CTI
TECHNOLOGY

The explosion in internet usage over the last 10 years has ensured that, from the biggest Fortune 500 companies to small one-man startups, almost every company now has a vital IT component (whether they know it or not).

Every business, including yours, has valuable IT assets such as computers, networks, and data. Protecting those assets requires that companies big and small conduct their own IT security audits in order to get a clear picture of the security risks they face and how to best deal with those threats.

The following are 10 steps to conduct your own basic IT security audit. While these steps won't be as extensive as audits provided by professional consultants, this DIY version will get you started on the road to protecting your own company.

1. DEFINING THE SCOPE OF YOUR AUDIT: CREATING ASSET LISTS AND A SECURITY PERIMETER

The first step in conducting an audit is to create a master list of the assets your company has in order to figure out what needs to be protected through the audit. While it is easy to list your tangible assets – things like computers servers, and files – it becomes more difficult to list intangible assets. To establish consistency in deciding which intangible company assets are included, it is helpful to draw a "security perimeter" for your audit.

What is the Security Perimeter?

The security perimeter is both a conceptual and physical boundary within which your security audit will focus, and outside of which your audit will ignore. You ultimately decide for yourself what your security perimeter is, but a general rule of thumb is that the security perimeter should be the *smallest* boundary that contains the assets that you own and/or need to control for your own company's security.

Assets to Consider

Once you have drawn up your security perimeter, it is time to complete your asset list. This involves considering every potential company asset and deciding whether or not it fits within the "security perimeter" you have drawn. To get you started, here is a list of common sensitive assets:

1. **Computers and laptops**
2. **Routers and networking equipment**
3. **Printers**
4. **Cameras, digital or analog, with company-sensitive photographs**
5. **Data - sales, customer information, employee information**
6. **Company smartphones/ PDAs**
7. **VoIP phones, IP PBXs (digital version of phone exchange boxes), related servers**
8. **VoIP or regular phone call recordings and records**
9. **Email**
10. **Log of employees daily schedule and activities**
11. **Web pages, especially those that ask for customer details and those that are backed by web scripts that query a database**
12. **Web server computer**
13. **Security cameras**
14. **Employee access cards**
15. **Access points (i.e., any scanners that control room entry)**

This is by no means an exhaustive list, and you should at this point spend some time considering what other sensitive assets your company has. The more detail you use in listing your company's assets (e.g., "25 Dell Laptops Model D420 Version 2006", instead of "25 Computers"), the better, because this will help you recognize more clearly the *specific* threats which face each particular company asset.

2. CREATING A 'THREATS LIST'

You can't protect assets simply by knowing what they are; you also have to understand how each individual asset is threatened. So, in this stage, you will compile an overall list of threats which currently face your assets.

What Threats to Include?

If your threat list is too broad, your security audit will end up getting focused on threats which are extremely small or remote. When deciding whether to include a particular threat on your 'Threat List', keep in mind that your test should follow a sliding scale. For example, if you are considering the possibility of a hurricane flooding out your servers, you should consider these things: how remote the threat is, and also how devastating the harm would be if it occurred. A moderately remote harm can still be reasonably included in your threat list if the potential harm it would bring is large enough to your company.

Common 'Threats' to Get you Started?

Here are some relatively common security threats to help you get started in creating your company's threat list:

1. **Computer and network passwords**. Is there a log of all people with passwords (and what type)? How secure is this ACL list and how strong are the passwords currently in use?

2. **Physical assets**. Can computers or laptops be picked up and removed from the premises by visitors or even employees?

3. **Records of physical assets**. Do they exist? Are they backed up?

4. **Data backups**. What backups of virtual assets exist, how are they backed up, where are the backups kept, and who conducts the backups?

5. **Logging of data access**. Each time someone accesses some data, is this logged, along with who, what, when, where, etc.?

6. **Access to sensitive customer data (e.g., credit card info)**. Who has access? How can access be controlled? Can this information be accessed from outside the company premises?

7. **Access to client lists**. Does the website allow backdoor access into the client database? Can it be hacked?

8. **Long-distance calling**. Are long-distance calls restricted or is it a free-for-all? Should it be restricted?

9. **Emails**. Are spam filters in place? Do employees need to be educated on how to spot potential spam and phishing emails? Is there a company policy that outgoing emails to clients not have certain types of hyperlinks in them?

3. PAST DUE DILIGENCE & PREDICTING THE FUTURE

At this point, you have compiled a list of *current* threats, but what about security threats that have not come on to your radar yet, or haven't even been developed? A good security audit should account not just for those security threats that face your company today, but those that will arise in the future.

Examining Your Threat History

The first step towards predicting future threats is to examine your company's records and speak with long-time employees about past security threats that the company has faced. Most threats repeat themselves, so by cataloging your company's past experiences and including the relevant threats on your threat list, you'll get a more complete picture of your company's vulnerabilities.

Checking with Your Competition

When it comes to outside security threats, companies that are ordinarily rivals often turn into one another's greatest asset. By developing a relationship with your competition, you can develop a clearer picture of the future threats your company will face by sharing information about security threats with one another.

4. PRIORITIZING YOUR ASSETS & VULNERABILITIES

You have now developed a complete list of all the assets and security threats that your company faces, but not every asset or threat has the same priority level. In this step, you will prioritize your assets and vulnerabilities in order to know your company's greatest security risks, and so you can allocate your company's resources accordingly.

Perform a Risk Calculation/ Probability Calculation

The bigger the risk, the higher priority dealing with the underlying threat is. The formula for calculating risk is:

Risk = Probability x Harm

The risk formula just means that you multiply the likelihood of a security threat actually occurring (probability) times the damage that would occur to your company if the threat actually did occur (harm). The number that comes out of that equation is the risk that threat poses to your company.

Calculating Probability

Probability is simply the chance that a particular threat will actually occur. Unfortunately, there isn't a book that lists the probability that your website will be hacked this year, so you have to come up with those figures yourself.

Your first step in calculating probability should be to do some research into your company's history with this threat, your competitors' history, and any empirical studies on how often most companies face this threat. Any probability figure that you ultimately come up with is an estimate, but the more accurate the estimate, the better your risk calculation will be.

Calculating Harm

How much damage would a particular threat cause if it occurred? Calculating the potential harm of a threat can be done in a number of different ways. You might count up the cost in dollars that replacing the lost revenue or asset would cost the company. Or, instead, you might calculate the harm as the number of man-hours that would be lost trying to remedy the damage once it has occurred. Whatever method you use, it is important that you stay consistent throughout the audit in order to get an accurate priorities list.

DEVELOPING YOUR SECURITY THREAT RESPONSE PLAN

When working down your newly developed priority list, there will be a number of potential responses you could make to any particular threat. The remaining six points in this article cover the primary responses a company can make to a particular threat. While these security responses are by no means the only appropriate ways to deal with a security threat, they will cover the vast majority of the threats your company faces, and as a result, you should go through this list of potential responses before considering any alternatives.

5. IMPLEMENTING NETWORK ACCESS CONTROLS

Network Access Controls, or NACs, check the security of any user trying to access a network. So, for example, if you are trying to come up with a solution for the security threat of your competition stealing company information from private parts of the company's website, applying network access controls or NACs is an excellent solution.
Part of implementing effective NAC is to have an ACL (Access Control List), which indicates user permissions to various assets and resources. Your NAC might also include steps such as encryption, digital signatures, ACLs, verifying IP addresses, user names, and checking cookies for web pages.

6. IMPLEMENTING INTRUSION PREVENTION

While Network Access Controls deal with threats of unauthorized people accessing the network, taking steps like password protecting sensitive data, an Intrusion Prevention System (IPS), prevents more malicious attacks from the likes of hackers.

The most common form of an IPS is a second generation firewall. Unlike first generation firewalls, which were merely content based filters, a second generation firewall adds to the content filter a 'Rate-Based Filter'.

- **Content-based**. The firewall does a deep pack inspection, which is a thorough look at actual application content, to determine if there are any risks.
- **Rate-based**. Second generation firewalls perform advanced analyses of either web or network traffic patterns, or inspection of application content, flagging unusual situations in either case.

7. IMPLEMENTING IDENTITY & ACCESS MANAGEMENT

Identity and Access Management (IAM) simply means controlling users' access to specific assets. Under an IAM, users have to manually or automatically identify themselves and be authenticated. Once authenticated, they are given access to those assets to which they are authorized.

An IAM is a good solution when trying to keep employees from accessing information they are not authorized to access. For instance, if the threat is that employees will steal customers' credit card information, an IAM solution is your best bet.

8. CREATING BACKUPS

When we think of IT security threats, the first thing that comes to mind is hacking. But, a far more common threat to most companies is the accidental loss of information. Although it's not sexy, the most common way to deal with threats of information loss is to develop a plan for regular backups. These are a few of the most common backup options and questions you should consider when developing your own backup plan:

- **Onsite storage**. Onsite storage can come in several forms, including removable hard drives or tape backups stored in a fireproofed, secured-access room. The same data can be stored on hard drives which are networked internally but separated by a DMZ (demilitarized zone) from the outside world.

- **Offsite storage**. Mission-critical data could be stored offsite as an extra backup to onsite versions. Consider worst-case scenarios: If a fire occurred, would your hard-drives or digital tapes be safe? What about in the event of a hurricane or earthquake? Data can be moved offsite manually on removable media or through a VPN (Virtual Private Network) over the Internet.

- **Secured access to backups**. Occasionally, the need to access data backups will arise. Access to such backups, whether to a fireproofed room or vault, an offsite data center, physically or through a VPN, must be secure. This could mean issuing keys, RFID-enabled "smart pass cards", VPN passwords, safe combinations, etc.

- **Scheduling backups**. Backups should be automated as much as possible, and scheduled to cause minimum disruption to your company. When deciding on the frequency of backups, be aware that if your backups aren't frequent enough to be relevant when called upon, they are not worth conducting at all.

9. EMAIL PROTECTION & FILTERING

Each day, 55 billion spam messages are sent by email throughout the world. To limit the security risk that unwanted emails pose, spam filters and an educated workforce are a necessary part of every company's security efforts. So, if the threat you are confronting is spam emails, the obvious (and correct) response is to implement an email security and filtering system for your company.

While the specific email security threats confronting your company will determine the appropriate email protections you choose, here are a few common features:

- **Encrypt emails**. When sending sensitive emails to other employees at other locations or to clients, emails should be encrypted. If you have international clients, make sure that you use encryption allowed outside of the United States and Canada.

- **Try steganography**. Steganography is a technique for hiding information discreetly in the open, such as within a digital image. However, unless combined with something like encryption, it is not secure and could be detected.

- **Don't open unexpected attachments**. Even if you know the sender, if you are not expecting an email attachment, don't open it, and teach your employees to do the same.

- **Don't open unusual email**. No spam filter is perfect. If your employees are educated about common spam techniques, you can help keep your company assets free of viruses.

10.PREVENTING PHYSICAL INTRUSIONS

Despite the rise of new generation threats like hacking and email spam, old threats still imperil company assets. One of the most common threats is physical intrusions. If, for example, you are trying to deal with the threat of a person breaking into the office and stealing company laptops – and along with them valuable company information – then a plan for dealing with physical intrusions is necessary.

Here are some common physical threats along with appropriate solutions for dealing with them:

- **Breaking into the office: Install a detection system**. Companies like CTI Technology have a variety of solutions for intrusion detection and prevention, including security surveillance.

- **Stolen laptop: Encrypt hard drive**. Microsoft offers an Encrypt File System, or EFS, which can be used to encrypt sensitive files on a laptop.

- **Kids + Pets = Destruction: Prevent unauthorized access**. For many small-business owners, the opportunity to work from home is an important perk. But having children and/or pets invading office space and assets can often be a greater risk that that posed by hackers. By creating an appropriate-use policy and sticking with it, small business owners can quickly deal with one of their most significant threats.

- **Internal Click Fraud: Education and Blocks**. Many web-based businesses run advertising such as Google AdSense or Chitika to add an extra revenue stream. However, inappropriate clicking of the ads by employees or family can cause your account to be suspended. Make employees aware of such things, and prevent the company's live website from being viewed internally.

CONCLUSION

These 10 steps to conducting your own IT Security Audit will take you a long way towards becoming more aware of the security threats facing your company, as well as help you begin to develop a plan for confronting those threats. It is also important to remember that security threats are always changing, and keeping your company safe will require that you continually assess new threats and revisit your response to old ones.