The Business of Data Security:

WHAT YOU NEED TO KNOW

LOCK DOWN THAT DATA

Today, some businesses store or share terabytes of electronic information including quarterly reports, billing statements or even sensitive client data. With that in mind, here's why you should rethink your data security.

You have a responsibility to your clients.

Your clients trust you with their information, so they expect a reasonable effort to prevent unauthorized disclosure or access to their data.

You must comply with government regulations.

Various federal, state and industry guidelines regulate the exchange ofsensitive information.

You should protect your reputation.

A data security breach at your office will almost certainly result in the loss of clients and possibly generate negative publicity.

COMMON CHALLENGES

Airtight data security is hard to achieve. For small and midsize businesses, the task can be overwhelming. Also, technological changes mean that security measures can become obsolete in a matter of months.

Businesses can address these challenges with a step-by-step plan.

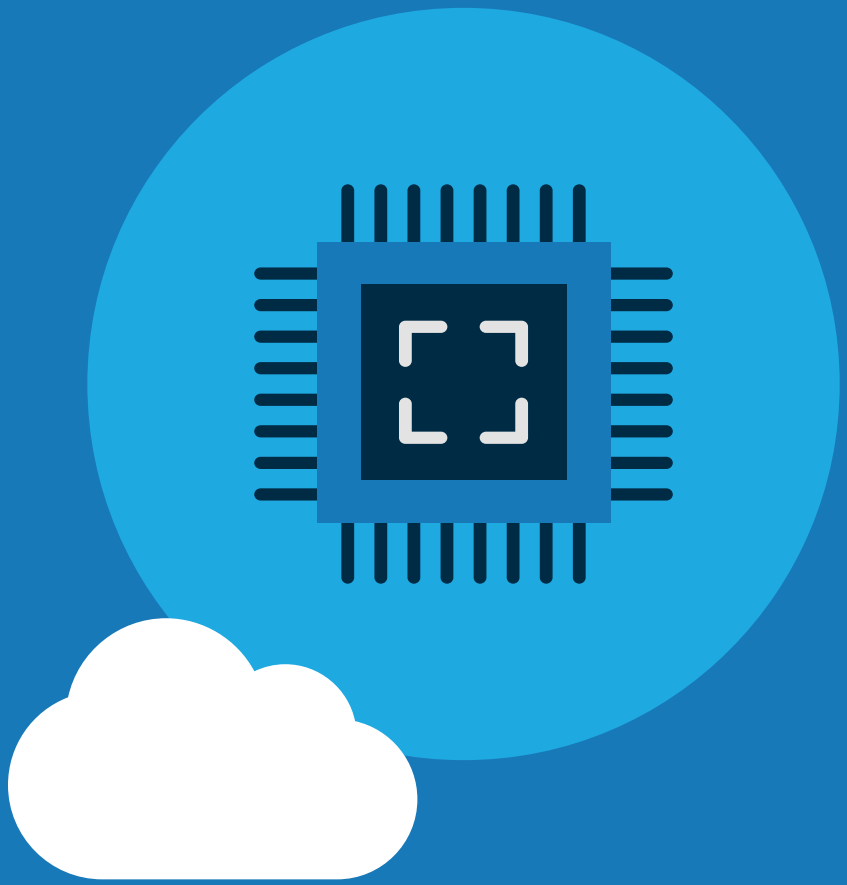
SECURITY: STEP BY STEP

Get Ready

Data security is only achievable if you're ready to lead the charge and make some changes.

Assess Risk

Security vulnerability occurs via your physical work environment, network security and mobile communication. How do you guard each area? **Take the following actions.**



PHYSICAL VULNERABILITY

- Make workstations inaccessible to the public.
- Lock away your routers and servers.
- If possible, incorporate industry standard protocols such as magnetic doors and keycard access.
- Maintain protection against natural disasters.
- Archive data offsite or in a secure cloud storage solution.
- Replace aging physical equipment.

UNSECURED NETWORKS

- Configure your firewalls correctly.
- Use strong, proven anti-virus and anti-malware software.
- Keep your software current.
- Password protect your network and make it invisible.
- Don’t transmit private data on public networks.

MOBILE DEVICE WEAKNESSES

- Make sure your device doesn't scan for and hook up to open Wi-Fi networks.
- Transfer files via secure software, such as file-sharing apps that encrypt data, rather than email.
- Enable security features such as remote wipe and automatic file deletion if you lose your phone.

RESEARCH REGULATIONS

Depending on the kind of data you're storing and transferring, you could be subject to more regulations than you know.

These include:

- The U.S. Securities and Exchange Commission (SEC)
- The Consumer Financial Protection Bureau's (CFPB) data security guidelines
- Various state data security laws
- Records disposal laws and protocols
- Industry standards such as Financial Industry Regulatory Authority (FINRA) rules

STAY AHEAD OF THE GAME

Serve clients to the best of your ability by staying current with your security. It's not possible to eliminate risk, but you can decrease it significantly by becoming aware of your security issues, learning everything you can and being proactive in your responses.

SET POLICIES AND PROCEDURES

Now that you understand what you need to do, decide how to do it. Develop a data security program, train any staff members and enforce protocols reasonably. For instance, if you cannot secure data onsite, look for offsite storage services that offer you features like advanced encryption methods.

Want to find out
how you can securely send
documents and data?

Visit Hogancg.com/Manage

Hogan Managed Services