ISSUE 023
June 2025
Independence, Missouri

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

News

CYBER INSURANCE: MORE IMPORTANT THAN YOU THINK

For small businesses navigating an increasingly digital world, cyber threats aren't just abstract worries—they're daily realities.

From phishing emails to ransomware, data breaches to accidental leaks, even a minor cyber incident can cause major disruption. These events can lead to lost revenue, damaged reputations, legal consequences, and regulatory fines.

Cyber Insurance is not a substitute for strong cybersecurity practices, but it's a crucial safety net when something slips through the cracks.

Let's explore how to evaluate and choose the right cyber insurance policy for your business—and how you can potentially lower your premiums by reducing risk.

What Is Cyber Insurance?

Cyber insurance (also called cyber liability insurance) is a specialized policy that covers the financial losses and response costs associated with cyber incidents. This can include:

- Data breaches
- Ransomware attacks
- Business email compromise
- Social engineering scams
- Network outages or data loss
- Legal defense and regulatory fines

Step-by-Step: How to Choose the Right Cyber Insurance Policy

1. Assess Your Business Risk

Before comparing policies, take stock of your digital footprint and risk exposure. A few questions to ask:

- *What types of data do we collect or store?* Sensitive customer data, payment card information, employee records, or health data may require higher levels of coverage and carry heavier regulatory responsibilities.
- *How dependent are we on digital systems?* If your operations rely on cloud apps, remote access, or digital payment systems, downtime could halt operations.
- *Do third parties access our network or data?* Vendors, contractors, and partners can introduce risk. If they're compromised, your systems could be affected too.
- *Do we operate in a regulated industry?* Healthcare, finance, education, and legal services often face strict compliance standards—and higher costs in the event of a breach.

2. Ask the Right Questions When Reviewing Policies

Not all cyber insurance policies are created equal. As you evaluate providers, be sure to ask:

- Does this policy cover ransomware payments and recovery costs?
- What about social engineering or phishing-based fraud?
- Are legal defense fees and regulatory penalties included?
- What's excluded from coverage?
- Does the policy offer breach response assistance?

Reading the fine print is essential to ensure you're not caught off guard during a claim.

3. Evaluate Coverage Limits and Deductibles

Once you know what's covered, determine how much coverage is enough.

Consider:

- The total value of your digital assets.
- Potential revenue loss during downtime
- Fines, legal fees, and customer notification costs.
- Also, assess the deductible—the amount your business must pay before the insurer steps in. Make sure it aligns with your financial capabilities.

4. Review Policy Renewal Terms and Adjust as Needed

Cyber threats are constantly evolving, and your policy should be flexible enough to keep up:

- Does the provider offer periodic risk assessments?
- Can you scale coverage as your business grows?
- Are you required to meet certain cybersecurity standards to stay covered?

Lowering Your Premium: How Cybersecurity Can Save You Money

Here's the good news—a more secure business is often rewarded with lower insurance premiums. Just like installing a security system can reduce your homeowner's insurance, implementing cybersecurity best practices can reduce your cyber insurance costs. Many insurers offer discounts or more favorable rates for businesses that:

- Use Multi-Factor Authentication (MFA): This is one of the most effective ways to prevent unauthorized access to accounts.
- Regularly Patch and Update Systems: Keeping your operating systems and software up to date closes known vulnerabilities that attackers often exploit.
- Provide Security Awareness Training: Educating employees about phishing, password safety, and safe internet habits helps prevent user-based errors—the #1 cause of breaches.
- Encrypt Sensitive Data: Whether stored or in transit, encryption adds a layer of protection that can mitigate exposure in case of a breach.
- Maintain Secure and Tested Backups: Having secure, offline backups can reduce the impact of ransomware and show insurers you're prepared for recovery.
- Deploy Endpoint Protection and Firewalls: Tools like antivirus, anti-malware, and next-gen firewalls provide foundational protection and are often required by insurance providers.

Pro Tip: Some insurance carriers will even conduct a cybersecurity risk assessment during the quoting process. The stronger your security posture, the better your quote could be.

How FCS Helps You Navigate Cyber Insurance With Confidence

At Ferguson Computer Services we don't just protect your systems—we can also help you through the entire cyber insurance process:

✅ *Assistance with Risk Assessment Forms*

Many insurance applications require detailed technical information about your cybersecurity posture. We can help you gather the necessary data, fill out the forms accurately, and present your security framework in a way insurers understand.

✅ *Implementing Key Security Measures to Reduce Premiums*

We help you meet (and exceed) insurer requirements—like enabling multi-factor authentication, setting up endpoint protection, encrypting sensitive data, and ensuring secure backups. These steps don't just strengthen your security—they may also lower your premium.

✅ *Ongoing Cybersecurity Management*

Our managed security services keep your protection up to date with monitoring, patch management, and continuous improvements—making sure you stay eligible for coverage and prepared for renewal.

✅ *Support During a Claim or Breach*

If something does go wrong, we are on your side—helping you document the incident, recover your systems, and work with your insurance provider to file a claim properly.

The Future: Cyber Insurance is a Must for Small Businesses

Cyber threats are no longer a concern only for big corporations—they're hitting small businesses every day. Choosing the right cyber insurance policy can mean the difference between bouncing back quickly and facing catastrophic loss.

By understanding your risks, asking the right questions, and combining smart insurance decisions with the right protection in place, your business can stay protected, reduce insurance costs, and respond confidently to whatever the digital world throws your way.

TL;DR

Cyber insurance is becoming essential for small businesses as cyber threats like ransomware, phishing, and data breaches grow more frequent and costly. While insurance can't prevent attacks, it offers financial protection when incidents occur. Choosing the right policy means assessing your risks, understanding what's covered, and reviewing exclusions, deductibles, and renewal terms. You can lower your premiums by strengthening your cybersecurity—implementing tools like multi-factor authentication, secure backups, encryption, and employee training. FCS can help to guide businesses through the entire process: from filling out risk assessments to putting in place the protections insurers require, to supporting you during claims.

ISSUE 023
June 2025
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

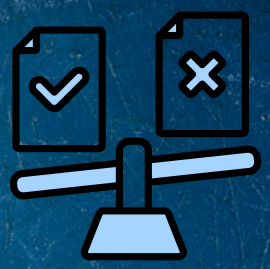
CLICK TO VIEW A SHORT VIDEO!

FREE INTERNET SERVICE CHECK

STOP OVERPAYING

GET FASTER SPEEDS

GET THE BEST VALUE



WE COMPARE FOR YOU

MICROSOFT LICENSING CHANGES IN 2025: WHAT YOUR BUSINESS NEEDS TO KNOW

Microsoft has introduced several significant licensing changes in 2025 that may affect how your business manages and pays for Microsoft 365 and related cloud services. Whether you're renewing licenses soon or just want to stay ahead of upcoming changes, it's important to understand what's new—and what it could mean for your bottom line.

Let's break down the most impactful updates, and explore the benefits and potential drawbacks of each.

Monthly Billing Surcharge Introduced

Microsoft is now charging a 5% surcharge for monthly billing on annual-term subscriptions. This change, which took effect in April 2025, applies to many popular services, including Microsoft 365, Office 365, Dynamics 365, and Power Platform subscriptions.

In other words, if you commit to a one-year subscription but choose to pay monthly rather than upfront annually, you'll now pay more overall.

✅ *Benefits of Annual Billing:*

Cost Savings – Switching to annual payment eliminates the 5% surcharge.

Better Value Over Time – Locking in a fixed rate for the year protects against mid-year increases.

⚠️ *Considerations:*

Upfront Cost – Annual payments require a larger financial commitment upfront, which might not suit all cash flow scenarios.

Need for Accurate Forecasting – You'll need to plan ahead for how many licenses you'll need for the entire year.

New 3-Year Subscription Options in CSP

As of June 1, 2025, Microsoft now allows businesses to purchase three-year terms for certain Microsoft 365 subscriptions through the Cloud Solution Provider (CSP) program.

This option is available for Microsoft 365 E3, E5 (with or without Teams), Teams Enterprise, and additional suites like E5 Security and E5 Compliance.

This marks a big shift from the typical monthly or annual commitments, giving organizations the ability to lock in pricing for three full years—a valuable hedge against Microsoft's regular price increases.

✅ *Benefits:*

Price Protection – Avoid unexpected increases during your term.

Simplified Budgeting – Fixed licensing costs make financial planning easier.

Less Frequent Renewals – Reduces administrative overhead and renewal disruptions.

⚠️ *Considerations:*

100-Seat Minimum – The three-year plans are only available for businesses with at least 100 users.

Reduced Flexibility – Long-term commitments might not suit businesses expecting major changes in headcount or service needs.

STAYING ORGANIZED WHILE WORKING IN THE SUMMER

Summer often brings a more relaxed pace at work—with coworkers on vacation, shifting schedules, and longer daylight hours. But those changes can also lead to distractions and disorganization if you're not careful.

Here are a few simple ways to stay on track and keep your productivity up while enjoying the season:

🌞 *1. Adjust Your Schedule to Match Your Energy*

If your workplace allows it, try starting your day earlier to take advantage of cooler mornings and quieter work time. You'll get more done before the afternoon heat (and distractions) kick in.

🗂️ *2. Declutter Your Digital Workspace*

Take time to clean up your desktop, archive old files, and organize your folders. A tidy digital workspace helps reduce stress and makes it easier to find what you need—especially if you're coming and going during vacation weeks.

📝 *3. Use a Summer-Specific To-Do List*

Create weekly checklists to focus on must-do tasks during a time when projects may slow down or team members are out. Keeping a list helps you stay accountable and prevents small things from slipping through the cracks.

📅 *4. Plan Around Vacations*

Check team calendars and coordinate ahead of time to make sure nothing gets delayed while someone's out. Set clear deadlines and make handoffs smooth by using shared calendars and project management tools.

🏖️ *5. Take Advantage of the Slow Season*

Use quieter weeks to get organized for fall: update documentation, clean out your inbox, refresh your goals, or tackle long-overdue maintenance tasks.

SMART SUMMER TECH: TIPS FOR USING YOUR WORK COMPUTER SAFELY AND EFFICIENTLY IN THE HEAT

As summer heats up, so can your office technology—literally. Warmer temperatures and seasonal distractions can impact how well your computer runs and how securely you're working.

Whether you're in the office, working remotely, or preparing for vacation, a few proactive steps can help keep your work computer running smoothly and your data safe.

Here are some smart summer tips every employee should follow:

1. Keep Your Computer Cool

Excessive heat can damage your computer and slow down performance. Make sure your workstation is well-ventilated and that your computer isn't pushed against a wall or stacked with paperwork. Avoid placing laptops near windows or in direct sunlight. If your laptop starts feeling unusually hot, shut it down and let it cool.

Bonus Tip: Never leave a laptop or mobile device in a hot car—even for a few minutes.

2. Watch Out for Summer Phishing Scams

Cybercriminals know that many employees take time off during the summer or work with reduced attention. Be cautious with unexpected emails—especially those that claim to be related to HR, travel plans, or urgent financial matters. Double-check email addresses and never click suspicious links or download unknown attachments.

3. Use Surge Protection

Summer storms can cause power surges or outages that damage electronics or lead to data loss. Always plug your computer and monitors into a surge protector, and save work frequently to avoid losing progress during a power interruption.

4. Lock Your Screen When You Step Away

With more people coming and going during summer hours, it's easy to get distracted. Always lock your screen (Windows: Windows + L, Mac: Control + Command + Q) when stepping away—even for a quick break. This simple step helps protect sensitive information from prying eyes.

5. Be Cautious with Personal Devices

Bringing in personal USB drives or using unauthorized apps on work computers can create security risks. If you need to transfer files, use approved methods like secure cloud storage or request help from IT. When in doubt, ask before you plug in.

6. Take Care of Portable Devices

If you're using a laptop or tablet during summer travel or remote work, be mindful of where and how you use it. Avoid working in areas with sand, water, or high humidity. Keep devices stored in padded, temperature-safe cases, and never leave them unattended in public.

7. Keep It Clean

Summer can bring more dust, pollen, and even spills. Take a moment to gently clean your keyboard, mouse, and screen using approved wipes or microfiber cloths. Keeping your equipment clean can improve performance and extend its life.

8. Plan Before Leaving for Vacation

If you're taking time off, it is a good idea to make sure your out-of-office settings are configured correctly, especially for email and internal tools. Let us know when and where you will be travelling so we can make sure to adjust security settings for logins outside of your typical office location.

Summer Technology Recap

Summer is a great time to relax and recharge—but don't let your guard down when it comes to your work technology. A few mindful habits can keep your devices running smoothly, protect your data, and ensure you're working safely all season long.

If you have any questions or need support, reach out to your IT team. We're here to help keep your summer—and your systems—running without a hitch.

ISSUE 023
June 2025
Independence, Missouri

SECURITY UPDATES: WHAT HAPPENS WHEN YOU DON'T HAVE THEM?

Your computer's operating system is the foundation of everything you do—from checking email and processing payments to accessing files and running business-critical applications.

For most businesses and individuals, that operating system is Microsoft Windows. But like any foundation, it needs maintenance.

That's where security updates come in—and they're more important than many people realize.

What Are Microsoft Security Updates?

Microsoft regularly releases security updates, also known as "patches," to address vulnerabilities discovered in its operating systems and software. These vulnerabilities could be exploited by hackers to:

- Install malware or ransomware
- Steal personal or financial data
- Take control of your computer
- Spread infections across your network

These updates are not just helpful—they are essential. They close the digital doors and windows that cybercriminals use to break in.

Why Security Updates Are Crucial

New security vulnerabilities are discovered every day. Microsoft responds by releasing patches typically at least once a month. Occasionally, they'll release emergency patches if the risk is severe.

If you're running a supported version of Windows and keeping it updated, you're much more likely to be protected from these emerging threats. On the other hand, outdated or unsupported systems are low-hanging fruit for attackers.

What Happens If You Don't Have an Operating System That Gets Security Updates?

Running an unsupported version of Windows—such as Windows 7 (ended January 2020) or Windows 10 (ending October 14, 2025)—means you're no longer receiving essential security updates. Here's what that means in real terms:

1. You Become a Target: Cybercriminals know which systems are vulnerable and no longer patched. They scan the internet looking for these machines. Running an unsupported OS is like leaving your front door wide open with a sign that says "No Alarm System Installed."

2. You Could Lose Access to Software and Services: Over time, other software developers stop supporting outdated systems as well. You may no longer be able to install modern applications or access secure websites. Even Microsoft 365 apps and browsers may stop functioning properly.

3. You Risk Compliance Violations: If your business is in a regulated industry—like healthcare, finance, or legal—using unsupported systems could put you out of compliance with industry standards, exposing you to fines or legal liability.

4. Increased Risk of Downtime and Data Loss: Unsupported systems are more likely to crash or become infected with ransomware. Recovering from an attack can take days or even weeks, leading to costly downtime, data loss, and reputational harm.

Real-World Examples

The WannaCry ransomware attack in 2017 exploited a vulnerability in older versions of Windows. It affected more than 200,000 computers in over 150 countries, shutting down hospitals, businesses, and government agencies. The fix for that vulnerability had been available—but only for systems receiving updates.

Countless small businesses fall victim to business email compromise and credential theft each year, often because of outdated operating systems missing key security patches that could have blocked the attack.

What You Should Do Now

Know What You're Running: Check which version of Windows you're using and whether it's still supported. Windows 10 will reach end-of-support on October 14, 2025—so now is the time to plan your upgrade.

Install Updates Promptly: Make sure Windows Update is turned on and configured to install patches regularly. Avoid postponing updates unnecessarily.

Upgrade Outdated Systems: If your PC or server is running an unsupported OS, it's time to consider an upgrade. In some cases, hardware upgrades may be needed to support Windows 11 or newer systems.

Security updates are your first line of defense in a constantly evolving threat landscape. Ignoring them is like leaving your business unlocked at night.

WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to another business in need of IT services. Referrals help us keep costs down so we can pass the savings to our clients.

If your referral ends up becoming a client - we'll gift them their first month of service at no charge AND we'll gift you a $500 Amazon Gift Voucher.

Simply introduce me via email to stan@fcskc.com and I'll take it from there. I personally promise we'll look after your referral's business with a high level of care and attention (just like we do with all our clients).
-Stan

We Want Your Feedback

Here at Ferguson Computer Services, we value your feedback greatly and would appreciate if you took time from your busy schedule to leave us a review. These reviews let us know what we are doing well and what we might be able to improve on in the future.

Leave a Google Review Leave a Facebook Review

TECHNOLOGY TRIVIA TIME

Technology Trivia Question of the Month! Send the correct answer to winner@fcskc.com to be entered to win a $50 gift card to Amazon.

Here is June's question of the month:

What is Cyber Insurance?