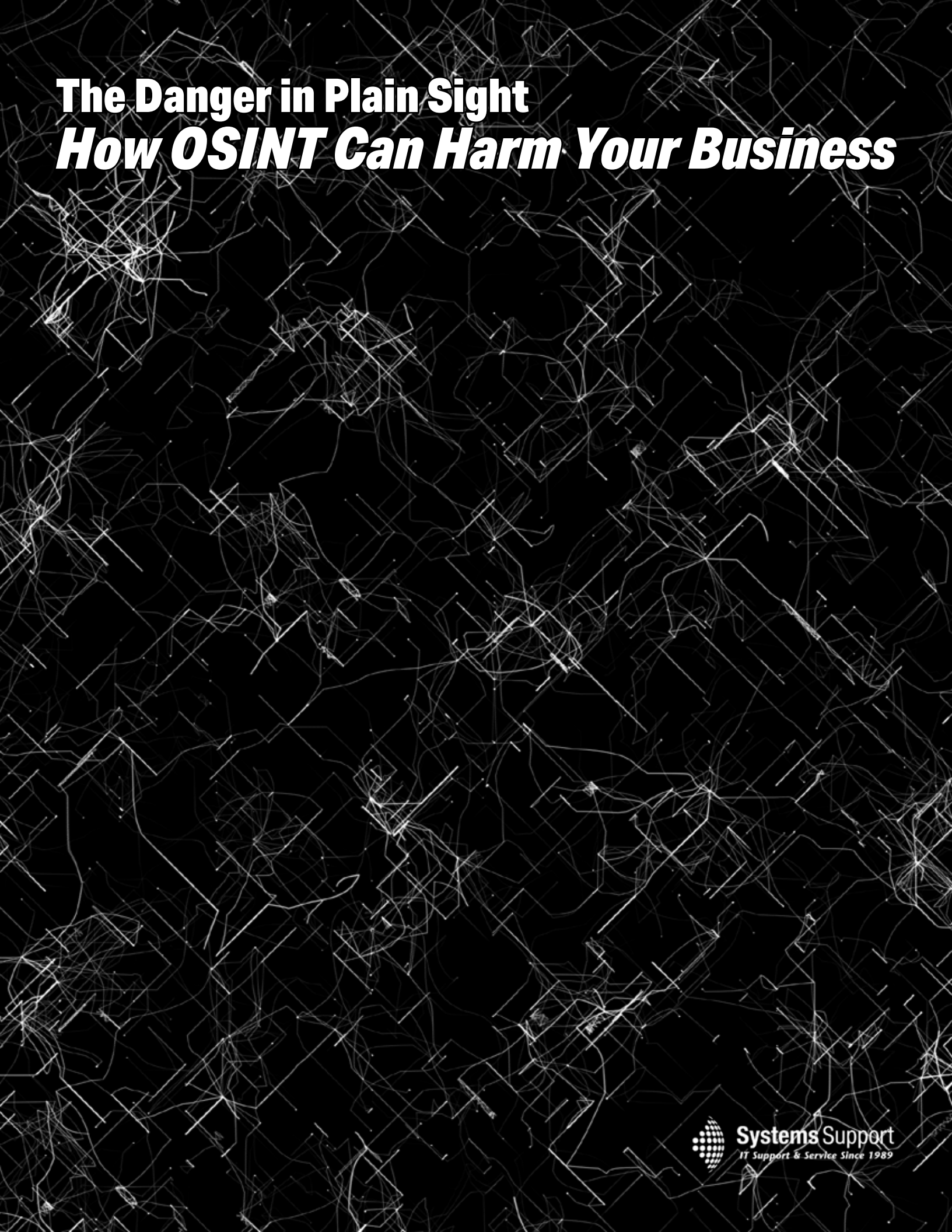
The Danger in Plain Sight
How OSINT Can Harm Your Business



Systems Support
IT Support & Service Since 1989

From The Desk Of: William MacFee
President, Systems Support Corporation

Dear Colleague,

In today's world, cybersecurity isn't just about firewalls and antivirus software—it's about awareness. What's online about your business, your team, and your processes might seem harmless, but in the wrong hands, it can become the first step in a very real threat.

That's where OSINT—Open Source Intelligence—comes in.

Most businesses don't realize just how much information they're putting out into the world every day. Job postings, social media profiles, outdated web pages—these can all paint a detailed picture of your organization for someone who wants to do harm. And often, without any breach or hacking required, just careful research and patience.

At Systems Support, we believe in a security-first approach. That means helping our clients see the bigger picture, and thinking holistically about cybersecurity. It's not just about protecting systems—it's about protecting your people, your reputation, and your future.

This white paper is designed to help you understand how OSINT works, why it matters, and what practical steps you can take to reduce your exposure. We've kept it straightforward and actionable, because we know most business owners aren't cybersecurity experts—and you shouldn't have to be.

If reading this opens your eyes to risks you didn't know you had, that's a good thing. And we're here to help you take the next step.

Stay safe and stay smart,

William MacFee,
President

Table of Contents

1.0 What Is OSINT ...03

- 1.1 How Hackers Use OSINT ...04
- 1.2: How Businesses Use OSINT ...05
- 1.3: OSINT vs. Dark Web Data ...05
- 1.4: Historic OSINT Incidents ...06

2.0: Key Vulnerabilities ...07

- 2.1: Hunting Grounds: Common OSINT Leaks ...07
- 2.2: How OSINT is Used to Attack ...08

3.0: How to Protect Your Business ...09

- 3.1: Reducing Your OSINT Footprint ...09
- 3.2: Striking the Balance - Transparency vs. Security ...10
- 3.3: Practical First Steps for Business Owners ...11

4.0: Conclusion ...12

Systems Support
IT Support & Service Since 1989
www.systemsupport.com

462 Plain St, Suite 206
Marshfield, MA 02050
(781) 653-7916
info@systemsupport.com

What Is OSINT?

OSINT stands for Open Source Intelligence. It refers to any information that can be gathered legally from publicly available sources. That includes things like:

- ***Your company's website***
- ***Social media profiles (yours and your employees')***
- ***News articles or press releases***
- ***Government and business filings***
- ***Public databases or search engine results***
- ***Files and documents available online — even ones you forgot about***

It's the same kind of information a potential customer might find when researching your business. But it's also the same information a hacker might use to plan an attack.

Cybercriminals use **OSINT** in the early stages of targeting a business. They search for employee names, email addresses, job titles, office locations, outdated software versions, and even photos or documents that reveal internal tools or processes. The more they can learn about you without alerting you, the more tailored — and dangerous — their next move can be.

But **OSINT** isn't only a threat. It's also a tool. Security professionals and IT teams use **OSINT** to monitor exposure, investigate incidents, and understand how a company looks from the outside in. Knowing what's out there is the first step toward securing it.

How Hackers Use OSINT

Open Source Intelligence (OSINT) is a double-edged sword. The same publicly available information that can help a business understand its market, track competitors, or make more informed decisions can also be used by malicious actors to target that very organization. Understanding how OSINT is used—both ethically and unethically—is critical to reducing risk and leveraging its power responsibly.

Most cyberattacks today don't begin with a technical breach—they start with research. By compiling publicly accessible data, attackers build detailed profiles of organizations and individuals. This reconnaissance phase allows them to identify weak points and create believable, customized attacks.

Common Sources of Attacker OSINT:

- ***Search Engines:*** Public-facing documents, press releases, company policies, and contact information.
- ***Social Media:*** Personal updates, employee titles, job changes, and behavioral patterns.
- ***Company Websites:*** Staff listings, downloadable files (which often include metadata), technology stack clues, and organizational charts.
- ***Public Databases and Registries:*** WHOIS records, state business filings, job postings, and court documents.

What They're Looking For:

- ***Employee Identifiers:*** Names, titles, and roles that help craft spear-phishing campaigns or impersonate leadership.
- ***Email Patterns:*** To guess internal email addresses or create spoofed domains.
- ***Outdated Technology Footprints:*** Clues about servers, CMS, or software in use—especially if known vulnerabilities exist.
- ***Company Behavior:*** Routine activity, event participation, or office closures that could time an attack for maximum impact.

How the Information is Used:

- ***Phishing and Social Engineering:*** Crafting convincing messages that mimic internal communications or vendors.
- ***Credential Stuffing:*** Testing exposed credentials against known usernames or email addresses.
- ***Impersonation:*** Posing as executives, HR reps, or IT support to request urgent action or sensitive data.
- ***Pre-Attack Mapping:*** Building an internal map of your infrastructure or decision-making chain to plan a broader attack such as ransomware deployment.

The more data available about your organization online, the easier it becomes for an attacker to build trust—or manipulate trust—without ever touching a line of code.

How Businesses Use OSINT

While OSINT can pose serious risks when overlooked, it also offers valuable advantages to organizations when used intentionally.

Security and Risk Management:

- ***Conduct Internal Searches:*** Review what's publicly available about your company, leadership, and employees.
- ***Audit External Content:*** Examine websites, social profiles, and digital documents for overexposed or outdated information.
- ***Monitor Mentions and Data Leaks:*** Use tools or alerts to track new mentions of your company, employees, or sensitive topics.

Strategic and Competitive Intelligence:

- ***Track Competitors:*** Public job postings, product announcements, or media coverage can reveal business directions and opportunities.
- ***Vet Third Parties:*** Investigate potential partners, vendors, or customers using financial filings, review sites, and industry-specific data.
- ***Understand Market Sentiment:*** Aggregated public opinion—forums, ratings, and user commentary—offers insight into market trends and consumer behavior.

The line between helpful data and harmful exposure is thin. For businesses, the real danger is not knowing what's already publicly accessible. Hackers use OSINT because it works. Smart businesses use OSINT to stay ahead of threats—and ahead of the curve.

OSINT vs. Dark Web Data: What's the Difference?

Not all information used in cyberattacks comes from shady corners of the internet.

OSINT is data that's publicly available — the kind anyone with a web browser can find. Think Google searches, LinkedIn bios, employee photos, or downloadable PDFs from your website.

By contrast, dark web data typically comes from breaches and leaks. It includes stolen passwords, personal information, or internal documents bought and sold through hidden marketplaces.

Here's the key difference:

- OSINT is about what you're already sharing, often without realizing it.
- Dark web data is what's been taken from you, usually after a breach.

Both are dangerous. But OSINT is often the first step hackers take — because it's easy, quiet, and legal.

Twitter Bitcoin Scam (2020)

What Happened:
High-profile Twitter accounts (Elon Musk, Barack Obama, Apple, etc.) were hijacked in a coordinated scam to promote a fake Bitcoin giveaway.

OSINT Angle:
The attackers used OSINT to identify internal Twitter employees and contractors with administrative access. They impersonated coworkers using info from LinkedIn and social media, then used social engineering to get access credentials over the phone.

Lesson:
Job titles and internal systems exposed on LinkedIn can be weaponized to gain internal access.

CEOs and CFOs Targeted in BEC Scams

What Happened:
Hundreds of businesses have lost money through Business Email Compromise (BEC) scams, where attackers impersonate a CEO or vendor and request wire transfers.

OSINT Angle:
Attackers build profiles using social media, press releases, and company news to learn executive names, roles, travel schedules, and vendor relationships. This info makes phishing emails believable.

Lesson:
Public info about employees and business operations can be used to mimic authority and bypass scrutiny.

Spear Phishing Attack on RSA Security (2011)

What Happened:
RSA, a major security company, was compromised through a phishing attack that led to the breach of SecurID authentication products.

OSINT Angle:
Attackers researched employees to find likely targets for malicious email attachments. One employee received a file titled "2011 Recruitment Plan," and opened it. It exploited a Flash vulnerability.

Lesson:
Even security companies aren't immune — attackers used job titles and organizational info to tailor convincing emails.

HUNTING GROUNDS

Common OSINT Leaks in Small and Medium-Sized Businesses

Small and medium-sized businesses (SMBs) are particularly vulnerable to OSINT-based threats. Unlike large enterprises, SMBs often lack dedicated security teams or regular information audits, making it easier for attackers to exploit freely available data. Here are some of the most common sources of OSINT exposure—and how they can turn into real risks.

1. Staff Listings on Websites

Many businesses list employees, leadership, and contact details on their websites to promote transparency or facilitate communication. But this can hand attackers a ready-made target list.

Risk: These listings often include names, job titles, and email addresses, which attackers use for spear-phishing, impersonation, or social engineering.

Example: A CEO listed with a direct email becomes a prime candidate for a business email compromise (BEC) scam.

2. Overexposed Social Media Profiles

Team members who post openly about their roles, schedules, or workplace routines create a trail that hackers can use to map internal workflows and identify potential weak points.

Risk: Public bios and posts on LinkedIn or Instagram might reveal who's on vacation, who's in IT, or who just got promoted—all valuable context for an attacker crafting a convincing phishing message.

Tip: Even seemingly innocent posts like "out of office all week" or "handling finance operations" can be leveraged by bad actors.

3. Job Postings and Career Pages

Job listings can unintentionally reveal your tech stack, internal pain points, or strategic plans.

Risk: Listings that ask for experience with specific platforms (e.g., QuickBooks, AWS, Microsoft 365) give attackers a clue about what systems are in use—and what exploits might be relevant.

Example: A posting for a "network admin to replace aging infrastructure" tells attackers the business might have outdated or unpatched equipment in place.

4. Exposed Documents with Metadata

Many businesses upload downloadable brochures, PDFs, or reports without realizing that embedded metadata (like author names, software versions, or network paths) can reveal more than intended.

Risk: Metadata in a PDF might show a username that matches an employee's login name—or reveal the file was created on an internal network labeled "HR-Server01."

Tip: Always scrub files of metadata before publishing.

5. Misconfigured or Outdated Websites

Old plugins, exposed directories, or unprotected admin panels can be indexed by search engines or

discovered via simple Google dorking.

Risk: These vulnerabilities are often the first exploited in opportunistic attacks.

Example: A contact form that leaks email addresses in its HTML, or a forgotten subdomain still hosting an old admin portal.

6. Business Registrations, Legal Filings, and Vendor Contracts

Public records may include addresses, ownership details, and contract awards—useful for attackers conducting reconnaissance.

Risk: Details like "registered agent" names and mailing addresses help attackers verify legitimacy or impersonate stakeholders.

OSINT isn't just theoretical—it's everywhere. The everyday ways businesses try to be accessible, transparent, and user-friendly can unintentionally provide attackers with the breadcrumbs they need. Knowing what you're exposing is the first step toward protecting it.

Of course this list isn't exhaustive; most businesses need to have a wealth of public-facing data to function whether it's so they can be found in a search or build credibility with clients who also trust but verify.

HOW OSINT IS USED TO ATTACK

Reducing Your OSINT Footprint

You can't eliminate all publicly available information about your business—but you can take control of it. Reducing your OSINT footprint is about knowing what's out there, minimizing unnecessary exposure, and establishing smart internal practices to limit future leaks.

Below are practical, scalable strategies businesses can implement to make themselves a harder target for attackers.

***

1. Audit What's Publicly Available — Regularly

Think like an attacker. Start with a simple search:

- Google your business, domain, and key employees.
- Use variations of email addresses and job titles.
- Explore what autocomplete, image search, and filetype searches reveal.

Why it matters: You'll likely be surprised by how much turns up. Old job listings, cached PDFs, and social media mentions can stay visible long after you've forgotten them.

Tip: Conduct this kind of review quarterly—or whenever you publish new staff pages, news articles, or career postings.

***

2. Tighten Website Content and File Management

Your website is a critical point of exposure—and a magnet for OSINT.

- Remove unnecessary staff listings or replace direct email addresses with contact forms.
- Scrub documents of metadata before uploading. Use tools like Adobe Acrobat or ExifTool.
- Minimize technical detail: Avoid disclosing your tech stack or security measures.

Why it matters: The less you share unnecessarily, the fewer angles attackers can exploit.

***

3. Review Job Listings for Technical Detail

HR doesn't always think like security. Many job posts contain valuable insight for attackers.

- Avoid listing every system, platform, and process you use.
- Generalize responsibilities instead of revealing internal operations.
- Use an HR contact form or anonymized job post email, not named individuals.

Why it matters: Job postings are a goldmine for anyone trying to identify your internal tech ecosystem.

***

4. Establish a Social Media Policy

Social media is a double-edged sword. It builds trust—but it can also create risk.

- Ask staff not to post sensitive info (e.g., travel plans, project names, client identities).
- Keep personal and business accounts separate where possible.
- Limit who manages or posts from company accounts and review content before it goes live.

Why it matters: Many OSINT-driven attacks start with a social media scan.

***

5. Train Employees to Recognize OSINT Risks

Awareness is your first line of defense.

- Incorporate OSINT education into cybersecurity training.
- Teach teams how attackers might use the information they share.
- Provide clear examples of social engineering attempts based on public info.

Why it matters: Your team is both your strongest asset and your greatest potential vulnerability.

***

6. Know When to Bring in Expert Help

Even if you've reviewed your site, scrubbed your files, and trained your staff, a third-party review can often catch what you've missed.

- Consider a professional OSINT audit.
- Use managed IT services to spot misconfigurations or open endpoints.
- Schedule periodic external assessments—just as you would a financial review.

Why it matters: Objective insights often reveal blind spots. And attackers don't care how big your company is—just how exposed you are.

***

Reducing your OSINT footprint isn't about becoming invisible. It's about managing visibility with intention. Know what's out there, keep what's necessary, and cut the rest.

Striking the Balance — Transparency vs. Security

Today's customers and clients expect to know the businesses they work with. They want to see real names, real people, and real values. Transparency builds trust.

But that trust can come at a cost.

Oversharing—especially online—can expose your team to phishing, impersonation, and targeted attacks. So how do you stay approachable and secure?

Here's the balance to aim for:

- **Be personable, not revealing**

Use first names, general roles, and group bios when possible. Avoid listing detailed job functions or personal emails on your site.

- **Be clear without overexplaining**

Clients want to understand your process—but don't need to know your backend systems, tech stack, or vendor relationships.

- **Choose contact forms over direct listings**

Instead of publishing team emails, route inquiries through a general form that gets triaged internally.

- **Post selectively on social media**

Culture posts are great—just don't include internal project names, client info, or exact schedules that could be exploited.

- **Train your team on boundaries**

Encourage staff to be thoughtful ambassadors, not open books. A little caution goes a long way.

Remember: You're not hiding; you're protecting. You can be accessible without being exposed.

Staying Ahead

Practical First Steps for Business Owners

Most small and medium-sized businesses aren't negligent—they're just unaware of what's out there. The good news is: you don't need to be a cybersecurity expert to start protecting your organization from OSINT-based threats.

Here are your first practical steps:

1. Search Like a Stranger

Open an incognito window and search for:

- Your name
- Your business name
- Key staff members
- Company email domains
- Your physical business address

Ask yourself: What could someone with bad intentions learn about us? Could this information be used to impersonate someone at my company, craft a phishing email, or gain trust under false pretenses?

2. Review Your Website and Content

Look for:

- Staff bios that include job titles, project names, or email addresses
- Downloadable documents like PDFs or spreadsheets—are they current? Do they contain metadata?
- Blog posts or press releases that mention systems, software, or vendors

Your website should market your business—not map out your internal operations.

3. Audit Social Media Presence

Examine your company profiles and employee accounts for:

- Oversharing (e.g., project details, travel schedules, internal tools)
- Unmonitored or outdated accounts
- Public discussions that reveal internal structures

Encourage your team to keep personal posts separate from professional platforms and to limit location-tagging or detailed work descriptions.

4. Review Job Postings and Recruitment Sites

Job boards can leak:

- What software you use
- What internal systems you're upgrading
- Who handles what responsibilities

All of these details are valuable to attackers trying to build a profile of your infrastructure and hierarchy. Share necessary job info, but avoid excessive detail.

5. Create an Internal Awareness Campaign

Your team is your best defense—if they know what to watch for. Set aside time for regular discussions on cybersecurity hygiene. Even a quarterly meeting can keep the risks visible and top of mind.

Your digital footprint already exists. The question is whether it's working for your business—or opening a door to someone else.

Small adjustments today can help you avoid big problems tomorrow.

Building a Long-Term OSINT Strategy

Cybersecurity isn't a one-time fix—it's an ongoing commitment. As your business grows, so does your digital footprint. New hires, new platforms, and new partnerships all expand the surface area attackers might try to exploit.

But the same tools hackers use against you can also help protect you—if you take OSINT seriously and use it proactively.

Build OSINT Awareness Into Routine Operations

- Quarterly Self-Audits: Use our OSINT Self-Audit Worksheet to review public-facing assets and identify any new exposures.
- Monitor Your Footprint: Set up alerts for key names and terms associated with your business using tools like Google Alerts or commercial OSINT platforms.
- Review and Refresh Policies: Ensure staff onboarding includes cybersecurity awareness, and revisit your acceptable-use and privacy policies annually.
- Limit Overexposure: When possible, centralize communication through official business channels. Avoid scattering sensitive information across vendor profiles, niche platforms, and multiple domains.

Know When to Bring in Reinforcements

For small and mid-sized businesses, internal resources may be limited. It's not about doing everything in-house—it's about knowing when to ask for help.

A knowledgeable IT partner can:

- Conduct deep-dive OSINT scans
- Review your public-facing digital infrastructure
- Identify technical and procedural vulnerabilities
- Train your staff on how to recognize and respond to social engineering threats

***

Your First Move: Contact Systems Support

You don't need to guess how exposed your business is—you can find out, today.

- Download: The Business Owner's OSINT Self-Audit Worksheet to get started
- Book: A free, 15-minute discovery call with our team at Systems Support

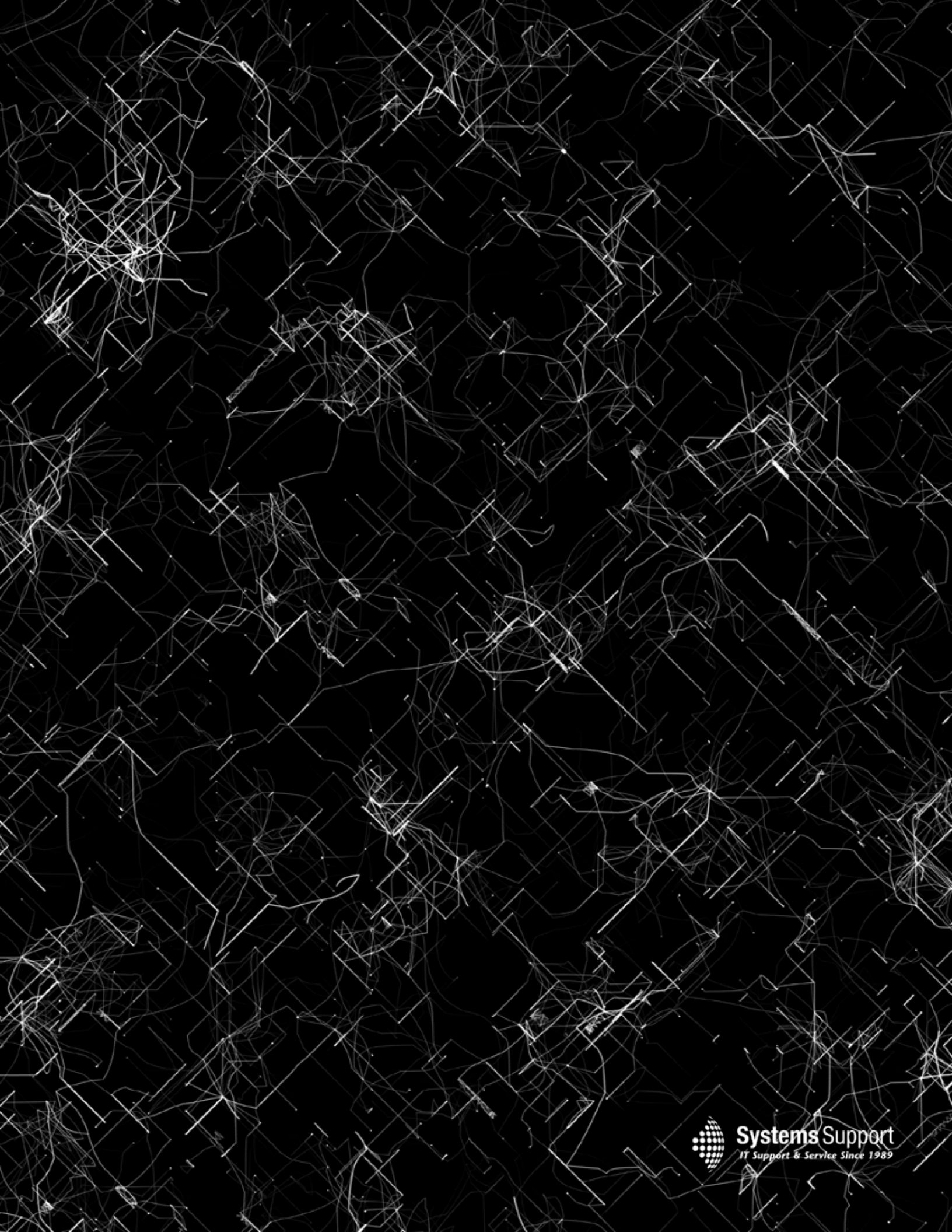
We'll help you understand your IT infrastructure and how you can improve your cybersecurity posture.

Go to: systemsupport.com/osint

Because if you don't look… someone else already is.

Systems Support

IT Support & Service Since 1989


Systems Support
IT Support & Service Since 1989