Keep Your Business from Getting Home-Aloned

As the holidays approach and offices empty out, cybercriminals are watching and waiting. Just like the Wet Bandits targeting vacant homes, threat actors know exactly when businesses let their guard down. This year, don't let your organization become their next target.

The Holiday Heist Problem

While you're already thinking about setting your Out-of-Office reply and finalizing travel plans, cybercriminals are setting traps of their own. Being prepared for the end-of-year period starts now and represents a perfect storm of vulnerability: distributed teams, rushed deadlines, and attention focused anywhere but security.

The statistics are alarming. **Cybercrime spikes by over 30% during the holiday season**, with ransomware attacks, phishing campaigns, and account takeovers reaching their annual peak. Why? Because threat actors know that when teams go remote, backups go ignored, and systems run on autopilot, detection and response capabilities plummet.

In short, the digital burglars know you're distracted — and they're counting on it.

30%

Holiday Cybercrime Spike

Increase in attacks during end-of-year period

3x

Phishing Surge

More malicious emails targeting businesses

Why Cyberattacks Surge During the Holidays

The holiday season creates a unique convergence of vulnerabilities that threat actors exploit systematically. Understanding these risk factors is the first step toward protecting your organization.

Reduced Staffing

Fewer eyes monitoring alerts and security tickets means significantly longer dwell times for intruders. When your SOC operates at half capacity, attackers have more time to move laterally undetected.

Increased Travel & Remote Logins

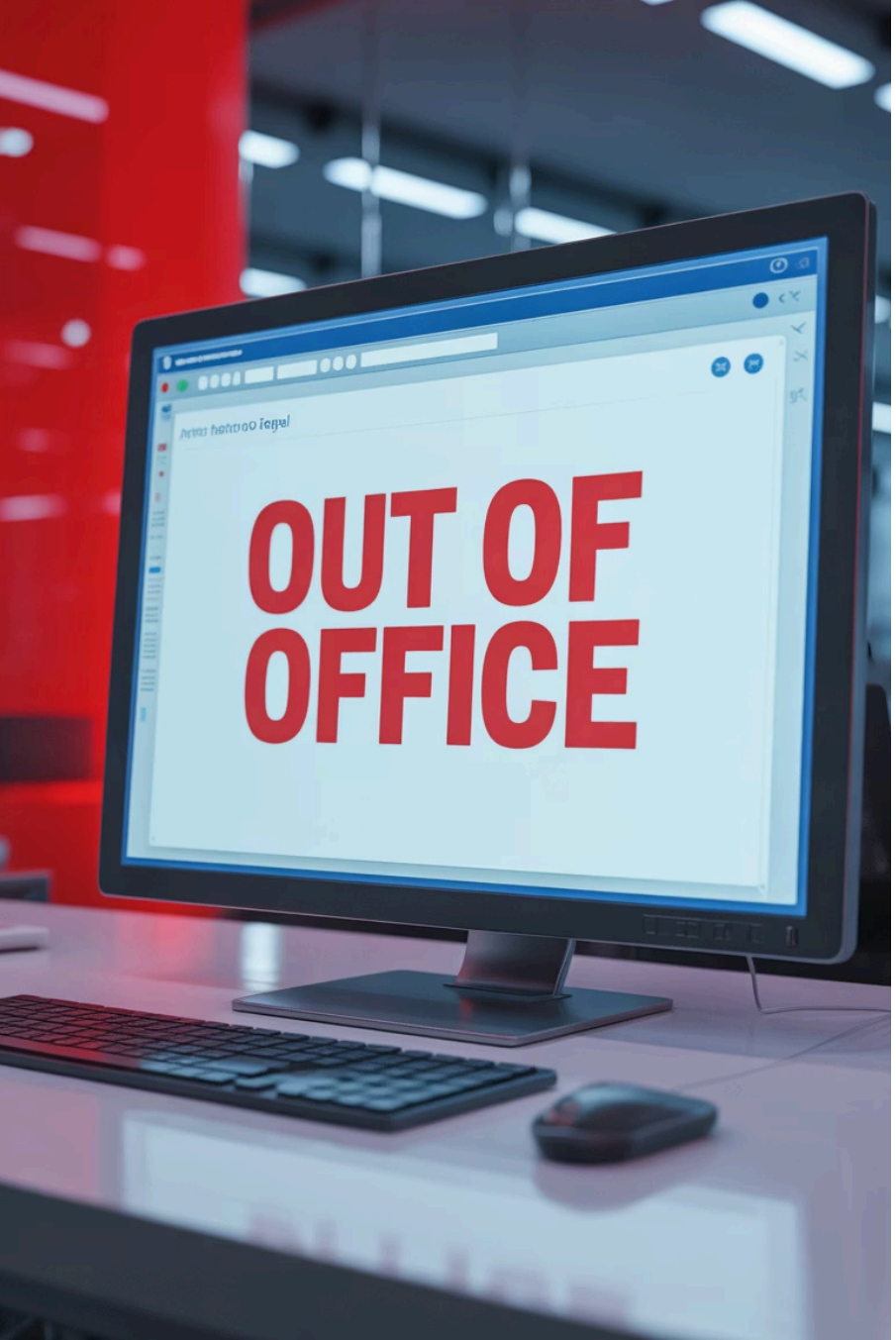
More VPN connections from hotel Wi-Fi and public networks create expanded attack surfaces. Each remote login represents a potential credential theft opportunity.

Financial Transaction Rush

Invoice fraud and business email compromise scams spike as teams rush to close books. Year-end financial pressure makes verification steps easy to skip.

Weakened Security Routines

Critical patches get delayed, updates postponed, and credentials shared in the rush to "just get it done before year-end." Security hygiene deteriorates under deadline pressure.



The "Out of Office" Factor

Every automated email reply broadcasting your absence is reconnaissance gold for attackers. Social media posts about holiday travel provide a roadmap of exactly when key personnel are unavailable. Combined with public LinkedIn profiles showing org charts, threat actors can map your entire vulnerability window before launching their attack.

Remember: Information that seems harmless to share can become weaponized intelligence in the wrong hands.

Defend Your Digital House

Just like Kevin McCallister preparing for the Wet Bandits, you don't need to panic — you just need a plan. Here's how to booby-trap your network and protect your business before the bad guys show up.

The following security measures form your holiday defense strategy. Each action reduces your attack surface and improves detection capabilities during the critical end-of-year period.

Essential Holiday Security Measures

01

Lock Every Digital Door

Enable Multi-Factor Authentication (MFA) on all accounts, especially email and remote login systems. Audit user access lists thoroughly and disable old accounts, contractor access, and former employee credentials before the break. Every orphaned account is a backdoor waiting to be exploited.

02

Unplug Unused Entry Points

Shut down non-essential servers, remote desktops, and open ports that won't be needed over the holiday period. Pause unnecessary scheduled tasks and confirm that critical backup systems are tested, current, and verified functional. Reducing your attack surface is your most effective defense.

03

Beware of Holiday Phishing

Stay vigilant for fake package delivery notices, surprise HR bonus announcements, and urgent travel update emails. Never click links from unknown senders — always verify requests through official channels. Attackers weaponize holiday urgency and generosity against you.

04

Train Your Team Before They Go

Run a quick security refresher covering phishing recognition, password hygiene, and safe remote work practices. Make it clear that security protocols don't take PTO. A five-minute reminder before the break can prevent a devastating breach in January.

Backup and Monitoring Essentials

Backup Like You Mean It

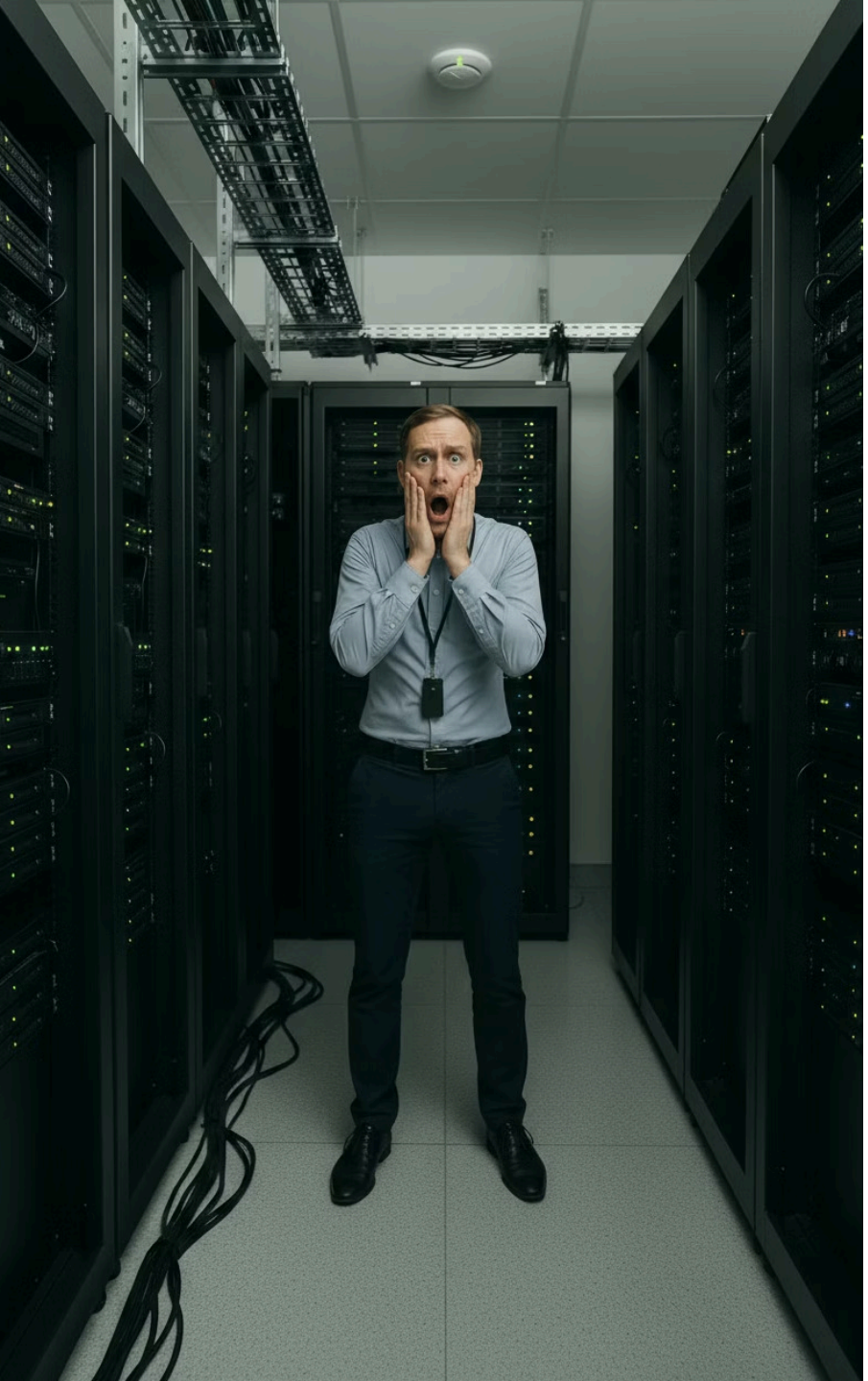
Confirm that off-site and cloud backups are encrypted and current. But don't stop there — actually test restoring a file or system before everyone leaves.

A backup untested is a backup untrusted. When ransomware strikes, you'll need confidence that your recovery plan actually works.

Know Who's on Watch

Ensure incident response contacts are up-to-date and reachable throughout the holiday period. Set up monitoring alerts to notify multiple team members if something goes wrong.

No single point of failure means faster response times when minutes matter most.



Holiday Cybercrime by the Numbers

Understanding the scope of holiday cyber threats helps justify the investment in year-end security preparations. These statistics reveal why attackers target this vulnerable period.

43%

Phishing Increase

Rise in malicious emails during November-December

67%

Longer Dwell Time

Attackers remain undetected longer during holidays

58%

BEC Fraud Jump

Business email compromise attempts surge year-end

These aren't random numbers — they represent real businesses that became victims because they underestimated holiday cyber risk. Don't let your organization become part of next year's statistics.

Cyber Command's Got the Lights On

Even when your office is quiet and your team is celebrating with family, **we're awake so you don't have to be.** Our 24/7 U.S.-based Security Operations Center monitors for threats, hunts for anomalies, and ensures your systems stay as protected as a well-booby-trapped suburban mansion.

Whether you need help performing a comprehensive Holiday Security Checkup or simply want a second set of expert eyes before your team signs off for the year, we've got you covered.

Relax. IT's Covered.

Holiday Security Checkup

Comprehensive pre-break assessment of vulnerabilities and exposures

24/7 SOC Monitoring

Continuous threat detection when your team is away

Incident Response Ready

Expert team on standby for immediate threat response

Five Things to Check Before You Clock Out

Your final pre-holiday security checklist. Complete these steps before setting your Out-of-Office reply to ensure your business stays secure while you're celebrating.

1. **Verify all critical backups completed successfully within the last 24 hours**
2. **Confirm MFA is enabled on all administrator and privileged accounts**
3. **Review and update incident response contact list with holiday phone numbers**
4. **Disable unnecessary remote access points and legacy VPN connections**
5. **Send final security reminder email to all staff about phishing awareness**

Ready to Secure Your 2025?

Don't wait until January to address security gaps discovered during a holiday breach. **Schedule your 2025 Cyber Readiness Review today** or book a complimentary 30-minute Year-End Security Checkup with our team.

Contact Cyber Command now to ensure your business starts the new year secure, compliant, and ready for growth.