

THE ALS GROUP

*Managing Risk to Influence Successful Outcomes*

## Hackers Don't Take Holidays: 4 Security Questions to Answer Before Thanksgiving

**Key Takeaways**

- Attackers strike when offices are empty, and the holidays are prime time.
- Before the long weekend, answer four questions: Is MFA on everywhere? Who's watching while you're away? Do vendors still have access they don't need? What is your team typing into AI tools?
- Your cyber policy responds best when your actual controls match what you told the carrier.

Hackers don't take holidays. They wait for yours. The office empties out, the IT team is on PTO, and the inbox fills with shipping notices, e-cards and year-end paperwork. In a 2025 Semperis survey, more than half of ransomware attacks hit on a weekend or holiday, and most organizations admitted they cut security staffing over the holidays (Axios).

**1. Passwords alone aren't enough: turn on MFA everywhere**

- Multi-factor authentication ("MFA") adds a second check before anyone gets in. Microsoft's 2025 Digital Defense Report found that phishing-resistant MFA blocks more than 99% of identity-based attacks.
- Your cyber insurance application almost certainly asked whether you use MFA. If the answer was "yes" but it isn't on for email, remote access and admin accounts, that "inadvertent" error can give a carrier grounds to challenge your claim.

**2. Someone has to be watching while you're away, and your backups have to work**

- Name the person or IT provider who will answer an alert over the holiday, and who has authority to shut systems down.
- Confirm your backups ran, are stored separately from your network, and have actually been tested. A backup nobody has restored is a hope, not a plan.

**3. Vendors with access to your systems need a check before the break**

- IT providers, software vendors and contractors often have remote access, and attackers know it. Confirm who has access and turn off what isn't needed.
- Make sure your contracts require key vendors to carry cyber insurance, and check how your own policy treats a breach that starts at a vendor.

**4. Your team's use of AI needs a simple rule**

- Free, public AI tools may keep or learn from what people type into them, including client names, financials and contracts.
- Set a simple rule: approved tools only, and nothing confidential in anything else. Insurers are starting to add AI-related language to their forms, so know where your policy stands.

**New Jersey**
**175 Main St**
**Woodbridge, NJ 07095**
**+1.732.395.4250**

**Florida**
**1800 NW Corporate Blvd Ste 202**
**Boca Raton, FL 33431**
**+1.561.437.0024**

**info@thealsgroup.com**
**thealsgroup.com**



**How ALS Helps**

We read your cyber policy the way a claims adjuster will: comparing your application answers to your actual controls, checking ransomware and vendor breach coverage, and flagging exclusions before they become a "surprise." As your "outsourced" risk manager, we make sure the coverage you are paying for responds when you need it. For more holiday-specific guidance, see our earlier CISA/FBI Holiday Cyber Advisory.

There you have it: four questions to answer before the turkey hits the table.

**Frequently Asked Questions**

**Why do cyber attacks increase during the holidays?** Fewer people are watching. Offices are closed, IT teams are thin, and employees are distracted by travel and shopping emails. Attackers time ransomware and phishing campaigns for exactly those windows.

**Does cyber insurance cover a breach that starts at one of our vendors?** Not always. Some policies cover it, some limit it and some exclude it. Read how your policy treats breaches at third parties, and require key vendors to carry their own cyber coverage.

**What if our cyber application says we use MFA but we don't use it everywhere?** Fix it now, and tell your broker in writing. Misstatements on an application, even honest ones, can give a carrier grounds to dispute or limit a claim. It is far better to correct the record before a loss than after.

**Is it safe to use free AI tools with client information?** Assume not. Many free tools may keep or use what you enter, and once confidential data leaves your control you can't pull it back. Use business-grade tools with clear data terms, and put a short written policy in place.

**How does ALS help with cyber risk without selling insurance?** We review your existing program from your side of the table, tie it to the controls you actually have, and tell you where the gaps are. If you need more coverage, we help you get it through your broker; if you're over-insured, we tell you that too.

*If you need more information on any of the topics covered here, or are interested in a Risk Management Assessment ("RMA"), please contact our Managing Principal, Albert Sica, at asica@thealsgroup.com or at 732.395.4251.*

Sources: Axios: Why hackers love the holidays (Semperis data); SOCRadar summary of the Microsoft Digital Defense Report 2025