LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

AUGUST 2026

THWARTING THE ENEMY

Why Counterintelligence Matters

Counterintelligence is more than protecting classified information—it is about protecting our employees, customers, business operations, and national security. Every organization that works with government agencies, critical infrastructure, or sensitive technologies is a potential target for foreign intelligence services, cybercriminals, competitors, and malicious insiders.

Many successful security breaches begin with something that appears harmless: a conversation at a conference, a LinkedIn connection request, an unsolicited email, or someone asking "just a few questions." Attackers are patient. They collect small pieces of information over weeks or months until they have enough intelligence to compromise an organization.

Every employee—regardless of job title—is responsible for protecting sensitive information and reporting suspicious activity. Security awareness is our first and strongest line of defense.

Think Before You Share

One of the biggest misconceptions in security is that only classified information requires protection.

In reality, adversaries often build intelligence by collecting dozens of pieces of publicly available or unclassified information. Information such as project names, employee roles, supplier relationships, software platforms, travel schedules, facility layouts, or organizational structures can all be combined to reveal sensitive operational details.

Before discussing work-related information, ask yourself:

✓ Is this information intended for public release?
✓ Does this person have a legitimate business need to know?
✓ Could this information be combined with other information to reveal something sensitive?

***Remember: Loose conversations create intelligence opportunities.**

Conference & Business Travel Security

Professional conferences, trade shows, vendor meetings, and industry symposiums provide valuable networking opportunities—but they also provide opportunities for adversaries to identify experts, collect information, and establish long-term relationships. Foreign intelligence

Foreign intelligence collectors frequently attend these events posing as:

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com

- Researchers
- Students
- Investors
- Customers
- Industry experts
- Recruiters

Common tactics include:

- Asking technical questions that appear harmless
- Offering future consulting opportunities
- Requesting copies of presentations
- Asking to continue conversations after the conference
- Connecting through LinkedIn after the event

Best Practices:

✓ Attend pre-travel security briefings.
✓ Use company-approved devices.
✓ Never leave laptops unattended.
✓ Keep conversations professional and appropriate.
✓ Report suspicious encounters after returning.

Stop Phishing Before It Starts

Cyberattacks rarely begin with sophisticated hacking. Instead, attackers rely on convincing employees to open malicious attachments, click dangerous links, or provide sensitive information voluntarily. Warning signs include:

- Unexpected invoices
- Password reset requests
- Urgent executive requests
- Fake vendor notifications
- Job offers requiring technical information
- Requests to bypass security procedures

Before clicking any link:

- Verify the sender.
- Inspect the email address carefully.
- Hover over hyperlinks.
- Contact the sender using a trusted method.
- Report suspicious emails immediately.

Remember: When in doubt - dont click.

Insider Threat Awareness

Insider threats are not always intentional. Employees experiencing financial hardship, personal stress, coercion, or workplace dissatisfaction may become vulnerable to exploitation without realizing it. Potential indicators include:

- Sudden unexplained wealth
- Significant financial problems
- Frequent policy violations
- Unusual working hours
- Downloading excessive amounts of data
- Attempts to access information outside normal duties
- Personality or behavioral changes

Reporting concerns early is about protecting coworkers—not accusing them of wrongdoing. Early intervention can prevent security incidents while providing employees with needed assistance.

Social Media Safety

Social media has become one of the most valuable intelligence collection tools available to adversaries. Photos, job descriptions, conference attendance, travel announcements, and comments about work projects can all reveal sensitive information. Before posting online, consider whether your post reveals:

- Customer information
- Project names
- Facility locations
- Security badges
- Computer screens
- Whiteboards
- Travel schedules
- Internal meetings

Even information shared privately may eventually become public. Think before you post.

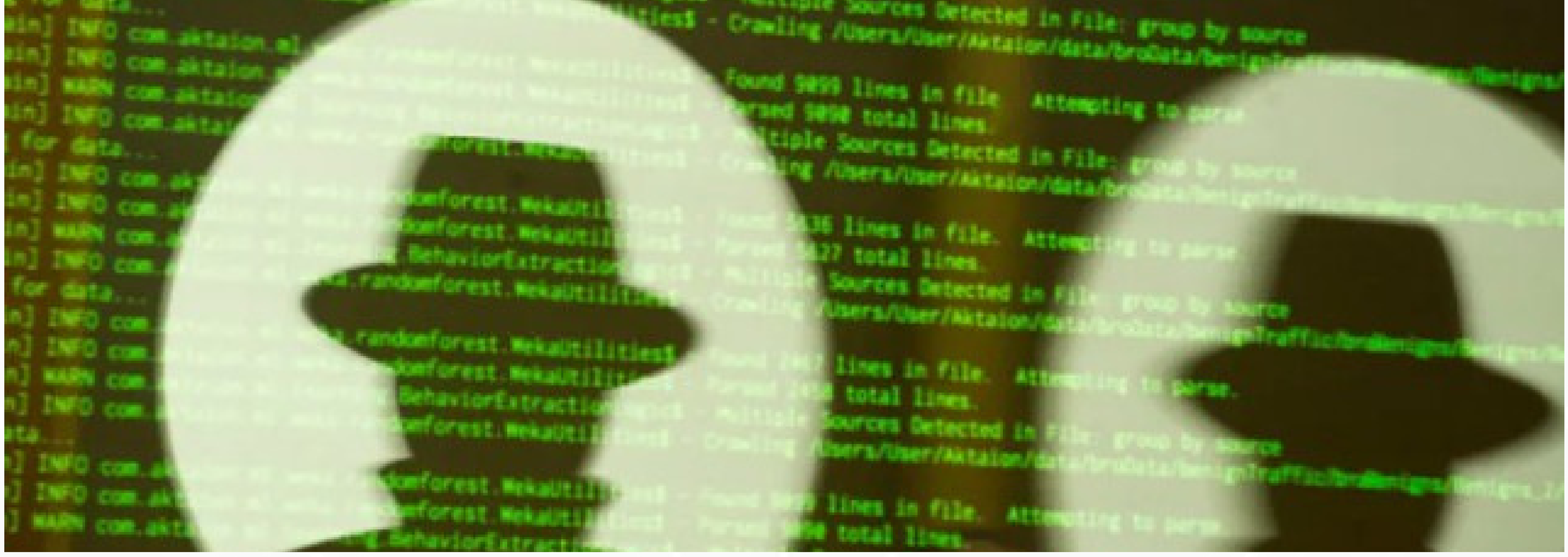
Security Check

Every employee can strengthen organizational security by practicing these habits every day.

DO:

✓ Verify identities before sharing information.
✓ Lock your computer whenever you leave your desk.
✓ Wear your identification badge visibly.
✓ Challenge unknown visitors politely.
✓ Report suspicious contacts immediately.
✓ Follow all cybersecurity policies.

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com



✓ Protect company equipment while traveling.
✓ Ask questions if you're unsure.

DON'T:
X Share internal information on social media.
X Discuss projects in public places.
X Click unknown links.
X Ignore suspicious behavior.
X Assume someone else has reported it.
X Circumvent security controls for convenience.

Report! Report! Report!

Security depends on timely reporting. Immediately report:

- Suspicious emails
- Social engineering attempts
- Foreign contacts
- Unauthorized photography
- Lost or stolen equipment
- Unusual computer activity
- Insider threat indicators
- Physical security concerns
- Unauthorized visitors

Never worry about "over-reporting." Security professionals would rather investigate ten harmless reports than miss one genuine threat.

Security Tip of the Month

Trust Your Instincts!!! If something feels unusual, it probably deserves a second look. Whether it's an unexpected email, an unfamiliar visitor, an unusual request, or someone asking too many questions, pause before responding. A few extra seconds of caution can prevent months—or even years—of security consequences.

Remember

Security is not just the responsibility of the Security Office or Information Technology—it belongs to every employee, every day. Together, we protect our people, safeguard sensitive information, and strengthen our organization's mission by remaining alert, informed, and proactive. Stay Alert. Stay Informed. Stay Secure.

Read at your own leisure:

- U.S. Department of Justice. (2026, June 30). Former soldier-turned-contractor found guilty of stealing over $1 million of MREs in El Paso. U.S. Attorney's Office, Western District of Texas. https://www.justice.gov/usao-wdtx/pr/former-soldier-turned-contractor-found-guilty-over-1-million-mres-el-paso
- U.S. Department of Justice. (2026, June 26). Former U.S. National Security Advisor, John R. Bolton II, pleads guilty to violating the Espionage Act. U.S. Attorney's Office, District of Maryland. https://www.justice.gov/usao-md/pr/former-us-national-security-advisor-john-r-bolton-ii-pleads-guilty-violating-espionage
- U.S. Department of Justice. (2026, June 24). Chinese citizen arrested, charged with money laundering and wire fraud conspiracy involving gold coins/bullion. U.S. Attorney's Office, Western District of New York. https://www.justice.gov/usao-wdny/pr/chinese-citizen-arrested-charged-money-laundering-and-wire-fraud-conspiracy-involving-gold-coinsbullion

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com