitted or is strictly limited (and if limited, how).
- It should specify that all data on equipment provided by the company is the property of the company and may be inspected at any time.[2]
- It should reference your Monitoring Policy and state that, as a condition of access to the network and systems, the users consent to such monitoring.
- It should include a provision that specifies that even if your company does not take disciplinary action regarding a particular unauthorized use of the network or a system, such failure by the company to take any action should not be interpreted as a change to the AUP or permitting such unauthorized use in the future.
- It should prohibit the use of the network and systems for any illegal act or breach of regulations (including those related to intellectual property, anti-hacking, anti-fraud and/or data privacy) or company policies, including, in particular, your Harassment Policy and your Privacy Policy.

If you provide services to external users and have a Terms of Service (TOS), your AUP should specifically require your employees and contractors to comply with the TOS when using those services in the way that a customer would.

From a legal perspective, an AUP can help limit the company's exposure to harassment or breach of confidentiality claims. The AUP also establishes the boundary for "lack of authorization" for purposes of the Computer Fraud and Abuse Act.[3]

The AUP should be regularly updated to cover new technologies. Employees should have the AUP explained to them as part of their orientation. The AUP should be included as part of your employee handbook, and a condition specifying that contractors will abide by the AUP should be included as part of any contracts with consultants or other third parties who might have access to your network or systems. Also, all employees (and contractors who will have access to your network or systems) should be required to sign a statement that they have received, read, understood, and agree to comply with the AUP. It might also be a good idea to do something to regularly remind people about the AUP such as posting it on physical and electronic bulletin boards or including a message regarding compliance as part of login banners or as a click-through screen as part of the login process.

Terms of Service

The Terms of Service (TOS) governs the use of customers or external users of your network or systems. Your TOS should:

- Clearly describe the service provided
- Claim ownership of the intellectual property included as part of the service
- Grant users a license to the intellectual property necessary for them to use the service
- Grant a license from the user to you for your use of any intellectual property provided the user as part of the user's using of the system
- Prohibit users from violating laws or regulations or performing any other acts that your company wishes to prohibit
- Specify whether or not users are allowed to link to your service and, if so, any restrictions on such linking
- Explain your Monitoring Policy and specify that, as a condition of accessing your network, systems, or services, the user consents to such monitoring

- Indicate that the user accepts the TOS and will use the service in accordance with it

If users access your service via a Web page or some other type of login screen, the TOS should be a click-through screen, preferably with the button at the bottom of the page. That way, users at least have to scroll through the whole TOS before clicking the button to accept.

Your TOS may be subject to certain legal requirements. For example, under the Digital Millennium Copyright Act, a Web site's TOS should include a contact for copyright violation claims. If your Web site, or any part of your Web site, is intended for children under the age of 13, there are very specific rules governing how you provide those services and what information you can collect. You should coordinate the development of your TOS with your company's general counsel.

Monitoring Policy

Sections 2511 and 2520 of Title 18 of the US Code create criminal and civil liability for improper interception of wire, oral, and electronic communications. Although there are exceptions under both the US Code and under state laws for system providers, relying on these exceptions is unnecessary if your company puts in place an appropriate Monitoring Policy. By explicitly requiring user consent to monitoring, your company can make access to your network and systems conditional on users accepting such monitoring. All users of your network and systems (whether employees, third-party contractors or customers) should be required to consent to monitoring.

Your Monitoring Policy should specify that your company has the right to monitor all network traffic and all data stored on equipment used for company purposes that is provided to an employee or contractor by the company or by any third-party contractor. Both your AUP and your TOS should reference this policy and explain it. Login banners should also reference the Monitoring Policy and state that access to the network or system is subject to monitoring at any time and for any reason, and that by accessing and using the network or system, the user is explicitly agreeing to such monitoring.

Monitoring traffic and behavior on your systems can allow you to detect misconduct in real time and can create logs that will be useful in an investigation and/or prosecution. Monitoring can also decrease employee Web surfing or other violations of the AUP.

In the future, the increased use of personal technology (e.g., cell phones, PDAs, etc.) to access corporate systems will require increased and more specific consents. If, for example, you open up your document management system so that it is Web accessible, an employee with a PDA and a wireless modem can download confidential information. Access to that system could require explicit consent from the user to monitoring of the activity and an agreement to provide access to the PDA on demand. (Note, such access will be easier if your company owns the PDA and provides it to the employee.)

Data Retention Policy

Your Data Retention Policy (DRP) may already exist. Frequently, companies have policies that specify how long paper records will be retained, both on-site and off-site, and what will be done with them after that period. They might be microfilmed, sent to a warehouse or just destroyed. Depending on your industry, it's even possible that your

Your Monitoring Policy should specify that your company has the right to monitor all network traffic and all data stored on equipment used for company purposes

Given the possible regulatory aspect of data retention, as well as the possible use of stored data in litigation, your general counsel should be involved in the development of your DRP

DRP is mandated by some regulatory agency. It's also very likely, however, that any existing DRP is already being violated by your computer users. If your DRP was developed prior to the widespread use of PCs, your DRP probably isn't even suited to dealing with electronic data.

Given the possible regulatory aspect of data retention, as well as the possible use of stored data in litigation, your general counsel should be involved in the development of your DRP.

Your DRP needs to deal with both paper and electronic data and must comply with any regulatory requirements imposed on your industry. Given the ease with which documents are now generated, you may even need to figure out how to deal with multiple copies or versions of both paper and electronic documents. Whatever policy your company decides to impose, the DRP and its implementation procedures should be clearly communicated to your users. The implementation of your DRP should also be audited.

IT Risk Management[4]

Your IT Risk Management Policy should be part of your overall corporate Risk Management Policy (assuming you have one). Your IT Risk Management Policy should include a procedure that tracks security risks (both external and internal) as they are identified, evaluates their potential risk to your business, identifies the appropriate fix, schedules a date for the implementation of the fix, and includes a follow-up procedure to ensure that the fix was properly implemented. For example, your policy should include:

1. Regular reviews of the relevant security vulnerability sources (i.e., Bugtraq, NTBugtraq, security reports published by software vendors, virus reports, security researchers, the various cracker Web sites, etc.) and, if appropriate, a procedure to ensure that such reviews are performed

In a diverse environment, your company may have multiple people responsible for various platforms and/or software packages, or your company may have various administrators with responsibility divided by geography. It's important to make it clear who will have the ultimate responsibility for monitoring security issues related to each platform or software package.

2. A determination of how the identified vulnerability applies to some aspect of your business

For example, a security hole that lets a script kiddie put graffiti all over your Web page can be embarrassing to your company or might result in your taking down the page until you can plug the hole. If your Web page is just information about your company, this might not be a big problem. If your Web page is the means by which your customers order, that's a different matter. It's important to understand how the vulnerability could impact your business if it were exploited.

3. A rating of the risk represented by the security issue (i.e., Critical, High, Medium, or Low) based on the potential impact of the security issue to the business (in terms of lost business, lost data (based on your DRP), public perception, potential cost, etc.)
4. A schedule for the implementation of the relevant fix for the risk (i.e., all Critical fixes will be implemented within one day, all Highs within one week, etc.)

5. A follow-up procedure that checks whether fixes were actually installed and, depending on the importance of the security issue, verifies whether the fix actually solves the problem

A follow-up procedure could vary depending on the rating of the issue. For example, you might want to ensure that all fixes for critical issues are implemented, and use statistical sampling for the remaining fixes. Alternatively, you might want to ensure that, regardless of rating, all fixes for a mission critical system are performed.

Finally, your policy should schedule regular audits of how your system stacks up against the known threats. This might involve having a "white hat" security firm attempt to penetrate your network. Such audits are an opportunity to test your priority ratings, as well. If a problem someone rated as "Low" allows the penetration team to take control of your system, then you might need to reevaluate that rating.

Incident Response Policy

Your response to an incident should never be ad hoc. Depending on the nature of your business and the type of incident, the personnel involved should have a clear plan for how to respond and whom to (and not to) inform (both internally and externally). Your Incident Response Policy (IRP) should be developed by a multidisciplinary team that includes (1) knowledgeable representatives from IT, Security, Legal, PR/Marketing, and Insurance/Risk Management and (2) selected third parties, including forensic experts, security consultants, and possibly law enforcement.

Your response to an incident should never be ad hoc

The IRP should identify initial indicators ("triggers") of an incident (obviously these must be updated regularly) so that those involved know when to initiate the response plan. Different indicators may require notice to specific people or certain actions. Regardless, such notice and actions should be precisely scripted. As part of the development of the IRP, your team should think through various scenarios and plan first responses to each of them. You should also identify in advance those external parties (preferably specific individuals) who will provide support during different types of incidents. For example, you might identify specific technical and forensic consultants, certain local or federal law enforcement officers, individuals at your ISP, external legal counsel, a crisis management firm, etc. These people should be included in the development of relevant sections of your IRP.

In developing your IRP, your team should have regular meetings with IT staff. Members of your incident response team should not be meeting each other for the first time when you have an incident. It is important for your team to understand who has access to your systems, what is the extent of their authorization (in particular and as specified in your AUP), what type of logs or backup copies are available (as specified in your DRP), what range of response and notice options are permitted by internal policies, and any external requirements.

ELEMENTS OF THE IRP

Trigger Events

This section of the IRP should identify the triggers for initiating the IRP. Such triggers might be based on particular networks or systems, data or events. Some triggers might result in the IRP being implemented automatically, others might require evaluation by designated parties. As part of identifying the triggers, your team should have a good understanding of the steady state "background noise" of the network and systems. The triggers should not be set so low that the IRP is always "crying wolf," but, at the same

Your IRP should clearly specify how evidence related to an incident is to be maintained and protected

time, they need to be sensitive enough to initiate the IRP when appropriate. One approach when implementing a new IRP would be to set the triggers very low and gradually raise them as the team and your company gain an understanding of which events actually constitute threats.

Incident Evaluation

Once an incident has been identified, your IRP should specify how that incident should be evaluated. The IRP should require those working the incident to prepare answers to questions that will be relevant to decision-makers. For example:

- Does the incident appear mischievous or malicious?
- Does it appear to be an isolated incident or part of a larger pattern?
- If the incident is network-based, is the upstream source more likely a victim or the originator of the incident? If not network-based, what is the source?
- What are the implications of contacting the source?
- Has your system been compromised? If so, where and for how long?
- What systems/files have been taken/tampered with?
- What is the value/potential harm resulting from such tampering/taking?
- From a legal perspective, does the incident create potential liability to customers, shareholders, or other downstream entities? What level of due diligence is required to avoid liability if the incident escalates?
- If there is an investigation, should participation in the investigation be limited to internal personnel? Should outside counsel be retained?
- Does the company have reporting obligations related to incidents of this type? If so, to whom?

Evidentiary/Forensic Requirements

Your IRP should clearly specify how evidence related to an incident is to be maintained and protected. You should work with your general counsel, law enforcement, and external forensic consultants in advance to develop this portion of your IRP. Proper evidentiary and forensic procedures will increase the likelihood that your company will be able to recover any damages and that an attacker will be prosecuted. These procedures do not kick in until after an incident has been resolved. They are an integral part of the incident response process.

Responses

Your possible responses to an incident range from ignoring it to immediately shutting down the affected system. Your IRP should specify under what circumstances you will ignore an incident, when and for how long you will allow it to continue while you observe and gather evidence, when you will take immediate action and, if so, what action you will take. Without the guidance of an IRP, the immediate response will probably be "Shut it down." Shutting it down lets an attacker know that you are aware of the problem and allows the attacker to move on and attack you in another way or attack someone else. Shutting it down might also compromise evidence, thereby preventing you from prosecuting an attacker.

In the long run, your responses to an incident should be tied into your IT Risk Management Policy. The positive side of an incident (if there is one) is that an incident will help you evaluate whether your rating of a particular vulnerability was correct.

Reporting Procedures

Your IRP should also specify what internal and external reporting will be done regarding an incident, including if and/or how an incident should be reported to law enforcement. The IRP should designate who has the authority to make any external reports regarding an incident and to whom they are authorized to make such report. For example, your risk manager or your general counsel may be authorized to call in law enforcement, but only the CEO would be authorized to communicate with shareholders and the media.

An important area to consider in the development of your IRP is under what circumstances you wish to involve law enforcement and at what level. Should it be the local law enforcement, or should it be the FBI? Either way, you should have an established relationship with whomever it will be. Bear in mind that once law enforcement is involved, the handling of the incident may be out of your control. Law enforcement may have a different agenda than you do.

Testing

Once you have your IRP in place, you should test it on a regular (and occasionally unexpected) schedule. You should also consider bringing in all of your external support for an exercise from time to time, so that you can see how your IT, legal, forensic, PR, and other experts interact. The likelihood of a significant incident and the potential impact to your business of that incident should determine how frequently and to what degree you conduct such tests. Such testing can be tied into testing of your IT Risk Management Policy.

Privacy Policy

These days, everyone is concerned about privacy. If you are in certain industries (finance or health care) or if you provide services online to children under 13, you are subject to very specific regulations regarding any information you collect online. If your business operates in Europe, you may be subject to the European Data Privacy regulations. Canada recently passed a data privacy act. And more privacy legislation, both in the US and abroad, is coming.

If you collect and store any personal information from customers, members or anyone else, you should have a Privacy Policy that clearly describes what data you collect, what you do with it, how people can opt out of having you keep or use their data and how they can contact you to correct any errors or opt out. If you have a Web site, there should be a link on each page of your Web site to the Privacy Policy. The Privacy Policy should clearly include a mailing address, email address, or phone number where people can contact your company regarding privacy questions.

Your Privacy Policy should be tied into your DRP. You should also consider in your IRP whether and/or how you will notify people if their data is compromised.

Once you have your Privacy Policy in place, your compliance should be audited on a regular basis by both your internal audit staff (if you have one) and your external auditors.

If you collect and store any personal information from customers, members or anyone else, you should have a Privacy Policy

Conclusion

Developing and maintaining this collection of policies is a lot of work. It requires coordination between technical and legal personnel, and the policies require testing. It's not enough to simply write a policy and then put it in a drawer. Once your draft policies have been developed, have them audited on a regular basis by your internal audit group (if you have one) and/or your external auditors. In order for your policies to do their job, everyone whose behavior is governed by a particular policy needs to understand and comply with it. Properly implemented, a good set of policies can substantially decrease both the operational and legal risks to your company. Doing it right is expensive and resource intensive, but the risks associated with doing it wrong or not doing it at all are too high.

NOTES

1. This article provides general information and represents the author's views. It does not constitute legal advice and should not be used or taken as legal advice relating to any specific situation.

2. Given the increasing capabilities of PDAs, there is an increasing likelihood that a company will, at some time, want to see the contents of an employee's PDA. If the PDA belongs to the employee, the company may not have the right to demand the contents of the PDA. If, on the other hand, the company has provided the PDA to the employee, then the company has the right to look at the data on the PDA at any time, just as if it were on a company-provided computer.

3. 18 USC § 1030.

4. Note, this section repeats information provided in "You've Been Cracked. . . And Now You're Sued," in the April 2001 issue of *;login:*.