Simplified Security

25 Tips To Help Companies Implement Security

continued ▸

by Ravi Char

Simplified Security: Why Is It Needed?

Short answer: Implementing security prevents or reduces losses due to risks, if risks were to be realized. Security without simplicity becomes an expensive proposition. Simplified security helps to keep the security costs manageable and still provide baseline security.

Long answer: My intent for writing *Simplified Security: 25 Tips To Help Companies Implement Security* is to help a company of any size implement information security in a simplified fashion. On one extreme, there are big companies who spend a lot on information security and don't get much out of it and on the other extreme there are small companies who think they cannot afford information security. I want to reach out to both extremes and advise them that by using simplified security a methodology, they can implement a baseline security level in a prudent budget without unnecessary expenses.

Bonus: Implementing security is not an option anymore. Recent law such as Sarbanes-Oxley mandates internal control of systems. Implementing security will not only reduce the vulnerability, but also help to comply with regulations. Moreover, a good security posture will help to gain the trust and confidence of customers and eventually generate more business.

Making Sense Of The 25 Tips

Provide Strategic Significance To Security	1 Constitute a security team
Understand Where You Are	2 Conduct Security Audit 3 Asset Risk Impact Assessment
Define What You Want To Do	4 Set Realistic Security Objectives
Create Policies	5 Formulate a Security Policy 6 Document Retention Policy 7 Data Backup Policy 8 Proprietary Information Protection Policy
Streamline Personnel Process	9 Sound Personnel Practice
Educate Employees	10 Security Awareness Training
Implement Controls	11 Implement Change Management 12 Implement Data/Document Classification 13 Implement Identity Management

Security Operations	14 **Incident Response Team** 15 **Vulnerability Management Team**
Secure Core (Widely Used) Applications	16 Implement Anti-spam (secures e-mail) 17 Implement Anti-Virus (secures desktop) 18 Instant Messaging Security 19 Implement Web Security 20 Domain Name Service Security
Secure Other Applications And System	21 Implement Application/System Security
Secure Entry/Exit Points	22 Remote Access Security 23 Perimeter Security
Secure Operations	24 Implement Operations Security
Secure Physical Location	25 Implement Physical Security

#1 Constitute a Security Team

Most of the start-ups do not have a security team. The rationale is, if the company is small there is no need for security: contrastingly, the smaller the company, the higher the risk of competitive threat due to loss of proprietary information. Smaller companies are ill equipped to handle security incidents which make them even more vulnerable.

Companies, large or small, need to have a single point of accountability for security. It is a good idea to constitute a security team consisting of core team members whose job is full-time security and also other cross-functional members. The security team should be headed by Chief Security Officer (CSO) who reports to CIO. The CSO is accountable for security in the company. The other alternative is to make the CSO report to the CEO which can vest higher power and leverage to the CSO and hence the CSO can implement security without being biased by the CIO's office.

Benefit: Single point of accountability.

Thought: Should venture capital firms fund a start-up company without security team?

#2 Security Audit

Performing a security audit even before setting a security objective is a rather new concept. My point is: without knowing where we are right now, how can we make decision on where we want to go and what we want to become? Moreover, the results of the audit can provide "points to ponder" and can help us set near realistic objectives.

It is a good idea to be audited by a third party. Also, combine compliance audit and security audit. By looking at the results of compliance audit and security audit, we can align security audit items along the line of compliance in order to gain synergy.

Last but not the least, an audit is a repeatable event. Audit should be performed at a frequency determined by the risk profile of a company.

Benefit: Company will know where it stands in relation to its security.

Thought: Is risk the only determining factor for the frequency of audit?

#3 Asset Risk Impact Assesment

This consists of three distinct phases.

1. **Asset Assessment:** In this phase the business unit leaders rank the priority of their business unit assets. They also estimate the maximum tolerable downtime for each asset. Using this data from various business units a company wide asset priority table is created.
2. **Risk Assessment:** Risk is a possibility that a threat will exploit vulnerability. The word s risk and threat are used interchangeably. In this phase, risks and threats that affect our prioritized assets are identified.
3. **Impact Assessment:** This is a phase where we measure the likelihood of risk being realized on an asset. If the risk event is realized once, then the loss is Single Loss Expectancy (**SLE**). If the risk event occurs at an Annualized Rate of Occurrence (**ARO**), we can compute the Annual Loss Expectancy (**ALE**). For a risk/threat event to happen vulnerability has to exist. A safeguard is countermeasure which removes vulnerability

and protects against one or more specific threats. The thumb rule is the annual cost of safeguard should not exceed the annual cost of asset loss!

There are five ways to react to a risk or threat: **1. Reduce**: implement safeguard to reduce risk; **2. Assign:** buy insurance; **3. Accept:** accept the consequences, make sure to document it! **4. Reject:** deny that risk exists; and **5. Transfer:** outsource the asset and hence risk.

Here is a sample worksheet for Asset Risk Impact Assessment.

Benefit: Ballpark cost of security budget is known and, hence, the company can allocate its budget wisely.

Thought: Under what circumstances is assigning the risk is a good idea?

#4 Set Realistic Security Objectives

Data from the security/compliance audit and approximate security budget cost from the asset risk impact assessment puts us in a strong position to set our security objectives, realistically based on our security context and budget. Once the list of objectives is set, we also need to make a decision on whether we need a **B**usiness **C**ontinuity **P**lan (BCP) and a **D**isaster **R**ecovery **P**lan (DRP). BCP involves assessment of risks, creation of policies, procedures to minimize impact of those risks on the organization if the risks were realized. DRP outlines the steps that an organization executes to resume normal operation after disaster strikes. BCP needs to be implemented to minimize the impact of those assets (which includes personnel) in an asset impact assessment. Not all assets will need a BCP. A company should identify the criticality of an asset and then decide if it really needs BCP. By being selective about assets that need BCP, significant cost reduction can be achieved.

DRP is where most companies overspend. The answer depends on the company's context. The key answer here is "maximum tolerable downtime". If a company can stay down for a month without significant impact — why spend money on a dedicated hot backup site? A prudent approach would be to have a reliable backup strategy of existing data and a plan to recover the data on duplicated servers within the specified time frame. There is no rule that every company needs a DRP. If a company is nimble enough they can always relocate to an area prone to fewer disasters if the cost of DRP is too high. By staying focused on critical assets a company can realize significant cost savings in DRP.

Benefit: Company will prudently spend on these high ticket items based on their security needs.

Thought: Can a disaster recovery plan be considered part of a business continuity plan?

#5 Formulate a Security Policy

One of the definitions of security policy from RFC 2196 is: "A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide." Now that you are aware of your objectives from Tip #4, it is much easier to set a security policy within the framework of your needs. A good policy should make sense, should be easily understandable and should *align* with company's overall business goals. There are three types of policies: Regulatory — mandated by legal requirements, Advisory — Acceptable practices and consequences of violation, Informative — Not enforceable, provides information.

A good policy (some of these are borrowed from Cisco) should contain: statement of authority and scope, acceptable use policy, identification and authentication policy, internet use policy, corporate network access policy, remote access policy and incident handling policy.

Policy is very powerful because it is a tool you can use to reduce the security cost. As an example if the cost of implementing instant messaging security is too high, we could have policy disallowing the use of instant messaging which literally costs nothing.

Benefit: Provides a framework to implement security.

Thought: Without a policy, can a company be legally empowered to pursue a lawsuit against an employee for misuse?

#6 Document Retention Policy

The term document is generic to include e-documents such as e-mail and web pages. The key drivers for document retention policy are:

1. Policy can provide a basis of legal protection. If a company does not have a schedule of document retention and destruction and if the opposing pursues a legal case against the company and accuse the company of selective, willful destruction of documents and hence evidence: the company is highly likely to lose the case.
2. A schedule of document retention and destruction can help prevent damaging documents becoming available for future litigation against the company.
3. Sarbenes-Oxley (SOX) Section 802 imposes criminal penalties which includes fine or imprisonment for not more than 20 years, or both.

Some guidelines for document retention program are:

→ **Industry standards** — Get inputs from others in similar trades about the retention time frame;

- → **Governmental requirements** — As an example, the IRS can audit tax records for up to seven years;
- → **Possible litigation** — If a company foresees a possible litigation, documents relevant to that litigation should be preserved for a reasonable time period;
- → **Cost of retention and destruction program** – Pros and cons of spending too much money on the document retention and destruction program vs. risks if this is not done.

Benefit: company has a valid legal defense against accusation of willful destruction of document and helps to conform to one of the section 802 of SOX requirements.

Thought: What is an additional step that needs to be done before destroying a document?

#7 Data Backup Policy

Data storage device failure and data corruption are fairly common. The lost data can severely impact a company's existence as a going concern and can result in bad publicity for the company. If critical customer data is lost it could result in a potential lawsuit against the company.

The **first step** in creating a backup policy is identifying the data that needs to be backed up. It is important to perform this step because it can reduce the amount of data to be backed up and hence the cost of the back up. This step also helps the company to classify the type of data (i.e., whether it is a database or flat file: if this is a database backup, whether it needs a hot backup or a cold backup). The **second step** is to determine the frequency of the backup: this depends on how frequently the data changes. The frequency of the backup determines the granularity of the data recovery point. In general, backup is accomplished by

suitably combining incremental backup and full backup. There are many backup schemes such as “Tower of Hanoi”, “Grandfather/Father/Son” and so on. Choose the scheme that works best for you. The **third step** involves identifying an off-site storage location for the backup tapes and the associated logistics involved in the off-site storage and retrieval. Make sure that the off-site location is not very close to the data location; this will expose both the locations to similar disasters and defeats the purpose of the off-site storage.

The **last step** is to publish the backup plan so that customers can properly set their data recovery expectations right.

Benefit: Company can rely on backup data in case of data loss, data corruption or a disaster.

Thought: When is a good time to run a backup job?

#8 Proprietary Information Policy

There is no use in classifying documents unless we educate employees about how to handle proprietary information. Companies need to have a widely published Proprietary Information Protection Policy (PIPP) which outlines the information protection requirements, some of them are:

1. Identify PIPP team members who are responsible for driving this policy.
2. Regular audit by PIPP team members: as an example, walk by employees’ desks during non-business hours and identify any unattended confidential information on the desk; then notify the employee of PIPP violation and advise them to be more careful. Educate employees about importance of tagging documents as confidential or under appropriate classification level and also educate them about the proper procedure for handling proprietary documents.

3. Install separate printers for printing confidential documents and/or making sure confidential document print-outs are not left unattended in the general print area. Install a document shredder or a bin for the purpose of disposing confidential documents.

The bottom line of PIPP is to educate employees about the importance of handling confidential documents, making them aware of the ramifications and tracking violations of the policy.

Benefit: Employees are educated about handling proprietary information.

Thought: Can PIPP help minimize threat of social engineering?

#9 Sound Personnel Practice

The majority of threats are internal. Employees often knowingly or unknowingly leak proprietary information. Imagine for a moment – confidential data is in the hands of a disgruntled employee. To lessen the chance of data leaks, sound personnel practices must be initiated. Some of the sound personnel practices are:

- **Job description** — This is the first step in the hiring process. Make sure to classify the security level of the job (i.e., whether the job warrants exposure to critical data).
- **Background checks** — Make sure you hire good people by running background checks on them. Moreover, hire people who have the appropriate security clearance with respect to their job classification.
- **Roles and responsibilities** — Determine employees' access profiles based on their roles and responsibilities. Don't grant them access to more data than what is necessary to get the work done.

→ **Cross training and job rotation** — Cross train employees so that there is no single point of reliance. By rotating jobs you can prevent collusion, information hiding and cheating.

Sound personnel practice does not mean we distrust employees; it means being selective about whom we trust and believing in the processes that can help expose trust violations.

Benefit: Company can minimize internal threats.

Thought: Why is a mandatory vacation for employees a good idea?

#10 Security Awareness Training

Social engineering is defined as the art and science of getting people to comply with your wishes. A simplistic example is to call up an employee, pretend to be an administrator and mention that there are problems with his account. Then ask for his password and the user will typically comply with the password request. What is the use of having the state of art firewall, if you have an employee who is ignorant enough to give out password of a critical system over the phone? The goal of Security Awareness Training (SAT) is to make sure that employees are educated about the company's security program.

Some of the key things that need to be communicated in SAT are: the importance and relevance of security policies to employees and ramifications of its violation, good and bad security practices, how employees can help to make security program a success and how to report security violations.

It is important publicize the security program extensively (for example, with flyers) and also to keep employees in the loop about changes in the program. SAT will provide a good frame-

work for the doing this. SAT should be designed to accommodate a non-technical audience or it will dilute the purpose of SAT.

Benefit: Company will have employees who are conscious of security and will act as a catalyst to implement security. This will also minimize social engineering security threats.

Thought: When is a good time for new employees to undergo SAT?

#11 Implement Change Management

Security is a function of configuration. Configuration in simplistic terms is a snapshot of the arrangement of various things in an infrastructure. For example, in a collection of servers, if one of the servers is upgraded, the upgrade task, however simple it may be, could have far reaching ramifications — good and bad. The objective of the change management mechanism is to minimize any bad ramifications. The change management mechanism not only keeps track of changes to the existing configuration, but will also enable a company to roll back the changes if there are any problems.

The change management mechanism should keep track of: date/time of change, duration of change, description of change, business owner of change, resources needed to implement change, systems/application affected, rollback procedure, list of approvers for change, security ramifications, and justification for change. Depending on the company's needs, there can be other things that the change control mechanism keeps track of.

The change management mechanism can be simplistically implemented as a web-based application. It is a good idea to follow up the change control by a postmortem report. Any change that bypasses the change management mechanism should be discouraged and dealt with appropriately.

Benefit: Company has a trail of changes that have been effected on its configuration.

Thought: Which division head is a mandatory approver for the change request?

#12 Implement Data Classification

Not all data is confidential; some is more confidential than others, some is for private use and some for public consumption. There are some general tips to help classify data: usefulness, timeliness, value, age, lifetime (or when it expires) of data; data disclosure/modification damage assessment, who has access/restriction to data and national security implications of the data

These are the typical business/private sector classification of the data or document:

- → Confidential — Highest level, used for data that is extremely sensitive and for internal use only. A significant negative impact could occur for company if confidential data is disclosed.
- → Private — Used for data that is of private or personal nature and intended for internal use. A significant negative impact can occur for the company or individuals if private data is disclosed.
- → Sensitive — Negative impact could occur if the data is disclosed.
- → Public — Disclosure does not have serious negative impact on organization. Also, the default classification bucket for data which does not fit the above categories.

Declassification is a process of changing the classification category of data or document: If a data or document no longer warrants the current protection level, it should be classified into a different level.

Benefit: Company can prioritize and allocate required security resources to protect data or documents according to classification.

Thought: Why is declassification very important?

#13 Implement Identity Management

Identity Management (IM) is managing user and group accounts. Identity management has three components: authentication, authorization and accounting. Authentication is who you are and authorization is what you can do. IM involves making sure that the proper authentication mechanism is in place and a proper authorization profile is set. There are multiple approaches for authentication: Single-factor authentication known as weak authentication is based on something you know (example: login and a password). Two-factor authentication known as strong authentication is based on something you know plus something you have (example: an ATM card). It is a good idea to use two-factor authentication since it is considered harder to break than login/password which is considered as a one-factor authentication.

A user having authorization to all the systems is not good either. A user's authorization profile should be set based on the user's clearance level. The authorization profile should be mostly set on a need-to-know basis. Group accounts are very risky to have. It is a good idea to minimize the use of group accounts. Other critical aspects of IM include account and password expirations. It is critical to audit user accounts on a regular basis. An active user account which continues to exist even after the user has left the company is not desirable. Accounts should be forced to change passwords on a regular basis. There has to be a mechanism to enforce users to choose a strong password. Last but not the least, all the authentication and authorization attempts should be logged, this is also known as accounting. Accounting provides the audit trail.

Benefit: There is an authentication, authorization and audit trail for users.

Thought: How do you determine the authorization profile for a user?

#14 Constitute Incident Response Team

Many companies are not prepared to handle security incidents. They try to mobilize resources to respond after the incident has happened; this type of panic mode response is not desirable. An incident response team consists of team members drawn from cross-functional teams. The incident coordinator should be a well-seasoned security professional. The team members are well experienced with handling security incidents. The team should set up a preexisting relationship with the legal department, public relations department and law enforcement officials. This preexisting relationship will ease the communication process during the security breach incident. As soon as a security breach incident is encountered, the team members group together and formulate a strategy for responding to the incident.

The incident response team has to: assess the tangible and intangible damage due to the incident, identify remedial actions such as patching the systems, assess whether the incident can cause in loss of faith or goodwill of customers, investigate the root cause of incident, decide whether to involve law enforcement officials, formulate a suitable public relations campaign about the incident, identify legal and compliance ramifications of this incident and lastly, keep senior management updated about the status, seek their opinion when needed and so on.

Benefit: Company is well-equipped to handle any security breach incident.

Thought: Who makes the decision whether to make the incident public?

#15 Vulnerability Management Team

Threat agents take advantage of vulnerabilities. Almost everyday new vulnerabilities are detected and some of the vulnerabilities are serious in nature. If these vulnerabilities are not addressed in a timely manner it will result in a threat event: which means threat agents take advantage of vulnerability. The Vulnerability Management Team (VMT) provides proactive vulnerability mitigation. Some of the typical tasks of VMT are:

- → Pro-actively monitor vulnerabilities, for example tracking the latest CERT advisory.
- → Work with application and system owners to make sure that vulnerabilities are addressed in a timely manner.
- → Make a decision about whether and when the vulnerability needs to be addressed and identify ramifications of addressing the vulnerability.
- → The VMT is a very important part of the security program. A system which may be secure today will not be secure tomorrow without the VMT.

Benefit: Company has a mechanism to act on newly discovered vulnerabilities and generate suitable action to mitigate the same.

Thought: How do you make a decision on whether to address vulnerability?

#16 Implement Anti-Spam for Email

Spam refers to unwanted or junk emails. Spam is one of the mechanisms by which viruses enter. Spam is also a major source of phishing which dupes gullible users to give out their private information.

Spam control can be implemented in many ways. The simplest mechanism is a spam filter at the user mailbox. This method of spam control is inefficient because it depends totally on user's ability to create an efficient spam filter rule. Centralized spam prevention software is another mechanism of spam prevention. An even more popular mechanism is to use a centralized spam prevention appliance. Another option is to outsource the spam prevention to an external vendor: inbound emails to the company go through the outside vendor gateway where the spam gets filtered and the resulting clean emails, which are free of spam, reaches the company. The type of spam control mechanism that a company chooses depends on its needs.

By implementing spam control, a company can not only prevent viruses from entering, but can also save valuable employee time which would have otherwise been wasted in sifting through their mailbox. It should be noted that spam is a type of Denial of Service (DOS) attack. Too many spams sent to a mailbox can overwhelm the user mailbox, making it harder to read legitimate emails and thus causing DOS.

Benefit: Company will prevent an attack vector for viruses and prevent other forms of attack such as phishing.

Thought: How can user awareness help keep users from being a victim of spam emails?

#17 Implement Anti-virus for OS

Computer viruses are a universal problem. A virus is defined as a malicious and destructive program designed to be passed unwittingly from machine to machine via floppy disks, downloading or other means. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself.

Anti-virus software must be installed on every user's computer and should be manageable from a centralized console. The anti-virus software should be programmed to run once every week or month in order to update new signatures and to scan for any virus signatures it missed since the last update. It is a good idea to schedule the anti-virus software to run on user's desktop during work hours or else most of the desktops may miss out the scanning.

Anti-virus software should be installed on production systems, too. It is a good idea to ensure that the anti-virus software will work smoothly with various other applications without affecting the performance of production systems. It is advisable to run on-access virus scanner on production systems; an on-access scanner will check for a virus in a file as soon as the file is accessed. Routine audits must be performed to make sure that all relevant production systems run anti-virus software.

Benefit: Company can save money by minimizing and/or preventing system and/or user downtime.

Thought: Is a two-tiered anti-virus solution a good idea?

#18 Instant Messaging (IM) Security

Security is as strong as the weakest link. Many corporations spend tons of money securing their applications, hardware, and infrastructure, but they forget to focus on seemingly trivial applications like IM. IM users can send: unencrypted information, share files, share their on-line status and send audio/video with users across the Internet. This makes IM one of the most popular entry points for threats. Many companies use a corporate version of messenger called enterprise messenger which works only within the company and not across the Internet. There are other vendors who make IM gateway managers which sit behind

the firewall and administer IM traffic. There is also a hybrid enterprise messenger solution which works not only within the company but also across the Internet.

There is no one right answer about how to secure IM in a corporate setting. These are some things that corporations can do to secure IM. **Policy** — have a policy about IM usage. **IM gateway** — implement IM gateway to help log, monitor, and administer IM traffic. **File sharing** — block file sharing through IM. **Audio/video** — block audio/video through IM.

At the near end of the spectrum, deploy an enterprise messenger solution which allows messaging only within the company. At the extreme end of the spectrum create a policy which disallows IM usage.

Benefit: Company has secured one of the most overlooked channels of threat.

Thought: Can IM be subject to spam?

#19 Implement Web Security

Even though web security can be addressed under the umbrella of application security, the pervasiveness of web applications and its vulnerabilities prompted me to dedicate a separate section. Web applications are one of the most exploited classes of applications. The very nature of being available over the network on a standard port makes it even more vulnerable. There are some tips for implementing web security:

Web Server Configuration: Keep your web server updated with the latest patches. Disable directory listing from your web server. Disable web server modules that are considered to pose a security risk. Audit the CGI or other scripts for any vulnerabilities before they are allowed to run on the web server. Run the web server in chroot jail and also make sure to run it under a non-privileged ownership such as nobody. Implement secure socket layer web server wher-

ever possible. Make sure to use certificate from a trusted vendor and do not use self signed certificates for production web servers.

Web Server Architecture: Implement a reverse-proxy or a load balancer to protect the real web server. Use network address translation to protect the real web server IP address. Implement high availability architecture through load balancing.

Benefit: Company is protected from one of most popular attack entry points.

Thought: Why do many sites allow some configuration setting on the web server even when the recommended setting is off?

#20 Implement Domain Name Service Security

Domain Name Service (DNS) is the glue that binds the Internet. DNS maps Internet Protocol (IP) addresses to user friendly names. The simplicity of DNS architecture makes it vulnerable to attacks. Messing with IP address to name mapping is known as DNS spoofing; this is relatively easy to do and makes DNS vulnerable.

These are some actions that we can take to protect DNS. **Avoid spoofing by encryption** — encrypt data transferred between master and slave servers: use a shared secret or RSA to encrypt data. **Restrict zone transfers** - confine it to trusted and known servers. **Don't list your private IPs of your zone** — disable ls query which lists all the servers in a particular zone. **Isolate internal DNS servers from external DNS servers** — use split horizon DNS architecture which in layman term means use two DNS servers: Internal DNS servers for intra-company query and to relay non-intra-company query to external DNS server. External DNS servers to service outside-world originating query for the zone's public IPs and to service the recursive non-intra-company query from the zone's internal DNS servers. The Split

Horizon DNS can be implemented with a single DNS server in BIND 9.x using views, but it is not recommended to use a single DNS sever serving intra-company and outside-world query at any cost. **Prevent outside-world induced recursive query attacks** — disable recursive query on the external DNS servers for outside-world originating queries. **Update/patch software** — use recent version of BIND. **Configure your firewall** – to log, monitor, and administer DNS traffic. **DNS registry check** — last but not the least, monitor your DNS registry at the root (i.e., perform a whois lookup regularly and make sure it returns the correct data).

Benefit: Company has protected one of the most vulnerable attack vectors.

Thought: Why are there only 13 root name servers?

#21 Implement Application/System Security

If a company wishes to move towards true end-to-end security, it has to focus on the application and the system on which the application runs. It's useless to have a secure system if the application that runs on it is vulnerable and thus provides an attack vector vice-versa. Some of the questions that need to be raised for application/system security are: Has the application/system been penetration tested? What is the failure mode of application/system (i.e., fail-safe or fail-open)? Are there any serious vulnerabilities in application/system that needs to be patched and whether the patch is up to date? What ownership does the application run as? Does it run as a privileged user, if so why should it run as privileged user? Does the application/system connect to the Internet? Does the application/system work well with anti-virus software? Does the application run on a hardened system? Does the application or system have access to confidential or proprietary data?

Answering the above questions will provide data points to work on to implement application security. As an example: if the application does not run on a hardened system then the

system needs to be moved to a less secure state in order for the application to run. This is a risky decision and a careful risk/benefit analysis needs to be done before taking such a decision. Security in general is a delicate dance. There is no one right solution. A company must choose a security posture that best suits its risk profile and maximizes the company's ROI savings.

Benefit: Company's application and the system on which the application runs is free of vulnerability

Thought: What are the ramifications of patching or hardening?

#22 Remote Access Security

Any external connection to your corporate network is an entry point for vulnerabilities. Virtual Private Network (VPN) is a technology that evolved to address the secure remote connectivity solution. There are many protocols that implement VPN and some are built into the OS. There are multitude of VPN protocols such as IPSec (Internet Protocol Security), PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) and SSL (Secure Socket Layer). If there are too many VPN users, dedicated VPN hardware is a choice. IPSec is a good protocol of choice since it is supported by many VPN vendors. IPSec provides stronger encryption than PPTP and L2TP. IPSec VPN is a good choice if the remote client base is large. IPSec can be used to tunnel data securely across two different locations. If there are less users (the processing overhead is less), SSL VPN is a good option. SSL VPN has less maintenance overhead (i.e., remote clients do not need any additional software installed). It works through the web browser. The advantage of SSL VPN can turn out to be disadvantage since users can connect from any unsafe computer which has a browser installed.

Here are some tips for remote access: always provide a secure access and use VPN technology rather than POTS dial-in; if you have large remote client user base IPSec is a preferred protocol of choice; if you want less staff maintenance overhead and higher remote client flexibility use SSL VPNs. It is good practice for VPN policy to include anti-virus, firewall checks on the remote client in addition to authentication.

Benefit: Company can ensure that employees connect securely to the corporate network and that they do not introduce vulnerabilities into the network.

Thought: How do you arrive at the optimal VPN policy?

#23 Implement Perimeter Security

The perimeter is the entry and exit point of Internet traffic of your corporate network. Gone are the days when an access list on the border router prevented undesirable traffic. Welcome to the world of viruses, worms, trojans and denial-of-service. Some tips for perimeter security are:

- → Implement committed access rate on the ISP router. This can prevent DOS originating from the Internet to certain extent.
- → Implement RFC 1918 and RFC 2827 filtering on the edge router, this prevents IP address spoofing. RFC 1918 filtering prevents packets with private IP address as source address being routed to the Internet and blocks packets with private IP address as source address coming from the Internet. RFC 2827 filtering prevents packets with non-inside source IP address going to the Internet and blocks packets with inside source IP address entering from the Internet.

- → Implement inline firewall which can police traffic. Inline means active listening and blocking mode. Firewall with application level filtering capability is recommended. A series of two firewalls from different vendors is recommended.
- → Deploy the public servers (external SMTP, external DNS and external WWW) in a separate zone called demilitarized (DMZ) zone. This zone has lesser security level than the private network.
- → Implement Intrusion Detection System (IDS) or Intrusion Prevention System (IPS). IPS operates in inline mode. If you are co-locating your servers at ISP, make sure their perimeter is secure before you co-locate. If you have a remote office, make sure you connect to them only through VPN, same applies to remote users.
- → Use Network Address Translation to mask the internal IP address.

Benefit: Company has a mechanism to police traffic that exits or leaves the corporate network.

Thought: What does SPAN mode connectivity for IDS mean?

#24 Implement Operations Security

Operations security can involve anything from system architecture to change control. For the purpose of this document, operations security involves three distinct parts: production system architecture, production system integrity and lifecycle management of application/system.

The production system architecture should be designed robustly. The recommended solution is a high availability architecture where members operate in either a clustered or load

balanced fashion. The high availability architecture makes system less vulnerable to threat events. If a threat event has occurred on one or more members, there are other members that continue to handle the requests. The architecture should also encompass a continuous monitoring and alerting mechanism in case of failure of any one of the components.

Production system integrity can be maintained by using a change management mechanism. No changes should be allowed on the production system unless it passes through change management.

Lifecycle management of a system/application should be performed with security in mind. When software or the system is upgraded, it is critical to assess the security impact of such an action. It is recommended to integrate security specification in the development and testing of the system and application. By doing this we can make sure that robust system and applications are released to the production environment.

Benefit: Company has an operational framework that is robust and is not vulnerable to threat agents.

Thought: Should penetration testing be a part of product testing?

#25 Implement Physical Security

No amount of technical controls can provide adequate security unless the physical environment of the company facility is well protected. Imagine, if someone could walk into the company office and walk away with a proprietary document, the ramifications could be tremendous.

Physical security can be divided into three parts. **Administrative** — this involves facility selection, site management and personnel control. **Technical** — this includes fire detection,

suppression, intrustion detection, CCTV, HVAC and smart/dumb access card. **Logical** — this includes fencing, lighting, locks, guards and dogs.

To implement a good physical security we need permutations of the various above components. It is a good idea to design a facility that houses the IT infrastructure with security in mind rather than implementing security as an afterthought. If designing is not an option, select a site that meets most of your security needs.

Some of the physical security controls that are mandatory are smart/dumb access card to facility, HVAC and CCTV. It is a good idea to have a guard to monitor the facility around the clock, if the company can afford it.

Benefit: Company will eliminate another major source of security threats.

Thought: What is the most important objective of physical security?

Looking for more?

I have continued to blog on simplified security. There are more than the above mentioned 25 ways to secure your company. Here is the link if you want to see what the latest on the same topic is: http://ravichar.blogharbor.com/blog/SimplifiedSecuritySecurity101

You can also read my musings about information security at: http://ravichar.blogharbor.com

info

ABOUT THE AUTHOR

Ravi Char is a Silicon Valley based Senior Information Security Professional. Ravi has over twelve years of experience in the IT industry. He has over six years of experience in the area of security. Ravi has proven ability to implement creative, cost effective, scalable security solutions on time and within budget.

At his current company Ravi is responsible for web systems architecture, security and PKI management. Ravi is also an advisor for a SOX startup company. Ravi is a CISSP. Ravi has numerous other certifications such as: Cisco Certified Security Professional, National Security Agency Certification, Project Management Certification from UC, Berkeley, Sun Certified System/Network Administrator. Ravi has a BS in Electrical Engineering from University of Mysore and MBA from San Jose State University. Ravi has a blog: "Musings on Information Security" at the URL: http://ravichar.blogharbor.com.

DOWNLOAD THIS

This manifesto is available from http://changethis.com/20.SimplifiedSecurity

SEND THIS

Click here to pass along a copy of this manifesto to others.
http://changethis.com/20.SimplifiedSecurity/email

SUBSCRIBE

Learn about our latest manifestos as soon as they are available. Sign up for our free newsletter and be notified by email. http://changethis.com/subscribe

info

WHAT YOU CAN DO

You are given the unlimited right to print this manifesto and to distribute it electronically (via email, your website, or any other means). You can print out pages and put them in your favorite coffee shop's windows or your doctor's waiting room. You can transcribe the author's words onto the sidewalk, or you can hand out copies to everyone you meet. You may not alter this manifesto in any way, though, and you may not charge for it.

NAVIGATION & USER TIPS

Move around this manifesto by using your keyboard arrow keys or click on the right arrow (→) for the next page and the left arrow (←). To send this by email, just click on  .

HAVING PROBLEMS SAVING TO DISK?

First, make sure you have the latest version of Acrobat Reader 6 which you can download from http://www.adobe.com/products/acrobat/readstep2.html. If problems persist, it may be due to your Acrobat Reader settings. To correct the problem (for Windows), a reader, J. Hansen, suggests going to your Acrobat Reader Preferences > Options > Web browser Options. Check the "Display PDF in Browser" option. Then click on Save to Disk  .

KEYBOARD SHORTCUTS	PC	MAC
Zoom in (Larger view)	[CTL] [+]	[⌘] [+]
Zoom out	[CTL] [—]	[⌘] [—]
Full screen/Normal screen view	[CTL] [L]	[⌘] [L]

info

BORN ON DATE

This document was created on 14 December 2005 and is based on the best information available at that time. To check for updates, please click here to visit:http://changethis.com/20.SimplifiedSecurity

ABOUT CHANGETHIS

ChangeThis is a vehicle, not a publisher. We make it easy for big ideas to spread. While the authors we work with are responsible for their own work, they don't necessarily agree with everything available in ChangeThis format. But you knew that already.

ChangeThis is supported by the love and tender care of 800-CEO-READ. Visit us at main site www.800ceoread.com or at our daily blog blog.800ceoread.com.