



If you've accepted the fact that your computer and networks are being attacked, and you should, then you should begin to develop and implement some "defense in depth" for preventing these attacks.

Here are some suggested steps:

Step 1: Obtain management buy-in

Get upper management buy-in and addition to their strategic agenda. This may take some education, proving and hard selling, but by doing so, you will not only get the support required on security projects, you'll get the budget too!

Step 2: Create an environment focused on training and awareness

About 50% of all information security related attacks reported to the FBI were from inside the organization reporting. While some of these were malicious in intent, most were a result of poor communication and training in company security policies, both physical and technology related. So, train your staff and users by developing communications and training programs informing them of your security policies (got one?) and potential losses, both corporate and personal. Teach them about malware and how it propagates. Teach them how to respond and report security issues, both physical and technical. The more they know, the more secure your business becomes!

Step 3 (for software developers): Employ secure coding techniques and processes.

Encrypt stored data. Implement application to application authentication and verify that it works. Characterize the input in advance for any code that accepts variable input from another source. Just like access privileges on a network, create code with "least" privileges to mitigate the risk of unauthorized access.

Step 4: Review and update your policies

Specify critical system access by applying "least privileges". If someone doesn't need access to the HR system, don't give it to them! One method for implementing this is to develop role based privileges where specific roles get similar or the same access privileges. Doing so will reduce the amount of effort required to maintain these privileges when resources change. Other policies to review and update include antivirus, backup and confidentiality. Also, create acceptable use policies. Sometimes the use logical to you doesn't match with company policy. Spell it out. And be sure and include consequences in your policies. Talk is cheap!

Step 5: Update your Disaster Recovery Plan (don't have one, get one!)

Recent legislation may require that you have a disaster recovery plan. If you have one, review and test it twice a year. Defining disasters, both intentional (DDOS) and unintentional (hurricane, fire) will also add depth and breadth to the quality of your DRP. If you don't have a DRP, get one!

Step 6: Perform a risk assessment

Threats and vulnerabilities combine to create risk. In order to create an effective risk assessment for your organization, you should create a detailed inventory of the physical and digital assets of your company. You should then identify potential threats from both internal and external sources. Then assess your vulnerability by examining weaknesses in your security posture that open you up to these threats. Build a risk matrix comparing the two and you will be able to then identify appropriate countermeasures should one of these threats materialize.

Step 7: Follow up with an audit

You've built the policies, shared them with your employees, updated your disaster recovery plan and identified your risk of being attacked. Now audit it and test it! Compare yourself to industry standards and verify against regulatory compliance standards. Have a third party provide a penetration test on your perimeter IT systems. Get a "secret shopper" to evaluate your physical security and test for socially delivered security attacks. If you don't test it, it may not work!

Step 8: Update your security software

Noting the daily downloads of antivirus patches, it's painfully obvious that the security software you bought yesterday is probably less than 100% effective today. Patch your hosts, update your firewalls, and change your browser (!?). Update it!



Step 9: Watch your borders

Verify that your borders are protected with up to date software and hardware devices like firewalls. You need to understand what's going back and forth over your network and computers. Or, get a third party managed security service provider. Because security products and processes are eventually compromised over time, security is not a product or process, it's a service. And the cost of intellectual property and corporate asset loss will justify the service.

While these nine steps will not guarantee a totally secure information security environment, they will go a long way in thwarting potential attackers. With so many targets to choose from, making yours difficult to penetrate will more than likely move them on to a less secure target.