Critical Questions

To Ask About Your IT Security

Security breaches and data loss will hit all-time highs this year.

Table of Contents

Small budgets, aging resources, and escalating threats have made it difficult for small to mid-size businesses to keep up with the ever-evolving tactics of cybercriminals.

As cyber-attacks continue to increase in our digital world, it has become increasingly important for SMBs to uncover their vulnerabilities and evaluate their security practices.

This guide will help you assess basic IT security considerations to reduce the risk of your business becoming part of the growing number of compromised organizations.

77% of businesses do not have a cybersecurity response plan in place. In some cases, it can take up to 6 months to detect a breach!

Internal Security

65% of businesses that have a password policy in place, do NOT strictly enforce it.

Believe it or not, the greatest security vulnerability in your business is your internal staff. Whether intentional or unintentional, if your staff has access to sensitive business information, they can cause critical data loss.

So the big question is –

How are you addressing the potential risk imposed by your users?

Evaluate your password policies

- What are your password requirements? Are they being enforced?
- How complex do you require passwords to be?
- How frequently are employees required to change their passwords?
- Are you using multi-factor authentication? If not, why not?

Business insurance companies are increasingly mandating the use of multi-factor authentication within a company's internal network. CCB has great options and can help you get MFA set up in your organization. Request a demo!

Evaluate your security awareness training

- Do your employees have too much control over their computers?
- Are you educating users on internet and device policies? How often?
- Is your team up to date on current security risks and phishing attempts?

Learn about CCB's Security as a Service

Cybersecurity

You’re probably asking yourself – “**Where is my business most vulnerable to cybercrime?**”

To identify areas of risk, you need to understand what you currently have in place.

Like all preparedness – awareness is KEY!

Cybersecurity is a fast-changing landscape, making it hard to stay up-to-date on the latest threats. For this exact reason, it’s essential to be continuously training and testing your users. They are your front-line – meaning they are the most vulnerable, but if well-trained, your best defense!

Evaluate your business’ cyber-attack strategy

- Do you have the ability to identify and remediate cyberthreats proactively?
- Does your firewall utilize the most current threat detection and prevention methods?
- What resources do you use to keep your business security current?
- Do you have anti-virus and malware protection on all network devices?

Aging IT infrastructure can increase downtime and cause gaps in your network security. Evaluate aging equipment and replace outdated versions of Windows or other software – your business will thank you.

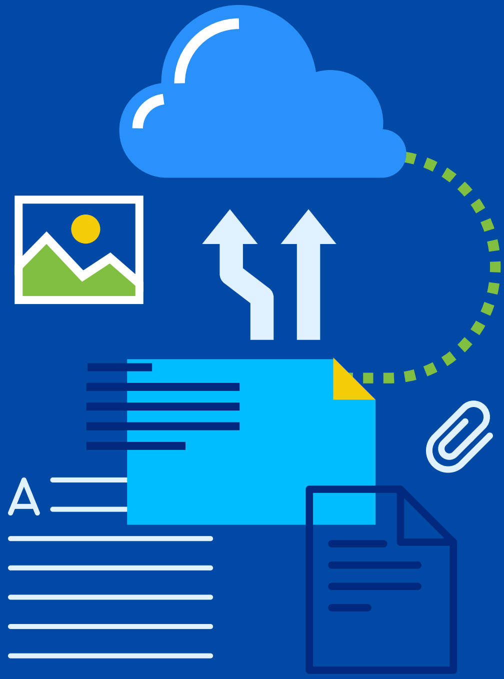
Learn about CCB’s Endpoint Detection & Response services

Backup and *Recovery*

Your data is your business' lifeline – your backup and recovery plans are an insurance policy, and what you choose can make or break your business when disaster strikes.

"So if I have a backup plan, I'm covered, right?"

Wrong. A backup plan shouldn't be "set it and forget it." Surprisingly, **34% of businesses admit to not regularly testing their backups**. With so much at stake, it's critical to be back up frequently and test regularly.



Evaluate your Disaster Recovery

- What data loss prevention policies do you have in place?
- Where are you storing your data, and how is it being protected?
- How long can your business afford to be down in an emergency?
- Do you know what applications are mission-critical to your organization and what order they need to be restored?
- What is your documented disaster recovery plan, and when was it created, reviewed or updated?

Protect against a single point of failure.

To protect your critical business data, be sure to have several trusted people trained on your DR plan.

Keep all aspects of your business protected.

Your operational needs will change with your growth - your backup and DR plans should evolve too.

Learn about CCB's Backup as a Service

Business Considerations

“Are unsanctioned devices a threat to my business? How can I protect against them?”

Monitoring third-party applications and unsanctioned devices is crucial to safeguard your data.

- Start by ensuring that your internal and guest wi-fis are separate and secured.
- Ensure your IT has access to any device using your business network.
- Does your data loss prevention policy address USB access?

Evaluate your compliance

When it comes to compliance, there are strict rules and guidelines for your IT environment and internal operations that vary depending on your industry.

Are you confident that you’re meeting regulatory compliance for your industry?

Violating compliance laws can lead to severe fines and penalties but can be avoided by implementing robust security compliance functions in your business.

Protecting against disgruntled employees

- Do you have a policy in place that addresses BYOD (bring-your-own-device)?
- How quickly are you able to remotely disable an employee’s machine?
- Have you locked down critical areas of your data based on employee’s roles and need for access?

Learn about CCB’s Device as a Service

Experience the **CCB difference**

You should be confident in your security measures.

Are you looking for ways to strengthen your security strategy?

CCB Technology can support you in the ways you need it most.

We can help with:

- **IT Security Consulting**
- **End-user Awareness Training**
- **IT Security Management**
- **Device Management**
- **IT Security Project Services**
- **Preventative Maintainance**
- **Backup and Recovery Services**

Managed IT is not one size fits all – our flexible Managed and Co-Managed IT Services are tailored to your needs.

We also offer consulting and one-off project services for the times when you need some added expertise or extra help.

How can we help you?

Schedule a call

Psst

We back our managed IT services with a **90-day money back guarantee** – and a pie in the face!

See it for yourself!
It's like nothing else in the industry!

Check it out