The Importance of IT Security Services in Safeguarding Data and Networks To Protect Your Assets

What role does cybersecurity play in protecting today's businesses? Reactive strategies can leave you vulnerable to cyberattacks and critical data breaches.

IRONEDGE®

IT Security Is a Top Concern for Businesses Today

Are you feeling the pressure of cybersecurity? With a shift towards digital systems and assets, businesses face an increased risk of cyberattacks on their businesses. Today's executives name **cybersecurity as the leading strategic challenge** impacting their outcomes.[1]

The cost of cybercrime is extensive and growing each year. In 2023, the FBI reported[2] that the following cybercrimes caused the greatest financial losses.

1 Business Email Compromise (BEC)

Over $2.9 billion in losses

2 Investment Scams

Over $4.57 billion (up 53% from 2022)

3 Ransomware

Over $59.6 million from 2,825 reports in 2023

4 Impersonation Scams

Over $1.3 billion lost and over 51,750 cases

In total, losses were estimated at $10.3 billion in 2022, and increased to $12.5 billion in 2023. The FBI also notes that more than 2,412 cybercrime reports are filed each day.

Total Loss Estimates

It's not a question of ***if*** you will face a cyberattack, but ***when***.

IT security plays a crucial role in helping your business avoid unnecessary expenses and problems caused by cybercriminals, hackers, and fraudsters looking for a weak link in your business.

How Ongoing Tech Evolution Impacts Your Business

As technology evolves, so does the cybersecurity landscape for businesses.

Increasingly Complex IT Environments

Today's businesses are adopting a wide array of new technologies — including cloud computing, Internet of Things (IoT) devices, AI-powered tools, and mobile applications. Managing and securing these complex IT environments becomes an increasingly intricate task.

Without proper management and oversight, the proliferation of disparate systems and devices can create security gaps, leaving businesses vulnerable to cyber threats.

The Impact

Businesses need to adopt holistic cybersecurity strategies that encompass all aspects of their IT infrastructure, including network security, endpoint protection, and cloud security.

Growing Importance of Data Security

Data has become one of the most valuable assets for businesses. The importance of data means businesses need robust security measures to protect sensitive information from unauthorized access, theft, or breaches.

Data breaches that expose sensitive information can lead to severe consequences, including reputational damage, legal repercussions, and financial losses.

The Impact

Businesses must implement encryption, access controls, and data loss prevention (DLP) measures safeguard sensitive data throughout its lifecycle, from storage to transmission.

Changing Compliance Requirements

Businesses must also consider compliance with regulatory requirements as they protect themselves from cyber threats. Regulatory standards around data privacy and security — such as GDPR, PCI DSS, GLBA, and HIPAA — are constantly evolving, imposing stricter mandates on organizations to protect consumer data.

Failure to comply with these regulations can result in hefty fines, legal penalties, and damage to brand reputation.

The Impact

Businesses need to stay abreast of changing compliance standards and ensure that their cybersecurity practices align with regulatory mandates to avoid costly consequences.

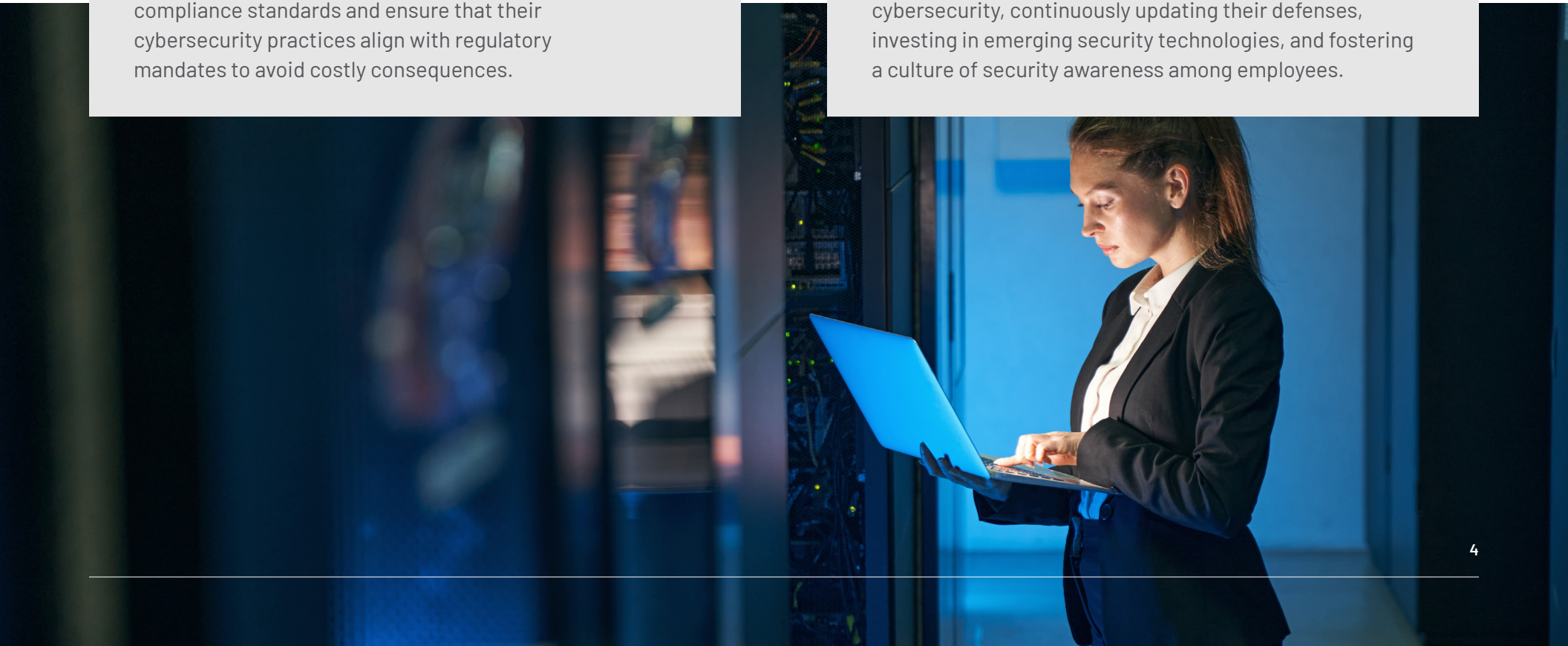
Rapid Pace of Innovation

While emerging technologies like artificial intelligence (AI) and blockchain offer exciting possibilities for business growth and efficiency, they also introduce new security challenges. For example, AI-powered cyberattacks and vulnerabilities in blockchain-based systems pose significant threats to businesses.

This continuous shift forces businesses to navigate changing threats and complexities — or risk falling behind in the wake of cutting-edge technology.

The Impact

Businesses must adopt a proactive approach to cybersecurity, continuously updating their defenses, investing in emerging security technologies, and fostering a culture of security awareness among employees.



The Role of IT Security Services in Your Business

IT security is essential for maintaining trust with customers, complying with regulatory requirements, and safeguarding the long-term viability of your business in an increasingly interconnected and threat-laden digital landscape.

IT security services involve ongoing monitoring, threat intelligence, and incident response to detect and mitigate security incidents promptly, minimizing the impact on business operations and reputation. Additionally, IT security services protect against cyber threats — including malware, ransomware, phishing attacks, and data breaches — by implementing robust security measures such as firewalls, intrusion detection systems, encryption, and access controls.

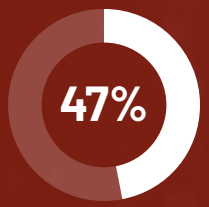
One changing aspect of IT is the shift from reactive to proactive services.

Traditional IT

Traditional IT vendors and in-house teams typically operate reactively, addressing issues as they arise with more of a pay-as-you-go pricing model.

Managed IT

Managed IT service providers take a proactive approach with partnerships that include ongoing monitoring, maintenance, and strategic guidance to optimize IT infrastructure and support business goals.



47% of businesses with fewer than 50 employees have no cybersecurity budget.[3]

Should You Outsource IT Support?

Outsourcing cybersecurity to a managed service provider (MSP) can help your business improve security without causing a capacity issue for your team. Here are five reasons you should consider outsourcing your IT support.

1 Benefit From Specialized Cyber Expertise

MSPs specialize in cybersecurity, bringing expertise, experience, and cutting-edge technologies to the table. By partnering with an MSP, businesses gain access to a dedicated team of security professionals who can provide round-the-clock monitoring, threat detection, and incident response capabilities, enhancing overall security posture.

2 Adapt To Changing Cyber Needs

MSPs offer flexibility, scalability, and agility, allowing businesses to adapt to evolving security threats and regulatory requirements without the burden of managing security operations internally.

3 Compete at the Highest Level

Leverage economies of scale to access enterprise-grade security solutions and services through your MSP — all at a fraction of the cost it would take to build an in-house security team.

4 Focus On Other Business-Critical Objectives

Outsourcing cybersecurity enables your team to prioritize other areas where they have more experience or competency. Rather than spending time on cybersecurity monitoring and staying up-to-date on tech trends, your team can focus on core objectives that help drive business success.

5 Harness Knowledgeable Insights and IT Strategy

The right MSP will have a solid understanding of tools, integrations, threats, and opportunities that could impact your business. When you outsource, you get an external perspective to analyze the strengths and weaknesses of your existing setup.

The #1 reason businesses outsource tasks is to **reduce expenses** and **add industry experience** to their teams.[4]

10 Ways To Safeguard Data and Protect Your Digital Assets

Are you doing enough to protect your data? Sustainability requires a methodical and strategic approach to cybersecurity. Here are ten things you (or your MSP) should do to safeguard your digital assets.

Implement Access Controls: Restrict access to sensitive data and systems based on the principle of least privilege, ensuring that only authorized individuals can access or modify critical information.

Encrypt Data: Protect sensitive data from unauthorized access, interception, or theft using strong encryption algorithms and key management practices.

Regularly Update Software and Systems: Keep all software, operating systems, and firmware up to date with the latest security patches and updates to address known vulnerabilities.

Use Strong Authentication Methods: Enhance identity verification with multi-factor authentication (MFA) or biometric authentication to prevent unauthorized access to systems and accounts.

Backup Data Regularly: Ensure data integrity and availability in the event of data loss, corruption, or ransomware attacks by storing regular backups securely offsite or in the cloud.

Educate Employees: Provide comprehensive cybersecurity training and awareness programs to educate employees about common threats, phishing scams, and social engineering tactics.

Implement Security Policies and Procedures: Develop and enforce rules on data handling, access management, passwords, remote work, and incident responses to ensure consistency and compliance.

Monitor and Audit Systems: Implement continuous, real-time checks of your systems, networks, and user activities to detect and respond to security incidents, anomalous behavior, or policy violations.

Secure Network Perimeters: Deploy firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and control traffic entering and leaving the network.

Conduct Regular Security Assessments: Perform regular security assessments, vulnerability scans, and penetration testing to identify and remediate security weaknesses, assess the effectiveness of security controls, and ensure compliance with industry standards and regulations.

REAL-WORLD EXAMPLE

Safeguarding Data for Curtis Wagner Plastics

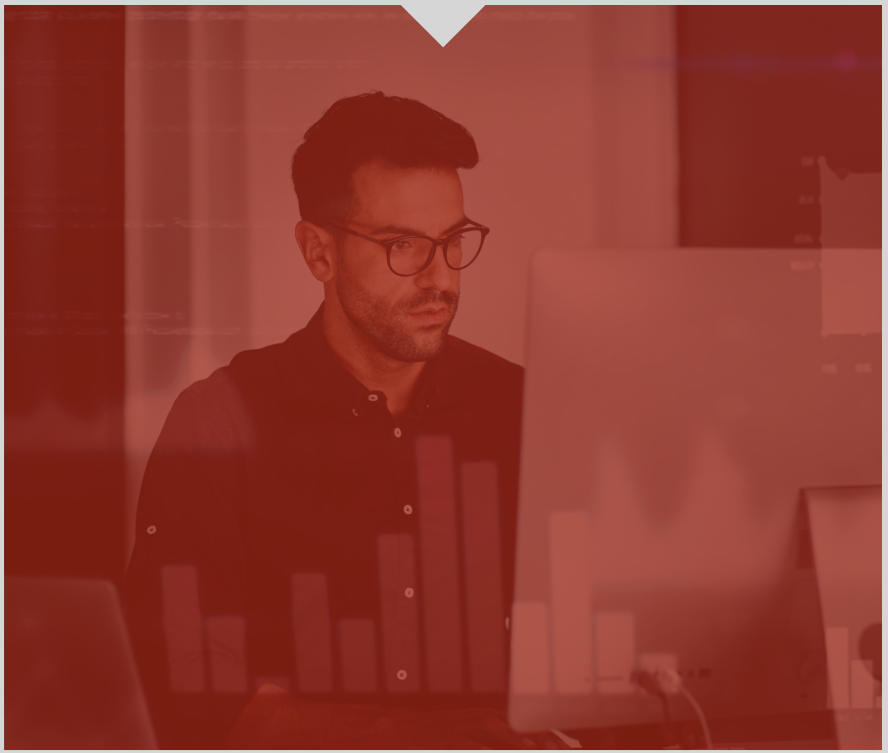
How do managed services teams help businesses prepare for disaster? When Curtis Wagner Plastics needed a better solution for securely backing up their data, they chose to work with IronEdge.

After experiencing a server crash, hard drive failures, and connectivity issues with their email server, the Curtis Wagner team wanted a reliable way to protect their data and reduce downtime.

IronEdge Group supported an email migration to Microsoft 365 using SkyKick technology and Azure AD Connect to safely synchronize Curtis Wagner's existing domain with the new solution.

When their server crashed during a historic ice storm, IronEdge was able to quickly transition to cloud-based domain services leveraging Azure Active Directory without needing to restore from backups.

To ensure data remained secure, the IronEdge team built redundancies in the IT systems to protect information during unforeseen disasters or catastrophic events. The migration also provided added convenience and reliability for employees working from home.



"Any time we had an issue or needed help from IronEdge, responses were swift and they fixed our issues quickly. Now I can do whatever I need to do and maneuver through the system without hindrance."

Tim Warner, Business Development Manager
Curtis Wagner Plastics

CWP

Trust IronEdge as Your IT Partner & MSP

Are you looking for a provider you can rely on for responsive support, proactive planning, and reliable services?

With an expanded geographic reach across Texas, the Southwest, Rocky Mountain region, and beyond, IronEdge offers managed IT services, cybersecurity, cloud services, project implementation, hardware solutions, and more. IronEdge has the expertise and industry knowledge you need for end-to-end cybersecurity support.

We'll partner closely with your team to understand your unique needs and goals, developing tailored cybersecurity strategies to safeguard your data and enable business growth.

Talk to our team today to get cutting-edge technologies and IT advice that fuels your vision.

LET'S TALK

Resources

[1] https://www.microsourcing.com/learn/blog/the-ultimate-list-of-outsourcing-statistics/

[2] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[3] https://insights.corvusinsurance.com/cyber-risk-insight-index-q1-2022/survey-findings-smb-cyber-readiness

[4] https://www.microsourcing.com/learn/blog/the-ultimate-list-of-outsourcing-statistics/

IRONEDGE®