

60 MUST-ASK QUESTIONS

Before Selecting a Cybersecurity Provider

CYBERSECURITY

BUYER'S CHECKLIST

Powered By

PULSE TECHNOLOGY

Protecting businesses across Illinois, Northwest Indiana, and Southeast Wisconsin

Choosing a cybersecurity provider can be difficult when every company seems to promise the same things: experienced experts, strong protection, and 24/7 monitoring.

For businesses across Illinois, Northwest Indiana, and Southeast Wisconsin, these questions will help you find a provider that understands your organization, the risks you face, and the level of support you expect.

Written by cybersecurity specialists, this checklist covers what to ask, what to watch for, and how to compare providers in six key areas.

6 QUESTIONING TOPICS

SECTION 01

Experience and Market Position

Questions 01–10 · Page 2

SECTION 02

Technology and Tools

Questions 11–24 · Page 3

SECTION 03

Service Delivery

Questions 25–35 · Page 4

SECTION 04

Compliance and Reporting

Questions 36–45 · Page 5

SECTION 05

Pricing and Terms

Questions 46–56 · Page 6

SECTION 06

Security Innovation

Questions 57–64 · Page 7

HOW TO USE THIS CHECKLIST

1. **Share it before the meeting**
   Send the questions ahead so vendors come prepared.
2. **Compare vendors**
   Create your own customized buyer's checklist.
3. **Watch for red flags**
   Know what to avoid and what to look for in a strong provider.

THE BIG PICTURE

$962M+

in reported internet crime losses across Illinois, Indiana, and Wisconsin in a single year.

Source: FBI Internet Crime Complaint Center

SECTION 01

Experience and Market Position

Evaluate the provider's experience and track record.

	QUESTIONS	VENDOR A	B	C
01	How long have you provided Managed Cybersecurity Services?	☐	☐	☐
02	What percentage of your business focuses on security vs. other IT services?	☐	☐	☐
03	How many clients do you currently serve in our industry?	☐	☐	☐
04	Can you share examples of handling incidents similar to our concerns?	☐	☐	☐
05	What is your current client retention rate?	☐	☐	☐
06	Can we speak with references in our industry?	☐	☐	☐
07	What is your typical client profile?	☐	☐	☐
08	How many clients does each SOC analyst typically manage?	☐	☐	☐
09	How do people, automation, and AI support monitoring and response?	☐	☐	☐
10	What is your experience with ransomware, email, and identity-based attacks?	☐	☐	☐

Red Flag
Vague answers about past incidents, or no references from businesses like yours.

Pro Tip
Ask about their most serious incident and how they responded. Look for specifics.

Look For
Strong retention, long-term relationships, and relevant industry references.

WHY IT MATTERS

88%

of security professionals have experienced at least one significant security problem caused by a skills gap.

Source: ISC2 Cybersecurity Workforce Study

SECTION 02

Technology and Tools

Understand how your systems and data will be protected.

	QUESTIONS	VENDOR	A	B	C
11	What security tools make up your core technology stack?		☐	☐	☐
12	How do you handle integration with our existing tools?		☐	☐	☐
13	What level of access will we have to your security platform?		☐	☐	☐
14	How often do you update your security tools and signatures?		☐	☐	☐
15	Can we maintain control of our security tools while you monitor?		☐	☐	☐
16	Where is our security data stored?		☐	☐	☐
17	How long do you retain security logs and monitoring data?		☐	☐	☐
18	Can we export our data if we terminate services?		☐	☐	☐
19	How do you protect our sensitive data?		☐	☐	☐
20	What data backup and recovery capabilities do you offer?		☐	☐	☐
21	How do you protect identities, devices, cloud apps, and remote users?		☐	☐	☐
22	Where do you use AI or machine learning in your security operations?		☐	☐	☐
23	Does our data ever get used to train AI models?		☐	☐	☐
24	How do you safeguard security data and analysis when using AI?		☐	☐	☐

Red Flag
Reliance on one vendor or unclear data protections.

Pro Tip
Request a demonstration using relevant scenarios.

Look For
Flexible integrations, custom APIs, and clear AI and data policies.

WHY IT MATTERS

53%

of breached organizations had not encrypted their sensitive data, both stored and in transit.

Source: IBM Cost of a Data Breach Report 2026

SECTION 03

Service Delivery

Clarify what to expect from onboarding and support.



	QUESTIONS	VENDOR	A	B	C
25	What does the onboarding process look like?		☐	☐	☐
26	How long does typical implementation take?		☐	☐	☐
27	What resources do you need from our team?		☐	☐	☐
28	How do you handle knowledge transfer?		☐	☐	☐
29	What training do you provide for our team?		☐	☐	☐
30	Who will be our day-to-day contact?		☐	☐	☐
31	Do security professionals investigate and respond 24/7?		☐	☐	☐
32	How often do you schedule service reviews?		☐	☐	☐
33	What metrics do you use to measure success?		☐	☐	☐
34	How do you handle change requests?		☐	☐	☐
35	What is your process for continual service improvement?		☐	☐	☐

⚠ **Red Flag**
Unclear account ownership or after-hours response.

◎ **Pro Tip**
Request an implementation plan for the first 30, 60, and 90 days.

🛡 **Look For**
Dedicated account support, security education, and regular recommendations.

WHY IT MATTERS

29 minutes

is the average time it takes cybercriminals to move beyond their first point of entry. The fastest took 27 seconds.

Source: CrowdStrike Global Threat Report 2026

SECTION 04

Compliance and Reporting

Assess their compliance and reporting capabilities.

	QUESTIONS	VENDOR	A	B	C
36	How do you support our specific compliance requirements?		☐	☐	☐
37	What compliance frameworks do you maintain?		☐	☐	☐
38	How do you handle compliance reporting?		☐	☐	☐
39	Can you support our auditors during reviews?		☐	☐	☐
40	How do you stay current with regulatory changes?		☐	☐	☐
41	What standard reports do you provide?		☐	☐	☐
42	Can we customize reports for different stakeholders?		☐	☐	☐
43	How do we access real-time reporting?		☐	☐	☐
44	How do you identify and prioritize our top cyber risks?		☐	☐	☐
45	How do you turn security data into actionable recommendations?		☐	☐	☐

⚠ **Red Flag**
Generic reports with little insight into your risks.

◎ **Pro Tip**
Request sample reports for technical and executive audiences.

🛡 **Look For**
Real-time visibility and actionable risk reporting.

WHY IT MATTERS

$1.36M

average post-breach response cost, including regulatory fines, legal fees, and credit monitoring.

Source: IBM Cost of a Data Breach Report 2026

SECTION 05

Pricing and Terms

Identify costs, contract terms, and exit options.

	QUESTIONS	VENDOR A	B	C
46	How is your service priced?	☐	☐	☐
47	What services are included in the base fee?	☐	☐	☐
48	What additional costs should we anticipate?	☐	☐	☐
49	What are your contract term options?	☐	☐	☐
50	How do you handle service level credits?	☐	☐	☐
51	How do you handle increases in our security needs?	☐	☐	☐
52	Can we add or remove services as needed?	☐	☐	☐
53	How do you price service changes?	☐	☐	☐
54	What happens if we acquire another company?	☐	☐	☐
55	How do you support international operations?	☐	☐	☐
56	What happens to our data and tools if we leave?	☐	☐	☐

Red Flag
Hidden fees, unclear pricing, or confusing terms.

Pro Tip
Ask what you'll pay now and what could change the cost.

Look For
Flexible terms, clear exit options, and transparent pricing.

WHY IT MATTERS

33%

of security professionals say they don't have the budget to staff their team adequately.

Source: ISC2 Cybersecurity Workforce Study

SECTION 06

Security Innovation

See how they respond to new threats and technologies.

	QUESTIONS	VENDOR A	B	C
57	What is on your technology roadmap?	☐	☐	☐
58	How do you incorporate emerging threats into your service?	☐	☐	☐
59	How do you evaluate and adopt new security technologies?	☐	☐	☐
60	How are you using AI today to improve threat detection and response?	☐	☐	☐
61	Which security tasks use AI, and which require human judgment?	☐	☐	☐
62	How do you test new AI capabilities for accuracy and security?	☐	☐	☐
63	How do you address risks from clients' use of generative AI?	☐	☐	☐
64	How do you share threat intelligence across your client base?	☐	☐	☐

Red Flag
No roadmap or clear answers about emerging technology.

Pro Tip
Ask what recent security innovation they introduced and what it solved.

Look For
Regular updates on threats, technology changes, and recommended actions.

WHY IT MATTERS

94%

of leaders expect AI to be the biggest force shaping cybersecurity in 2026.

Source: World Economic Forum Global Cybersecurity Outlook 2026

Evaluating Your Cybersecurity Options?



Whether you're comparing providers or taking a closer look at your current cybersecurity readiness, the Pulse Technology team of experts can help.

Let's Talk.

E: info@pulsetechnology.com

P: 1-888-357-4277

W: PulseTechnology.com

70 YEARS PULSE TECHNOLOGY

PULSE TECHNOLOGY

About Pulse Technology

We are an award-winning, family-owned business with decades of dedication to the industry. We are a complete office technology partner providing Managed IT and products to help your business run smoother and keep you ahead of the curve.

Our Locations

ILLINOIS
201 Commerce Drive
Schaumburg, IL 60173
(888) 357-4277

INDIANA
3801 E Lincoln Hwy
Merrillville, IN 46410
(800) 837-1400

WISCONSIN
Brookfield, WI 53005
(262) 249-6400