KELSER

Network Security Checklist

Many businesses do not have adequate network security. Here's how to make sure you do.

You depend on your network for your most important business operations, such as communication, inventory, billing, sales, and trading with partners. Yet up to now, you may have held off on protecting your network, for several possible reasons:

- Network security might seem too complex, and tackling it might seem like too much work. But you can take a step-by-step approach, then use a consultant to help you complete your security plan.
- You may think network security is an expense that won't help your business grow. Instead of thinking about it as a technical concern, consider it a business continuity issue. Networks have become a basic part of doing business, which makes security planning as important as sales and marketing.
- You may believe that smaller companies are less likely to be a target of attacks. But as large companies beef up their network security, hackers are increasingly focusing on small and medium-sized businesses.

General Planning Tips

The following tips can help you develop and win support for an effective network security plan:

- Focus on return on value rather than return on investment. Consider the harm a network security breach could do to your business, such as lost revenue or customer litigation.
- Never assume that network attacks will come only from outsiders. Your employees can accidentally create security vulnerabilities, and disgruntled or former employees can cause considerable damage.
- Don't be tempted to confront security concerns with a piecemeal approach rather than a single, unified strategy that protects your whole network. Otherwise there will be gaps that could be exploited.
- Maintain scheduled assessments tests of the vulnerability status of all systems and devices connected to your internal network.
- Regularly have the integrity of your internet facing IPs tested for penetration.
- Find the right balance between security and usability. Making your environment as secure as is practicable without inhibiting employee productivity requires well planned policies and effective technology. It’s tough to figure all that out on your own so get help from an expert.

KELSER

Network Security Checklist

Every business should have a written thoughtfully prepared network security plan in place. A thorough policy will cover topics such as:

- ☐ **Acceptable use policy**, to specify what types of network activities are allowed and which ones are prohibited
- ☐ **E-mail and communications activities**, to help minimize problems from e-mails and attachments
- ☐ **Antivirus policy**, to help protect the network against threats like viruses, worms, and Trojan horses
- ☐ **Identity policy**, to help safeguard the network from unauthorized users
- ☐ **Password policy**, to help employees select strong passwords and protect them
- ☐ **Encryption policy**, to provide guidance on using encryption technology to protect network data
- ☐ **Remote access policy**, to help employees safely access the network when working outside the office

Answering the following questions can help you develop your own policy:

Inventory Your Current Security Technologies

Do you have any of the following?

- ☐ **Firewall**, to keep unauthorized users off your network
- ☐ **Virtual private network (VPN)**, to give employees, customers, and partners secure access to your network
- ☐ **Intrusion prevention**, to detect and stop threats before they harm your network
- ☐ **Content security**, to protect your network from viruses, spam, spyware, and other attacks
- ☐ **Secure wireless network**, to provide safe network access to visitors and employees on the go
- ☐ **Identity management**, to give you control over who and what can access the network
- ☐ **Compliance validation**, to make sure that any device accessing the network meets your security requirements

KELSER

Identify Your Most Important Digital Assets and Who Uses Them

- Exactly what are your company's digital assets (such as intellectual property and customer records)?
- What are they worth?
- Where do those assets reside?
- Who has access to these assets, and why? Can all employees access the same assets?
- Do you extend access to business partners and customers?
- How do you control that access?

What Would a Security Breach Do to Your Business?

- What is the potential financial impact of a network outage due to a security breach?
- Could a security breach disrupt your supply chain?
- What would happen if your website went down?
- Do you have e-commerce features on your site? How long could the site be down before you lose money?
- Are you insured against internet attacks, or against the misuse of your customers' data? Is this insurance adequate?
- Do you have offsite backup and recovery capabilities to restore information if necessary after a security breach?

Consider Your Current and Future Needs

- How do you expect your business plan to evolve over the 2 years? 5 years?
- How recently have you updated your network equipment? Software? Virus definitions?
- What type of security training if any, do you provide to your employees?
- How will growth affect your digital assets and their value to your business as a whole?
- In the future, are you likely to have a greater need for remote employees, customers, or partners to access those digital assets?