EXECUTIVE REPORT

2026 Cybersecurity & Business Risk Report

What Eye Care Practices Need to Know

REDUCE RISK. PROTECT WHAT MATTERS.

STRENGTHEN RESILIENCE. DRIVE GROWTH.

EMPOWER CONFIDENCE. SECURE THE FUTURE.

Prepared by

IT4Eyes

IT4EYES
AN STS COMPANY

Executive Summary & 2026 Eye Care Threat Landscape

Cybersecurity is now a patient-care and business continuity issue—not just an IT issue.

Eye care practices are increasingly connected and increasingly targeted. From EHR and imaging systems to optical POS and cloud platforms, operational reliance on technology keeps growing. Understanding the 2026 threat landscape is the first step toward building a stronger, more resilient practice.

What Changed in 2026

- AI-assisted phishing is more convincing and harder for staff to spot
- Attackers increasingly target practice management, imaging, and cloud-based systems
- Third-party vendors and connected tools expand cyber risk across the practice
- Downtime now impacts scheduling, billing, patient communication, and continuity of care

Most Common Eye-Care Risks

- Phishing & Email
- Ransomware
- Stolen Credentials
- Third-Party Vendor Risk

Key Takeaway

The goal is not to eliminate all risk. It is to reduce exposure, protect patient data, and recover quickly when disruptions occur.

Cybersecurity by the Numbers

A few key statistics that highlight the growing cyber risk facing eye care practices.

1,008,597
internet-crime complaints reported to the FBI in 2025

$20.9B
in reported internet-crime losses during 2025

$3.04B
in reported business email compromise losses during 2025

31%
of organizational breaches analyzed began with vulnerability exploitation

62%
of breaches analyzed involved a non-malicious human element

$4.99M
global average cost of a data breach

What These Figures Mean for Eye Care Practices

Eye care practices store and manage highly sensitive patient data—making you a prime target for cybercriminals. The financial, operational, and reputational impact of a breach can be significant.

Cybersecurity isn't just an IT issue—it's a patient trust issue.

Important to Remember

A single cyber incident can disrupt appointments, delay care, result in regulatory fines, and erode patient confidence.

Proactive security today helps protect your practice, your patients, and your future.

IT4EYES
AN STS COMPANY

Source: FBI IC3 2025 Annual Report; Verizon 2025 DBIR; IBM Cost of a Data Breach Report 2025.

The Top Risks Facing Eye Care Practices

Most incidents begin with a manageable weakness — but the impact on patient care and operations can spread quickly.

1 Phishing, business email compromise, and payment fraud

Fraudulent appointment requests, vendor emails, payroll changes, and executive impersonation can turn a believable message into data loss or direct financial loss.

2 Ransomware and operational disruption

Attackers may encrypt systems that support scheduling, EHR access, imaging, billing, communication, or optical operations—bringing patient flow to a halt.

3 Stolen passwords and account takeover

Reused passwords, phishing pages, and weak access controls can expose email, cloud files, practice-management platforms, and administrative accounts.

4 Unpatched systems and connected technology

Unsupported or delayed updates on workstations, network gear, imaging devices, and connected tools can create easy entry points for attackers.

5 AI-related risks and shadow AI

Employees may place sensitive patient or business information into unapproved AI tools or connect AI apps to practice systems without oversight.

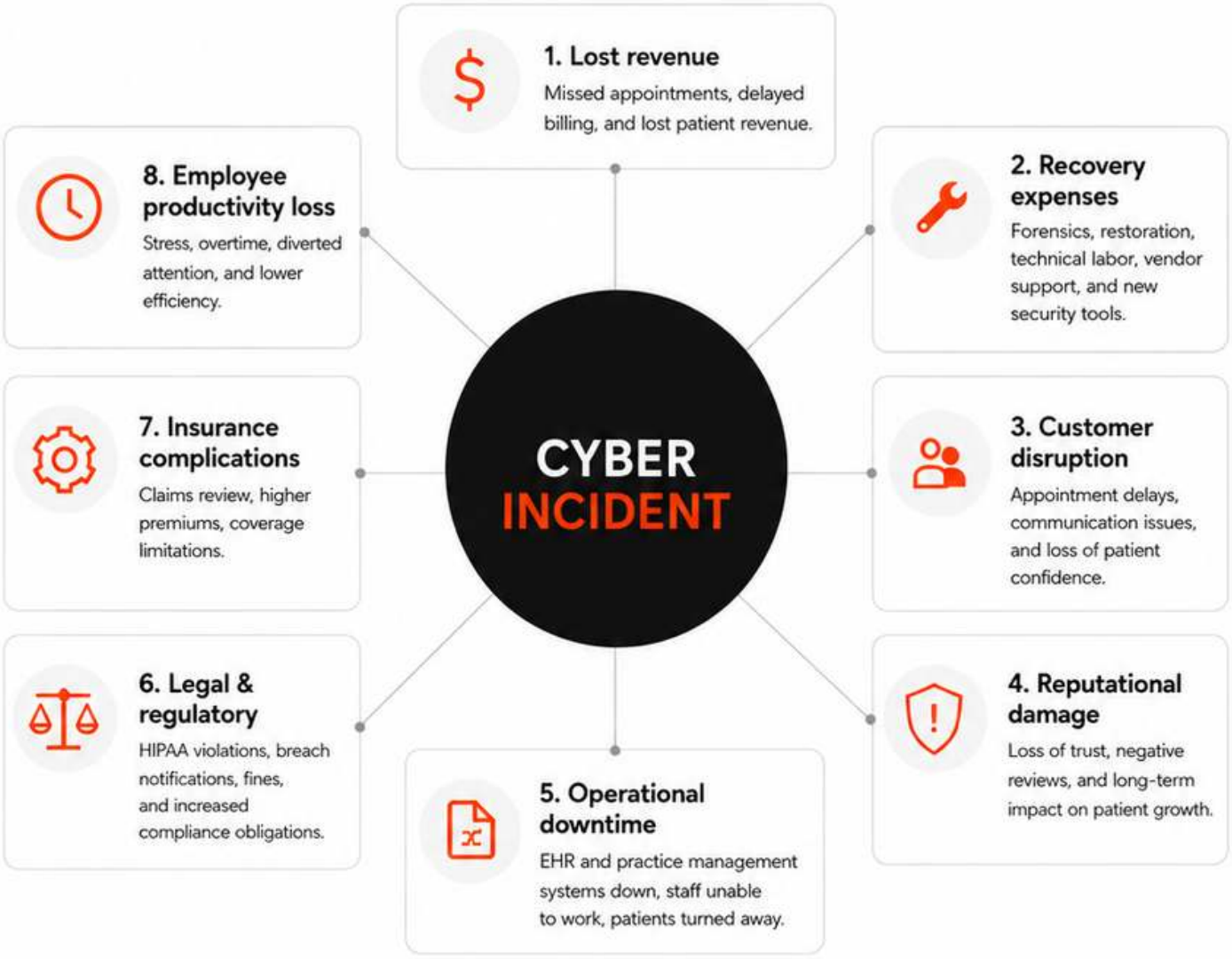
6 Vendor and third-party risk

A vendor, software provider, billing partner, clearinghouse, or cloud service can become the path into the practice—or a source of operational disruption.

Sources: FBI IC3 2025 Annual Report; Verizon 2026 DBIR; CISA small-business and ransomware guidance.

How Cyber Incidents Affect Eye Care Practices

The greatest cost is often the interruption — not the initial technical event.



The greatest cost of a cyber incident is often not the ransom or stolen data.
It is the interruption to patient care.

How long could your practice continue serving patients if your EHR, files, scheduling, billing, or other critical systems became unavailable?

IT4EYES
AN STS COMPANY

Source: Content: CISA #StopRansomware Guide; IBM Cost of a Data Breach Report 2025.

AI, Cloud Applications & Emerging Risk

AI tools and cloud platforms create real efficiencies for eye care practices, but unmanaged use introduces new exposure.

AI-ENABLED ATTACKS ARE RISING

Attackers use AI to automate phishing, generate malware, and exploit vulnerabilities at scale—often faster than practices can adapt.

SHADOW AI CREATES BLIND SPOTS

Employees may use public AI tools to draft messages, summarize patient notes, or upload files without IT knowledge—often without realizing the risk.

PATIENT DATA CAN BE EXPOSED

Information entered into public AI tools may be stored, used for training, or accessed by others if safeguards are not in place.

AI CONNECTED TO PRACTICE SYSTEMS

AI plugins and integrations can access EHR, files, calendars, and apps—expanding the potential impact of misuse or compromise.

HUMAN REVIEW IS ESSENTIAL

AI-generated content can be inaccurate, incomplete, or biased. It should be reviewed carefully before use in a clinical or administrative setting.

WHAT EYE CARE PRACTICES SHOULD DO

- Establish an AI acceptable-use policy
- Define which tools are approved
- Prohibit input of sensitive patient data into public AI tools
- Review AI permissions and integrations
- Provide employee training and guidance

45% of breaches involved cloud-based activity

1 in 4 malicious breaches studied were AI-enabled

Cyber Resilience:
Protect, Detect, Respond, Recover

Strong cybersecurity is more than prevention. Resilience means the business can withstand disruption and recover quickly.

PROTECT

Reduce the likelihood of an incident by implementing strong security controls.

- MFA & access controls
- Patch management
- Email security
- Endpoint protection
- Employee training

DETECT

Monitor your systems and environments to identify threats early.

- Continuous monitoring
- Threat detection
- Log analysis
- Vulnerability alerts
- User behavior review

RESPOND

Act quickly and effectively to contain threats and minimize business impact.

- Incident response plan
- Clear responsibilities
- Communication plan
- Containment steps
- Third-party coordination

RECOVER

Restore critical operations and return to normal operations as quickly as possible.

- Tested backups
- Recovery priorities
- Business continuity
- Lessons learned
- Continuous improvement

Resilience is not built in a day—it is built through consistent planning, testing, and improvement.

2026 Priorities for Eye Care Practices

Focus on what matters most. These six priorities help reduce risk, strengthen resilience, and protect patient care and practice operations.

1 KNOW WHAT YOU DEPEND ON

Maintain an accurate inventory of devices, software, EHR, imaging systems, vendors, and data. The practice can't protect what it doesn't see.

2 PROTECT ACCOUNTS

Require MFA, use a password manager, and limit access based on role so staff only reach what they need.

3 PATCH AND MODERNIZE

Keep workstations, network gear, and supported clinical systems up to date. Replace outdated technology before it becomes a liability.

4 STRENGTHEN FINANCIAL SAFEGUARDS

Verify payment requests, confirm vendor changes, implement approval processes, and protect against business email compromise.

5 TEST BACKUP AND RECOVERY

Back up critical data, test restores regularly, and make sure the practice can recover quickly after disruption.

6 PREPARE PEOPLE AND PLANS

Train employees, run phishing simulations, and keep downtime and incident-response plans ready.

Cyber resilience means making the practice **harder to disrupt—and easier to recover.**

Questions Every Leader Should Ask

Use these questions in leadership meetings or annual planning sessions to evaluate the organization's cybersecurity posture.

TECHNOLOGY

- [ ] Which systems are critical to daily operations?
- [ ] Are any systems unsupported or approaching end of life?
- [ ] How quickly are critical vulnerabilities addressed?
- [ ] Are all devices monitored, managed, and protected?

ACCOUNTS & ACCESS

- [ ] Is MFA enabled on all critical systems?
- [ ] Are administrative accounts separated from daily use?
- [ ] How often do we review user access?
- [ ] How quickly is access removed when an employee leaves?

RECOVERY & RESPONSE

- [ ] What data and systems are backed up?
- [ ] When was our last successful restoration test?
- [ ] How long would it take to recover critical operations?
- [ ] Do we have an incident-response plan?

PEOPLE & VENDORS

- [ ] How are employees trained on security?
- [ ] Do we test employees with phishing simulations?
- [ ] Which vendors have access to our data or network?
- [ ] What AI tools are employees using, and are they approved?

A useful answer should identify a named owner, a documented process, evidence that the control is working, and a date for the next review.

From Cybersecurity to Practice Resilience

The strongest practices are built through consistent decisions and continuous improvement.

No eye care practice can guarantee that it will never experience a cyber incident. Even well-protected practices can be affected by phishing, vendor issues, cloud outages, or vulnerabilities in the systems they rely on every day.

The practical objective for 2026 is straightforward: make the practice harder to compromise, limit the damage an attacker can cause, and be prepared to restore operations when something goes wrong.

Recommended next steps:

- Review your cybersecurity posture
- Evaluate backup and recovery readiness
- Assess technology lifecycle and security health
- Review vendor access and third-party risk
- Evaluate AI usage and patient-data protection
- Test incident response preparedness

Not sure how your practice would answer the questions in this report?

IT4Eyes offers a complimentary 10-minute **Cyber Risk Conversation** to help eye care practices determine whether a deeper review would be worthwhile.

435-313-8132

Primary sources

- FBI Internet Crime Complaint Center, 2025 IC3 Annual Report.
- Verizon, 2026 Data Breach Investigations Report and May 19, 2026 findings summary.
- IBM, Cost of a Data Breach Report 2025 and July 29, 2026 findings summary.
- CISA, Cyber Guidance for Small Businesses and #StopRansomware guidance.
- NIST, Cybersecurity Framework 2.0 and small-business implementation guidance.

Educational notice: This report provides general educational information and is not legal, regulatory, insurance, or compliance advice.