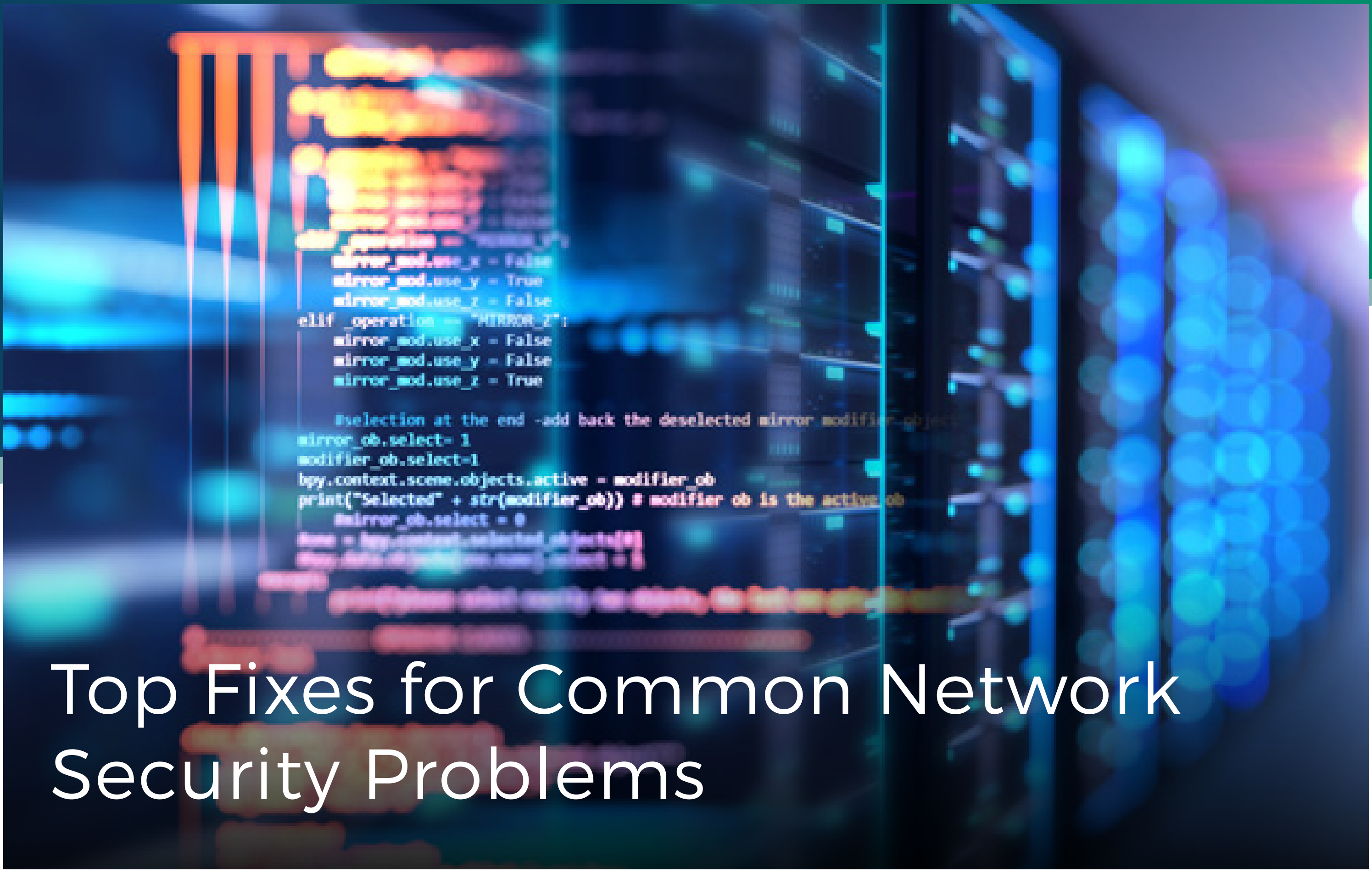
Why Cybersecurity Breaches Should Be Avoided

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.



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….*