5

Tips to Avoid Network Security Problems

COMPUQUIP
CYBERSECURITY

Table Of Contents

Why Cybersecurity Breaches Should Be Avoided

It's common sense that cybersecurity breaches are bad and that organizations should take precautions to avoid them. But, why should breaches be avoided? The major reasons are that cybersecurity breaches can negatively impact both a business and its customers in different ways, including:

Loss of Revenue/Business

Following a major network security breach, businesses often suffer a major loss of revenue as consumers lose faith in the company's ability to protect sensitive data. For example, as reported by the New York Post, "Target reported a profit drop of $440 million for its fiscal fourth quarter as a result of the credit card breach… Profit fell to $520 million, or 81 cents a share, from $961 million, or $1.47 a share, a year earlier." While an older example, this profit loss shows just how devastating a loss of public trust from a breach can be.

Why Cybersecurity Breaches Should Be Avoided

Risk of Business Closure

According to reports featured on Inc.com, “60 percent of small and midsized businesses that are hacked go out of business within six months.” A major network security breach is something that many businesses don’t have the resources to aid in recovery. Preventing such breaches in the first place, or at least creating a plan for dealing with security incidents to minimize their impact, may prove crucial for ensuring business continuity.

Identity Theft

One of the major goals of many cyberattacks is to steal sensitive, personally-identifiable information (PII) that can be used to commit fraud. Whether attackers use the data themselves or sell it to others, customers (and business employees) are exposed to identity theft. This, in turn, can lead to financial loss for customers, as well as lawsuits against the business for failing to protect customers’ sensitive information.

What Are the Common Network Security Problems That Lead to Breaches?

There are many network security problems that can lead to a cybersecurity breach—far too many to address every issue in a single document of reasonable length. However, some of the most common network security issues that the Compuquip team has found include:

Unknown Assets on the Network

Many organizations fall behind on mapping and assessing the assets on their business networks. Some common unknown assets include employee-owned mobile devices, IoT-enabled appliances (smart fridges, Wi-Fi printers/copiers, clocks, etc.), and newly-installed workstations. These devices aren't accounted for in any network security architecture, so they can be an entry point for attackers.

Abuse of User Account Privileges

Internal employees often abuse their access privileges in some fashion (whether maliciously or accidentally), which can easily lead to a data breach and the misuse of customers' PII. In some cases, attackers may even hijack an employee's account to carry out their attacks. The greater the level of access the misused account has, the more damage may be incurred.

What Are the Common Network Security Problems That Lead to Breaches?

Unpatched Security Vulnerabilities

Software programs can be incredibly complicated, so they may have unanticipated interactions with one another or unknown exploits when they're first released. Software developers frequently create security patches for their software to close these security gaps—but many businesses neglect to apply the patch until it is too late.

Lack of an Incident Response Plan

An incident response plan (IRP) is a company's strategy for responding to a security incident and minimizing the damage such incidents can cause. Unfortunately, many organizations lack an IRP or do not have the resources to properly enact their plans.

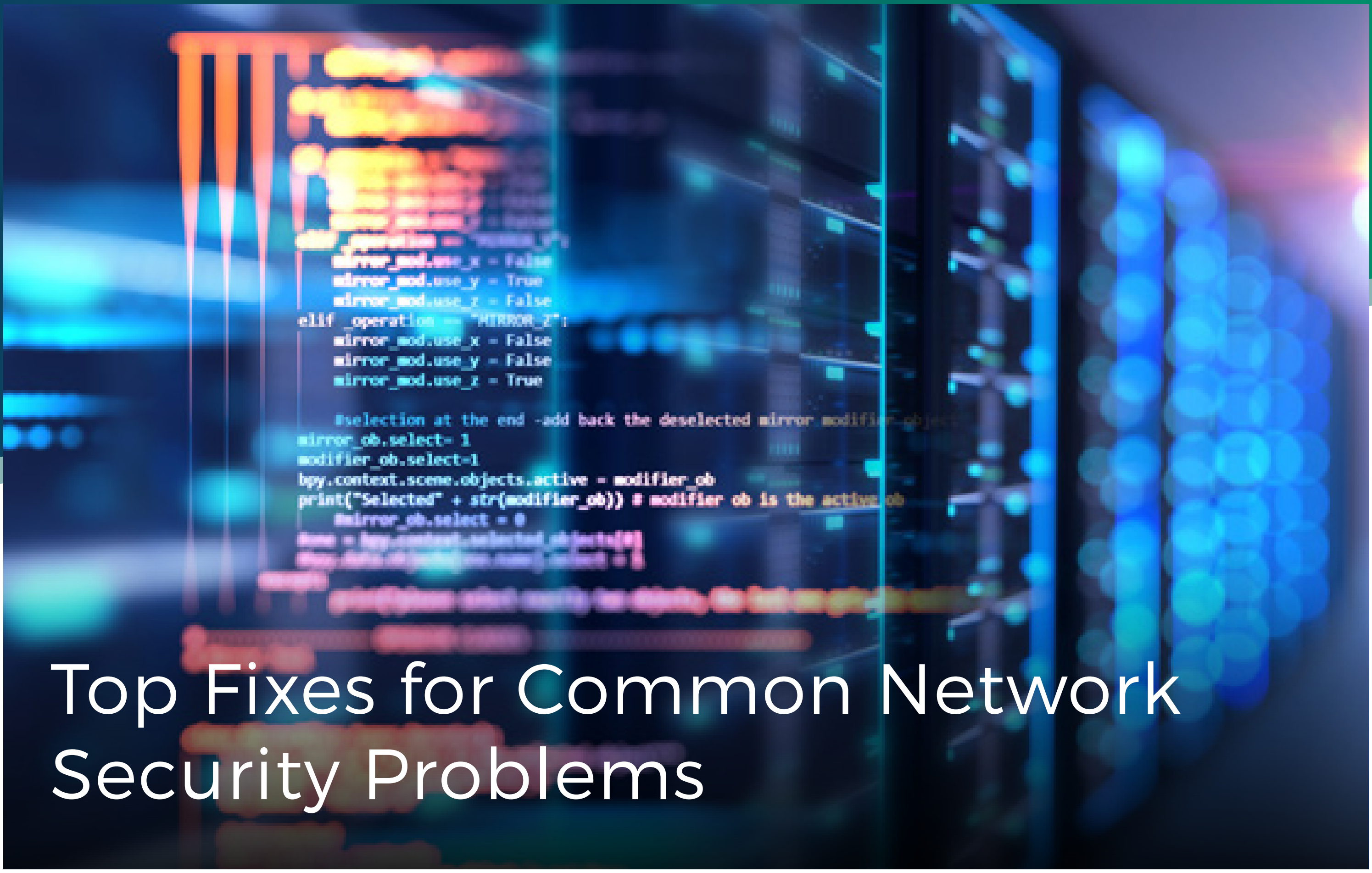
No Strategy for Dealing with Internal Security Breaches

Many organizations have the basic perimeter security they need to keep an outside attacker from getting in. However, they often have nothing to prevent someone already on the business' network from moving from one system to the next. This gives attackers free rein to steal data and corrupt multiple systems—increasing the impact of a security breach.

Lack of Service Level Agreements (SLAs) for IRPs and Disaster Recovery

One issue with many organizations that have an incident response or disaster recovery (DR) plan is that there are no enforceable service level agreements for the plan. They have no established timeline of when the breach should be contained/ eliminated, nor when any compromised systems and data should be restored.

Any one of the above issues could either cause a security breach or allow a breach to be much worse than it needs to be. So, how can your organization solve these network security problems? Preferably before a malicious actor can leverage one to cause a breach?



Top Fixes for Common Network Security Problems

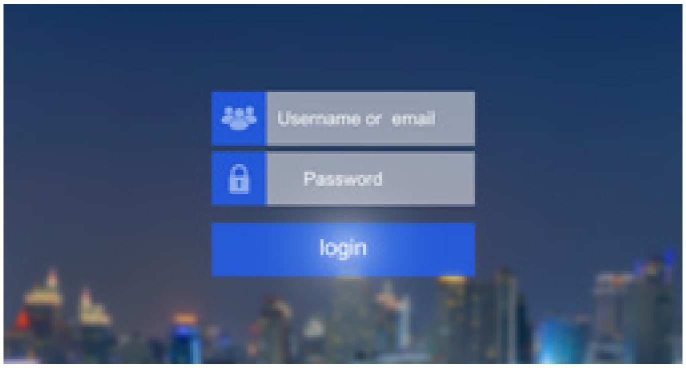
Solution #1: Network Security Audits

Running periodic network security audits is one of the easiest ways to identify unknown assets and vulnerabilities on your network. In a network security audit, a cybersecurity expert (or a team of them), will review and assess your organization's security architecture and review its performance based on industry best practices. This often involves thoroughly auditing all of the security endpoints (i.e. devices) on your network and any operating systems or software that they use.

In addition to auditing the efficacy of your current security architecture, an auditor will help identify specific gaps in your security architecture and make recommendations about how to close those gaps to improve security for your organization—hopefully preventing a future cybersecurity breach. Some cybersecurity companies may even [provide additional technology implementation and consulting services](#) to align recommendations with your organization's budget and help onboard any new cybersecurity solutions as needed.

> *"...auditor will help identify specific gaps in your security architecture and make recommendations about how to close those gaps to improve security for your organization...."*

Solution #2: Applying a Policy of Least Privilege for User Accounts



One of the simplest and most effective ways to curtail the abuse of user account privileges is to apply a policy of least privilege (POLP) to all users. A policy of least privilege basically means giving each user access to only the bare minimum data and systems that they need to fulfill their job function. For example, instead of giving a materials engineer access to the company's financial records server, you would restrict them to the design database and AutoCAD software.

This way, if the employee ever misuses their access privileges (or if their account gets hijacked in a phishing attack), the damage that they can do will be limited. In fact, when combined with intrusion detection/prevention systems (IDS/IPS), a policy of least privilege can help speed up intrusion detection, since the access requests from the misused account will be outside of the normal behaviors for that account (which makes them easier to identify as malicious).

Solution #3: Create and Adhere to a Patch Management Schedule

While many companies worry about "zero-day" exploits (unknown security vulnerabilities that have yet to be identified by software and cybersecurity companies), the truth is that most of the exploits attackers use are old. According to CSO Online, zero-day exploits account for "a little less than 1 percent" of the security exploits identified in 2016. Instead, as CSO Online also states, based on reports collected in 2016, "out of all detected exploits, most came from vulnerabilities dating to 2007." These vulnerabilities were nearly a decade old when the attackers used them against their victims.

The easiest fix for this problem is to create and maintain a regular patch management schedule. Checking for security patches to business software and operating systems as infrequently as once every other week or once a month can help to close security gaps without putting too much strain on the business processes that rely on the software being updated.

If there aren't sufficient internal resources to effectively manage the patch schedule and keep software up to date, it may help to contract a managed security service provider (MSSP) to handle vulnerability management.

Solution #4: Create Defense-in-Depth by Isolating Systems

Using defense-in-depth strategies that isolate the different systems on a business network can be a crucial strategy for blunting security breaches—particularly those that start from the inside or leverage hijacked user accounts. While setting up a layered defense with multiple internal firewalls and access controls can be difficult, the benefits are well worth the effort. Some key benefits of using a defense-in-depth strategy include:

Slowing Down Attackers

Having strong internal security layers that isolate systems means attackers have to spend more time and effort on breaking out of whichever system they manage to breach first. This, in turn, slows them down and buys more time for the security breach to be detected, contained, and eliminated.

Stronger Data Security

Having a segmented network with isolated systems makes it easier to protect your organization's most sensitive data. This has an enormous impact on data breach risks and the likelihood of an attacker being able to steal or corrupt sensitive information. It also makes enforcing a policy of least privilege easier by keeping unauthorized users from having access to systems that store sensitive data.

Reducing Damage from Successful Attacks

If an attacker takes more time to break out of one system and into another, then it is more likely that they will be stopped before they can access too much sensitive data. This limits the damage that even a successful attack may cause.

Solution #5: Creating Incident Response Plans

> *...No business is too small to be a target, nor too large to be immune. Incident response plans are how organizations can prepare to minimize the damage caused and recover quickly from a breach.*

Even the strongest network security measures aren't immune to a data breach. Eventually, there will be an attacker who is skilled, persistent, or just plain lucky enough to find a security gap they can use to breach your cybersecurity. No business is too small to be a target, nor too large to be immune. Incident response plans are how organizations can prepare to minimize the damage caused and recover quickly from a breach.

When creating an incident response plan, it's important to set specific goals for the plan and to set aside sufficient resources to meet those goals. The basic goals of any IRP are:

Stop the Attack

The first step of any incident response plan (after identifying that there is an incident to respond to, of course) is to contain the attack so it cannot cause further harm. This usually involves cutting off the attacker's access to your systems (either by isolating or disabling them as necessary) or revoking their access privileges.

Investigate the Attack Method

To prevent future attackers from using the same methods to breach your network security, it is important to investigate the methods behind the attack and to close those security vulnerabilities ASAP. Here, gathering forensic data for analysis (such as event logs from your IDS or security information and event management [SIEM] solution) is crucial for understanding the attacker's methods and thwarting future attempts.

Notify Affected Parties

If customers, investors, employees, etc. may have been affected by the breach, it is important to notify them so they can take appropriate measures to avoid identity theft and fraud.

Restore Assets to the Network

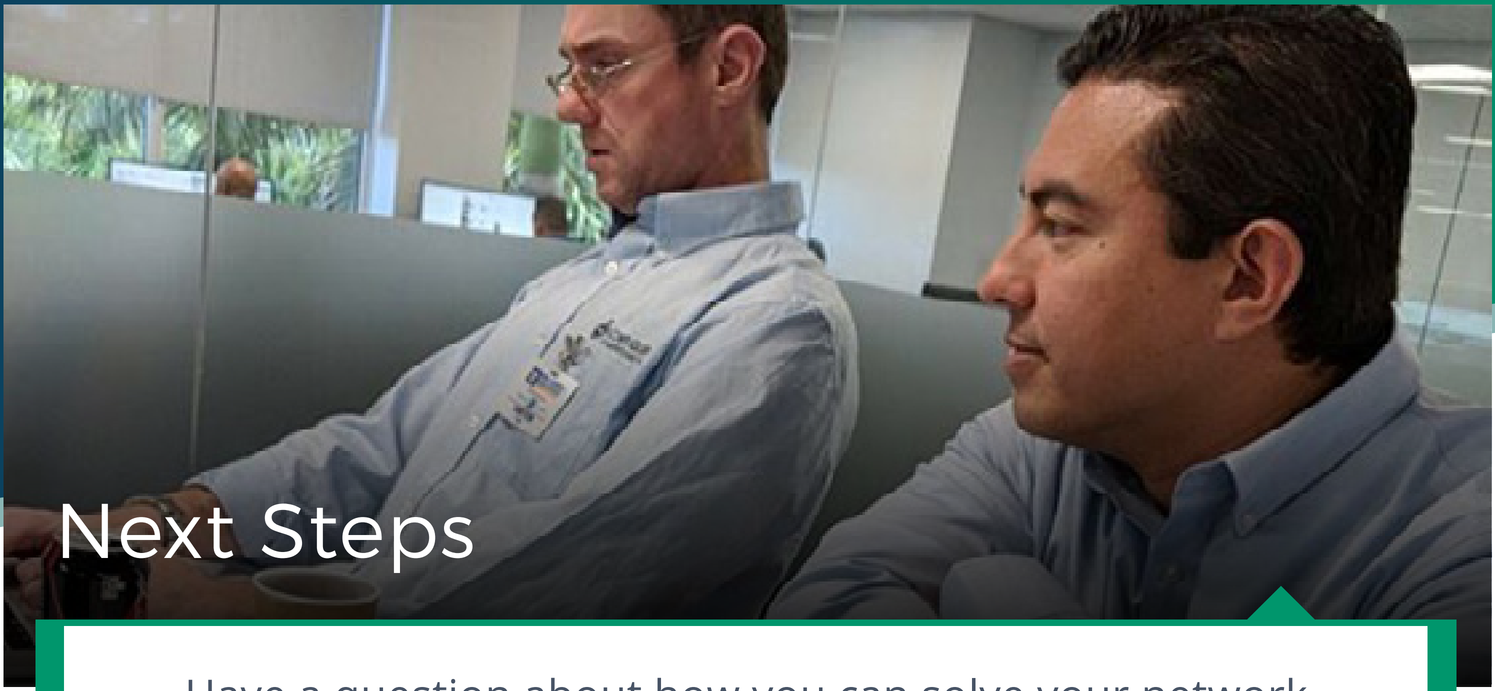
Once the attack is contained, the organization needs to return to normal operations as soon as possible. This often involves restoring compromised assets to full working order (by wiping the drives and restoring from a backup) or replacing the affected assets entirely.

> *An MSSP will typically have the necessary experience to recommend the best solutions for data backup, intrusion detection, and data collection to optimize your response plan....*

To meet these goals, it is necessary to be prepared to enact the IRP. This means having the resources in place to identify an attack in progress, contain it, investigate it, notify any affected parties, and to restore or replace compromised IT assets as needed to return operations to normal.

Managing an IRP internally can be a massive challenge—which is why some organization use managed security services to provide the labor and expertise to create, organize, and enact the response plan.

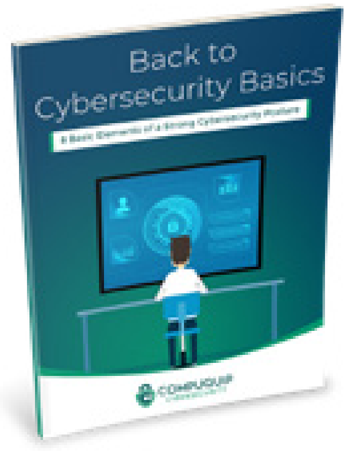
An MSSP will typically have the necessary experience to recommend the best solutions for data backup, intrusion detection, and data collection to optimize your response plan—as well as the expert manpower to enact the plan quickly and efficiently should the need arise. This helps to ensure that service level agreements for disaster recovery can be met consistently.



Next Steps

Have a question about how you can solve your network security issues before they become a liability? Reach out to the Compuquip Cybersecurity team for help and advice:

Contact Us Today


Back to Cybersecurity Basics
8 Basic Elements of a Strong Cybersecurity Posture
COMPUQUIP CYBERSECURITY

Back to Cybersecurity Basics

8 Basic Elements of a Strong Cybersecurity Posture

Download Now

COMPUQUIP
CYBERSECURITY

Email: info@compuquip.com

Phone: 789-641-5437

Address: 2121 Ponce De Leon Blvd. Suite 530
Coral Gables, FL 33134

Follow us on: