

Rocky Dunkman
Owner/CEO

CC&M Provides Comprehensive Incident Response and Disaster Recovery Plans to Their Customers

Leading Managed Technology Services Provider Helps Local Businesses Plan Ahead for Any Situation

GREENWOOD & GREENVILLE SOUTH CAROLINA – October 27, 2026 - CC&M a leading managed technology services provider (MTSP), is protecting small to mid-sized businesses (SMBs) from cyberattacks by implementing incident response and disaster recovery plans. Cybercriminals are increasingly targeting SMBs over large corporations because stricter penalties and harsher regulations have forced larger organizations to fortify their networks from attack, whereas most SMBs try to overlook this threat from affecting their organization. Cybercriminals have responded by searching for the "low-hanging fruit," which is underprepared SMBs that are far too busy and under resourced to develop a comprehensive IT cybersecurity defense strategy. CC&M has responded to this by developing comprehensive incident response and disaster recovery plans for its customers to ensure that they remain in business in event of a costly breach.

"Most business owners overlook cybersecurity because they are far too busy. Additionally, they're undereducated on how they can mitigate these risks without needing to hire a CTO or become an IT expert themselves. While they remain focused on growth, some business owners take out cybersecurity insurance policies in an attempt to secure their organizations. However, these cybersecurity insurance policies often become voided if the organization doesn't have incident response and disaster recovery plans in place, which the company actively implements within the organization. In the event of an incident, insurance companies will do everything they can to avoid paying, and they can routinely exploit ignorance or negligence on the business owner's part when it comes to cyberattacks," stated Rocky Dunkman, Owner/CEO of CC&M.

Incident response and disaster recovery plans are necessary to ensure that cybersecurity insurance policies will be honored, in addition to minimizing the impact on an organization. An acceptable incident response plan includes written procedures for multiple departments, including legal, IT, insurance, and even public relations, so that in the event of a breach the threat can be neutralized immediately. It's vital that the threat is instantly contained, remediated, and removed, so that critical systems can be restored right away. According to the 2021 "Cost of a Data Breach" report from IBM, they found "nearly 75% of organizations don't have a consistent enterprise-wide incident response plan." They also found, "The cost of a data breach is around 50% or $2.46 million lower on average for those that have an incident response plan versus those that don't."

For non-technical owners, it can be challenging to assess how well the organization is prepared, due to their lack of personal expertise. Yet, there are still ways to know if your current provider is adequately preparing your organization. For example, one thing the business owner should expect is access to a constantly evolving SOP (standard operating procedure) that details how each department should respond to different types of breaches. IT providers should be spotting new techniques ahead of time and developing responses to new tactics. Additionally, many reputable providers also implement, "tabletop exercises" with customers, which are akin to NASA launch tests, where staff practices their responses by talking through the exact steps they would take. This is beneficial because it aligns everyone's efforts, ensures collaboration and is also very

useful in the event where you need to prove legitimacy for a cybersecurity insurance claim. It's much tougher to assert negligence, when the business is continually optimizing their specific response plan SOPs in addition to actively doing "tabletop exercises" to simulate cyberattacks on a regular basis.

It's pivotal for organizations to set aside time to develop their incident response plan so they can secure their organizations and reestablish the "peace of mind" necessary to build a thriving business. "Businesses are heavily reliant on virtual infrastructure, and this is not going to slow down. However, with an ounce of preparedness, they can establish the solid foundation upon which a legacy can be built," added Dunkman. "Business owners shouldn't have to deal with this but it's important that we protect our customers, which is why we educate them, even when it's a somber topic such as this."

ABOUT Computer Consultants & Merchants Inc (CC&M)

In 1992, Computer Consultants & Merchants was founded to bring technology services and equipment to businesses in the Orlando, Florida area. In 2001 they expanded their footprint by adding offices in Greenwood and later Greenville covering the Upstate of South Carolina. CC&M streamlined the way companies do business, and the Company became successful for its expertise and service. Providing consulting, business acumen, and of course maintenance services that have always included parts and labor for clients.

Computer Consultants has evolved to meet the changing needs of businesses, providing clients with exemplary technology consultation, Business phone Systems, Access Control with Video surveillance, Cyber Security, Managed Print, integration and Managed services are still the core of everything we provide.

Thirty years later CC&M is still doing what it does best, providing its clients with advanced technology solutions and stellar service!