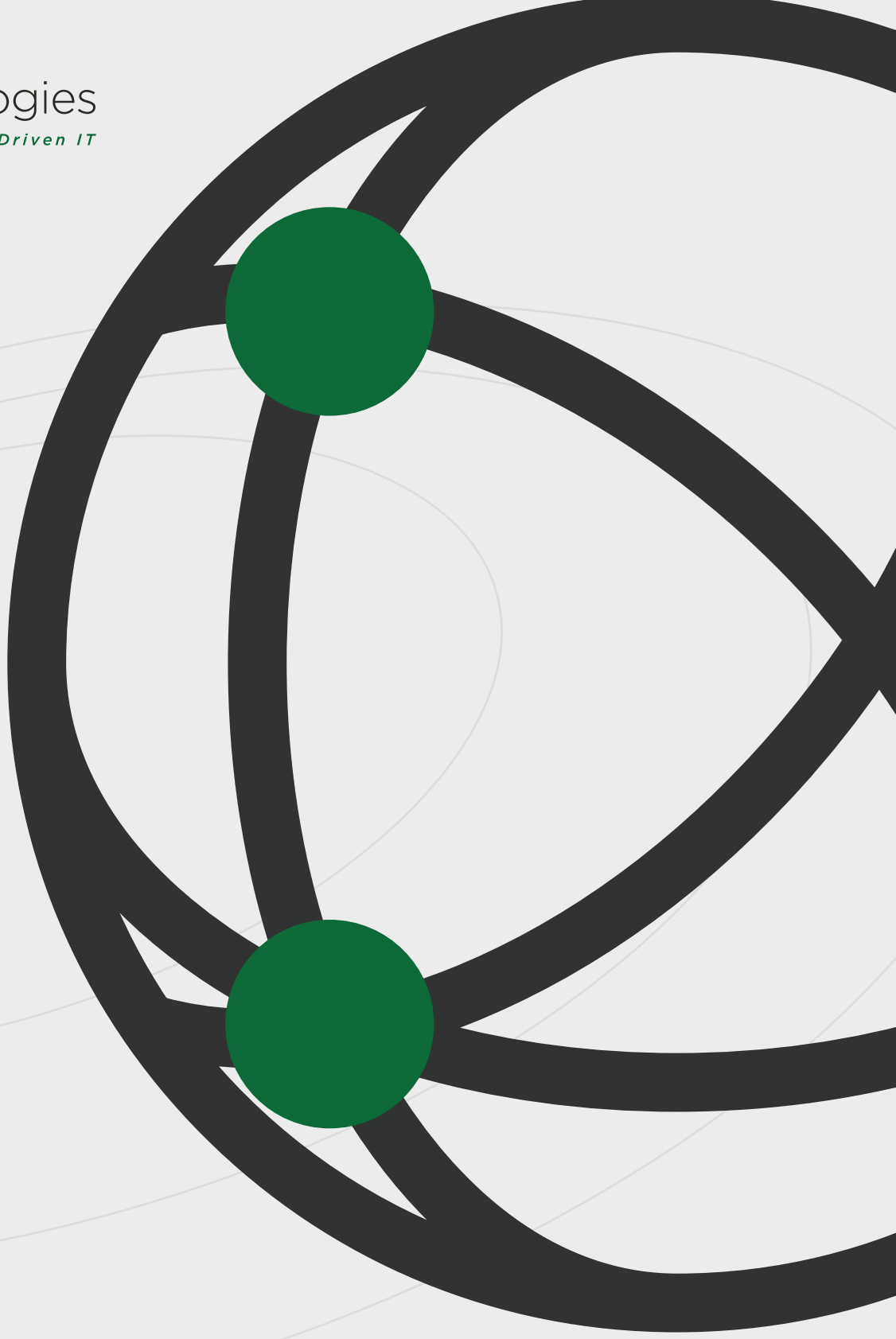
pch technologies

*Performance Driven IT*



# THE IMPORTANCE OF CYBERSECURITY

www.pchtechnologies.com

# CYBER SECURITY ESSENTIALS

If you think data breaches are a headache for your company, wait until you discover the average price tag of being the victim of one. The average cost of data breaches has jumped to $4 million, a 29% increase since 2013, and will continue to rise as more and more sensitive data is targeted by cyber criminals and requires protection and storage.

That's why it's critically important to get ahead of the security threats before you – and your customers – become the next victim of a cyber attack.

## BEING PROACTIVE IS ONLY HALF THE BATTLE

It's a tough pill to swallow but the biggest risk to your data security, and the leading cause of data breaches, is human error. More often than not, it's simple inattention to detail that leads to that error since nearly 40% of the time it is people, not technology, that compromises your data and systems. Every year companies make great efforts to implement the latest technologies to improve cybersecurity, develop new strategies for preventing data breaches, and create or expand upon internal processes that support cybersecurity.


The average cost of data breaches has jumped to **$4 million**

However, no matter which of the latest security technologies, anti-virus software and network security tips and tricks you implement, you still have to maintain a proactive attitude towards combatting cyber attacks. That starts with educating your own internal teams on the absolute importance of being vigilant in identifying activity that just looks out-of-place or doesn't make much cyber sense, and ensuring everyone is on the same page with network security best practices and the policies to anticipate and address concerns.

## START TIGHTENING YOUR CYBERSECURITY WITH AN AUDIT

If you aren't sure where your weaknesses are, how will you know what you need to fix them? The fact is, you won't and that's why one of the first things you should do to protect your business is identify the right outside cybersecurity consultants to perform a comprehensive cybersecurity audit of your network.

**A Cybersecurity Audit should cover the following areas:**

### Your IT Infrastructure

A detailed review of your organization's structure, including the IT infrastructure currently in place involves examining where you stand, how you work, and what it will take to protect what you have today. Does the equipment and software you currently have deliver the high quality and capabilities to serve your cybersecurity needs, or are there gaps and pitfalls to address? Sometimes completing the picture is as straightforward as complementing your existing IT infrastructure with a few additional pieces of equipment or software, and then getting them all working in concert as a cohesive unit.

### External Scans for Vulnerabilities

Where are the weak points in your existing network security systems? An external scan reveals the cybersecurity vulnerabilities that can be exploited.

**40%** OF DATA BREACHES ARE A RESULT OF HUMAN ERROR – NOT YOUR TECHNOLOGY.

**EDUCATING YOUR EMPLOYEES ON NETWORK SECURITY BEST PRACTICES AND POLICIES IS AN ESSENTIAL SAFEGUARD.**

Does your network have ports open and accepting any and all web traffic types? Is your network security software currently deployed and optimized to detect the latest malware and ransomware programs floating around the internet right now? Are there unprotected "back door" openings in your network created from unauthorized workaround solutions? That's what you need to find out so action can be taken before intruders turn weaknesses into trouble.

Where are the weak points in your existing **network security systems?**

## Full Inventory of Devices and Software

Computers, routers, phone systems, printers and even the fax machine all maintain connections to your network. Because your business IT network is one of the most valuable assets you own, it's important to maintain a full inventory of all devices and software for full visibility into your network resources. Besides identifying opportunities for updates and greater efficiencies, maintaining this inventory system can also significantly reduce the effects of network downtime as can can readily and quickly identify problem devices and software and resolve those issues nearly immediately.

## Best Practices Documentation

The size and scope of your network will determine just how extensive your best practices documentation should be. Best practices documents should include those details and processes that are relevant to your unique network and overall IT infrastructure, so no two best practices documents will look just alike.

If your network is small with a single firewall and just a couple of switches, there isn't a lot to document unless your team is new to supporting your network. On the other hand, a larger network consisting of multiple access points, a half-dozen servers and network switches and multiple people monitoring them requires much more expansive documentation to outline and detail the critical aspects and activities of your network.

## Data Backup and Recovery Policies

The best tool at your disposal in times of critical disaster or failure is your data backup and recovery policy. There are a multitude of ways to backup and recover data, but which one is right for your business? This is the key question to be addressed and determined during any audit. A weak data backup and recovery policy simply means it will become that much more difficult to recover valuable data even in the most limited breach situation.

## THERE ARE NO SHORTCUTS TO PROTECTING YOUR BUSINESS

You can't take shortcuts and expect to receive the level of protection your company and your customers deserve for the valuable, personally identifiable information you are responsible for keeping safe. Cyber terrorists don't give up easily and actually view networks with basic security measures as low-hanging fruit ripe for the picking. So It's too risky to simply set up a firewall, install some security patches or software and then call it a day. There's only one sure way to protect your company from cyber criminals and that's by doing things right from the start. A security audit from PCH technologies will help you discover where to start and what you need to fully protect your business.

pchtechnologies

11 ENTERPRISE COURT
SUITE 100
SEWELL, NJ 08080

**856.754.7500**

**www.pchtechnologies.com**