



AN OBVIAM WHITE PAPER

Strategic Security Planning

From Reactive Defense to Business Resilience

A practical guide for business owners, executives and IT leaders on turning security spending into a funded, measurable, leadership-owned plan.

Obviam, a Modern Office Methods company
info@obviam.com | 513-699-1111 | obviam.com
October 2026

Contents

Executive Summary	1
Key Numbers at a Glance	1
1. The Problem: Security Without a Plan.....	2
Five Symptoms of an Unplanned Security Program.....	2
Why It Matters Now	2
The Overlooked Attack Surface: Print and Imaging Devices.....	2
2. What Strategic Security Planning Means	3
Six Principles	3
Built on a Recognized Standard.....	3
3. The Obviam Framework: Five Planning Questions	4
Why Questions Instead of Products.....	4
4. From Plan to Roadmap: Risk, Compliance, Budget and Metrics	5
Compliance Obligations by Industry.....	5
A Phased 12-Month Roadmap.....	5
Budgeting the Plan	6
Metrics Leadership Should See	6
5. Choosing a Strategic Security Partner	6
6. Conclusion	7
About Obviam	8
How to Cite This Paper	8
Sources	8

Executive Summary

Most organizations do not have a security problem. They have a planning problem. They buy tools after an incident, an audit finding or an insurance renewal, and end up with a stack of products that nobody can tie to business risk.

The cost of that approach keeps rising. IBM's 2026 Cost of a Data Breach Report puts the average breach at a record \$4.99 million globally and \$11.5 million in the United States. Verizon's 2026 Data Breach Investigations Report found that nearly half of all breaches now involve a third party.

Strategic security planning replaces the reactive cycle with a documented, business-owned program. It answers five questions leadership can act on: what we protect, what could stop us, what we must prove, what we fund first, and how we know it is working. This paper explains each question, shows how they map to the NIST Cybersecurity Framework 2.0, and offers a practical checklist for choosing a security partner.

Key Numbers at a Glance

Finding	Figure	Source
Global average cost of a data breach, 2026	\$4.99 million (record high, up 12%)	IBM / Ponemon, 2026
U.S. average cost of a data breach, 2026	\$11.5 million	IBM / Ponemon, 2026
Average healthcare breach cost	\$6.64 million (highest of any industry)	IBM / Ponemon, 2026
Average financial services breach cost	\$6.29 million (up from \$5.56 million)	IBM / Ponemon, 2026
Average time to identify and contain a breach	247 days	IBM / Ponemon, 2026
Breaches contained in under 200 days vs. over 200 days	\$4.32 million vs. \$5.65 million	IBM / Ponemon, 2026
Breaches involving a third party	48% (up 60% year over year)	Verizon DBIR, 2026
Breaches involving ransomware	48%	Verizon DBIR, 2026
Vulnerability exploitation as the initial way in	31%	Verizon DBIR, 2026
Share of ransomware victims that are small organizations	96%	Verizon DBIR, 2026 (via Cyber Readiness Institute)

See Sources at the end of this paper for links to each report.

1. The Problem: Security Without a Plan

Reactive security fails because it answers the last threat, not the next one. Each purchase may be sound on its own. Together they leave gaps, overlaps and no clear owner.

Five Symptoms of an Unplanned Security Program

1. **Tool sprawl without coverage.** Overlapping products protect some systems twice and others not at all. Nobody can say which risks each tool reduces.
2. **Security owned by IT alone.** Leadership signs the budget but not the risk decisions. Security becomes a cost line instead of a business choice.
3. **Compliance as a yearly scramble.** HIPAA, GLBA, PCI DSS, CMMC and cyber insurance questionnaires are handled one at a time, with evidence rebuilt each cycle.
4. **Blind spots at the edges.** Vendors, cloud apps, remote workers and connected devices sit outside the main controls. Verizon found third-party involvement in 48% of breaches in 2026, up 60% in one year.
5. **No way to show progress.** Without baseline metrics, leaders cannot tell whether last year's spending lowered risk.

Why It Matters Now

Attackers are moving faster and using automation. One in four malicious breaches IBM studied in 2026 was AI-enabled, and those cost about \$1 million more than average. Vulnerability exploitation is now the leading way in, at 31% of breaches.

Speed is the deciding factor in cost. IBM found breaches contained in under 200 days cost \$4.32 million on average, against \$5.65 million for those that ran longer. Containment speed depends on preparation done months earlier, which is exactly what a plan provides.

Smaller organizations carry outsized exposure. Small organizations made up 96% of ransomware victims in Verizon's 2026 data. They often lack a dedicated security leader, which is the gap strategic planning and a virtual CISO are built to fill.

The Overlooked Attack Surface: Print and Imaging Devices

Multifunction printers and copiers are full network computers. They store scanned images, connect to email and file shares, and often run outdated firmware with default settings. They are rarely in the scope of a security assessment.

Obviam's parent company, Modern Office Methods, has managed print and imaging fleets since 1957. That history means Obviam's planning includes devices other security firms tend to skip: MFP hard drives, scan-to-email credentials, print servers and fleet firmware.

2. What Strategic Security Planning Means

Definition: Strategic security planning is the practice of setting security priorities from business risk, documenting them in a funded multi-year roadmap, and reviewing progress against measurable outcomes at the leadership level.

It is different from buying security products, and different from a one-time assessment. An assessment is a snapshot. A strategic plan is a living program that turns the snapshot into decisions, owners, budgets and dates.

Six Principles

- 1. Business first.** Start with the operations, data and obligations the organization cannot afford to lose, then choose controls.
- 2. Leadership owns the risk.** Executives decide which risks to reduce, transfer, accept or avoid. IT and security partners carry out those decisions.
- 3. Prioritize by impact.** Fund the controls that reduce the most likely and most costly risks first, not the newest tools.
- 4. Build compliance in once.** Map controls to every framework that applies, so one set of evidence serves auditors, insurers and customers.
- 5. Plan for the bad day.** Assume a breach will happen. Rehearse response and recovery so containment is fast.
- 6. Measure and revisit.** Track a small set of metrics and refresh the plan at least yearly, or after any major change.

Built on a Recognized Standard

The National Institute of Standards and Technology released the Cybersecurity Framework (CSF) 2.0 in February 2024. It organizes security into six functions: Govern, Identify, Protect, Detect, Respond and Recover. The Govern function, new in version 2.0, places security strategy, roles and risk tolerance with leadership.

Obviam's planning approach uses CSF 2.0 as its backbone. That gives clients a common language with auditors, insurers, partners and regulators, and makes progress comparable year to year.

3. The Obviam Framework: Five Planning Questions

Obviam builds every security plan by answering five questions with the client's leadership team. Each question maps to NIST CSF 2.0 and ends in a concrete deliverable, so the plan is both business-readable and audit-ready.

GOVERN: Leadership sets risk tolerance and owns every answer			
Planning question	What it covers	NIST CSF 2.0	Obviam deliverable
1. What must we protect?	Critical operations, sensitive data, systems and connected devices, including MFPs	Identify	GRC assessment and asset inventory
2. What could stop us?	Likely threats, weak points, and vendor and third-party exposure	Identify	Risk assessment and vendor risk review
3. What must we prove?	Regulations, contracts and cyber insurance requirements we must evidence	Govern	Compliance management and control mapping
4. What do we fund first?	Controls ranked by business impact and cost, set in a dated roadmap	Protect	vCISO-led roadmap and security policies
5. How will we know it works?	Continuous monitoring, tested response and recovery, a leadership scorecard	Detect, Respond, Recover	Monitoring and leadership scorecards
↻ Revisit yearly, or after any acquisition, new system, new regulation or incident			

Figure 1. The Obviam strategic security planning framework.

Govern sits above the five because leadership owns every answer. The cycle repeats at least once a year, and again after an acquisition, a new system, a new regulation or an incident.

Why Questions Instead of Products

Product-led plans start with what to buy. Question-led plans start with what the business cannot afford to lose, so every control has a reason a CFO can follow. The answers also become the evidence auditors, insurers and customers ask for, which removes duplicated work.

The framework works at any size. A 40-person accounting firm and a 400-person manufacturer answer the same five questions; only the depth of each answer changes.

4. From Plan to Roadmap: Risk, Compliance, Budget and Metrics

A strategic plan earns its keep when it turns into a funded, dated roadmap that leadership reviews. Three inputs shape it: the organization's risks, its compliance obligations, and what it can spend this year.

Compliance Obligations by Industry

Most organizations answer to more than one framework. Mapping controls once, across all of them, cuts audit effort and avoids conflicting fixes.

Industry	Common obligations	Planning focus
Healthcare	HIPAA Security Rule, cyber insurance requirements	Patient data access, medical and imaging devices, downtime procedures
Financial services and accounting	GLBA and the FTC Safeguards Rule, PCI DSS for card data	Written information security program, vendor oversight, encryption
Manufacturing	CMMC and NIST SP 800-171 for defense suppliers	Protecting controlled information, plant-floor and office network separation
Education and public sector	FERPA, state data-breach laws	Student and citizen records, account hygiene, limited staff
Any organization that takes cards or carries cyber insurance	PCI DSS, insurer underwriting questionnaires	MFA, endpoint detection, tested backups, incident response plan

A Phased 12-Month Roadmap

A first-year roadmap usually moves through four phases. Each ends with a leadership checkpoint before the next begins.

Phase	Timing	Key activities
1. Baseline	Months 1–2	Run a risk and governance assessment against NIST CSF 2.0. Inventory systems, data, vendors and connected devices, including the print fleet. Agree on risk tolerance with leadership.
2. Close the critical gaps	Months 3–4	Fix the issues most likely to cause a breach: MFA everywhere, patching of internet-facing systems, privileged access, and backup testing.
3. Build the program	Months 5–9	Write or update policies, stand up continuous monitoring, launch security awareness training, formalize vendor risk reviews and rehearse the incident response plan.

Phase	Timing	Key activities
4. Measure and reset	Months 10–12	Re-score against the baseline, report results to leadership, and set the next year's priorities and budget.

Budgeting the Plan

Tie every roadmap item to a specific risk and an estimated loss it reduces. That turns the security budget into a set of business decisions leaders can rank.

IBM's 2026 data gives a useful anchor. The gap between a breach contained in under 200 days and one that runs longer averages \$1.33 million. Organizations that use AI and automation across security operations saved nearly \$2 million per breach on average.

Metrics Leadership Should See

Keep the dashboard short. These measures show whether risk is going down.

Metric	What it tells leadership	Review cadence
NIST CSF 2.0 maturity score by function	Overall progress against the baseline	Twice a year
MFA coverage of users and critical systems	Exposure to stolen passwords	Monthly
Time to patch critical vulnerabilities	Exposure to the leading breach entry point	Monthly
Phishing simulation report and click rates	Strength of the human layer	Quarterly
Vendors reviewed vs. total critical vendors	Third-party risk coverage	Quarterly
Last successful backup restore test	Ability to recover from ransomware	Quarterly
Incident response exercise completed	Readiness for the bad day	Yearly

5. Choosing a Strategic Security Partner

Few mid-sized organizations can justify a full-time chief information security officer and a security operations team. A partner can fill that role, but only if it plans with you rather than sells to you. Use these questions to tell the difference.

Ask the partner	Why it matters	What a strong answer looks like
Do you start with an assessment tied to a recognized framework?	Without a baseline, progress cannot be measured	A governance, risk and compliance assessment scored against NIST CSF 2.0

Ask the partner	Why it matters	What a strong answer looks like
Who acts as our security leader?	Someone must own strategy, policy and leadership reporting	A named virtual CISO who meets with your executives on a set schedule
How do you prioritize recommendations?	Long, unranked findings lists rarely get fixed	Findings ranked by business impact and cost, turned into a dated roadmap
Which frameworks will you map us to?	Overlapping obligations multiply audit work	One control set mapped to every framework that applies to you
What is in scope, and what is left out?	Unassessed devices and vendors are where breaches start	Endpoints, cloud, vendors and connected devices, including printers and MFPs
How will you monitor between reviews?	Threats do not wait for the annual assessment	Continuous monitoring with defined alert response times
How do you prepare our people?	Many breaches start with a human mistake	Ongoing awareness training, phishing simulations and leadership briefings
What will we see each quarter?	Leaders need proof the investment is working	A short scorecard of the metrics in Section 4, in plain business language
Are you vendor-neutral on tools?	A plan should drive tool choice, not the other way around	Recommendations justified by risk, with options at different price points
Will you be here when it goes wrong?	Response speed sets breach cost	A tested incident response process and local, reachable people

6. Conclusion

Security spending without a plan buys activity, not resilience. Breach costs are at a record high, attackers are faster, and half of all breaches now come through someone else's door.

A strategic security plan gives leadership what reactive spending never does: clear priorities, one compliance story, a funded roadmap and proof of progress. The organizations that recover fastest from an incident are the ones that planned for it.

Next step: Schedule an Obviam strategic security assessment. You will receive a NIST CSF 2.0 baseline, a ranked list of risks in business terms, and a first-year roadmap your leadership team can act on. Call 513-699-1111, email info@obviam.com or visit obviam.com to start the conversation.

About Obviam

Obviam is the cybersecurity company of Modern Office Methods (MOM), a second-generation, family-owned technology provider founded in 1957 and serving businesses across Ohio, Pennsylvania, Northern Kentucky and southeast Indiana. Launched in 2024, Obviam delivers security consulting, governance, risk and compliance assessments, virtual CISO leadership, compliance management, and continuous threat detection and monitoring. Its mission is to stand in the way of cyber threats as a proactive guardian and trusted advisor to its clients.

Obviam works alongside Optimized IT, MOM's managed IT division, so security plans connect directly to the systems, devices and print fleets clients already rely on.

Contact Obviam: info@obviam.com | 513-699-1111 | obviam.com

How to Cite This Paper

Obviam. *Strategic Security Planning: From Reactive Defense to Business Resilience*. Modern Office Methods, October 2026.

When quoting a statistic from this paper, please also credit the original report listed below.

Sources

- [Ten Takeaways from IBM's 2026 Cost of a Data Breach Report](#) — Baker Donelson (summary of IBM / Ponemon Institute, Cost of a Data Breach Report 2026)
- [2026 Cost of a Data Breach Report: AI Wreaks Havoc on Budgets](#) — SecureWorld, August 28, 2026
- [2026 Data Breach Investigations Report: Infographic for SMBs](#) — Verizon, May 2026
- [Security Priorities Revealed in Verizon's 2026 Data Breach Report](#) — The National CIO Review
- [Verizon DBIR 2026: Small Businesses Face Escalating Cyber Threats](#) — Cyber Readiness Institute
- [Cybersecurity Framework 2.0](#) — National Institute of Standards and Technology
- [Modern Office Methods announces new cybersecurity company: Obviam](#) — The Recycler, April 11, 2024