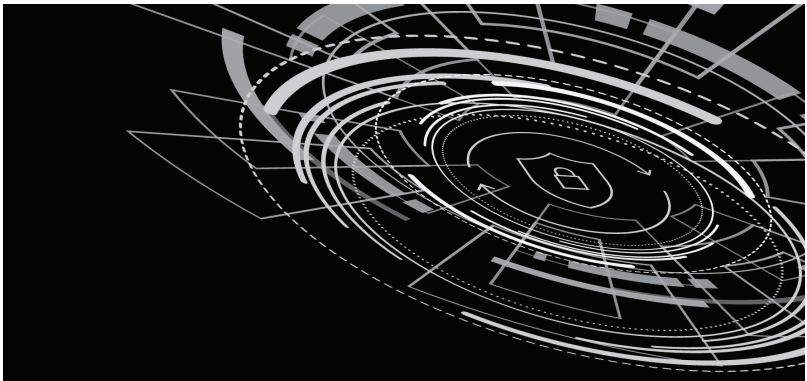
CYBERSECURITY:
THE SILENT BATTLEFIELD

Leverage The Power Of Cybersecurity
With Compliance To Defend Your Business
From Invisible Cyber Predators

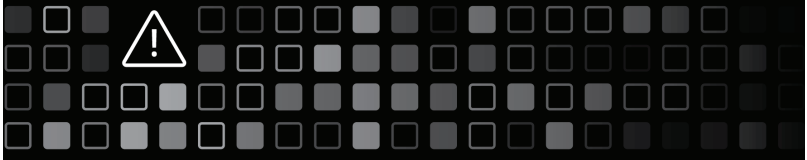
ADAM CROSSLEY

FEATURING CYBERSECURITY
EXPERTS FROM AROUND THE WORLD



CYBERSECURITY:
THE SILENT BATTLEFIELD

Leverage The Power Of Cybersecurity With Compliance To Defend Your Business From Invisible Cyber Predators



FEATURING CYBERSECURITY EXPERTS FROM AROUND THE WORLD

BigRedMedia
a TMT company

Nashville, Tennessee

Chapter 1:
The Critical Cyberthreats: How To Protect Your Business From Downfall

Adam Crossley
CEO, Fairoaks IT

What if you lost $100,000 or $200,000 simply because you clicked the wrong button?

An action that took you less than 10 seconds and – POOF! – your money disappears without a trace and is unrecoverable.

As a cybersecurity expert who has helped countless small and medium-sized businesses (SMBs) protect their digital assets, I've seen firsthand the devastating impact a cyberattack can have. Recently, a prospect I met sent $120,000 to a bad guy's bank account. The small business owner didn't realize what happened until days later when the actual vendor called and asked where his payment was because it was overdue. An investigation ensued. The FBI got involved. But nobody could do a thing because the bad actors had immediately converted the money to cryptocurrency, making it untraceable.

Here's how it happened: Bad actors hacked into the CEO's email six or seven months prior. They lurked in there, watching and paying attention to the vendors, accounts payable, and so on. They found a particularly susceptible vendor and pretended to be that vendor. They bought a domain name that was extremely similar to the vendor's, so it looked the same at a quick glance. The bad guys stole the vendor's email signature and emailed the CEO to tell him they were updating their accounts payable information and that their next payment should go to the new account. Of course, the updated information was the bad actor's bank account and routing information.

Gone are the days when only big businesses were targeted. Now, small businesses are increasingly at risk – about 10 times more than two years ago. The bad guys cast a wide net, targeting 1,000 businesses versus 10 large ones. The cost of a cyberattack can be crippling, with 95% of incidents at SMBs resulting in losses of up to $653,587. Even worse, 50% of SMBs report that recovering from an attack took 24 hours or longer.

Historically, small businesses haven't invested in the protections they need to safeguard themselves, and the bad guys know it, making small businesses easier targets. So, what are the top threats facing SMBs?

Threat #1: Social Engineering

Social engineering involves exploiting human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security. Attackers utilize information they know about a person to gain and manipulate their trust.

Tactics include:

- **Phishing Emails:** These fraudulent emails appear legitimate, tricking recipients into revealing sensitive data or clicking malicious links. Phishing emails account for approximately 80% of reported security incidents. For example, an attacker targets a company on LinkedIn, learning the CEO's name and who their admin is. They gather personal information about the CEO and use it to impersonate them. They create a fake email account – usually a Gmail or Yahoo account – mimicking the CEO and request urgent financial assistance from the admin. The admin complies, believing the request is legitimate.
- **Phone Scams:** These involve fraudsters impersonating trusted entities, such as tech support, to extract information.
- **Impersonation:** Attackers pose as colleagues or executives to deceive employees. With artificial intelligence technology, impersonation can now occur over phone calls by replicating someone's voice.

Threat #2: Ransomware And Malware

Ransomware attacks will cost businesses an estimated $265 billion annually by 2031. Ransomware is triggered by opening a malicious email attachment, leading to file encryption and ransom demands for decryption.

Malware, similarly installed via email, is capable of multiple types of theft, including keyloggers that capture keystrokes, allowing bad actors to access sensitive information, such as bank account passwords.

Threat #3: Weak Passwords And Improper Storage

Weak passwords pose a significant vulnerability, as they are easily guessable. Never use the same password for multiple platforms. Storing passwords in unprotected Word documents or browsers like Google Chrome or Microsoft Edge is highly insecure.

Threat #4: Poor Patch Management

Over 60% of data breaches occur because of unpatched vulnerabilities. Many users postpone updates, ignoring the crucial security patches from software vendors like Microsoft and Adobe. Malicious actors can exploit unpatched software to steal information or install ransomware. While some users may think updates are just for new features, most address security issues.

Threat #5: Insider Threats

Whether malicious or accidental, insider threats contribute to 34% of data breaches. Although insider threats are less frequent than other types, they tend to have a higher impact.

Insiders can access sensitive information, such as account and Social Security numbers, making these threats particularly concerning. Examples include disgruntled employees who are being terminated or contractors with malicious intent. For instance, Russian hackers planted USB drives in a U.S. nuclear power plant parking lot. Unsuspecting employees picked up the USB drives and used them, giving the hackers access.

What Can SMBs Do To Protect Themselves Against These Threats?

SMBs are attractive targets for several reasons. Many lack dedicated IT security teams, resulting in outdated software, unsecured networks, and significant security gaps. Employees may have a lower awareness of cybersecurity best practices. Perhaps most crucially, SMBs often have limited financial and human resources to invest in comprehensive cybersecurity measures.

But here's the good news – protections once available only to big corporations are now accessible to SMBs. Managed services providers (MSPs) offer enterprise-grade security services at an affordable cost, employing trained cybersecurity professionals to manage and mitigate risks.

So, what practical steps can SMBs take to fortify their defenses? It starts with the fundamentals:

- **Multifactor Authentication (MFA):** MFA stops 70% of basic attacks by requiring additional verification beyond passwords. It is essential for protecting email and financial accounts, including *all* bank accounts, investment accounts, and payroll accounts. Physical security tokens (peripheral devices required to gain access to electronically restricted devices), which are impossible to hack, are recommended for critical accounts. While MFA strategies may feel inconvenient, they are *absolutely* necessary. The extra 30 seconds you spend verifying and authenticating can prevent a bad actor from gaining access to your email, bank account, etc. It's important to always verify any requests for sensitive information by calling the sender directly.

- **Strong, Modern Endpoint Protection:** Install robust security software on devices. This includes antivirus as a base layer, with managed detection and response (MDR) added for enhanced security. Zero-trust architecture prevents unauthorized actions on a computer, stopping malware and ransomware before they can be executed.
- **Proper Backup And Disaster Recovery Services:** BDR services mitigate ransomware damage by restoring recent backups. Frequent backups ensure data recovery, even if you're attacked. BDR is preferred over simple backups to ensure comprehensive protection. Regular backups only back up files, which means that if your computer gets infected with ransomware, catches on fire, is stolen, etc., you'll lose all your settings and programs. It would take a day or two to completely rebuild your computer. With BDR, not only will your files be backed up, but image backups also allow quick restoration of *entire* systems, preserving all your settings, programs, and even your background picture. With BDR, you can be up and running within 20 to 30 minutes.
- **Managed Detection And Response Services:** MDR monitors for suspicious behavior within your IT ecosystem, such as keyloggers sending your keystrokes to a random location; it spots and shuts down malicious scripts and monitors your network traffic to look for attack behavior. MDR provides continuous monitoring, detection, and incident response for all types of IT security situations, and a competent MSP can run this entire system for you.
- **Password Managers:** Password managers address password fatigue and reuse by making it effortless to generate strong, complex passwords and save them securely, eliminating the need

to remember them. Password managers provide secure storage and encryption, making them an inexpensive and easy-to-use solution. An MSP can import passwords from browsers with a single click, making the transition seamless.

- **Patch Management:** Regularly apply security patches to keep operating systems and applications up to date. Monitor vulnerabilities by staying informed about security advisories. IT partners must understand the status of all patches across your IT ecosystem, including PCs, servers, and third-party applications. While some MSPs can only patch operating systems, comprehensive MSPs can also patch third-party software. To evaluate your IT company, request a patch status report. If your IT company delays or cannot provide a prompt report, it's a red flag indicating they might not be managing patches effectively.
- **User Activity Monitoring Systems And Access Controls:** Limit access based on roles and responsibilities to prevent malicious actions, protect sensitive information, and ensure that no single person has full authority over financial transactions. Monitoring employee computer activity is also essential for detecting unusual behavior. For example, create policies that separate duties, such as requiring multiple checks when money leaves your business accounts. An MSP plays a critical role in this process. Your provider should be familiar with industry-specific policies and local regulations so they can advise you on what can be legally monitored and provide necessary monitoring services.

But technology is only part of the equation. Regular security awareness training reduces human error, which, in my experience, causes 92% of breaches or potential breaches. Your employees are your

first line of defense. The following sections offer insight into what you should invest in, starting with security awareness training.

Security Awareness Training

Educate your staff about cybersecurity threats and hold them accountable to company policies and procedures. Teach them to use strong passwords, handle customer information securely, and spot and report malicious behavior. Encourage the use of secure password management tools to further protect sensitive information.

User awareness training educates employees about common social engineering tactics and includes phishing simulations tailored to specific industries. For instance, look for a system that sends fake phishing emails that look like they are from a system you may use. One email example is "Your Adobe or Microsoft 365 password has expired. Click here to reset it."

Conducting Background Checks

Do a deep and multistate background check on all employees, especially those in critical roles. Employees considered for HR, accounting, and critical infrastructure groups should be treated as if you were hiring someone to work at a nuclear power plant.

Compliance with state or federal regulations requiring background checks is also essential to avoiding liability. If you hire an employee with a history of criminal activity and they do something malicious, you could be held responsible.

Implementing Robust Policies

Policies should include access controls, data handling guidelines, strong password policies that require complex passwords, and incident response plans. Policies help ensure employees follow security protocols and protect employers in case of legal issues resulting from breaches. A good MSP can provide a cybersecurity-focused template to make this easier and ensure you cover all your bases.

Cyber Insurance

Cyber insurance is essential for financial protection against breaches and ransomware attacks. While the measures listed above should be your primary focus, cyber insurance is your safety net if all else fails and your company is breached. However, *full adherence* to security policies and measures, such as MFA and endpoint protection, is required for coverage and claims. Implementing security measures and training can also reduce insurance premiums.

In the last ransomware incident my company was called in to resolve, the client received an $800,000 Bitcoin ransom demand to unencrypt its data. The underwriter was fully prepared to transfer the $800,000 Bitcoin to the Russian state-sponsored group responsible.

Outsourcing Security Operations

Business owners frequently feel overwhelmed by IT tasks, let alone managing IT security, which can be a significant burden. Outsourcing a security operations center (SOC) and managed detection and response to a qualified MSP can alleviate this, providing SMBs with expert security without the cost of an in-house team.

A SOC is a centralized unit offering broad security management, including continuous monitoring, detection, and incident response. It handles various tasks, such as observing network traffic, investigating security incidents, managing compliance, and performing vulnerability assessments and forensics.

MDR specializes in rapid threat detection and response, using artificial intelligence and threat intelligence to swiftly identify and react to sophisticated attacks. With 24/7 monitoring, MDR teams watch for anomalies and potential threats around the clock. While AI aids in quick detection, human cybersecurity engineers are essential for spotting unusual behavior and delivering rapid incident responses.

When selecting an MSP to outsource these security services, choose one that understands the challenges of small businesses and offers personalized security plans. Ensure the MSP has industry experience and knowledge of your business sector's specific security needs. Verify their ability to support and secure your critical business applications and provide on-site support if needed. Ask about their security-breach experience and response strategies to evaluate their SOC and MDR capabilities and certifications.

While the cybersecurity landscape may seem daunting, SMBs are not defenseless. By understanding the threats, implementing robust security measures, and fostering cybersecurity awareness, SMBs can significantly reduce their risk. Partnering with a knowledgeable MSP is crucial, offering SMBs access to scalable, enterprise-level, cost-effective security. With continuous monitoring, incident response, and threat intelligence tailored to their specific needs, small businesses can navigate the digital landscape with confidence and resilience.

About Adam Crossley

Adam Crossley serves as CEO of Fairoaks IT, a distinguished cybersecurity and managed services provider with a prominent presence in Charlotte, North Carolina, and Franklin, Massachusetts. Under Adam's expert guidance, Fairoaks IT has fortified businesses and provided comprehensive IT consultations for over three decades. With a mission to ensure security and efficiency, Adam brings together his vast experience in cybersecurity, IT management, and process improvement and applies it to deliver enterprise-level IT security and support for his clients.

Founded in 1991, Fairoaks IT has become synonymous with reliable and professional IT services. Catering to business owners in Eastern Massachusetts, Rhode Island, and Charlotte, NC, the company's team of talented IT professionals, led by Adam, are adept at transforming IT nightmares into seamless, secure operations. Responsible for securing thousands of users, Adam is recognized for his dedication and excellence in IT. His commitment to cybersecurity is unwavering, offering a sanctuary of safety and efficiency to small and medium-sized businesses.

Adam's journey to the top of Fairoaks IT is marked by a rich and varied background, encompassing critical roles in the defense sector, public company mergers and acquisitions, government compliance, and process improvement. His tenure with Sikorsky Aircraft on the U.S. Navy's Seahawk helicopter program underscored the importance of mission-critical operations, a focus he now brings to his clients' IT and

cybersecurity needs. Adam's strategic insights have been instrumental in ensuring compliance with stringent standards like NIST 800-171, CMMC, and FTC Safeguards, helping many clients secure more contracts by getting them compliant and bolstering their defenses against cyberthreats.

Throughout his career, Adam has coordinated numerous cybersecurity incident responses, ranging from minor breaches to major incidents. His expertise in this arena is not only recognized but celebrated, as evidenced by his receipt of the prestigious Soteria Award, honoring him as one of the "Most Trusted MSPs in America." Furthermore, Adam has shared his knowledge and insights through his Amazon #1 best-selling book, *The Compliance Formula*, a valuable resource for businesses striving to achieve optimal cybersecurity practices.

Adam's expertise has garnered attention from major media outlets, including MarketWatch, Newsmax, Business Insider, and Fox. His thought leadership and commitment to cybersecurity have made him a sought-after voice in the industry, further solidifying Fairoaks IT's reputation as a leading IT service provider.

Outside his professional realm, Adam is a licensed private pilot, a passion that mirrors his meticulous and calculated approach to IT management. Adam's adventurous spirit is evident when navigating the skies or exploring the great outdoors. However, his most cherished moments are those spent with his caring wife and two young sons, Theodore and Harrison.

For more information, contact Adam Crossley at Fairoaks IT:
Phone: 844-835-8218
LinkedIn: linkedin.com/in/adam-crossley-04296a235/
Email: adam@fairoaksit.com
Web: FairoaksIT.com

CYBERSECURITY:
THE SILENT BATTLEFIELD

ABOUT ADAM CROSSLEY

Adam Crossley is the CEO of Fairoaks IT, a leading cybersecurity and managed services provider with offices in Charlotte, NC, and Franklin, MA. With over three decades of experience, Adam has helped businesses secure their IT infrastructure, ensuring efficiency and compliance. His expertise spans cybersecurity, IT management, and process improvement, delivering enterprise-level security solutions to small and mid-sized businesses.

Founded in 1991, Fairoaks IT is renowned for its reliable, professional IT services across Eastern Massachusetts, Rhode Island, and Charlotte, NC. Adam and his team specialize in transforming IT challenges into secure, streamlined operations, protecting thousands of users. His deep commitment to cybersecurity has earned him recognition as one of the most trusted MSPs in America.

Adam's career includes critical roles in the defense sector, public company M&As, and government compliance. His work on Sikorsky Aircraft's Seahawk helicopter program reinforced his focus on mission-critical operations—an approach he now applies to cybersecurity. He has guided numerous businesses through compliance with NIST 800-171, CMMC, and FTC Safeguards, helping them secure contracts and strengthen defenses against cyber threats.

A seasoned incident response expert, Adam has managed breaches ranging from minor security issues to major cyberattacks. His leadership in the field earned him the prestigious Soteria Award, recognizing his excellence in cybersecurity. He is also the author of the Amazon #1 best-selling book The Compliance Formula, a go-to resource for businesses navigating cybersecurity challenges.

Adam's insights have been featured in MarketWatch, Newsmax, Business Insider, and Fox, solidifying his reputation as a thought leader in IT security.
Beyond his professional life, Adam is a licensed private pilot, an adventurer at heart, and an avid outdoorsman. However, his greatest joy comes from spending time with his wife and two young sons, Theodore and Harrison.

Designed and Produced by Big Red Media
Printed in the USA

BigRedMedia
a TMT company