BUILD A CYBERSECURITY PLAN YOU CAN EXECUTE THIS QUARTER

Tailored solutions. Transformative outcomes.

Protect what you've built with security that fits your needs.

A breach can disrupt operations, damage trust, and drain resources.

The challenge?
Threats keep changing, but budgets rarely do. Too many tools can create confusion. Without a clear, prioritized cybersecurity strategy and roadmap, teams end up chasing alerts and audit findings instead of actually reducing risk.

CLA One Digital approaches cybersecurity as part of a unified data and technology strategy — designed around your organization, your industry, and the outcomes that matter most to your people.

What you'll take away

- A clear way to prioritize risks and security investments
- How to maintain audit-ready evidence for standards like PCI (Payment Card Industry), HIPAA (health data rules), or NIST CSF (an industry agnostic and widely adopted cybersecurity framework).
- How to incorporate technical aspects like penetration testing and incident response into your first 100 days

The path to building a strong cybersecurity foundation:

Baseline → *Harden* → *Prove*

Baseline
2 – 3 weeks

Identify your most critical assets systems and data that matter most

Review current protections across your systems, network, and applications

Document your current state alignment with key standards (PCI, HIPAA, NIST CSF) to create a baseline for future improvements

Build a prioritized listing of gaps and remediation items with owners and deadlines

Harden
30 – 60 days

Deploy multi-factor authentication (MFA) on all remote connections

Set patching timelines for software updates; validate and isolate backups

Improve monitoring and alerting for high-value systems

Strengthen the protections in place on end-user devices (laptops, mobile devices, etc.)

Conduct an incident response tabletop exercise (practice using the plan to establish who does what, how you communicate, and how evidence is handled)

Prove
by day 100

Perform a penetration test of your network and key applications that focuses on real business impact, not just a list of technical issues

Gather evidence for audits and exams; track the progress and status of key remediation projects

Share results with leadership: risk reduced, next steps, and budget alignment

Why milestones matter

Cybersecurity progress can feel invisible until something goes wrong. Milestones make it tangible. They show leadership, and auditors, that the team is moving fast and focusing on what matters most.

Hitting these checkpoints also ties directly to business outcomes: lower risk, stronger compliance posture, and clear evidence for audits. Here's what the first 100 days look like in practice.

By day 30:

- Baseline items are complete
- Top 10 gaps identified with owners and dates

By day 60:

- MFA, patching, and backup improvements in place
- End-user protections have been reviewed and hardened
- Incident response runbook and tabletop exercise done

By day 100:

- Penetration test completed
- Evidence organized
- Roadmap updated

Industry-specific moves

Every industry faces different risks, regulations, and operational realities. A one-size-fits-all approach doesn't work. These quick "plays" give you a starting point tailored to your sector, so you can focus on priorities built to work in the world you operate in.

- **Financial services** — Protect customer and account data, strengthen controls against fraud and social engineering, enforce strong identity and access management for employees and third parties, and maintain audit-ready evidence for regulatory and examiner reviews.
- **Health care** — Safeguard patient records under HIPAA, secure medical devices, validate backups and recovery for electronic health records, and maintain evidence for compliance audits.
- **Manufacturing** — Build operational resilience, segment operational technology networks and devices, and test recovery plans. Recovery point and recovery time objectives can help you assess how much data you can afford to lose and how fast you must recover.
- **Nonprofit** — Protect donor data, manage vendor risk, train staff regularly, and test the donation process for security risks.

Metrics that matter

Cybersecurity is about demonstrating progress, not just compliance.

The right metrics help you focus on what reduces risk, supports resilience, and keeps people productive. Metrics give leadership and auditors confidence the program is working. And they connect directly to business impact: faster patching means fewer disruptions, stronger MFA coverage reduces breach risk, and quicker response times limit downtime and financial loss.

Key numbers tell the real story:

- **Multi-factor authentication coverage** — % of users and systems requiring MFA for access to critical applications and remote connections
- **Time to detect and respond to security incidents** — Average time between detection and containment or remediation
- **Phishing and social engineering resilience** — % of employees who fall for simulated phishing attempts or report suspicious activity
- **Backup and recovery readiness** — % of critical systems with successful backup testing and documented recovery objectives
- **Third-party cyber risk coverage** — % of high-risk vendors that have undergone cybersecurity review and ongoing monitoring

Common pitfalls

Even with the right intentions, cybersecurity programs can lose sight of how peopleactually work. These mistakes are easy to make, and costly if ignored. Knowing them upfront helps keep your plan on track and your progress visible.

PITFALL

Buying tools before setting priorities

Try this instead: Strategy first, spend second

PITFALL

Collecting evidence after the fact

Try this instead: Document as you go

PITFALL

One-and-done testing

Try this instead: Schedule retests and track closure

Cybersecurity action checklist

A checklist keeps everyone aligned on the essentials: what needs to be done, who owns it, and what success looks like. Use it to brief executives and show measurable progress.

- ☐ **Assign clear executive ownership for cyber risk,** with defined accountability, regular reporting, and authority to act.
- ☐ **Require and enforce MFA** for remote access, privileged accounts, and systems with sensitive or critical data.
- ☐ **Maintain an inventory of systems** using sensitive information and understand how the data flows across the organization.
- ☐ **Perform regular backups** of critical systems and test restoration procedures to support ransomware recovery and business continuity.
- ☐ **Formally assess third-party cybersecurity risks** introduced by vendors, service providers, and outsourced IT functions.
- ☐ **Confirm core systems are hardened and segmented** using baseline security standards and logical segmentation to limit cyber incident impact.
- ☐ **Confirm existence of a documented incident response plan** including executive, legal, finance, and comms roles, and conduct periodic tabletop exercises.
- ☐ **Monitor cyber risk through consistent metrics** that provide visibility into risk reduction and control effectiveness over time.
- ☐ **Promote ongoing security awareness training** emphasizing real-world threats such as phishing, fraud, and social engineering.
- ☐ **Schedule independent cyber risk assessments** to validate controls, identify gaps, and benchmark cybersecurity maturity against peers and regulations.

A unified digital strategy, built around your business

With a clear 100-day roadmap, measurable milestones, and industry-specific priorities, you can help reduce risk, help satisfy compliance requirements, and give leadership confidence that progress is real.

From risk to readiness

CLA's cybersecurity readiness assessment is the first step. It helps you identify critical assets, uncover gaps, and create a prioritized action plan tailored to your business. From there, our digital team can guide you through strengthening controls, validating backups, and demonstrating resilience with evidence auditors can trust.

Ready to move from uncertainty to clarity? Start with a readiness assessment and take the fast path to stronger security and peace of mind.

Schedule your cybersecurity readiness assessment introductory call today. →

We'll get you there