

The Latest Byte

by One Step Secure IT

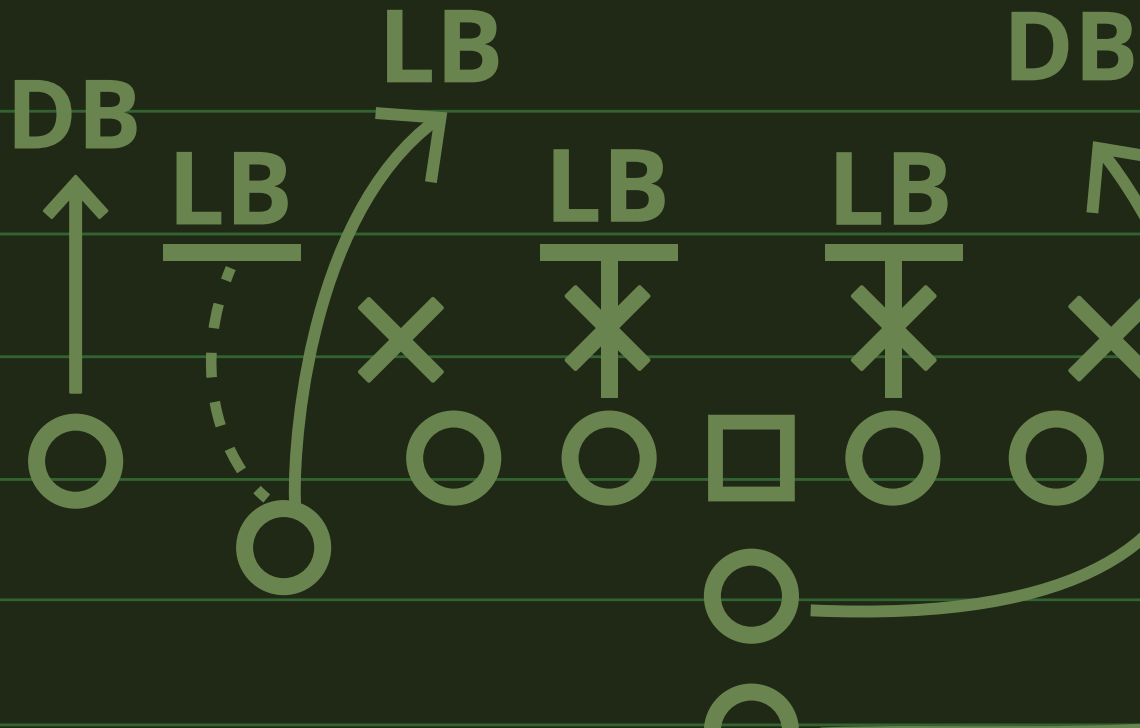
YOUR
SECURITY
PLAYBOOK

Is Your Team Ready to Run the Plays?

Football season is in full swing, and while fans are watching their teams battle for playoff position, cyber criminals are running their own plays against your business, looking for any gap in your defense.

In this issue, we're breaking out The Security Playbook, our guide to the strategies, tools, and teamwork that keep your organization ahead of the opposition this season. Strong security means disciplined fundamentals, the right players on the field, and a game plan ready before the other side even snaps the ball.

Do you have a Game Plan for what happens after a breach? It's time to make sure your defense is playoff-ready.



About Us

One Step Secure IT is an outsourced IT and cybersecurity company with over four decades protecting our customer's data from breaches to alleviate the dread of cyber attacks, costly downtime, and loss of customer trust.

Our Expertise Includes

- Cybersecurity Services
- Information Security Services
- Managed/Co-Managed IT Services
- Compliance Services

Bringing Our Clients Stronger Protection and a Smarter Way to Use AI

Two new solutions we've vetted and are now offering to our clients.

Fully-Managed SIEM + SOAR Platform

Building an in-house security team is expensive and leaves gaps. A SIEM gives you enterprise-grade protection, 24/7 monitoring, instant threat detection, and automated response, without hiring a security staff.

Why Leaders Love It

24/7 SOC Coverage

Expert eyes on your systems around the clock

One Unified Platform

No more juggling disconnected security tools

Total Visibility

On-premises, cloud (M365, AWS, Azure), and remote workers, all covered

Runs Silently

Zero drag on business performance

Compliance on Autopilot

Monitoring and reporting built in threats caught in minutes, not hours. Compliance headaches gone. Your IT team freed up to focus on growth instead of firefighting.

Secure, Enterprise-Grade AI for Your Team

Your employees are already using AI, often without approval, oversight, or security. That's a data risk waiting to happen.

Get 50+ leading AI models behind one secure, governed platform, giving your team real AI power without exposing company data.

Key Benefits

- **Secure by Design**
Company data never touches public AI models
- **Employee-Ready**
No technical skill needed to adopt
- **Centralized Control**
Manage access & policy from one dashboard
- **Consistent Results**
Standardized outputs across teams
- **Scalable**
Fits a 10-person team or an enterprise

Unlock faster content creation, smarter document analysis, automated busywork, and safe internal collaboration without the risk of shadow AI.

Give your team the productivity edge of AI, with the governance leadership demands.

Learn more about our newest solutions.
(623) 227-1997 | www.OneStepSecureIT.com



THE SECURITY DEFENSE PLAYBOOK

How to Protect Your Business Like a Pro

General best-practice guidance. See disclaimer at the end of the article.

Every great football team shows up to game day with a playbook. Not because they know exactly what the other team will run, but because they've prepared for the most likely scenarios, drilled their responses until they're automatic, and built a team that knows its role when the pressure is on.

Running a business in today's threat environment isn't so different.

Cyber attacks are no longer a remote risk reserved for large corporations or financial institutions. Small and mid-sized businesses are increasingly targeted, often because attackers know they're less likely to have the defenses of a Fortune 500 company. The good news is that you don't need an enterprise IT budget to protect your business well. What you need is a playbook.

Why Every Business Needs a Security Playbook

In football, a playbook is the collection of strategies a team uses to move the ball, defend their end zone, and respond when things don't go according to plan. In cybersecurity, a security playbook serves the same purpose: it's a documented set of strategies and responses your business uses to prevent attacks, detect threats early, and recover quickly when something goes wrong.

The absence of a plan is a risk. According to IBM's 2025 Cost of a Data Breach Report, organizations without an incident response plan and team paid significantly more per breach. They took longer to contain it than those who had prepared in advance.

If your office flooded tomorrow, you'd probably know to call your insurance company, contact a restoration service, and notify your team. You'd have a rough plan

because you've thought about it before. A cyber incident deserves the same level of preparation, and the stakes are often higher.

The Four Positions on Your Security Defense Team

A strong football defense doesn't rely on one player. It's a coordinated unit with defined roles. Your cybersecurity strategy works the same way. Here are the four core "positions" every business needs covered:

No. 1

The Defensive Line: Prevention

This is your first layer of protection. It includes tools and practices that stop threats before they reach your systems: firewalls, endpoint protection (antivirus and anti-malware software on your devices), multi-factor authentication (MFA), and keeping software up-to-date. These are your linemen. They don't make headlines, but without them, everything else falls apart.

No. 2

The Linebackers: Detection

No defense is perfect, and some threats will get through the line. Detection tools, like security monitoring software and email filtering, are your linebackers. They watch for unusual activity and flag it before it becomes a full-blown incident. Many businesses don't realize they've been compromised for weeks or months. Good detection cuts that window dramatically.

No. 3

The Safeties: Response

When a threat makes it through, your response plan kicks in. This is your incident response plan, a documented, step-by-step guide for what happens when something goes wrong. Who gets called? What

systems get isolated? Who communicates with customers or vendors? Your safeties are the last line of defense before a major breach, and a clear response plan is what keeps a bad situation from becoming a catastrophic one.

No. 4

The Coach: Governance and Leadership

Someone has to call the plays. In a business context, this is leadership's role: setting expectations for security, approving the budget for tools and training, and making sure the team is prepared. Cybersecurity decisions ultimately belong at the leadership level, not just the IT department.

Building Your Incident Response Plan: A Practical Starting Point

An incident response plan (IRP) doesn't need to be a 50-page document. For most small and mid-sized businesses, a clear, actionable, short document covering the following areas is enough to get started:

Identify Your Key Assets

What are the most critical systems and data your business depends on? Customer records, financial data, your email system, your point-of-sale system? List them. These are what you're protecting.

Define What Counts as an Incident

Not every odd email or slow computer is a crisis. But knowing in advance what warrants an immediate response, such as a suspected phishing attack, ransomware notification, unauthorized login, or data theft, helps your team act faster and with less confusion.

Assign Clear Roles

Who is responsible for each step of the response?

This should include:



WHO to contact first (internal IT, your managed IT provider, leadership)



WHO communicates externally (customers, vendors, regulators if required)



WHO makes decisions if the business owner or executive is unavailable



WHO contacts your cyber insurance carrier (and where the policy and hotline number are kept)

Document Your Response Steps

For each type of incident, write out the basic steps your team takes.

For example, if a ransomware attack is detected:

STEP 1

Disconnect affected devices from the network immediately (do not shut them down)

STEP 2

Contact your IT provider and security team

STEP 3

Notify your cyber liability insurance carrier immediately. Policies often require notice within 24–72 hours and approved vendors. Keep your policy number and hotline handy

STEP 4

Do not pay the ransom without consulting your IT and legal counsel

STEP 5

Begin documentation of what happened and when

STEP 6

Notify leadership and follow your communication protocol

STEP 7

Plan for Recovery

Response and recovery are two different phases. After containing the incident, you need a plan for getting systems back online, restoring from backups, and communicating with stakeholders. Know where your backups live, how current they are, and how long it would take to restore your systems. If you don't know those answers, that's a gap worth addressing now.



The Drills: Why Testing Your Plan Matters

Even the best playbook fails if the team hasn't practiced. Football coaches run the same plays hundreds of times in practice so that when they're called in a high-pressure moment, the response is muscle memory.

The cybersecurity equivalent is a tabletop exercise, a facilitated discussion where your team walks through a simulated incident scenario. No actual systems are touched. You simply talk through: "If this happened tomorrow, what would we do?"

These sessions often reveal gaps that nobody anticipated: unclear decision-making authority, outdated contact lists, missing backup copies of critical data, or team members who didn't know what their role was.

A tabletop exercise doesn't require a big investment of time or money. Even a 90-minute session once a year with your leadership team and your IT and security team or partner can meaningfully improve your readiness.

Three Plays You Can Run Right Now

You don't need to overhaul your entire security posture overnight. Here are three concrete steps you can take in the next 30 days:

1. Turn on multi-factor authentication (MFA) everywhere you can.

MFA requires a second form of verification, usually a code sent to your phone when logging into an account. It's one of the single most effective steps a business can take to prevent unauthorized access. Enable it on email, financial accounts, and any system that stores sensitive data.

2. Verify your backup situation.

Ask your IT and security team or provider: How often are our systems backed up? Where are those backups stored? Have we tested a restore recently? Backups are only useful if they work when you need them. This conversation takes 15 minutes and could save your business massive headaches.

3. Have the conversation with leadership.

Cybersecurity is a business continuity issue, not just an IT issue. If your leadership team has never discussed what a cyber incident would mean for your operations, finances, or reputation, schedule that conversation. It doesn't need to be technical. It just needs to happen.

Defense Wins Championships and Keeps Businesses Running

The teams that win consistently aren't always the ones with the flashiest offense. They're the ones with disciplined, prepared defenses that know how to respond under pressure.

The same is true for your business. A well-prepared company that knows how to detect, contain, and recover from a cyber incident will fare far better than one caught completely off-guard, regardless of how sophisticated the attack is.

You don't need to have all the answers today. You just need to start building your playbook.

Ready to build your **security defense** playbook?

Talk to the team at One Step Secure IT.

We work with business leaders to create practical, right-sized security strategies. No jargon, no pressure. Schedule a free conversation.



(623) 227-1997



www.OneStepSecureIT.com/contact

DISCLAIMER: This article is for general information only and is not legal, technical, or insurance advice. Every organization's risks and coverage differ, so consult your IT provider and qualified legal and insurance professionals before acting on this content.

Why Pro Sports Teams Could Run Circles Around Your Business

by Scott Kreisberg

Founder & CEO of One Step Secure IT

There's a provocative idea that's been circulating in sales leadership circles for years, popularized by renowned sales management author Jack Daly: professional sports teams are run better than most businesses.

At first glance, that sounds like a throwaway line meant to grab attention. But when you unpack it, the comparison reveals a glaring gap in how most companies operate versus how elite sports organizations are managed.

As Daly put it:

“If most businesses learned how to run themselves the way sports teams do, I guarantee they would achieve more sales and faster growth with lower costs and operating expenses.”

He's been making this argument for over a decade through his book *Hyper Sales Growth*, keynote speeches, and a series of articles. And he's not alone. McKinsey & Company reached strikingly similar conclusions in their research on what it takes to build world-class teams.



So, what do
sports teams do that
most businesses
don't?



They Have a Written Playbook

Can you imagine a football team taking the field without a specific game plan for that day?

Without studying the competition beforehand?

Daly asks business leaders to honestly assess whether their team operates with that level of preparation. Elite sports teams script out scenarios, rehearse responses, and know exactly what to do when the opponent shifts. In business, too many sales calls and client interactions are handled on the fly with minimal preparation.



They Always Recruit

Think about the top college football programs. They lose their best players every three to four years, yet they remain at the top of the standings season after season. How? Because they never stop recruiting. Daly argues that most businesses treat hiring as a reactive event triggered by an opening, whereas sports organizations treat it as an ongoing, always-on discipline. There's always room for a top performer.



They Practice Relentlessly

There's hardly anything that happens on a sales call that couldn't be anticipated in advance. Yet most sales teams spend almost no time practicing. Sports teams, by contrast, may practice five days for every one day of actual competition. Daly's point is that top-performing salespeople are "canned." They've rehearsed their responses so thoroughly that they sound natural, not scripted.



They Hold People Accountable

In sports, if you don't perform, you don't make the cut. There are clear performance standards, and underperformers are replaced. Daly's advice is blunt: hire slowly, fire quickly. He argues that keeping underperformers hurts everyone, including the underperformer, who likely knows they're struggling and would be happier elsewhere.



They Operate as a True Team

On a sports team, when one player scores, the whole team benefits. Individual stats matter, but the scoreboard is what counts. Daly notes that in too many businesses, "teamwork" is really just individuals competing against each other for the top spot on the leaderboard rather than collaborating to maximize the team's overall result.

It's Not Just Daly Saying This

McKinsey & Company reached remarkably similar conclusions in their research on building world-class teams. Their "Worst to First" framework identified four pillars drawn directly from elite sports: set uncompromising standards, build a roster with the right mix of capabilities, create a detailed playbook for consistent execution, and establish an edge through confidence and trust at every level. Their finding echoed Daly's core thesis: talent alone is never enough. Culture, clarity, and disciplined consistency are what separate champions from the rest of the pack.

Harvard Business School has also explored this territory extensively, examining how sports metaphors, blocking and tackling, calling audibles, and bench strength reflect transferable management practices rather than just colorful language.

The concept is simple but uncomfortable: if you ran your business with the same rigor, preparation, accountability, and relentless recruiting that a professional sports team brings to every season, your results would dramatically improve. The question is whether you're willing to adopt the discipline that makes the difference.

References

1. Daly, Jack. "3 Lessons from Sports Teams that Every Business Leader Must Adopt." Growth Institute Blog. <https://blog.growthinstitute.com/sales/business-sports-team>
2. Daly, Jack. "Want Hyper Sales Growth? Then Don't Focus On Sales Growth." Growth Institute Blog. <https://blog.growthinstitute.com/focus-hyper-sales-growth>
3. Daly, Jack. "Sports Teams vs. Business Teams." LinkedIn Pulse, October 29, 2014. <https://www.linkedin.com/pulse/20141029152327-34412378-sports-teams-vs-business-teams>
4. Daly, Jack. Hyper Sales Growth. Forbes Books. <https://books.forbes.com/books/hyper-sales-growth>
5. McKinsey & Company. "Worst to First: What It Takes to Build or Remake a World-Class Team." <https://www.mckinsey.com/capabilities/transformation/our-insights/worst-to-first-what-it-takes-to-build-or-remake-a-world-class-team>
6. ELAvate Global. "'Sports Teams Perform Better than Most Sales Teams' Says Jack Daly." <https://www.elavateglobal.com/sales-blogs/sports-teams-perform-better-than-most-sales-teams-says-jack-daly>
7. Harvard Business School, Baker Library. "Sports: Lessons for Managers." Working Knowledge. <https://www.library.hbs.edu/working-knowledge/sports-lessons-for-managers>
8. All icons provided by thenounproject.com

EVENT RECAP

Arizona Technology Summit Highlights

One Step Secure IT was proud to participate in the Arizona Technology Summit again this year! Our team engaged with local business leaders and industry peers to discuss the latest in IT solutions and cybersecurity. Headquartered in Phoenix, we're committed to strengthening security for businesses across Arizona.



UPCOMING EVENT

National Automobile Dealers Association Tradeshow

The NADA Show 2027 is bringing the auto retail community together on...

Dates: February 17–20, 2027

Location: Orange County Convention Center in Orlando, Florida

Booth: #469

One Step Secure IT
22520 North 18th Drive
Phoenix, AZ 85027



www.OneStepSecureIT.com | (623) 227-1997

Connect with us @OneStepSecureIT

