**Weak Configurations:**

The first reason for a vulnerable system is weak configuration. The weak configuration of a system

comes in many different forms, with the following being the most common configuration mistakes:

■■ Open permissions Not configuring permissions on a system or in an application can leave

the system wide open to attackers. Ensuring that guest or anonymous accounts do not have write

access to data on the system is critical.

■■ Unsecure root accounts Best practices with administrator accounts such as the root account

in Linux and the administrator account in Windows should be followed. Common best practices

include renaming the default account, setting a strong password on the account, and limiting the

creation of additional root-level accounts.

■■ Errors Errors are mistakes made in the configuration that could leave the system open to

attack. For example, not limiting zone transfers on a DNS server could leave the DNS data open

to the attacker.

**Third Party Risks**

There are risks to working with third-party companies as well. Actions performed by third-party

companies you work with may leave your company vulnerable. The following are a few examples:

■■ Vendor management How a vendor manages their products may present vulnerabilities to your

environment that uses that vendor’s products. For example, how does a vendor’s system integrate

into your network? Does it use secure protocols? Does it need an account on the network? If a

product is older, it is possible that the vendor no longer supports the product. A product no longer

supported does not have patches created anymore, which means you could be open to zero-day

attacks.

■■ Supply chain If you are working with a supplier that does not follow security best practices, you

could receive a product from the supplier that has been compromised that you then connect to your

network.

■■ Outsourced code development Unsecure application code is a big cause for vulnerabilities on a

system. Outsourcing the development of a component to be used by your applications could cause

them to be unsecure if the outsourced company does not follow secure coding practices.

■■ Data storage You may be storing data with a third-party company—maybe as an alternate site to

store data backups. Verify the third-party company is securing the system that holds your data, but

also take steps of your own to ensure the data is encrypted and that only your company can decrypt

the data.

**Improper or Weak Patch Management**

Lack of a patching strategy is one of the biggest reasons for vulnerable systems because a patch

has the security fixes for known vulnerabilities.

Be sure to apply patches to the following on a regular basis:

■■ Firmware Apply updates to the firmware on devices such as servers, routers, switches, and any

other hardware device that may exist within your company.

■■ Operating system (OS) Patch the operating system on a regular basis and look to patch

management software to automate the deployment of patches.

■■ Applications Ensure that applications are patched as well. A vulnerability in an application may

cause the entire system to be vulnerable to an attack.

Legacy Platforms

Legacy systems are something you should watch for on the network, as many legacy systems no

longer have vendor support, which means they are most likely not patched anymore. Also, a legacy

system may be using older protocols that are unsecure. If you are using legacy systems on your

network, look to placing them on their own network segment to help reduce the chances that the

systems are attacked.

A company that does not learn how to manage the vulnerabilities that exist on a system could face

disastrous results.

The following are potential impacts to a business that does not reduce the vulnerabilities that exist

in their products:

■■ Data loss A vulnerability on the system may result in you losing access to data. For example,

an attacker could exploit the vulnerability and delete the data or encrypt it with ransomware.

■■ Data breaches A data breach occurs when an unauthorized person gets access to

confidential data. A data breach is also known as a data leak or data spill. The data breach may

include information such as health records, financial data, and intellectual property. The impact of

a data breach could be disastrous to a company due to the cost of investigating and recovering

from the data breach, but the company could also see damage to its reputation

■■ Data exfiltration Data exfiltration occurs when someone transfers data from a computer or network

without permission to do so. Examples of sensitive data that an attacker may want to transfer from a system

are financial data (such as credit card numbers), personally identifiable information (PII), and usernames and

passwords. To prevent data exfiltration, you can disable USB ports so that portable storage such as USB

flash drives and USB external drives cannot be connected to a system, or you can use data loss prevention

(DLP) features to block sensitive data from being copied or e-mailed outside the organization.

■■ Identity theft A vulnerability in a system could result in identity theft, where personal information

about a person is stolen, allowing the attacker to assume the victim’s identity.

■■ Financial loss A vulnerability could result in financial loss due to many reasons. First, the

vulnerability may allow the attacker to crash production systems, resulting in loss revenue, but there is

also the cost of recovering the systems and the intangible cost of reputation damage.

■■ Damage to reputation As mentioned a few times already, a vulnerability being exploited resulting

in a system compromise could cause damage to the company’s reputation. Customers may choose to

no longer do business with your company if they feel their data is not secure.

■■ Availability loss A vulnerability could result in the loss of availability of a system or service. For

example, a vulnerability in a back-end database may cause an e-commerce web application to not be

able to display products or take online orders.