

**What nformation Security**

**Policies Are**

CLLENT CALLED *ME* UP ONE DAY AND asked me to come to his office. Once I arrived, he asked me to install a firewall so that his network would be secure. I asked him for his company's security policy so I could configure the firewall. He gave me a curious look and asked, "What do I need that for?"

In the years since the explosion of the Internet, this response is still the rule rather than the exception. Companies have comprehensive employee policies, sometimes filling two-inch binders, but do not have information security policies. If they do, they will hand you 5 sheets of paper that cover the assets of a multimillion-dollar corporation.

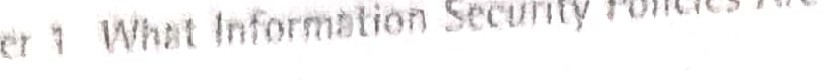
Just as employment policies describe the practices that employees and managers must take, security policies describe how the company wants to protect its information assets.That is an important concept to remember: Information is an asset.You might not be able to assign it a value, but your competitors might pay thousands or even mil­ lions of dollars to understand or even steal those assets.

### About Information Security Policies

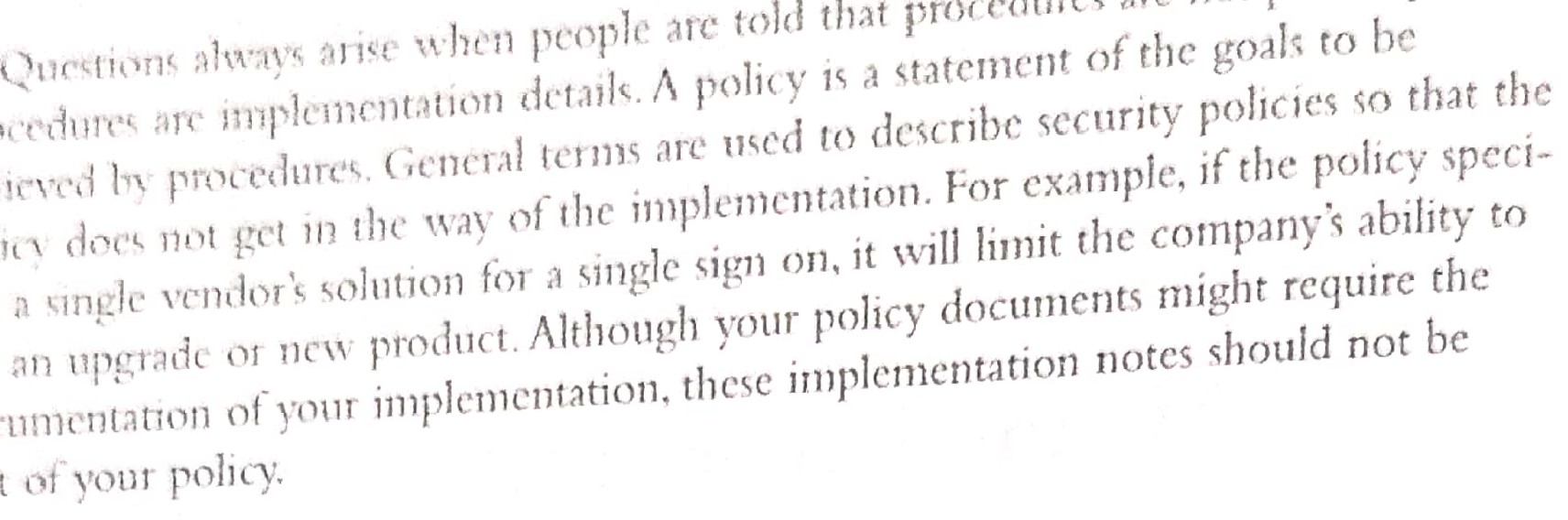
Information security policies are high-level plans that describe the goals of the proce­ dures. Policies are not guidelines or standards, nor are they procedures or controls.

Policies describe security in general terms, not specifics. They provide the blueprints for an overall security program just as a specification defines your next produce.

o Scanned with OKEN Scanner



O. Scanned with OKEN Scanner



*r * s Are Important

Altlinugh policic, do nor discms how, properly defining what is beingprotected assures rh;npn percontrol is implemented. Policies tell you what *is* being p ocected and what n?,trict1ons ,hould be put on those controls. Although product select10n anddevelop­ mentcwle are not discussed, policies wiU help guide in product selection andbest pract1 'i during development. Implementing these guidelines should lead toa more

. ecur *s,·.*rem.

Whe;1 management participates in the creation of information security policies,it demonstrates that management supports the effort, lending credibility to the entire securityprogram. Having management support is always important.Without leadership, employees will not take policies seriously.Therefore, if you do not have the support of your upper management, your program is doomed to fail before you finish writing

the policy.

How You Gain Management Support

First you can try to reason with them. You can point out that the systems and data have *real* costs. You can demonstrate how an outsider or a disgruntled insider can easily access sensitive information that could damage the company's business functions. You can show them studies, articles, even this book. But if this doesn't convince them, you might have to wait until *your* first disaster.

Management *might* say that everybody is responsible for *his* or her own security.That might work in the short term, but it prevents the company from working with itself If one department uses one standard and another department uses another standard, interoperability *could* be a problem. Policies ensure that the company uses the same

standards in every security instance.This consistency makes it easier for the company to integrJte, interact with customers, and maintain a sense of security throughout the system.

Finally, an information security policy will help avoid liability. We live in a litin·iou society. If you try to enforce rules that are not expressly written, you will be sued. If you fire an employe\_efor security violations that have never been written, presented ro the en:ployee, or previously enforced, that employee also can sue your company. I know it sounds harsh, but the realjty can be devastating when the subpoena arrives.

When Policies Should Be Developed 5

## - I · Pol· .ie Should Be Developed

ldc.,lh-. tlwl Cl timl' t( ,dfine • ur p licics.lwu]J l c before your firs security prob­

,Jm. Hy ,foin this c.,rl '.your. I.' ·urit, adrnini trator will underst;ind what to protect

* 1 d "hat<nforce111:m 111c:1.mes c;in be used. Also it is alw;iys easier to write policy for

•,1k,·l'k linti11fr.1strucu1r rather than trying to retrofit it into an existing business em·1·on m nt.

1itigatino-**Liability**

A you might r nught not knO\v, all business processes come with a certain amount of ri-k. afeguard• are placed into our business processes to n1.itigate this risk.A security

P licy take business processes into consideration and applies best practices to protect them. Thi can help reduce the liability after loss of critical data.

As ecurity and virus protection become an integral part of the evening news, law­ enforcement has increased efforts into catching and prosecuting perpetrators. More and more of the courts are asked to apply our paper-based laws to the electronic frontier.

Companies without policies have found they have few liability claims because the courts understand explicit policy and not the best practices. It is to the company's legal advantage to have this written down before being challenged in court.

The new economy has put a premium price on electronic information. Electronic information and the machines that store it are so integral to business processes that companies have been looking to insure these assets. As part of a process, insurance companies have been questioning the security policies and practices of the company. The first question an insurance company will ask is to see your security policy.

Without a security policy, most insurance companies will not consider issuing an insur­ ance policy. Insurance companies know that without having gone through the policy­ making process, the company does not know what assets it is protecting, therefore making them too risky to insure.

Finally, a security policy that includes software development policies will help guide development of more secure systems. By setting these guidelines and standards, devel­ opers can be appropriately constrained, testers can know what to look for, and admin­ istrators understand what is required during this process. Custom development always represents a great cost and liability. By drafting and.implementing software develop­ ment polices and by giving developers guidelines to follow, liability can be mitigated.

#### After a Security Breach

Implementing policy after a security breach is like dosing the barn door after the CO\\' has escaped. Although it might seem too late, there may be cows in the barn that you can save. Never think that because it happened once it cannot happen again. Because it happened once it likely will happen again.

When developing policy after a security breach, never focus on the area broken.

Although it is a concern, it is just one of many areas that should be a concern. Always

o Scanned with OKEN Scanner

*C* . kr 1 I\' 

Jt,(,l,. ,'l tlh' wh, ,' pittnr •-· m,,.,,. ,,1w j'I\ hkrn ,1lom'. This i the only·way to write a

""'f'tl1t\n. h,,n,1,\"l t,h ..,.

u 1'llf • , rlll liatK

i.. ('\'<'t rn ,, 1,. i::,, -1,rnmcm *c,* ntr,ll'tl r , those wli,),·ork for government contractors,

.n,,1 ,'th '1 hi i,;l',,c, \Yt rk.ini:: in ,,r *-.1:* that irn·olvc rile public sector must provide a way

,,"' c:1 ir,..' rJ. r ti 'li" ,,·.--t'-'lll-". r s.1fe ;,11d se ·urc. l11crc:1si11gl,, governments and other

,:mt,,,"t'r. I ,l\",' ,t., ,1•1 J -m.mdinc: w ,11\_kfi11cd inform:1tio11 ecurity policies. Part of

·;,,-,y,, ,, mi li,1 1c, *i:* h,lYit !.!•1': -curiry p ]icy. E, en when st:irting new development,

.

. .- - T ·itY p,,!ic.Y:-h ,,- rh - -ust mer that •ou are serious about his or her security

'--01 ".-..Cl 1 .

,.\_ ,· n 11·'1 t .- curity rcquin.,ments seem to change all the time. One thing that has

·1, t d anf d *i:* th, r -quir mrnt that agencies set security policies, how the contractors

- ; m • li..:-i s.. :t 1 h ,,. they work"·ith their own policies. As more requests for pro­

F *.als* 1 it th str ,. th r guirements for security policies also will increase. If your

*c* m. any w r *·s* \\7th the gon:rnment in any capacity, from contracting, to compliance, t nts. the presence of a security policy that can help avoid liability will be a F *1* 1ary 01 ern.

De.rnonstrate **Quality Control Processes**

}J n::::w, -ich compliance, companies also might want to demonstrate that their processes

:al] within quality control standards. International Standards Organization (ISO) 9001

e. cribes a standard to demonstrate quality control in all business processes and proce­ ure . If your company wants that type of accreditation, the policy will serve as a

guideline for the implementation of a measurable security program required by quality conrrol candards.

# How Policies Should Be Developed

Before policy documents can be written, the overall goal of the policies must be deter­ mined. *ls* the *goal* to protect the company and its interactions with its customers? Or

*,,·ill* you protect the flow of data for the system? In any case, the first step is to deter­

*mine* what is being protected and why it is being protected.

*Policies* can be written to affect hardware, software, access, people, connections, net­ work, telecommunications, enforcement, and so on. Before you begin the writing process, determine what systems and processes are important to your company's *mis­* sion. This will help you determine what and how many policies are necessary to com­ plete your mission. After all, the goal here is to ensure that you consider all possible areas for which a policy will be required.

**o** Scanned with OKEN Scanner

7

d t l \ ittcn

h1hn 111 flt ,Jj l' 1111(1' p )111 I{' tfo nnt h;iv' t0 \,(, ,) mtrir de ClliilCfli ·r() r, :c- j• *r,,1*·i·r.

: 1 I!! 1t'' ' '11111 m:i l1 n11 nf 111: JW dol nmrnt,. ji,q hk the nrg.,ni1 cion of th1, l-•<1 1<.

* 1)

r,itl,t•i th,n1 1•tf(·;1n1, l'f <.t::itrmcm . I rliY1ded th boo up m o,chrtpti:r, *(>f re* (\.me top-

,· \' r;ithc1 thnn tnin!?-to \\"lite nne polic, document \1,:rite indtridu.-1! doc 1mcnt,

,1 1tl \';111them charter, Df :nm rnfonmtion ,ecurity policy. By cloin§! ,o. they ,ire e.-1 ·er *w* Uih1('N:md,'.a,1c-r to di,tributc. and easier to proYidc individu.:il trJining '-·ith bcc;1u e-each ro1icy \'ill ha ·e m own cction. Smaller sections arc aho c,F,ier to modify

1

;m .- upd:i(·C'.

I·fow many rolicies should you \nitc? 1 hate to answer a quc tion with a que rion. buth(,,,. many areas can you identify in your scope and objectives? For eJch sys em

, irhin your business scope and each subsystem within your objccti ·es, ;ou should define one policy document. It i all right to have a policy for email separate from one for lnternetusage. lt is not a problem to have a policy for anti-virus protection and a separate policy for Internet usage.A common mistake is trying to write a policy as a

ingle document using an outline format. Unfortunately, the result is a long. unman­ ageabledocument that may never be read, let alone gain anyone's support. Figure *l.* l has sample list of policies that could be written.

Popular culture is full of examples showing chat people have short attention pan . And face it, information security policies are not exciting topics. Subsequently, keeping the policies short, to the point, with clear statements, logically organized in a cleanly designed document will give your document a better chance of being read. Do not try to overwhelm your audience.

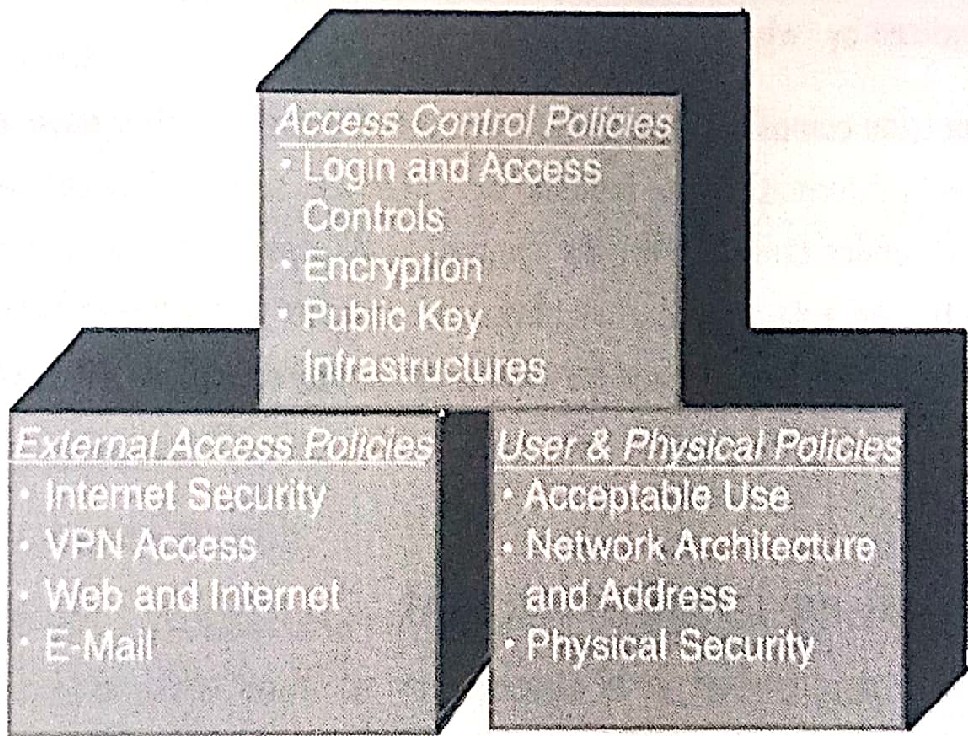


Figure 1.1 A sample list of areas that can have their own policit·s.

o Scanned with OKEN Scanner

*('I.* r 1  J('

1 

, ,,11! , ·,1\· h" 11111111-1. nd \'l)lll l1lli,1q1nt'ltlll' 1 It pr1fon1;11 follri'ik :-i 'i' 'iment.

, : I. '11.h·,1,. 1'1 ,111d11 t)ll 1hr cnl11t' t'tllctp11 c. By doing o, policy\: rit<.:n c;in oht;iin ;i

!: :it u1Hit 1q 1111h1h!t,11 thL' 1t'.1ch of 11111.11 mation tr hnology \·itl1i11theorg,rnization.

* lrl t'tl1 1t1w1kc,.d1c \_10.1t·em ominou,, it ;illo\ tl1r author tocomic!'reveryaspect

,., bi- ;ir.-hllt'(l\llL'.

\ pn 1-.(a n, · , ,c,1.mc nt. the organi7atio11111ay \ ·ant to do omesecurity penetra- 11l n ll',tlll!!. Thi, r,..' tinµ 1.hould be performed l oth on the intcrn;-inl etwork andexter­ 1,1ll t ic\l rwry k:110\\11 ace ,1. point and to di cover any unknown acc s points.This

br0;id a, L.,mcnt rr \ltk imigbt nc ess:1ry to understand the configuration of the net­

,\_,, rk.Th1, information should l e used to determine configuration, access, and other r0lic1e,. Al,l t"ill -ontirm h w the network supports the organization's mission.

Som administrators might feel that they could explore the system, determine the ri k,. and inYcnr ry the enterpri e them elves. Although they could possibly do an ade­ quat ·job.it i always better to hire an outside company to perform this activity.The rt"dominant r ason i chat they do not know your system, best practices, or other

inside in ormati n that could prejudice the assessment.The outsider can come to your co 11- any and explor your systems from a hacker's point of view: Here is a potential layground. let· ee \vhere we can play!This will allow them to expose vulnerabilities, w akne e , and other problems that you will consider when writing the policies.

Why Hire Outsiders to Do a **Risk Assessment?**

Some might feel that their own systems and security professionals could perform the risk assessment. I do ot agree. While the people your company employs may be very competent, they are too intimate with operations to be able to tell a technical risk from a process risk. Outsiders do not have the same ties, so they cannot be prejudiced by "what has been."

When selecting an outside company to do a risk assessment, make sure they have the resources to under­ stand the latest security information and industry best practices so that they can provide a complete risk assessment. They must understand all the risks involved in all aspects of information technology. Because these companies do this on a daily basis, they have more insights into what to expect as they perform their tests. This objective point of view will be invaluable during your policy process.

Review, **Approval, and Enforcement**

As with any corporate document, it is customary to have review procedures. Informarion security policies are different types of documents.The review process should consider not only the technical aspects of security, but also the legal aspects of it a it relates to the organization. Prior to authoring any policies, there should be a clear understanding of the overall review process. Obviously the authors will perform the first review and then different levels of corporate review should occur. If your

l..

Scanned with OKEN Scanner

Summary 9

·'l'n11• nyh,1:,-1 \'h. tc( lnCnn11,1tit n Otri er (CIO) th:lt per. 011 . hould hr.:on the review

·,,mmtlkt'.l cp.mnll'nt lw,Hh w divisi )ll lwach that will he affect ·cl by a policy also I tinl.l1,.',bl' h 1'\'i '\,\'ltld providt: cn111mct1ts. l:;inally, ;1s mu Ii as everybody hates th ·,rnw,,h··m ·nt. th' ·oq or.it· attorneys also. hould he involvcci. Attorneys under-

t•,nd th'r.1mil1r.1til n,s

r the poli·y ill :,r •as such a. c11force111cnt ;ind what can be

1. 'lll' t,, enf)l\',' th' t olicy.

Th •'Prro\-.1\ l n *c* ·ss i. ,\ simple mat:r<.:r of the management agreeing to the final wrsit.)111.f th' d ·mn 'llt. Their approval should come after it is reviewed. However, if n .H :t t·rn 'nt fails t bless thcs, documents, its effectiveness will be limited.

Fiiully:.1frcr the p li y is written, approved, and administrators implement its direc­ h\' '. th' poli ·y must be enforced. Policies that are not enforced will be broken at wilJ. lt i th':-,Hnc a· Ln, s that are not enforced in society. Why go through the process of

-1 ',lti1g s cnrity policies if the provisions are being ignored?The policy must have

pi \isions f◄ r enforcement, and these measures must be carried forth.

## Summary

* 1. ecurity policies

11 Are djstinct from guidelines and standards.

11 Are distinct from procedures and control.

* + - Describe security in general terms; they do not describe how to implement. Policies are important to
    - Assure proper implementation of control.
    - Guide product selection and development process.
    - Demonstrate management support.
    - Avoid Liability.
    - Achiev consistent and complete security, avoiding fragmented efforts.

1. Policies should be developed
   * Before security problems occur.
   * To avoid liability.
   * After a security breach.
   * To document compliance and demonstrate quality control processes (for example, ISO 9001).
2. Policies should be developed by
   * Setting the scope and objectives for the policy document.
   * Defining what policies need to be written.
   * Performing a risk assessment/analysis or EDP audit.
   * Defining effective review, approval, and enforcement procedures.

o Scanned with OKEN Scanner

1ng Your Policy Needs

ow THAT WE KNOW WHAT SECURITY policies are and have the support of manage­ ment, the next step is to understand exactly what is being protected. This understand­ ing goes beyond the hardware and software that makes up the system. It is very important to understand the business process that the technology supports.Your policy could sit on the shelf collecting dust if it prevents the company from doing business.

Identify **What Is to Be Protected**

In the first few pages of this book, I have repeated that the information security poli­ cies must protect the company's mission or business process. I did this because it is a common mistake to try to look at the computers and software from a technical point of view instead of why they were purchased. If you remember that computers are the cools for processing the company's intellectual property, the disks are for storing that property, and the networks are for allowing that information to flow through the vari­ ous business processes, then you are well on your way to writing coherent, enforceable security policies.

**o** Scanned with OKEN Scanner

1 C'lrnplrt 

, ;l·(h,.1·,...-, **1d** .' ft, arc

* . ,··. ., 1 , ] I :ire ;incl software components that

,'npp1 r11111: llh1,1' bmmc , pr()( :,.:-;o,itc t le i;i c. . .I ..

w·ll h· p1\)(L'l°tl'd h' 1hc. l'.·, ·1~1 .. *,r* . it 1s llllJJ0rtant to have a omp etc mven-

pl 1c1 s. 1c1cme, •

' • 1 . 1 l .

h)t ,· *cit'* tht' ,\·,tern, whirh . hm1d *111c* ti( • nm:ip

*(* the network There arc many ways

* I h 1.

O

11 t·rc-:1lt' tl1i,• mwntory or produce;l net\ 01•k map. Re •g'ardlcss of .w 1a.t met oo..s a.re

I. .h b

mc-d. \'( l1 s11011ld 111;1kc sure that *CPrrytI11*·*11.*

* cIoc.ui1e1 •ntcd• Following 1s a samp1e 11st of

bard\\'•arc and . ol.tw,1rc .items tli;1t couId appe:ii. on 'an invento.r.y. .T 11s m1g t.not he. a.

1.

*c* mpkte fot I( r your spcc1*·.*1*r.*1ciiv,·roiiiiicnt,· you should consider how to ta11or t 1s 11st hr yom comp,rny's purposes.

**ample ltwcntory List**

- - -- 4- - ·----

**Hardware**

PUs

"bo:ird

**111** keyboards

,. terminal

" workstations·

" personal computers grams

* + printers

**11** disk drives

"' communication lines

**11** terminal servers

11 routers

,. diagnostic equipment

**Software**

* + source programs
  + object programs
  + utilities
  + diagnostic programs
  + operating systems
  + communication pro-

One way to map the network is to show how the data flows through each system. A *data flow map* can show how the flow of data supports the business process as well as highlight areas where it is important to apply security and survivability measures. **In** turn, that map can be used to inventory where data is stored, including databases, how it travels through the system, backups, audit, and administrative logging information.

##### Non-Computer Resources

Inventories, like policies, must go beyond the hardware and software. There should be a list of documentation on programs, hardware, systems, local administrative processes, and other documentation that describes any aspect of the technical business process.

These documents can contain information regarding how the business works and can show areas that can be attacked. Remember, the business processes can be affected by industrial espionage as well as by hackers and disgruntled employees.

o Scanned with OKEN Scanner



l 'tn *ify \i* h.:it *Is* o 8 Pro e ted *13*

fl; 1 I IC1w,tinppin :ind 'utvivability

*u•,·wn/til,ti* 1' tli ;1b1lily lo di lrrmm how *rl* syslrm ;ii \t:iin its issin',?.i<I criiic31·1roc ,,1;; 1n tr.P l11r t·m-cof t,Wid \ fotf1n \, ;inrJ :i1·ridcn1,. 11i l);isrd on the r· arrh o rformPd in ihr CERT Cii(itclin;it,on l'rfl!cr ;it ()11ncgic f ,cllon Univ r 1ly (v,w1.cert.org). Their re arch d mo"lstratrs ha inqc;:id of u ing 1hc lrc1ditinnal fortrtss-likc ecu ity mod I, nctwor s hould b consid r d a unbo•;nrled, indepcnrlcnt rn\it,cs ith defined communications paths and sp ci 1c trwt *r* lation hips.

/lnaly inga yskm for '.-u1vivability involves understanding the business requirem nts of the net1nor . h architecture of the network, how it isu cd to satisfy those requirements, and a trade-off analf'.lis to cn;urc thesurvi ability measure also maintain the business environment. Part of the analysis and the usagerequirement is the understanding of how data flows through the system. By understanding his

7

flow, an analysis of critical processescan illustrate where resistance should be applied and demonstrates necessary limits placed on the architectureby the business requirements.

Formoreinformation on CERT's survivability research, see Appendix B, "Resources."

imilarly, the inventory should include all pre-printed forms, paper with the organiza­ tion's letterhead, and other material with the organization's name used in an "official" manner. Using blank invoices and letterhead paper allows someone to impersonate a company official and use the information to steal money or even to discredit the orga­

nization. So, include those supplies in the inventory so that policies can be written to protect them as assets.

##### Taking Inventory of Human Resources

The most important and expensive of all resources are the human resources that oper­ ate and maintain the items inventoried. To inventory the people involved with the operations *and* usage of the systems, data, and non-computer resources will provide an insight as to what policies are necessary.

Creating an inventory of people can be as simple as a typical organizational chart of rhe company.This can be cumbersome, however, if you are including a thousand or even a few hundred people in one, big document. Moreover, organization charts are notoriously rigid and do not assume change or growth. The inventory, then, could include the type of job performed by a *department,* along with the level of those employees' access to the enterprise's data. For example, if the company has a large sales department, creating an organization chart with everyone's name may serve the egos of those included, but the chart becomes unmanageable. Rather, the inventory can include the "Sales Department" noting that some number, which may be unspecified, of salespeople work there.

One positive aspect of this exercise is that management can gain an understanding of who is working for the organization and in what area. As part of this process, man­

agement can see duplication in processes, identify strengths and weaknesses, and show where there might be organizational problems. This type of analysis is similar to surviv­ ability of network systems-but on a human scale. Managers should not have to be reminded to :ict appropriately during this process.

o Scanned with OKEN Scanner



  .,, nlin '1 rrf



1 .

.

I r ,  **1.tl**

**f r t ted**

l ',· ,, 111,, .11 ,·1 t< m ,. i·1, 1't "' i1111k1,1.1nd1111• h()\1' c.1d1 *:* tclll ;indnet\·ork conipo

., ll[ l ,h .-i' '-1'!1 \1111 llt'I\ •111 m1rh1 h,1 T :l \Y\1c.'Jll I( '-Ill J'Ol t lit'(\ 'Ork-b:Vir,dlutlwn­

{1,1,i,,,:,. 'll .p1,iJwi ..,111'1'«'>rltll!! rntl,llll'I lil..t,' c1\'kc\, 1 ut .11c,11! the "Ytclll ac.ccs cd

l1I I

.1 • 1I \ , 1' , l"ll 1 ., 1.\,,·d • •im1)t1, , ,•qc1m? lh· urnkt.1111ding lim i11fon11au011

,.,\_. ,,m, •• n .1i-ci·,<i',i. hlll lw,11ld l c :ibk to 1dc11tif)' 011, ·h<Ill our policic should t'·"',, ,., r •·1• i1tl'l ,c,11,1dn:i!H'IJ1 f )l d. t:t ,K *c* :ire

1

I

l " ' ' I ' '

•

,

. utlltin,,·d *:md* nn:n11hnri7ed *:iccc,,* to resource ;md/or information

:1111 1c11t •d and or u1uutl101i7l·d di clomrc of information

.. "ludmc- 1•nfi.1rc mcm l n. crdurcs



Pnm:in ,·. the focu ";11be on who can acce resources and under what conditions. F:>r *c* ·a:11pk. hu 11an re- our e data Gill be :iccessed by authorized human resource per­

nn ,j but not b\_- th general u er population.The policy might need to aUow direct ac.:-,, of *p* r. nal data but houl<ldefine what "direct access" means. Of course, the poli -y v:oul limit ace s to those who should not have this type of access as well.

/-Jrer you d tine who can have access, a consideration needs to be made as to what enforc m m me hanisms and penalties should be placed on unauthorized access. Will rhe or anizarion work with law enforcement?What disciplinary action will be placed on employe who \iolate the policy? Legally, what can be done?

Lesrality of the organization's actions is very important. In this litigious society, it is important to ·pecificaUy state the ramifications of violating the policy. In some states, it may be enough for the policy to say that the employee can be dismissed and "prose­ cuted to the fullest extent of the law." However, others may require specific language explaining the applicable laws. This is where having a lawyer on the policy-writing committee can be helpful.

This advice extends to access of the organization's systems through external means. By saying "e>..1:ernal means" we are not limiting access to just the Internet. Access can come through VirtuaJ Private Networks (VPNs), private networks (such as a customer nerwork chat uses Frame Relay), or modems. These access points must be defined, and *policie* must be created for what can and cannot be accessed from them. Because access policies are a very important basic protection to any organization, the topic will be covered fully in Chapter 5, "Authentication and Network Security."

*As* the softv.iare development cycle gets condensed to work within what has been called ''Internet time," we all must live with bugs and user errors. These are uninten­ tional intrusions on the secure operations of a network that can interrupt mission-crit­ ical operations. Although it is difficult to anticipate what to do in the case of failure or errors, *it* should be included as part of the analysis. One way to think about how to consider non-intentional problems as well as possible intrusions on the systems is to use Survivable Network Analysis Method **(SNA)** for analyzing network survivability.

See Appendix Il for pointers to the papers on the SNA Method.



**Q::Scanned with OKEN Scanner**

Data Security Considerations 15

urvi able Network Analy is Method

\\fhcn analyz:ing tie network for survivability using the SNA method, the first three steps are togather

tie svstemdefinition, understand essential capabilities, and assess compromisable capabilities beforeper- fo1mi11g ti e su • b'I' I •

rviva Irty ana ys1s. These steps arc essential for the analyst to understand the nature of the

mission for which the e systems work-thus understanding and allowing for necessary tradeoffs in design thatcan beimportant to the analysis. Using SNA, the architecture and usage scenarios are used to ana­ lyze how thenetwork is used.

Thekey to SNA is that it requires the definition of two types of network usage scenarios:

1. Normal usage scenarios (NUS)
2. Intrusion usage scenarios (IUS)

NUS analysisdefines how the system and components should be used under "normal" conditions. Thus anything that is not normal can be considered for intrusion analysis. IUS can be defined to understand the

potential impact of a successful attack or accident. This type of analysis is very useful to understanding how thenetwork components inter-operate.

## Data Security Considerations

Everything we do with computers and networks allows the flow and usage of data. Every company, organization, and government agency is focused on the collection and use of data, regardless of their function. Even manufacturers have critical data-handling aspects of their operations that include pricing, shop floor automation, and inventory controls.The handling of the data is so important that in defining the policy needs and collecting inventories, understanding the use and structure of the data (as well as where it is stored) should be a requirement of all involved with writing security policies.

#### Handling of Data

How will data be handled? There are many aspects of dealing with data that must be considered when writing policies.The policies must consider how data will be handled and how to maintain the integrity and confidentiality of the data. In addition to the handling, consideration must be made to how handling that data will be audited.

R.emember, data is the lifeblood of your organization; you should have mechanisms to trace its life through the system.

What about using third-party data that may be confidential and proprietary? Most data sources have associated usage and auditing agreements that are included with the acquisition of that data. As part of the inventory of the organization's data, external ser­ vices and other sources should be added to the inventory.The inventory also should identify who works with the data and under what conditions this data is collected and possibly disseminated. •

a Scanned with OKEN Scanner

i 1 '1 pt"T. i1 ff)mi111 r.cd

.. r,r d H nrlling ilf : t 'l nl'll I i'\{ll

rtt'>, 1,1 1,, l.,,,,1 t ckfmtd ., :my ,nlminiltion colic trd, bought, or qivcn hy n *5our* outside the om- P• ,\ M, 1, tin1r, thi 0,11,1 come vilh opyri9ht *or* c,onfirfrnlinlity agrccrrwnts thatdict:itchow th·

i!1f0m1, 1in11 1, 111.rrl. \\/licthtr 11 i infn1111:11io11or 1hr our ·r to a vendor's1;:itcst releasem,

h(' in pl:h to nfurcr the nqr 111 nt by whirh thr1t dr1ta is acquired ;Jnd *us*d.

echanisms mu:-,t

On lrap , the- cPllc t,on of info,mntion from public d;.ita sources that Dre incorporated into other v,orks. It: ca.y for rrnpl er to ut-and-pa t i11formation from web sites and other sources into internal doc­ m,rnt<.. While thi. i legal under fai1-u c standards, tl1e employeeshould provideproper attribution,

r pe,:-1;:il , if the information i quoted v rbalim. Yes, they should know better. However, this should be

rcinfor.:-cd by the: policy and be included in thesecurity awarenessprogram.

Ju t ;.\_ orh r rganizarions hare inform:ition with you, you also might want to share information with th 111. Whether it is because of a partnership agreement or other

bu. in •s r lationships, mcchani.ms must be in place to protect the disseminated data or

t lmology tran for a. intdlcctual property. When writing these policies, some of the

* nsid ration for di . eminating intellectual property are

c: U.e of company information for non-business purposes " Definition of intellectual property-handling requirements

* + Tran fer of information to a third party:
    1. Confidentiality agreements
    2. Full-disclosure records " Protection of disclosed data

Ir is difficult to anticipate how the business circumstances define what can be disclosed and how, but the policy should include a review of these processes. One way to under­ stand their impact on policy is to understand how current agreements are handled.As pare of the inventory process, any attorneys working on the committee can gather these agreements and notes on current discussions. Using this information, policies can be v,rritten as guidelines to protect the company in information and technology transfers.

A common omission to these policies is the requirement to classify information.

One conm1on method is the use of security labels. Although the use of security labels is not consistent across all operating systems, databases, and software programs, policy writers should consider how to mark data for their level of security. There are many circumstances where this is necessary. In particular, personnel or health care informa­ tion Jre prime candidates for security labeling.

##### Personal and Personnel Data

During the course of business, an organization can collect personal and personnel information in many ways. Those involved in e-commerce may collect information from access to their web site. Companies that sell products and services can collect



**a Scanned with OKEN Scanner**

-

###### Data Security Consideratiom 17

cmh m T ll.lt;\ thro11Ji rde1•/ , . • I II

. . . \_t-

tul ct h111 er rnqnmcs ·an v· ,J-1 , I · ·

nuy or ustomcr crv1 c c;ills. Even ;i cs c;i or potcn-

\_ • • *1* lt: u P r. 11a 1t1format1011about a person or a company.

Rc,-.,.,1d.k.s 1t lll w thi•

ch• t··' i•sJ qm•r d

, pol·t y t:itcmcms should be createIc *(*r*'*or cvery-

l'I *c* to mhk-rstand how th data is u.ed.

###### rivac lie and Public Policy in the United States

I \\'rite ti i , public:p licy makers i•n wash'ington are d.iscussing the practi.ce of collecti·on and handi1' ng

ofpeonal 'ataduring the normal business cycle. In recent news,the Federal Trade Commission (FTC) has r ommended thatcongress pass laws requiring companies to disclose how they handle information they collect from ac ess to web sites• Th.is came af ter find•ing that many web s·ites do not have posted pri•vacy

licies or olicies that are followed.

Currently, the FTCprivacy guidelines are merely guidelines and not part of public law. At the FTC's request,

C ngressislookinginto the issue. As with many controversial issues, predicting what Congress will do can be a full-time job.

One thing toconsider when beginning this process is how your organization operates outside your home coun ry.U.Sc. ompanies doing business in Europe, for example, might be subject to strict privacy laws in Germany andScandinavia. Although thesepolicies may not be popular within your organization, it will help when working outside the United States. For further information, see Appe11dix B.

When considering privacy policies, the observance of privacy must be defined so that the organization not only observes the employee's or customer's right to privacy, but also that the employee observes the organization's right to privacy. Policies can be writ­ ten to state that private, proprietary, and other similar information should not be dis­ closed without prior consent.

Privacy policies are not easy to define. Because policies are guidelines and not pro­ cedures, some organizations prefer to define exactly what is protected in procedures documents. One of the best ways to determine how to partition this is to gather what should be included in privacy policies and look for one or a short number of common statements.Those statements become the policy. How the data is handled then becomes a matter of procedure.

#### COTS Licensing

Policies for Commercial Off-The-Shelf (COTS) software licensing must consider that in most cases, the organization does not own the software or the data governed by those licenses. COTS licenses allow you to use the software under specific restrictions. This means that COTS policies should be based on following those licenses.

The software industry has been increasing their licensing enforcement procedures through the Business Software Alliance (BSA) industry consortium. Working from tips that usually come from disgruntled employees, the BSA audits and reports on the licensing status to the owner of the software. After an investigation, the BSA supports the company in filing breach of contract lawsuits against offending·companies.

o Scanned with OKEN Scanner

\ h, tt1 ? n1' l tl •**mt**• ',",ti! P11lk *rtrl*

- I l l 1·111lt1tl•· ihc11criodif *re* iC\. ofIi CJ!mg' f!Tecment,

< Ct.) I I 1]1'11'\ ' ]l'\ll l .... d f t

.

1I11111:· -

l t ' i •rnd

1 - r·(0 t\\'\r, lie·n c'and r cor o rcgi tr;'ttinn

1. :1111k 1;1t•<; h 1 •11 qn, 1 H 1 • r

00

L'' H c11 l' t

, )

11

J•' ic·,,

copying should be in luded and

t'II pn J11cr ·1th wndo1- dt ltH)ll,I ), 0 JC T *r* thoseresource'

lll,ul,limnd:,tc q1 Kt m.111.1gc111c,nrt nd ,·,c0llll\_t,1b1.l? o OT • !)oli.ciewithothers·

1 lnw be.mi ont' rn11111on theme when dmm 111g , . . . ••.

. , l 1 11lietreatc I a. such.1 Ill 1 nota far-fetched idea

I.. t·, :m:.' licen c, 1n' ;i<;,c t :1!1l iouc b •

, l ' • 1· • ·tI ct ti1at h:1vc v,1luc can be counted, andcan e dcpreci- Thc,c ic1·n *c* an: tang11 c a\_" • • ' • f • •

:i.td like the rn.-ichirn:·;·y n the shop floor.Thi will ple;iscthehie F111anc1al Official

i1:c o.r heha. not co;1 idcr d the v,,lue of software todctermme theamountspent

on pn.1 rty. planr. and 111:1terials.

# kups Archival Storage, and Disposal of Data

p liciesabout the handling of d:1ta backed up to external sites or off-site media isas

imr,ortanat mationa.

for online accessible information. Backup data can contain nancial infor­ hi tory of customer interaction, and even copies of current busmess. If the

datai not to be kept, what would happen if the competition were able to obtain and anah-z that information?What if they found data that should have been discarded?

Backup policie , therefore, must reflect on the processes themselves, cover how the data is archived. and provide direction for what to do when data is to be discarded.

##### Backup Considerations

Wny doe your organization back up information from its computers? Is it to recover from system crashes? Preserve critical data? Does your organization want to keep a snap hot of system software? How often are these backups made? Are they made daily, weekly, or monthly?And how do you do them? How often is this process reviewed and verified?

All good questions, but how do the *answers* to these questions enable the backups to

support the recovery-critical business processes after a failure? An inventory of the business process also should include the recovery processes and the information pro­ cessing that is necessary to support them. That knowledge will help determine how to ansvver those questions and set policy.

A common mistake in setting backup policies is to mandate the special options available in the software package the company is using. When determining how back­ ups support the business process, policy writers should try to confine the document to describehat should \_bedone and avoid mandating special options. The following are a few quesnons to be considered when analyzing backup policies:

* Which data will be backed up?
  + Only user data?
  + The whole system?
  + Entire database or journal files?

**o Scanned with OKEN Scanner**



###### 13a kup , J\rchivr1ISltorag , r1nd Disposal of D;it;i 19

l lwt nlll'n . honld hacl-..u1 s be m;i :le?

* • l nps 10 ) \H'l or111ed: automated, multip c co11c . or mec 1;1

1-hn • m b:i·I-. 1 *1·* 1 · 1· •

H.nw nftc 11 nrc tlic backup procedure rcvic ved?

\'\'ill \'Ol ll. c.' off- itc or 011- ite storage for backup 111cdia? Ho\ , ·ill you ccure th on-me tor.ige ,1l''a?

\\,lll,·ill be allowed t ) erfonn the backups?

\. ho will be allm,ed to have acce s to the restorable data?

\Vh will be allowed to restore that data?

chival **Storage of Backups**

For ome. the la t con ideration of handling backups is how to store the media or safe­ guard th data. As part of the audit and inventory of operations, special note should be mad of current practice. If the current practice does not safeguard data, then here *is* your chance to make the safeguards policy.

\Vhenconsidering backup archiving, one of the first concerns might be whether themediawill be stored on-site or off-site. Some organizations have storage vaults for storing tapes and disks. For them, policies for on-site storage should be sufficient.

Ochervvise, understanding the current and best practices can help create a workable policy.

Several years ago, I retrieved a tape from the vault where my company stored its backup tapes.The vault was climate controlled and specially designed to store up to 6 years of 9-track tapes.The tape I chose was created only 18 months earlier. I mounted rhe tape on the local drive and tried to read its contents. After spinning for only a few hundred feet, the driver printed an error and the system refused to read the tape.

After trying several tapes, I looked at the service log and found that the system's field engineer adjusted the drive heads after someone complained about not being able to read a tape sent by a client. Although the adjustment was necessary, tapes for the three months prior to the repair date were unreadable. Had we known this would be a problem, there would have been a chance to recover the data. Unfortunately, there was not a policy on handling the data or checking the backup. Since then, I have insisted on a clause to include testing the archive.

That brings me to another point:Why was the vault nearly filled with six years of archives? Did we need six years of data? We did, but does the data that your organiza­ tion stores require it to be saved for that long? If not, then how long? In cases where the retention time is longer than the life of the media (the typical life of magnetic tape can last an average of two years), maybe you should consider a policy that specifies *write-once media.* Notice that I said "write-once media." Remember the lesson learned in Chapter 1,"What Information Security Policies Are": By considering a policy with general wording, you allow the people creating the archives to determine the best

o Scanned with OKEN Scanner

...

t·l *C*l111 -,l1.*'('\* I l" I1, I 1·111l

* 1l)1,, ti)t !111· 11 *c* t'f 1ww terhnologi<•, th.u rn:i.y ;1110

the d;tt,'\

It' h· 1;\ lm•c,1 k111 c·1 di,111 n11 n·nt npltt)n •

: n f .,, M·a

·Pl'm",h.'J\fo,nr... , ., cn111nw11 pr.1ctic whl'll thmc J. r:icticillg industri:il cspio11agc

* + l· ' 111 : rm:1lh"'n ,)11 dwi1 t:1rgct. cnllc:1guc who mnl t, ork in this :trca would Sttr­

i.,rl'L n t' with ,t\Wil' c1bout Yhat .omc rnmpallic. throw out.011c d:iy, he hit the jack-

1•,"\. He ,-, lkttd 11101" t1 an t"'( dozen c,utridg' tapes from the dumpster of a

:-,,mr,,tir0r that ccmtain d inf rmation that the comp:my should h:1vc nude sure was kept (onfidt"ntial.

H w d1. ls y... ur organizati n dispose of d:w1? If you are throwing :1way tapes with­

' ut Gasin th 1 1. tl en th dumpster Jiver will surely find your company's secrets.

r) •,errnining 11 ''" th data is di posed of is as important as determining what data to di card. Make ,·ur that this policy specifies how to erase or discard the data *a11d* that it define. a re uir ment for verif) ng that the data can no longer be read.

On way to ensure that this policy will be carried out is to assign the responsibility t discard the data to one person and the verification to another.The policy should mandate that a regular schedule or a rigid procedure be followed so that both responsi­ le partie ca,n . rify that those who should not see it could not access the data.

### Intellectual Property Rights and Policies

Every organization, regardless of its function, has intellectual property that t protects from disclo ure. Even if the organization does not have information security policies, it p·obably ha rules and procedures for safeguarding its intellectual property. Not every organization puts the same emphasis on this property, however. For example, a com­ pany that i a price differentiator will guard its manufacturing process to prevent its competitors from discovering how they can keep their prices down.

Intellectual property policies are probably the most difficult for most information security professionals co write. Not only are these policies tied to the business process, but the body of law covering intellectual property covers volumes and can differ between states and countries.When planning and writing these policies, it is highly advisable to consult an attorney whose specialty is in this area. In the preliminary stages *o(* planning, the following are a *few* considerations for in ellectual property pohcies:

* *l+'ho owns the rig/its to the intellectual property?* Assignment of patent, copyright and other intellectual properly rights should be stated in a policy, whether it is within the information security, corporate, or employee manuals. Having this spelled out in a coherent policy can provide a solid basis to protect the company's property in court if that should become necessary.
* *Mll1at arc the rights to programs and documentation?* After ownership of the intellec­ tual property has been established, what rights do employees have with the

**o Scanned with OKEN Scanne**

Intellectual Property Rights and Policies 21

progr;imsp, r C!\S ·, and documentation?While :-in employee might have access to

them:-imial that cl ·scribl!s the latest business process or the new re-engineering pbt s.tht' policy may prevent them from taking that manual out of the plant or talkmgabout that inform;ition with others. And the policies can define who tl\_1ose"others" are. III fact, some policies require that procedures define access

rights to the document and processes:

* *Afsl o,1rcc3* <ij *i1!(on11atio11 should lim1e a11 attrib11tio11.* Graphical User Interfaces (GUls) and t\_heWorld Wide Web make it easy to gather then construct information by copymg from the browser window into the window running the editor or word-processing program. Sometimes it is too easy. Making copies of someone

else's work and incorporating it into your own without attribution is plagiarism. Yes, you cm use small sections under the "fair use" laws, but these sections must be attributed to the original author. The policy statement can say that the company will not tolerate plagiarism while leaving attribution standards to style guidelines.

a *Labe/i,1g.for paternity rights to i11tellecf11al property.* If the work is covered under patents, copyrights, or nondisclosure, it must be labeled with the appropriate information. Without quoting the cases, several have gone against the· owners of intellectual property when they did not make their rights known nor took mea­ sures to protect those rights. Some companies mandate that all printed material contain the words "Company Confidential" on all pages. Labels must be conspic­ uous and clearly state ownership.Your attorney who specializes in intellectual property law can help in this area.

When working with intellectual property, whether it belongs to your organization or you acquired it from someone else, make sure you know your rights under the agree­ ment. For example, many software programs allow the user to create one copy for backup purposes but not allow more than one copy to be running at any given time. As for written works, there are still "fair use" laws that allow a limited number of copies for personal use. Once the usage is allotted for business purposes, you should talk with your attorney about what is and is not allowed.

Technical People and Intellectual Property

There are many urban legends regarding the handling and protection of intellectual property. One of my favorites says that a way to copyright a work without filing the necessary papers is to mail ten copies to yourself. The postmark on the unopened envelopes would be enough to establish the date and location of

the work.

Technical people tend to work hard on an idea, and then they take these legends seriously in an attempt to save money. Later, they find that these schemes offer no protection. Intellectual property is such a complex subject that myths and legends should not be your guide in protecting your organization's most important asset. Instead, talk with an attorney who specializes in this area. The attorney will tell you that all you've done with those ten envelopes is added money to the coffers of the postal service.

o Scanned with OKEN Scanner







i, ,

an l ,< rer .. s

' I l l 1 - t) \'l'I\ 1111 11 lll,lll()ll \l'(llrll r rn:iiling lit.fhl'\' lis s give lll' \r1

l

1m. ,1''-111 -,ry

j 'l , , . . .

ll }' I I l 1 1 111 t 11 , :111,l othl'1 n1hwr.1b1lit1c,; that c:111c;imc sccurit\,' pr L

1 by

l \ l'l' ,,j' I 1.\1 ,'

11 I l , *J* On

l,••r' \\'ll

t , 1 m'l wni , :--.l1m' ,11-e l..!l'lh'J.ll while otheVi arc nm

1111 \\' Cll ' ·' , . .

;q, 11\11,11'1\11.1'1,',1,1IJI,'·•;itn ti) u c1 *n(* th:it wndor\ product. 1mt couta111mformaticJn

11111,111,,1 h, rnci-,"·hik th, l\' l Cl)rncs from th· manufa turcr.I knm: that the nt1n,

t'l'l 1-1

rn:nlmc:]iq, l ;in1 on i O\'Crkill to 111ml ad111i11istr,1tors, but the point is that as 1

,, 1v-l.. , nh n; rl1'nt . I am kept ''l to date 011 lhe l:itcst infonmtion.

·c, *c,nc* d::1,·. \'1.. ll ,,r .ittin in your cubicle, :md you discover a security hole that

, nc\. pnblici,cd: if mack d by :i h::1ckcr or ;i di. gnmtled employee, could bring clown th 0r\_ ;miz:it11n. \ nrt,\·ork. 1 ather than trying to bury the information, you try to

f'l1 Jici7 it.

Some Fn p1 feel that incid nt reporting is ;rn important service to the Internet c0mrnunity they go out of their way to report problems they found. Many of these o,pnizati n ha\e a policy for incident reporting.You can send the information to

on::; :{I different in ident re ponse organizations.To help these services, your organiza­ oon -ould ha\'e a policy to work with one (or a fev-.r) incident response team(s)

th·ou b one point of contact. By limiting the responsibility to one person, or a backup. information can be efficiently transmitted from a single, authoritative source, and it will not be lost in a sea of messages that might even conflict.

The CERT Coordination Center

T e granddaddy of all the incident response teams is the CERT Coordination Center (CERT/CC) at Carnegie Mellon University in Pittsburgh. Founded as the Computer Emergency Response Team in cooperation with the Department of Defense following the Internet Worm in 1988, CERT/CC collects information about security incidents and investigates whether or not it is a problem that should be publicly disseminated. Although CERT/CC's methods are considered controversial, they do provide a valuable service to the com­ munity. CERT/CC is not theonly incident reporting service. Appendix B provides a list of a few others.

Incident Response **Strategies**

01 the mher end of incident handling is incident response. Incident response is neces­ sary when unauthorized access of your net\vork is detected; when a response team contact your oi:ganization to say that problems exist, and that they appear to be com­ ing for your organization's computers; or when someone reports to a public service

rhat 'l problem was found in the operating system or support software that your orga­ mzanon runs.

Lih.· incident reporting, incident response policies should have one point of contact. Th::n person should be responsible for collecting these reports and preparing a response to them, regardless of from whom they come. In fact, the contact person should be able to determine if an incident report is applicable to the organization.The policy could give this person the power to do whatever is necessary to solve any problems

a Scanned with OKEN Scan

Incident Response tind Forensics 23

.m,mf: fa"m tlw, rcpNL or pn)\'idc Lhc ability to dra, on others ll ·ccss:1ry to diag­

n '-l' t1 ' j"'l\)bkm,

0

l'tli1w with \'C'llLJ )t· . I · · · k. ·] ·d

\\ I:"' Jl- 11p101 tct rc\J)OllSe teams 1us rnlar to wor ·111g wit 1 m c-

l'" 'lld'llt o·ire, c:-.': t I I · ·

' • . • • • CL t 1c \'Cll< or may co11tr;1ctually require your orga1JJzat1011to

thl, )Sa' } :mrnlar 1oim or co11t::lct. For CX::llliplc, your organization might want the

.:-,-nntyc•tt1.·. er tohandk incidem response . Your vendormight want to bypass thi

i''r OJ tow rkwith, Y-tcm admini tr;itors. Allowing this requires only a minor adjust­ mrnt l1lP heyandcan be written in a way to alJow for working with vendor teams.

C n1puter **Crin1e**

*- s:*writethis,1 -am looking at three different guidelines for prosecuting people under ditlrentatt mptsat defining what is a computer crime. E;ich guideline tries to tie the

localjuri diction's ca e law (the decision and opinions made by the courts) to the writ­ tenla\\'.The only consistent theme is the inconsistency of their requirements.

Under tandingwhat is a computer crime differs bet\veen jurisdictions. Even in the United Statese, ach of the federal court circuits may have different interpretations of thesame law. ff you are a company in New York, the rules may not be applied the ame toyouroffice in Silicon Valley. The key to understanding what is allowed in your area is tomake an appointment to speak with the district attorney, attorney general, or solicitor that you would work with.They know the judges and the standards of evi­ dence necessary to successfully try a case.

However, writing a policy saying that the company will work and report all crimi­ nal activity may not be in the company's best interest. Take the story of the bank whose systems were infiltrated by hackers who stole nearly $11 million! That bank ini­ tia1Jy chose not to report the incident to any law enforcement authority fearing nega­ tive publicity.With billions of dollars in assets, it was easy to write off $11 million in "lost" funds.

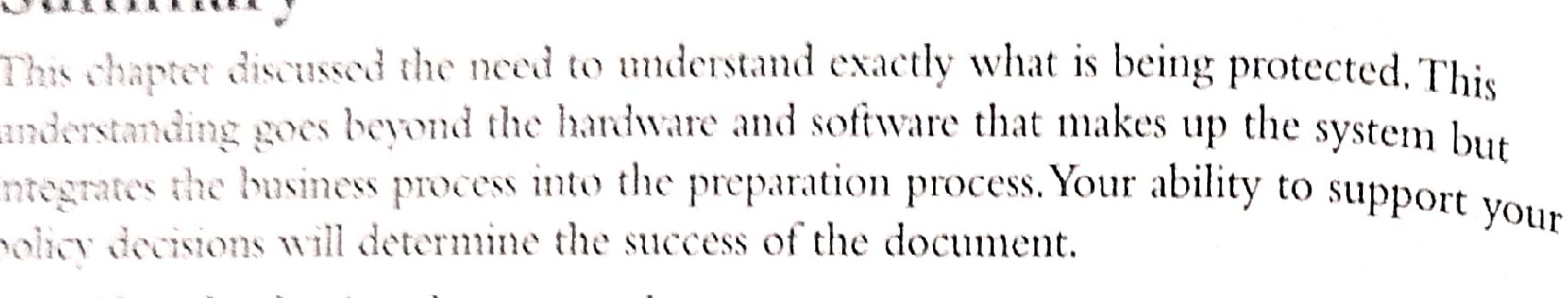
One day, the bank had to report the loss in response to another lawsuit. When the press found out about how this bank lost $11 million, the negative publicity was enough to affect the price of their stock and garner additional scrutiny from federal regulators.The end result was a public relations problem, which costs.

Determining what to report and under what considerations is not something to take lightly. Policies in this area must be discussed among executive management, who must bear the burden of the decision should something happen. On the other hand, requesting that management make the decision about the appropriate policy forces them to consider security policies. How they answer will tell you how seriously they are taking these efforts. At this stage of policy writing, it is good to know how much support really exists.



Scanned with OKEN Scanner

\\_ ., **l't** ' . l 



1:,'1li \\"h.1t i, t, l \' pt\ t\;(-td:

H,: *,iii'.* ,--, ] - bo.1r,k k\;yl x1rds, terminals, workstations, personal co111\_ 'ut T. prim *T:.* :fok drives. c rnnmnication lines, terminal servers, and

1\.. H 'r .

" ·,\_frmi". S nr • pr grams, object programs, utilities, diagnostic progra111s,

-.r -nting ·yst ·m•..md communication programs.

" *.m1.* During exe nrion. stored onJi. ne, archived offiine, backups, audit lo~t,>, d:it.:il .1ses. or in t1 111sit over communication media.

" *DLY11111cnr,Hfo11.*On pro6rams. hardware, systems, and local administrative pro -edures.

**11** *~1111,lirs.* Paper, forms, ribbons, and magnetic media. Id ntit , from whom it is being protected:

* Unauthorized access to resources and/or information
* Unintended and/ or unauthorized disclosure of information
* Bugs and user errors

,, Data ecuriry considerations:

., Handling of data (integrity and confidentiality)

* Handling of third-party confidential and proprietary information (who's allowed and under what conditions)
* Protection of disclosed data (confidentiality agreements and full-disclosure records)
* Personal and personnel data (rights to privacy and disclosure policies)
* COTS licensing policies (periodic review, registration, evidence of compli­ ance, and copying)

1. Backups, archival storage, and disposal of data:
   * *Backups.* What, when, how, how often, and how often reviewed.

* *Archival storage of backups.* On-site storage versus off-site, protection of archive, documentation, testing, retention period.
  + *Disposal of data.* Who is responsible and how it is verified.

1. Intellectual property policies:
   * Information as an important company asset
   * Assignment of patent, copyright, and other intellectual p operty rights

**o Scanned with OKEN Scanne**

Summary **25**

11 ttribmion or sources for inforrnation

" Libding for paternity rights to intellectual property

* Protection of inteUectual property rights (notices and due diligence)



1. Incident re ponse :rnd forensics:

" Incident reporting and response strategies

* + Determining who has this responsibility

**a.** \Vorking with industry and vendor response teams

1. Computer crime:

11 Understanding that a computer crime really is only considered such according to law enforcement

* + Determining what to report and under what considerations
* Working with law enforcement



o Scanned with OKEN Scanner



**Information Security Responsibilities**

F YOU ARE READING THIS BOOK IN chapter order, you probably want to start writing the policies. However, before you start to write your policy documents, you should really have a clear definition of the roles and responsibilities of the individuals in the organization with respect to security.As we have discussed in the first two chapters, management support is crucial for a successful information security program. Along with its support should come responsibility to the ongoing maintenance of this pro­ gram. This chapter will emphasize the responsibilities of management and the roles of those who must provide front-line enforcement. The understanding of these groups is necessary for a successful security program. The chapter ends by discussing awareness training and support.

# Management Responsibility

Management's responsibility goes beyond the basics of support. It is not enough just to bless the information security program; management must own up to·the program by becoming a part of the process. Becoming part of the process is showing leadership in the same manner as it does in other aspects *bf* the organization.

When I tell this to people in management, I get a reaction of shock or horror. After all, they are not trained in technology or information security. I explain that they do not have to understand how it works, but they need to be involved to ensure that the

o Scanned with OKEN Scanner



\ hn1.ttr '.1 Info,malil n :ec11rit I csponsibiliti s

1 11,1nc,,J'l\ l'l'' (• ;irl' p1\)1('1'tcd an\_ci not hind ·rel by securi\_tydecision:. Management h:1 ,piYitict:\1:il (<.1r the r a111nt1011, .111d rnost securitynd 111format1on systemPro\_ t h'lnal, :ire not in th po.ition to un\_d r. tand or appreciate thee\_nuances-1:his is rtot a lnoc. agaimr ma11:1g'rncnt or tcclm1cal people, but year. of nusunderstandings h:tve

,,·1:atcd ;mim 1 it-y bet V"en the two group·.

Both gt up.·honld tmd:rstand tk1t - curity is not somethin\_g that\_can be wrapped m a pacbg and bought off the helf. lt 1s a goal that both parties strive to maintain.1

Cl m . after the ;maly\_is of risks, costs, and the requirements to ensure that inforrnationt

1. not t o .ecur to access. Management is responsible for doing the analysis and con­ vc ing thi. to tl1e technical people respomible for implementing these policies.

Infonnation **Security Management Co1nmittee**

One of the \Yays to help bridge the divide between the two groups is to create an *Iifmnatio11Semrity lvfo11age111e11t Co111111ittee.*This committee will be responsible for reYiewing changes in the business plan and determining how the security policies should support those changes. Another purpose of this committee could be to review the procedures, assuring that they comply with the policies as well as requests for exemptions to the policy.

To make this conmuttee a success, it should be made up of a diverse population and be imilar in makeup to the group that authored the policy document. However, the difference is that this committee should consist exclusively of management representa­ tive who wiJJ understand the implication of the policy from both the business and technical perspectives. This assumes that technical management understands the issues and has access to information to help make good decisions on security issues. Not every member needs to be executive-level management, but it would be a good idea for the conunittee to be represented by someone from the executive suite.

##### Information Ownership

One of the more difficult tasks for management, or even the management committee, is to assign responsibility for information assets or controls-also called *irifor111ation own­ ership.* By designating an owner, that person becomes responsible for maintaining the information asset according to policy.

Information ownership is not an easy concept for many people. In the traditional security model, data and controls are kept on'the servers under the watchful eye of an adm.inistrator or administrators.That administrator, then, must understand how that sys­ tem is used and how to set access controls. Problems occur when the administrator has co manage a diverse set of controls for many di erent servers, databases, data stores, or just "assets."To keep a sense of order, the administrator makes policy implementation decisions based on the least commo.ndenomi \_ator of everyone those systems serve.

◄

**Q:, Scanned with OKEN Scanner**

Managcm nt R sponsibili 29

.ln tlm '\,n '-• \izc-lit -··'ll" • U•.'11a1.1·c\ tlic ad111.11.11strator ,cl, the clas,1.fi at1. on, 11s1c1v1ty,

,11h,tKC. '. c mm!•" for the da

l •1 to 1)C 011s·1stent \ 1· th the ;w;c.,mcnt ot h·is orh

er J·Ob .

Thcr.

1. 11( 1mar,1nt *c* that these • -tt·t ·1t1

'bl •I h 1· •

,., ' ,l 11 mtc. \VJ H.: compat1 C Wit l t C po icy a, It

;tinphcs to cvc, n· 11 r\_ n tl•l'lt "Cc, sc-,s. tI1c 1•11*r*11rmat1·011.

·• <.!.

Confl1·ct can occurb et ween

n.c-r. 1 911irin ac c • to inforlllation and administrators who have made the wrong

a .umpn m.

11alt rn:H-iY' method would be to assign ownership of the data and control,.The

mi r w uld ber spomible for defining access to the data and determining how the

·ontrolsare to be set. The owner would work with a security and/ or systems adminjs­ tratr to ma nag the information assets.The owner would determine the sensitivity and cla ificat-ion instead of leaving it up to the administrator.This result would be che managing of assets to satisfy the needs of the owner.

The mvner would be responsible for handling variances from generally accepted practices. 1f the request for information requires controls that are inconsistent \vith pol­ icy. the owner is then responsible for the necessary changes and subsequent repercus- ions. Some organizations require information owners to request variances in writing and sign a disclaimer raking full responsibility for any potential problems. Because many do not want to take the career risk involved with this responsibility, requests for variances are rare.

The downside to information ownership is that the owner is responsible for main­ taining controls in a manner consistent with the security policy. Further, some owners may feel that the requirement to take full responsibility is not fair or not worth the risk, thus they do not follow procedures and ignore policy. From the beginning, the owner must understand the impact of the responsibility he or she has to the informa­ tion.The only way to mitigate this problem is through proper security awareness train­ ing, support from management, and consistent and stringent enforcement.

Another problem with information ownership is that it only really works well in diverse organizations where data can be partitioned among potential owners. I have not seen this work well in marketing organizations or in others where data is thor­

oughly integrated in the environment. Information ownership also can be a problem in smaller organizations where there may not be enough people to support this concept. One company I worked with that tried information ownership made all 20 employees co-owners of the data.Although this was done as a morale booster, it also helped maintain the integrity of the data.

If your organization is not comfortable with the concept of information ownership,

you might want to adjust your policies to create committees of responsibility. By creat­ ing small committees, they can do the same thi\_ngowners would do, but no\_single per­ son would have to accept responsibility. Rather, the entire committee becomes the responsible party.This creates a situation with addfrional checks and balances when

variances are requested.

o Scanned with OKEN Scanner



l h fllN 3 Info n1 tk n \_ccurit lksµonsibilitic

, -**i;:ninc· ufc. rn** , **tion wncr hip**

The :-ir t ;nk (-.t .Nip;ning infonmti )il ownership is to m;1ktcakehoklcrsthe owner of tlwir 0\rn dar,:i'.imJ ly. the owner of fin:rncial clata shou dbesomeoneunder the Chief

-1·i1rll1C·l;ll

t-11-Ct'rT.

l11•S •L

lll),t111 ,c·i•s)' 1Jrocc",s• The point 1s not to create catch-all

dcpanm"nt . unlcs-;it t'it$ the business process.This also 1 1eans thatthe Info mation

, yH,im Drp;irtment must not be the owner of inform t1on\_exc\_ept that h1ch is n'tc1·,J for operariom such *: s* configuration, user identificatwn rnformation, domain name s nice (DNS). and the like.

/\.., part of the process, you should talk to the stakeholders. By dis ussing infonna­

tion O\rnership with those directly involved, you can understand then concerns.You might ewn get ideas regarding how to assign or structure ownership.

m1ership should be assigned based on a high-level inventory of information asset .You can use the same inventory as created during the preliminary processes (described in Chapter 1,"\Vhat Information Security Policies Are"). I suggest the high-level list be used so that there are not too many information owners. It may require addirional analysis into who should own what information, but limiting it toa fev,,rkey players will help manage the process.Then, each major information type should have a designated custodian assigned from the inventory.

**Security Responsibilities for Information Ownership**•

If your organization decides to assign information ownership, you have to consider what responsibilities these owners have. Guidelines written into the policy should define the specific controls information owners are allowed. By "specific," I mean what controls they can work with, not how those controls are implemented. These policy statements also can discuss the administration of the access controls in terms of the parameters they are allowed to administer.

The most important responsibility given the information owner is the granting and revoking of access to the company's information.As you begin to draft policies, those dealing with the access of information should include how these policies affect the information owner. Further, access policies also should consider recovery capabilities for the data and the access control processes. For example, the policy can mandate that

* If the information owner is not available, the owner should designate someone to act on his or her behalf.
* Passwords used in management of the information are also held in a password or key escrow so that they can be accessed should something happen t.othe owner.
* There are mechanisms to override the information owner.

Remember, the mechanisms you are considerin.gare.p.olicies.Avoid the temptation to

define the procedures information owners will follow.



. -. ·

o Scanned with OKEN Scanner

Role of the Information Security D partment 31

Inf n **ation Security Co111pliance Plans**

\):/hrn disrnssing 1mn:1gcmcnt's responsibility and compliance, you should concentrate

on how rnamgemcnt should respond to enforcement as well as when policies are bro­ ken.Thcse pl.ms go beyond the i sue of management support. These discussions should center on the roles management should play in the information security arena.

\Vhen it comes time for awareness training, management's sessions are exclusive and abbreYiated compared to what everyone else must go through. Rather than separate management, see if you can integrate management into the security plan. Make man­ agement an active participant. While it is not necessary to have an executive actively review log files or site-inspect facilities (although they might be a good ideas), they shouldbe involved with settling disputes and counseling employees that violate policy. Should a problem require the assistance of law enforcement, members of management should be on hand as an active participant in the investigation.

This may be tough to sell to nontechnical management. Even in the move to auto­ mate business processes, management that does not understand technology tends to hide behind their technical people or consultants. Although information security is not really a technical issue, it is seen as such. One way to include them in the process is to have them own the processes,just as other managers own the data. By making them the owners of the processes, it will give them a sense of responsibility, which ,vill not allow them to wilt behind their desks and management committees. For that sector of management whose ego needs a boost, giving them responsibility will add to it.

## Role of the Information Security Department

The Information Security Department is responsible for implementing and maintaining organization-wide information security policies, standards, guidelines, and procedures.

They should provide security awareness education and ensure that everyone knows his or her role in maintaining security. Simply, the Information Security Department pro­ vides the mechanisms that support the security program outlined by the policy.

This department must be able to strike a balance between education and enforce­ ment (see the "Security Awareness Education" section that follows). It will be difficult to find this balance.The policies guiding this group should be written down to ensure that these roles are clearly defined. They should be viewed as a partner in the business process. lf implemented as an enforcement-only group, the Information Security

Department will be feared. Fear can elicit advers re\_actions to its real purpose, which can undermine the purpose of these policies. \_ •

Chapter 12, "Compliance and Enforcement/' as its name makes obvious, is dedi­

cated to compliance and enforcement, an integral component of security awareness education. Read ahead if you need more information about the role of training before continuing with the policy-writing·process.



* Scanned with OKEN Scanner



h. r \ 1, Info;m tirn• r. 111 ,it

R I on ibilitic

, c- nr,i ,., r ncss Edu ti n

,c imrl',rta1,c of sccwit, a1•;irencss training and education canno:bc\_o ers atcc.J. By \_taking the policy eri11usly and teaching all of the stakcl1oldm about their role in maintaining it, thcy will embrace the

n,lie\ 11s an intcgrril part f their job . This is not easy. One pr bl mishat over thclastdecade, industry. leading ompan,c ha\'enot demon trated a concern for security in their products. The results areprod. uct, that h vc in ufficicnt ecurity measures installed into environments that further weaken the intormation ecurity program. The dichotomy can be confusing.

·ecurity 21 arene training requires clear communication. One thing you might consider for your organi­

.:ation i hiring a technically competent communicator for the Security Department. This person would do the training, educate the department to the concerns of its users, and act as a liaison between users and the department. Having someone who can communicate will help raise the confidence level users should have for the department.

##### se of Consultants for Information Security

Outsourcing has been a staple of the computing industry since companies offered time- haring ervices on expensive mainframe systems. Today's outsourcing environ­ ment can provide information processing services for every aspect of the organization

including information security. '

There are some serious concerns in using consultants or outsourced services for

information security.When determining policy goals for the outsourced environment a few things should be considered: '

**11** *ltVork with i11-ho11se Information Security Department.* It *is* highly recommended,

even if information security is outsourced or consultants are used, that the orga­ nization maintain a small department-even if it consists of only one security

ex-pert. Information security is something that requires a trust relationship among the users of the information and those enforcing the policy. It may be difficult for some co trust an outside source.

* *Set clearg11idelines.* As with any outsourcing or contractor agreements, clear guide­ lines on the roles and responsibilities must be defined for these outs ders. It may not be in the organization's best interest to provide these outsiders open access to che information assets. Therefore, a clear *statement of work (SOW)* should be included as part of every outsource information security agreement that clearly

outlines guidelines. The SOW should not be part of the policy documents, but its guidelines should be stated.

* *Deter111ini11g responsibility.* Another aspect of the **SOW.**should be to determine the responsibility of the outsourcing or contractor *in* the organization's information security environment. Policy should include the responsibility of anyone working as part of this environment. •
* Scanned with OKEN Scanner

O her Information S curity Roles 33

Othe • **Inforination Security Roles**

For ;rnyinformat! ll s' uriLy progr;irn to be successful, it must be integrated into every aspect oftheenvironment. Integration must include statement of work and responsibil­

itieswirllinthebu ines enviroumcnt,job ckscriptions, and how these will be audited wd monitored.

##### Integrating Infor111ation Security into the Business Process

A primaryt::isk in assigning roles in the information security process is how informa­ tionsecurityintegr:1tes into the business environment. As part of that integration,jobs that upport security through the processes should be defined. For example, one way to do this is todefine a sepantion of duties and control over company assets by coorcli­ nating efforts with everyone, including owners of data and facilities. By having these

defined as part of the business process, there is no ambiguity as to who is responsible and when.

Another role to consider is how security is administered throughout the organiza­ tion. A typical environment should have a centra information security management group.The central group is in charge of the monitoring and enforcement of the policy and procedures. Consider an approach from unbounded systems (see the description in Chapter 2, "Determining Your Policy Needs") where the central security management group designates security administrators for multi-user and multi-departmental systems. Each department then supplies it<; own security officer or liaison who will help main­ tain the security program for the department. This has the effect of putting enforce­ ment closer to the users, sort of like police departments returning to the concept of the cop walking the beat.

The closer placement of security enforcement will help with the control of real­ time connections with third parties. Not only do threats exist from employees, but cus­ tomers, vendors, and anyone else with connection to the organization's information assets can violate policy. These liaisons can be responsible for educating these outsiders as well as monitoring and providing enforcement. This works in smaller organizations. Many compartmentalize themselves into "departments" that can participate by assign­ ing one person as a security liaison, especially when working w th people outside the organization.

This, however, is not a perfect solution. Some people who work in this environment for an extended period might find ways to abuse the system and exploit it, for what­ ever reason. One way to combat this is not to allow a person to be the security liaison for more than a short period of time, one or two years for example. At the end of the term, they pass the job to someone else. Another 'fay is to set a policy.of checks and balances. One manageable process is the organization's pro·curement system. Even though most purchases have an approval process, many times those approvals are passed along and paid without further notice. Instead,\_asec'1rity liaisor1 itpi the Accounting

Department should look for anomalies in purchases anq orders shipped.- . • •

* Scanned with OKEN Scanner



Thmc ,\'J,c, ,h"' ,;.ir\'ll\!L' :il"t·mmtmg t 'II nw it j,, not ,111 c.1 y J0b and i\ .l job th,it

, 1111 ,•t bl J,111, 1 \ 1uq ol1\\"ll'.1 he forcmil ;iccountant mmt know the bu inc

*,.x\' \.* n1 tr•JTll't'-, ·cndn, - nl'W l mme . old bu 111c ,. and hm • the money AO\-

ii1r11n h ,hl tirµ.11112:-itt(mal m,Khi1w. u ing thi\ kno vlcdgc. the forcmic :iccouncanr <:J

,"ld 1,1·,,1c,- 01 pu1Yh.1i,c nrder and determine if there arc umm1al purcha cs oralesn h;i: JJIJY md1c:nc an int1.:rnal problem.

Th,· tinal ;irc:i rhat !-hould h:m:-a role in the informati\_on security proccsc;i thesofi

, ·:irL' devdopm nr cydc. \Viiether.ofiwarc is developed mtcrnally or by contractors or

1( tl l o gamzat10n purchase. Commercial Off-The-Shelf (COTS) products, the goal

,b nuld be to build secure sy terns '\\'herein errors or manipuhtions can be trapped. Policy for l·oding and t ring tandard also can a si tin the quality assurance process. l\1o eow·r. ming a paradigm such as survivability (as described in Chapter 2) can form. a ba i • for designing"oftware that does not cause or reveal problems when deployed.

n i riduaI Infonnation **Security Roles**

One \Yay ro ensure that every current and future employee\_or user n ws that security is part of his or her job function is to make it part of each JOb descnpt1on. Spelling Out th,eecuriry function or expectations within the job description demonstrates the *com\_* minnem to information security as well as emphasizes that it is pare of the job. After it is made part of the job description, it becomes something that can be considered in performance evaluations.

Outside contractors, vendors, or other people that provide external services directly on che company's network should include similar language within their SOWs. Aswith employee , thi reinforces the company's commitment as well as makes the contractors' or vendors·adherence ro the organization's security requirements a factor in their qual­ ity-of-service evaluations.

Auditing and **Monitoring**

Aucliring and monitoring are important for enforcement and compliance of security. However, if this is not a role within the business process, there is a danger that it may never be done.Think of this process as the quality control of your information security program.That way, the roles required to provide internal audit of information system comrol will be a natural occurrence and not considered a surprise attack.

ln brcr chaprers, we will talk about the independent review process. For now, however, consider ir a role of someone to arrange and supervise this review.

Understanding **Security Management·and Law**

Enforcen1ent . . . ·

s*I* write this, it is being reported that Microsoft was allegedly hacked by overseas mrruders. News reports are saying chat the hackers supposedly used viruses to plant

**o** Scanned with OKEN Scanner

###### Understanding Security Management and Law Enfo,c men **.35**

Tt\)jan Hor.*e* rograms, h:ickers were able to downloadJVlicroo. ft'sproprietary source

code. . Thrr h:ive.bcrn othei·*r*tamous •mtrus1· ons and manhunts*r*1or h e perpctrJtor .

t

Untnrtunatel '·with the exception of a few high profile cac, most ofthe electronic rr- passers do not get caught.

. Co.mpared\_ to ot.he.r 1·e"so

f]aw en1*c*orce111ent, computer cr·nne and

1·1*r*11ormat·1on

t\_oren ics are 111 then- mfancy. Like in tbe days of the Old Westt, he police today must tace theproblemsthat arise from any new experience. First,there are jurisdictional

concen ,•Thenature of the Internet, multi-national corporations, andthe growth in worl?wideteleconmmting blurs the borders bet\veen states, provinces, countries, and contments. If theyever find the perpetrators of the Microsoft break-in and that person is fromoverseas, under whose laws will they be prosecuted?

Whose Jurisdiction Was It?

In1999c, omputer students in the Philippines wrote a virus that attacked a popular commercial mail pro­ gramthat caused millions of dollars in estimated damages from the cleanup. When the experts traced the messages to the Philippines, the U.S. Justice Department worked with Philippine officials to have the hackers arrested. Justice Department officials claimed that they had jurisdiction over the alleged crimes even though the perpetrators were Philippine citizens on home soil. Philippine officials could not arrest them because there were no laws covering their alleged charges.

The United States does have an extradition treaty with the Philippines, but how effective is it to bring these hackers to the United States to stand trial? Thus far, the hackers have been charged with misde­ meanors and are still in the Philippines. It will take a long time for diplomats to understand the impact of computer crime and the treaties that are necessary to protect national and international infrastructures.

Another problem is understanding how computers impact the law. Although there are a number of laws covering computer crime, they are still writte\_nto conform to a paper-based world. Even though there are examples of how the laws covered the tele­ phone as it evolved, legislators have yet to learn from those experiences, leaving us with a variety of laws.

I am telling you this not to discourage you from working with law enforcement when a crime is committed. On the contrary, I want to prepare you for what will seem like an uphill battle to bring an alleged criminal to justice.The first thing you can do is to know the law. I understand that administrators and security people are not trained

in the law, but there are many resources that can help you understand what kind of protections the law provides (references can be found in Appendix B,C'Resources").

Another important aspect of the law is understanding what is required to prosecute crimes in your jurisdiction. Not only are the laws different across borders, but in the United States, applications of federal laws differ between .the districts of th,e U.S. Courts. Unfortunately, the federal district courts are like fiefdoms; precedents in one do not affect another until ruled on by the Supreme Court.This means you have to understand what the rules are for the district where your case will be handled.

o Scanned with OKEN Scanner



, Pe ,ii 11,1, bl' t •,, ,, t(1 undn·<,t;i11<i wh,'\t it will ukc j<,to a k your loc;1l Jav

t'nf11rcl'n l'!ll , f1lt·1:ik 1·, 11; wry com1non for 1 h ·sic.lcl curit profoi.onah to di,

11

dwn j l:111 w11h J1l)lt(l .rnd prrnccutor.. H( • v r, with the CXC 'ptio11of the Fnr ,,

,Li\"ll:"h the nt1,111al Jnfr;t tructurc l rotcctio11 'c11tcr (NIPC), you may not getcoo

er.1th n t (.Y;m. c the)· m:iy Jh t under. tand ho, to hcl1. p,

[lo 1c e an IP .

The ational Infrastructure Protection Center was formed in 1998 by a presidential directive to sen., .

. . e dS a

resource from hich law enforcement could gain knowledge on how to protect the growing critical .

. rnfor-

matian infrastructures. Although it is a noble concept, there are some who believe that the FBI should

collect and keep this information. Some have even harked back to the days of J. Edgar Hoover keepingnot files on alleged subversives. Should the FBI be involved with collecting this data?

£\!though it has stumbled a bit, the NIPC has provided a lot of good information to law enforcement. The NIP"'s I fraGuard programis designed to bridge the public and private sector to protect information

re ou ce . Itssuccess will depend on the cooperation it receives from industry. To learn more about the NIPC, visi• its web site at [www.nipc. gov.](http://www.nipc.gov/)

The primary area of focus after a crime has been committed is the handling of evi­ dence.As part of your preplanning, learn the rules of evidence. The rules of evidence are the guidelines prosecutors must follow to legally use evidence in court. Use the guidelines to outline policy for handling data, systems, networks, and log files after a crime has occurred. Expand this into clear procedures to accompany the policy to make sure evidence is properly protected. After all, without evidence a prosecutor can use, there can be no case, and the criminals remain free.

## Information Security Awareness Training and Support

After the policies are written, there must be communication among the writers, man­ agement, and everyone in the organization so that all understand the policies and impact. In this final step of the planning process, the planning for training should be considered. It is reasonable to mandate that training be required for anyone with access to company computers and networks. Human !\esources should have complete records, including information on training cours s required·and taken as well as all signed documents showing acceptance of definea' corporate policies.

Management should not only set aside time for training; they should *encourage* it.

One company I was involved with mandated training during specific time periods; and unless employees were involved with a client or **ill,** they were required to attend. The policy allowed the employee to be suspended without pay until he or she attended the

. '

.......

**o Scanned with OKEN Scanner**

Summary **37**



(OtlrSC or watchC'd iL 011 vid • t ,*,r* • l · b · ·

coape. 1ou m1g 1t not want to go to this extreme, ut 1t 1s

,1 - xi \\'.l' t get 100-pnccnt compliance.

Remember v*1*ou ·ire w1•1·t· 1. . .

. • • mg many po 1C1es and customizing them to your env1ron-

!lH.'nt.Tin m. .eans t.ha'.t you c·'11111ot P]an on a"

one-s·ize-fiits-all" tra1·111·11g program. J)jan

11 custom1zm0• tra111111g "S 1·t 1· ] h · d h

;-, ' " e ates to t *e* contents of the policy. Also undcrstan t at

:vero) nedocsnothave to be trained in all areas of the policy-Help Desk personnel,

111

t r •cx:1111ple' do n.otn.

eed to be tt•a•med ·

software development secun·ty polt·c1·cs. As

youpl n yourtr::unmg policies and programs, keep this in mind to ensure that each aspect 1s properly covered.

## Summary

Managementsupport is crucial for a successful information security program. Along withits support is a responsibility to the ongoing maintenance of this program. We emphasizethe responsibilities of management and the roles of those who must provide

enforcement.To have a successful security program, these groups must have a good understanding of their function and be willing to take action. The level of compliance measures this success. Compliance can only happen if everyone knows about the poli­ cies through a comprehensive training and awareness program.

1. Management responsibility:
   * Participate and support an Information Security Management Committee.
   * Information ownership includes assignment of responsibility for informa­ tion asset controls; someone is the designated owner, and the owner deter­ mines sensitivity and classification, including handling variances from generally accepted practices.
   * Devise information security compliance plans for management.
2. Role of the Information Security Department:
   * Policies should state that the Information Security Department is responsi­ ble for establishing and maintaining organization-wide information secu­ rity policies, standards, guidelines, and procedures.
   * This department is responsible for education, enforcement, and protection.

* In outsourcing or use of consultants for information security, set guidelines determining responsibility to work with the in-house Information Security Department.

1. Other information security roles:
   * Regarding the integration of information security into the business process, define the separation of dut es an control over company ass\_e s:

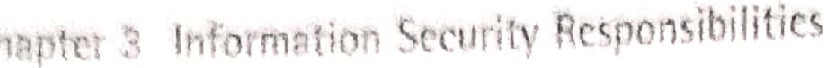
coord•matm•

g e*a*w*-.0* rts wi· th everyone, mcludmg owners of data and facilities.

.. '..

o Scanned with OKEN Scanner





11 ,1,11,1tl' ,1,L'curit\' adininima1n1· for ;ill multi-n ·r 5 '. tern vliilch .

,l , , , , . , r'CCI:f,

t **l;\t** L';\(·11

J I,,-L111,,111 ,• l1tuld have ,111 rnfornwt1011scrnrny !i;i1·.,,on

>'--

111 l

lll " .. •

* + - ])ctt't mine tlwL'curity rcspon,ihilitie forr al-titnc connectior "·

thmi pJrti1.'S.

""lth

* + - * l'vlakc pil ,·ision for a forcmic review of invoice for abnormalPllr- cha cs or.ales.

Place information security rcsponsi ilitiesii jobdecripti ns and inthird\_ parl)· conlTact.,:md consider them m performanee evaluations of both.

1 *c* arding auditino-and monitoring, the internal audit of information

sys-

.. t> . . .

tem -ontrols is a key role mtegrated mto the business process.

Information ownership and custodial responsibilities:

In assi2-riing information ovmership, the Information Systems Depart,,,

;::, ' . . . '"ent

must not be the owner of infonnat1on except that which rs needed for

operations. Ownership should be made using a high-level inventory of information assets.There should be at least one designated custodian reguired for all major information types.

**m** As pare of the security responsibilities of information ownership, define allowed controls and how those controls will be administered. These con­ trols should have guidelines for granting and revoking access to the com­ pany's information and provide recovery capabilities.

J. Understanding security management and law enforcement:

* Understand and know the law and the rules within your jurisdiction.

., Understand the rules of evidence and how to ensure that the evidence is admissible in court.

Ill Preplan the company's responses with law enforcement and prosecutors to understand how to handle data and conduct an investigation after a crime has been committed.

1. Information security awareness training and support:w
   * Training must be required for all workers with access to company comput­ ers and networks. Human Resources should have signed forms saying it is required and another verifying the courses taken by each employee.
   * Management must allow time for training and should encourage it.
   * Training must be customized to the contents of the\_policy.

**o Scanned with OKEN Scanner**