

# Information Security Checklist

## “Protecting Your Information Assets”

Cris DeWitt, CISSP - Jeff Kopp, MCP, DCSE

### Introduction

Securing your sensitive data, intellectual property or even personal identity can be a daunting task. Doing a good job can lead to increased operating efficiency, while leaving potential vulnerabilities unaddressed can lead to poor public opinion, decreased operating efficiency, even bankruptcy. With every day, you have more threats announced, more vulnerabilities exposed and more solutions to evaluate. So where do you begin to secure your information assets?

This whitepaper and checklist will help guide you through the process of securing your information assets. More importantly, it will highlight that security is not a one-time implementation, but rather an on-going process. Protecting corporate information assets today requires 24x7 monitoring, maintenance and response. Keep in mind that while implementing some of the items below may raise your security posture, a comprehensive security plan of action is required to significantly reduce your risk of attack.

### First, and Foremost – Policies

At the heart of EVERY good security implementation are effective, well-written, thorough policies. Policies provide numerous functions. They set the expectations for your employees (PC users) on what is and what is not acceptable use of the corporate computer systems, as well as document your internal IT processes. These pre-defined expectations and processes can protect your organization from a whole slew of issues, including, but not limited to:

- Sexual harassment lawsuits initiated by your own employees after receiving numerous offensive spam emails (the precedent HAS been set).
- Wrongful termination lawsuits following unacceptable PC usage by an employee
- Regulatory compliance issues
- There are MANY more ....

You don't need to hire a team of lawyers to write your policies so only lawyers can understand them, but you do need policies and you do need to be clear and thorough. Start with a good template. Many of these can be found online. Make your first stop for sample policies <http://www.sans.org>.

Like your entire security plan, policies are dynamic. Security threats and laws do change, so should your policies. As your policies change, your user base needs to be kept aware of these changes. Which policies you will need varies greatly, depending on your industry and corporate responsibilities, but at a minimum, consider keeping the following on file:

- PC Acceptable Use Policy
- Email Use Policy
- Web Usage Policy
- Password Policy
- Data Retention Policy

Don't forget, once you have your policies developed, you need to train your users on these policies and have them sign documents stating that they have read and fully understand them.

## Layered Security

Many organizations think that if they have a good external-facing firewall, they are secure. Nothing could be further from the truth. With threats coming from both internal AND external, a good firewall at the perimeter is just the beginning of a secure IT posture.

Think of security in your organization as an onion. An onion has multiple layers, so even if attackers breach your perimeter, they do not get to your confidential information. Maybe an attacker succeeds at getting an infected attachment to one of your user's email boxes and that user unknowingly double-clicks the attachment. The attacker just got past your firewall and through your email filters, but, hopefully, there are many more layers of security before the attackers hit paydirt, your sensitive data. Suppose the program embedded in that malicious email attachment is prevented from doing anything else it wants. It cannot install onto the PC because the OS is hardened and the logged in user does not have the privilege to install programs. Maybe the outbound ports it needs to communicate back to the attacker and receive further instructions are blocked at the firewall. Maybe the user has Read-Only access to the registry so the program cannot auto run itself every time the user reboots. All of these layers increase the resistance the attacker would encounter to steal your private data. Most attackers are looking for easy wins (unless they want specific data from a specific company) and will take the path of least resistance to get data they can use to their advantage. The more layers of security your organization has, the more resistance the attacker encounters, and the less of a target your organization becomes.

## Managed Security

So, you have all the latest and greatest security hardware installed and configured, you have a security company performing quarterly penetration tests, and you have all of your employees aware of all of your expertly written policies. How secure are you?

You simply cannot know how secure you are unless you have someone or something quantifying your security level. One of the best ways to quantify your level of security is to gather the access and system logs for ALL of your critical and security-related systems. But then, you have to read every entry in those logs and determine if those entries are security related or not. If they are security related, you have to respond quickly to mitigate the risk. For small organizations, this could require headcount costs that a small company simply cannot afford. For larger organizations, it may simply not fit into their core competency, and be cheaper to outsource. For these purposes, there exists the Managed Security Services Provider (MSSP). A MSSP can aggregate ALL of your critical system logs (down to the desktop logs if you wish), filter the security related events and show you your real-time security posture as well as archives of your posture over time. If an incident does happen, these MSSP's can even remotely access your critical systems to prevent further attack or take actions to prevent the attack of zero day threats that they have identified for you.

## Putting It All Together

Today's networks are vastly different from those of just a few years ago. Today, functionalities including VPNs, on-site email/web/application servers and the increased use of the Internet for critical business tasks have opened up countless vulnerabilities. Addressing these vulnerabilities requires constant vigilance.

Reviewing, re-writing and implementing policy changes takes diligence and time, but is an absolute requirement if you intend to take advantage of today's Internet-connected information systems. Most organizations simply do not have the man-power, budget or expertise to thoroughly create AND maintain their own Secure Posture. You don't monitor your own fire alarms, do you? Managed Security Service Providers can automate tasks and services and provide 24X7X365 real-time visibility into an organizations security posture; a task that would normally consume a full-time IT department of

roughly 5 dedicated human resources. The more obstacles, or layers of defense, an attacker encounters, the less likely your organization is to be a victim of their attacks.

## The Check List

The following check list should serve as a starting point only. It is, by no means, complete for any given organization. It is intended to be rather vague to fit into the majority of organizations; tailor it as needed for your environment. This checklist should evolve as you discover steps that help implement YOUR secure network.

## Policy Development

- Key policies identified – acceptable use, remote access, information protection, perimeter security, baseline host/device security...
- Affected parties are identified.
- Policy development team is identified.
- Policy design process is drafted.
- Policy review “board” is identified.
- Approvers of policy are identified.
- Key policies are developed.
- Procedures are defined for each policy stating how policies are enforced.
- Policy implementation plan is created.
- Support staff affected by policy has reviewed the policy.
- Signature acceptance of policies by all employees.
- Policy refresher overview courses are offered at least once per year to all employees.
- Policies are updated with audit/review recommendations at least once per year.

## Awareness Training

- Policies are complete, documented, and accessible.
- Identified target audience(s) for training.
- Goals of training are identified, analyzed, and mapped to corporate mission in this area.
- Training classes have a regular, recurring schedule.
- Training is integrated into new hire training.
- Training incorporates latest security trends, in addition to corporate policy information

- Training follows standard instructional design principles.

## Router Considerations

- Latest patches and updates are installed.
- You subscribed to router vendor's security notification service.
- All unnecessary ports, especially known vulnerable ports are blocked.
- Ingress and egress filtering is enabled. Incoming and outgoing packets are confirmed as coming from public or internal networks.
- ICMP traffic is screened from the internal network.
- Administration interfaces to the router are enumerated and secured.
- Web-facing administration is disabled.
- Directed broadcast traffic is not received or forwarded.
- Unused services are disabled (for example, TFTP).
- Strong passwords are used.
- Logging is enabled and audited for unusual traffic or patterns.
- Large ping packets are screened.
- Routing Information Protocol (RIP) packets, if used, are blocked at the outermost router.
- Logs are being monitored 24x7x365.
- Router is being maintained 24x7x365 in response to log analysis.

## Firewall Considerations

- Firewall purchase consideration was given to multi-service, best of breed devices
- Latest patches and updates are installed.
- You subscribed to router vendor's security notification service.
- Effective filters are in place to prevent malicious traffic from entering the perimeter.
- Unused ports are blocked by default.
- Unused protocols are blocked by default.
- IPSec is configured for encrypted communication within the perimeter network.
- Intrusion detection is enabled at the firewall.

- Logs are being monitored 24x7x365.
- Firewall is being maintained 24x7x365 in response to log analysis.
- Firewall is being penetration tested periodically, results documented, vulnerabilities addressed.

### Switch Considerations

- Latest patches and updates are installed.
- Administrative interfaces are enumerated and secured.
- Unused administrative interfaces are disabled.
- Unused services are disabled.
- Available services are secured.
- Static port assignments.

### Server Considerations

- Server role has been strictly identified.
- OS uses secured, permissions-based file system.
- File system is encrypted.
- Latest OS patches and updates are installed.
- Latest application patches and updates are installed.
- Administrative interfaces are enumerated and secured.
- Unused services are disabled.
- Minimize OS service permissions
- Access authentication uses strong passwords.
- Available services are secured.
- Regular penetration tests are being performed, results documented and vulnerabilities addressed.