The Digital Manufacturing & Cybersecurity Institute

The Cybersecurity Buyer's Guide

for Small and Medium-Sized Manufacturers

Prepared by MxD | Version 1.0 | August 2025

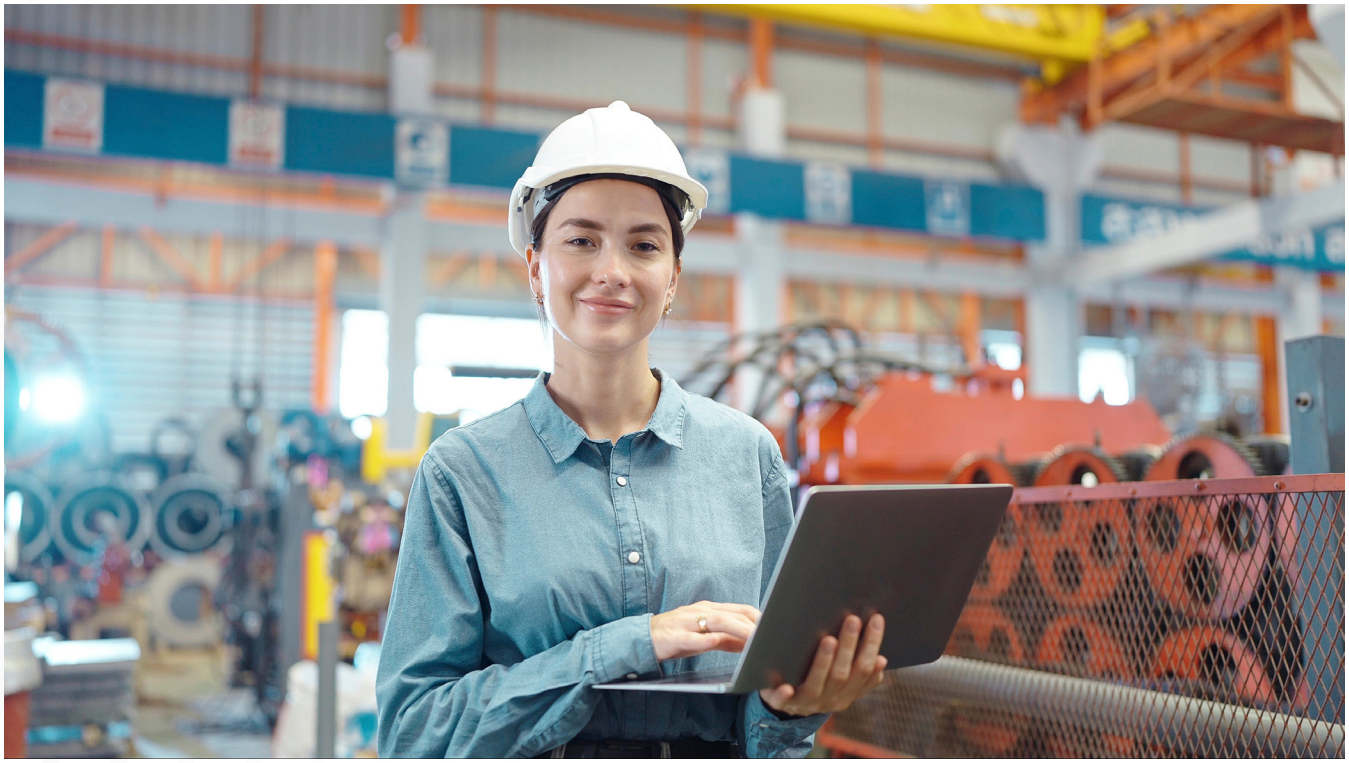
Table of Contents

Introduction

Cybersecurity technology reduces your exposure to risk, helps protect your investment in technology and equipment, and safeguards the valuable information you use to run your business. To significantly improve the state of cybersecurity in your company, you will eventually have to buy a cybersecurity solution: software, hardware, or a service.

But buying cybersecurity technology is a challenge for even the most technically-savvy. The marketplace for solutions is massive, and if you do not understand the cybersecurity lexicon, you could quickly become confused and frustrated. Most cybersecurity solutions are also designed to support general purpose office environments, not manufacturing ones and the complications innate to such work.

To help remedy this situation, MxD has created this Buyer's Guide to help you make informed and confident cybersecurity technology purchasing decisions. It provides you with a framework you can use to assess your needs, evaluate options, and increase the likelihood of the successful procurement, installation, and operation of cybersecurity technology that will protect your business.



Before You Start Shopping

Understand Your Enterprise and Its Parameters

The quote “to know thyself is the beginning of wisdom” is attributed to the ancient Greek philosopher Socrates, and it serves as a timeless reminder that knowing your strengths and weaknesses is essential if you hope to succeed at any undertaking. In the context of cybersecurity, knowing what you have and are trying to defend against are key pieces of information you should acquire before you ever speak to a solution vendor.

Know What You are Protecting

Before you start looking at options to protect your company, you need to determine what it is you are trying to protect. Are you concentrating on your back office, or do you want to include any computerized machines on your shop floor? Do you know how many PCs or other devices you are trying to protect? Where are they? How old are they? What version of operating systems and software are running on them? In addition to your own edification, every vendor you talk to is going to need this information so they can determine whether they have a solution that will address your problems.

Know Your (Human) Limitations

Particularly in small and mid-sized manufacturers (SMMs) the availability of Information Technology (IT) or Operational Technology (OT) talent, much less cybersecurity talent, is sparse. Some firms have an IT generalist on staff, and often that’s not their primary or only role in the company. There is nothing wrong with that approach when the available talent pool is so shallow, but it is a limitation you must acknowledge because the solution you procure cannot be so complicated that you cannot operate it.

Know your (Other) Limitations

Do you use WiFi in your facility? How well does that signal travel throughout your physical plant? Does the equipment you use have the kind of interfaces necessary to connect to modern technology? Are you using equipment that uses a proprietary protocol or language that isn’t compatible with third-party technologies? Do you have power reliability problems at your facility? These and other factors could play a significant role in determining what sort of cybersecurity technology you can employ.

Determine Your Budget

How much are you willing to spend? Is that a one-time deal or are you willing and able to do it on an annual basis? Have you factored in annual price increases? Paying for a service contract? Paying for training? Like everything else we buy, the list price is rarely the final price we end up paying.

Establish Evaluation Criteria

What are the most important things to consider when evaluating your options? It can be easy to get lost in attractive presentations and lose sight of what's important. Clear evaluation criteria can keep you focused on what matters:

- **Key Features:** The functions or capabilities that are essential for meeting your needs.
- **Performance:** The standards or metrics you are going to use to evaluate whether a solution meets your needs.
- **Compatibility:** How well does a given solution integrate with the technology you already have?
- **Usability:** Will the person responsible for operating and maintaining the solution be able to do so without extensive (and expensive) training?

These criteria are a starting point. Taking the time and effort to establish criteria specific to your company's needs will help you make a better decision.

Stepping Into the Breach

Do Your Research

Unless you are exclusively a Ford or Chevy person, you probably visit several different dealers when you are looking for a car. When you need some work done on your house the mantra of "get three bids" always comes to mind. The same principle holds true when you are buying cybersecurity technology. There is never just one vendor in each product or service category, and when you are evaluating solutions, you want to be able to compare apples to apples.

A basic internet search for a particular type of solution will produce an overwhelming number of options, so we recommend talking to others in your field, or larger up-stream partners, to find out who they use for their specific cybersecurity solutions and use that list as your starting point. Their vendors may not be the best option for you, but they can direct you to other companies who are better suited to meet your requirements.

Vetting Vendors

Before you get too far along, it is important to remember, especially if you are a part of the defense industrial base, that you ensure you do business with vendors who are not prohibited from doing work with or in support of the government.

SAM.gov

If you do not already have one, you should create an account on sam.gov. Once you're logged in go to the search function and enter the name of the company you're considering. Select "Entity Information" and "Exclusions" to see if they are suspended or debarred.

Department of State

The Department of State's Directorate of Defense Trade Controls maintains a Debarred Parties List. The Office of Foreign Assets Control maintains the Special Designated Nationals and Blocked Person List.

Once You Are Talking to Vendors

When you engage with a vendor, the first thing they are going to want to do is set up a capability briefing. Have the answers about your firm and what you are trying to do on hand because in the course of this call they are going to ask.

When the briefing is done and it's time for you to ask questions, work your way through the sample questions provided later in this report, plus whatever criteria you feel are important to your business.

Finally, ask the sales representative you are talking to "who are the two firms you usually find yourself competing with for customers?" They should have no problem sharing that information, and it gives you a sense of who you should talk to next.

Understand Solution Requirements

Whether the solution you are looking at is software or a piece of hardware, run locally or in the cloud, you need to understand specifications and requirements in order to know if you can operate the solution with the resources you have, or if in addition to the security solution, you need to procure new equipment or upgrade current services. Some things to consider:

- **Required CPU, hard disk, and memory.** If you are running old computers and outdated operating systems, the solution you are considering might not function well, if at all.
- **Compatibility.** Make sure that if a solution must interact with technology beyond basic IT (e.g. OT, IIoT), that it works with the devices and protocols your operation uses.
- **Network Bandwidth.** Solutions may assume you have high-speed network connectivity, or that legacy network architectures will support new technology. Your low-end ISP connection or weak Wi-Fi on the factory floor may be a chokepoint that hinders performance.

Evaluate Security and Privacy

- **Product Security.** Ask the vendor how they ensure the security of their solution as it is being developed? Do they follow secure coding practices? Do they subject their work to independent code reviews?
- **Compliance.** Ask the vendor what specific cybersecurity standards or frameworks the product complies with. Depending on what you do and with whom you do business, compliance with NIST 800-171, ISO 27001 or others may be required.
- **Data Security.** Find out what the vendor's data security practices are. Do they encrypt data at rest (while it is on a computer or in a database) and in-motion (while it is being sent over the network)? How do they protect encryption keys?
- **MFA.** Find out if the solution you are considering allows for multi-factor authentication (ideally it should).
- **Privacy.** Find out what data the solution collects and sends back to the vendor, and what the vendor does with that data. You do not want a vendor to use data about your systems or company in ways not directly and exclusively related to the service they are providing.

How to Verify Vendor Claims:

- **Request Documentation.** Does the vendor have a dedicated "security" or "privacy" section on their website, or a "trust center" where you can confirm their compliance and credentials? If not, ask for copies of credentials, certifications, sanitized audit findings, and sanitized penetration test results. Sanitized results are fine if they convey sufficient information about what problems were identified and how they were resolved.
- **Read Case Studies.** A case study is an examination of a real-world example of how a company used a particular product or service to achieve a specific goal or solve a particular problem. A good case study will

describe the customer and their challenges, the features of the product or system used to address those challenges, and how well the solution performed.

- **Get Testimonials.** Ask to speak with other customers to understand their experiences with the vendor. There is arguably no greater validation of vendor claims than a testimonial by a satisfied customer. The more similar that customer is to your firm the better. Some questions you might ask other customers:

Usability

- How would you rate the overall ease of use and intuitiveness of the solution? Were there any significant onboarding or training challenges?
- How well did the solution integrate with your existing systems and workflows? Were there any compatibility issues or the need for significant customization?

Reliability

- How reliable has the software been? Have you encountered frequent crashes, errors, or downtime?
- How responsive has the vendor been in addressing any technical issues or providing support? What is their typical response time and the quality of their support?

Effectiveness

- How closely do expectations meet reality with regards to real-world performance and utility?
- What specific security problems or needs has the solution helped you address? Can you quantify any improvements or benefits you've seen?
- How well does the solution scale to meet the needs of your business?

Other Factors

- How satisfied are you with the value you receive for the cost of the software (including initial purchase, subscription fees, and any ongoing maintenance or support costs)?
- How often does the vendor release updates and new features? How has the vendor's commitment to ongoing development and improvement been in your experience?
- What are the biggest strengths and weaknesses of the solution, in your opinion?
- Knowing what you know now, would you choose this solution again? Are there any other vendors or solutions you considered that you feel are worth mentioning?

General Questions to Ask Vendors

The following questions are a starting point to help you assess vendor solutions, regardless of what sort of solution they offer.

"What is the typical customer profile for your product or service?"

Are they offering solutions that are suitable for companies like yours? "Enterprise" (large scale) solutions are usually ill-suited (and too expensive) for SMMs. Solutions designed for markets other than manufacturing may not address issues that are unique or important to the space. Likewise, they may have features or functions that are superfluous to needs.

"How does your product differentiate itself from competitors?"

If everyone claims to do X, Y, and Z; how is their approach superior to others? What is their secret sauce that makes them the most suitable for you? Who can corroborate their claims?

"What level of technical expertise is required to use the product effectively?"

If the solution requires a cybersecurity expert to operate, it might be a non-starter. If they offer training on how to use the solution, is it free or does it cost extra? What about technical support if issues arise after purchase?

"Can you provide case studies and testimonials of successful implementations?"

There is no better validation of claims than happy customers.

"How can we evaluate the effectiveness of your product safely and realistically?"

You do not want to test someone else's product on your production system. If they have a test environment that they can demonstrate their solution on, how realistic can they make it relative to your own enterprise?

"What are the terms, costs, and service level agreements associated with service and support?"

A certain amount of service and support will be included in the price you pay, but you may want to consider paying for more responsive support and access to subject matter expertise. If up-time is critical for you, you want some assurance that when you call, they will pick up the phone and respond as quickly as possible.

Questions for Specific Cybersecurity Solution Vendors

These questions are a starting point. They are not comprehensive, and you should develop questions that are specific to your current and anticipated needs. Consider eliciting questions from peers or partners who have procured such technology before in preparation for your discussion with a vendor.

Questions for Firewall Vendors

A firewall is a network security tool that monitors, evaluates, and acts on incoming and outgoing network traffic based on security policy. Think of it like a filter for your network: traffic may or may not flow into or out of your network based on the rules you set up for what is considered 'good' and 'bad'. There are different types of firewalls:

- **Packet Filtering Firewalls.** Examine data packets based on their source and destination IP addresses, port numbers, and protocol (e.g., TCP, UDP). They can block traffic from specific IP addresses or allow only certain types of traffic.
- **Stateful Inspection Firewalls.** Keep track of the state of network connections. They can identify and block malicious traffic that may appear legitimate at first glance.
- **Application-Level Gateways/Proxy Servers.** Act as intermediaries for specific applications like email or web browsing. They can inspect the content of data packets and block malicious content, such as viruses or malware.
- **Next-Generation Firewalls.** Combine multiple security features, such as intrusion prevention systems (IPS), malware detection, and other capabilities, into a single device.

Features to look for when considering a firewall purchase:

Performance:

- How much data can the firewall process without impacting network performance?

Security Features:

- Can it detect and block malicious network activity in real-time?
- Does it support VPN connections for secure remote access?

Management and Monitoring:

- Can you monitor network traffic and security events in real-time?
- Does it provide detailed logs and reports for analysis?

Scalability:

- What is required (technical actions and costs) to upgrade should your needs grow?
- What is the expected lifespan of the equipment/how long do they expect to be able to support a given model or device?

Intrusion Detection System Vendors

An Intrusion Detection System (IDS) is a device or software application that monitors network traffic and systems for malicious activity or policy violations. Think of it as a burglar alarm for your network. It constantly watches for suspicious behavior and alerts you if something looks wrong.

Types of Intrusion Detection Systems:

- **Network-Based IDS (NIDS)** monitors network traffic passing through a specific network segment and analyzes data packets for malicious patterns.
- **Host-Based IDS (HIDS)** monitors activity on individual computers or servers. It can detect threats that may not be visible on the network level, but its 'view' is limited to the specific host it's installed on.
- **Signature-Based IDS** looks for specific patterns or signatures of known attacks. It is effective against known threats but can miss new or unknown threats.
- **Anomaly-Based IDS** monitors normal network behavior and flags any deviations from that baseline. It can detect unknown threats but also generate a large number of false positives.

Questions to ask when considering an IDS:

Detection Accuracy

- What are your false positive/negative rates?

Performance

- What kind of impact does the product have on network performance?

Usability

- How easy is it to install, configure, and manage?

Reporting and Analysis

- Does it produce accessible and actionable reports on detected threats?
- Does it have the ability to analyze threat trends and identify patterns?

Integration

- Will it integrate with my current technology?
- Does it integrate with other security technology (that you might be considering)?

Scalability

- If you have plans to grow, will the solution scale to meet the anticipated increased demand?

Intrusion Prevention System Vendors

Intrusion Prevention Systems (IPS) go beyond simply detecting threats (like an IDS) by actively blocking or preventing them in real-time. Think of it as a security guard that not only sees a burglar trying to break in but also physically stops them from entering.

Types of Intrusion Prevention Systems:

- **Network-Based IPS (NIPS)** Monitors network traffic for malicious activity. Can actively block malicious traffic by dropping packets, resetting connections, or altering traffic flow.
- **Host-Based IPS (HIPS)** Monitors activity on individual computers. Can block malicious software, prevent unauthorized access, and enforce security policies.
- **Signature-Based IPS** Relies on pre-defined signatures or patterns of known threats. Effective against known attacks.
- **Anomaly-Based IPS** Monitors normal system behavior and flags any deviations from that baseline. Can detect unknown threats.
- **Behavior-Based IPS** Analyzes the behavior of applications and users to detect suspicious activity.

Questions to ask when considering an IPS:

Prevention Capabilities

- Does it actively block or prevent threats in real-time?
- How effective is it in stopping attacks before they cause damage?

Detection Accuracy

- What are the false positive/negative rates?

Performance

- What kind of impact does the product have on network performance?

Usability

- How easy is it to install, configure, and manage?

Reporting and Analysis

- Does it produce detailed and actionable reports on detected threats?

Integration

- Can it integrate with other security tools (e.g., firewalls, SIEM systems) and work with my existing technology?

Scalability

- If you have plans to grow, will the solution scale to meet increased demand?

Endpoint Detection and Response (EDR) Vendors

Endpoint Detection and Response (EDR) is a cybersecurity technology that continuously monitors endpoints (laptops, desktops, servers, etc.) to detect and respond to cyber threats. Think of it as a security camera for your devices. EDR goes beyond traditional antivirus by:

- **Proactively hunting for threats:** It doesn't just wait for threats to be detected; it actively seeks out and identifies suspicious activity.
- **Providing deep visibility:** It collects extensive data on endpoint activity, allowing security teams to track malicious activity and understand the "why" behind threats.
- **Automating responses:** It can automatically take actions to contain and mitigate threats, such as isolating infected devices or blocking malicious processes.

Types of EDR Solutions

- **Cloud-based EDR** offers centralized visibility and management across all endpoints.
- **On-premises EDR** is deployed and managed within the organization's own infrastructure.
- **Agentless EDR** Relies on network traffic analysis rather than agents installed on each endpoint.

Questions to ask when considering an EDR System:

Threat Detection Capabilities

- How does it detect sophisticated attacks like fileless malware, ransomware, and zero-day exploits?
- How does it identify suspicious behavior patterns, such as unusual process executions or data exfiltration?

Response Capabilities:

- Can it automatically isolate infected devices, block malicious processes, and roll back changes?

Visibility and Reporting:

- Does it provide a clear picture of security posture across all endpoints?

Integration and Management:

- Can it integrate with other security tools?
- Does it allow for easy management and configuration of EDR policies across all endpoints?

Scalability and Performance:

- Can it scale to support a growing number of endpoints?
- How much of an impact does it have on endpoint performance?

Network Security Monitoring Vendors

Network Security Monitoring (NSM) is the continuous and ongoing process of observing and analyzing network traffic and system activity to detect and prevent security threats. Think of it as a sophisticated surveillance system for your entire network. It goes beyond basic monitoring by:

- **Proactively hunting for threats:** It doesn't just wait for alerts; it actively seeks out and identifies suspicious activity.
- **Providing deep visibility:** It collects and analyzes vast amounts of data from various sources across the network.
- **Enabling threat hunting:** It empowers security teams to proactively search for and investigate potential threats.

Types of Network Security Monitoring Solutions:

- **Security Information and Event Management (SIEM):** Collects and analyzes security logs from various sources (firewalls, IDS/IPS, servers, endpoints). Correlates events to identify potential threats. Provides dashboards and reports for security analysis.
- **Network Traffic Analysis (NTA):** Focuses on analyzing network traffic patterns for anomalies and malicious activity. Utilizes techniques like deep packet inspection, protocol analysis, and machine learning.
- **Threat Hunting Platforms:** Specialized tools designed for security analysts to proactively search for and investigate threats. Offer advanced search capabilities, threat intelligence feeds, and investigation workflows.

Questions to Ask When Considering an NSM System:

Data Collection and Ingestion

- Does it have the ability to collect data from various sources (firewalls, IDS/IPS, servers, endpoints, cloud environments)?
- Can it handle large volumes of data with minimal latency?
- Does it support the ingest and analysis of OT protocols?

Threat Detection and Analysis:

- Can it identify and alert on threats in real-time?
- What kind of technology (machine learning, behavioral analysis, etc.) does it use to detect threats?
- Does it leverage threat intelligence feeds to improve threat detection?

Investigation and Response:

- Does it allow security analysts to quickly and intuitively investigate alerts and incidents?
- Can you automate certain response actions, such as blocking malicious IP addresses or isolating infected systems?

Reporting and Visualization:

- Does it provide clear and concise visualizations of security data?
- Does it allow for the identification of emerging threats and security trends?

Scalability and Performance:

- Will it scale to support planned growth?
- What kind of impact does it have on network performance?

Security Information and Event Management Vendors

A Security Information and Event Management (SIEM) system is a software solution that collects, analyzes, and correlates security logs and events from various sources across an organization's technology infrastructure. Think of a SIEM as a central command center for all security-related information.

Questions to ask when evaluating SIEM solutions:

Data Collection and Ingestion

- Does it have the ability to collect data from all the potential sources you may employ (firewalls, IDS/IPS, servers, endpoints, cloud environments, OT, IIoT, etc.)?
- Can it normalize data from different sources and enrich it with context?

Threat Detection and Analysis

- Can it identify and alert on threats in real-time?
- Does it use machine learning, behavioral analysis, and other advanced techniques to detect sophisticated threats?
- Can it correlate events across different sources to identify complex threats?

Threat Intelligence Integration

- Can it leverage threat intelligence feeds to improve threat detection and analysis?

Investigation and Response

- Does it allow security analysts to quickly investigate alerts and incidents?
- Can it automate certain response actions, such as blocking malicious IP addresses or isolating infected systems?
- Does it provide tools for managing and tracking security incidents?

Reporting and Visualization

- Does it provide clear and concise visualizations of security data?
- Does it allow for the identification of emerging threats and security trends?

Scalability and Performance

- Can it scale to support growing data volumes and increasing complexity of the threat landscape?
- What kind of impact does it have on system performance?

Usability and Maintainability

- Does it have a user-friendly interface with intuitive navigation?
- Is it easy to configure, manage, and maintain?

Proposal Evaluation and Selection

Proposal evaluation is a critical step in the procurement process that involves a systematic assessment of proposals submitted by vendors in response to your requirements. Effective proposal evaluation is crucial for several reasons:

- Informed Decision-Making: It helps ensure you make your decision based on facts and data, not buzzwords or “eye candy” that distracts you from your true needs.
- Risk Mitigation: A careful evaluation of proposals helps identify and mitigate potential risks associated with vendor performance and project implementation.
- Optimal Resource Allocation: It helps ensure that resources are allocated to the vendor who can deliver the best value and meet the organization’s needs.
- Compliance and Legal Considerations: It helps ensure that the procurement process adheres to any legal and regulatory requirements.

How to Conduct Proposal Evaluation

Proposal evaluation is not difficult, but it does take time and effort to do them well. A solid effort to prepare for the process, and discipline during the process, can add significant value.

Establish an Evaluation Team

The evaluation team should include people who are going to be involved with the implementation or operation of the solution (IT, OT) as well as those why may be impacted by it (operations). It should also involve anyone who may have to deal with the vendor (e.g. accounting, legal).

Develop Evaluation Criteria

Each member of the evaluation team should be responsible for addressing the needs and equities of their company teams or units. Company team leaders should arm evaluation team members with requirements (must haves), desires (nice to haves), and any issue or factor that might be a showstopper to the company.

Review Proposals

Everyone on the evaluation team should take the time to carefully read each proposal. Reviewers are encouraged to take notes about anything that is not clear or that they have questions about. No two proposals are alike, but all of them should have certain key criteria that should be carefully considered:

- **Technical Approach:** How does the vendor propose to use their technology to solve your problem? Is it reasonable and suitable for your company?
- **Project Plan:** A description of the vendor’s project management methodology, timeline, and resource allocation. Do they have the right people in the right roles?

- Pricing and Cost: Is the price listed all-in or are there additional fees or add-ons that are required to make the solution meet your needs? Is the price in line with what others are proposing? If they are skewed one way or another, why? When is a given device or solution expected to reach end of life and is it in sync with however many years of support you're paying for?

- Service Level Agreements (SLAs): What will the vendor do, when will they do it, how well they will do it, and how all of this will be measured. What do they get if they do better than expected; what do they suffer if they do poorly?

- Risk Management: Does the vendor anticipate any risks and how do they propose to mitigate those risks?

Evaluate Proposals

There are multiple approaches to evaluating proposals. They can be as complicated or as simple as you prefer. One of the easiest is to create a scoring matrix that allow reviewers to assign a numerical score to each of the evaluation criteria being used for the proposal. The proposal with the highest score wins (See Appendix B).

Conduct Vendor Interviews (Optional)

A well-done proposal should stand on its own, but sometimes there are issues or items in a proposal that need elaboration or clarification. In such cases conducting an interview with the vendor is warranted.

If you are just interviewing a vendor to clarify a point, then it isn't necessary to interview all of them, but if you are making the interview a part of the selection process, then you should give each vendor a chance to articulate their capabilities and deliver their pitch in the interest of fairness.

Make a Decision

With clear selection criteria and a full understanding of what each vendor brings to the table, selection of a winner should be straightforward. Having said that, people are only human and can have their objectivity swayed by various factors. There are a couple of things you can do to help ensure that you are making the best choice:

- If using a numeric evaluation scheme, limit the numeric range to force evaluators to make hard calls. There is a lot more leeway for a decision that is measured between 1 and 10 than there is 1 and 5.

- Have evaluators explain why they ranked vendors the way they did. This forces people to think hard about their decisions and helps you identify when subjectivity may be overcoming objectivity.

- If you find yourself in a two- or more-way tie, consider weighing certain evaluation criteria more heavily than others based on how important they are to the company's success.

- It may also be helpful to consider factors such as the vendor's longevity, reputation, financial stability, and other factors that can contribute to project success. Big companies are likely to deliver but may not treat you as well as larger customers; small companies might have a great new innovative approach, but a weak financial footing might put the whole project at risk.

Post Procurement

Successfully deploying and operating a cybersecurity solution is a coordinated effort that involves both you and your new vendor partner. The signing of an agreement is just the start of a series of efforts that lead to successful implementation.

Kick-Off Meeting

A kick-off meeting is an initial meeting between your company and the selected vendor to officially launch the project. A successful kick-off meeting will:

- Ensure that both parties have a shared understanding of the project scope, goals, and objectives.
- Define the communication channels and protocols to be used throughout the project.
- Identify points of contact and outline the roles and responsibilities of each team member.
- Create a detailed project timeline with key milestones and deadlines.
- Discuss potential risks and develop mitigation strategies.
- Agree on a process for addressing issues and resolving conflicts.

Who is Involved?

From your side, a typical list of kick-off meeting attendees would include a project manager, the people who will be involved in implementing the new solution, the people who will be involved in operating the new solution (if they are not one in the same), and anyone else in the company who will be impacted by the implementation.

The vendor will bring a project manager to the meeting, as well as any technical staff who will be responsible for implementing the solution, and often someone with “customer success” in their title, who is responsible for making sure you are happy with your purchase.

Vendor Performance Management

Cybersecurity is a process, not an end-state. Victory is not declared once you've accepted the implementation of your new solution. Monitoring vendor performance helps ensure you are getting full value out of your relationship and enables you to take corrective action if needed.

How to Implement Vendor Performance Management

Define Performance Metrics, Incentives, and Penalties

- Develop clear and measurable performance metrics that align with the organization's goals and the specific services or products being provided by the vendor.
- Capture metrics in a service level agreement (SLA).
- If your budget allows, consider implementing an incentive program to reward high-performance/early delivery.
- Establish and enforce penalties for non-compliance with SLA or poor performance.

Establish a Performance Monitoring System

- Track and monitor vendor performance against the defined metrics. This does not have to be elaborate; a simple spreadsheet or other document that captures the metrics to be evaluated, dates, etc., will suffice.
- A certain amount of deviation from the planned schedule should be expected – rarely does a project go exactly to plan – but delays and other issues should be blips, not trends. If issues persist, get all pertinent stakeholders together to see what can be done to get back on track.

Regular Performance Reviews

- Conduct regular performance reviews using a structured approach (e.g. KPIs, etc.) to assess vendor performance and identify any areas for improvement.
- Performance goals should be meaningful and achievable; you want the project to succeed but not if it means setting someone up for failure.

Feedback and Communication

- Establish regular communication channels to discuss performance issues, address concerns, and seek improvements.
- Establish a communications schedule that balances keeping people informed while still giving them time to get the work done. You do not want people to spend more time explaining what they are going to do than they are doing it.

Summary

Cybersecurity is not a static state; it is an ongoing process that requires continuous vigilance and adaptation to effectively deal with evolving threats. By investing in appropriate cybersecurity technology, you can protect your business, maintain customer trust, and minimize risk.

All technology, especially cybersecurity technology, has a half-life. Make it a point to re-assess your cybersecurity needs on a regular basis and re-evaluate whether the cybersecurity protections you have in place are up to the task for need updating.

While the popularity of security technologies and methodologies waxes and wanes over time, the basic principles and approaches covered in this guide should support your decision-making efforts regardless of what solutions are in vogue.

Appendix A: Asset Inventory

ID	Description	Manufacturer	Model	Serial	Location	Date Purchased	Custodian
1	Accounting Laptop	Dell	ABC123	9743Z1	Office	4/1/22	S. Smith

Appendix B: Vendor Evaluation Criteria

Sample Vendor Evaluation

	Vendor 1			Vendor 2			Vendor 3		
	Score	Weight	Assessed	Score	Weight	Assessed	Score	Weight	Assessed
Criteria	Rate each item 1-5, with 5 being the best; Add weighted value 1-5 based on how important a given criteria is to you; Assessed Value is score * weight.								
Company									
Experience	5	4	20	3	4	12	2	4	8
Financial Stability	4	2	8	3	2	6	4	2	8
Offering									
Usability	4	4	16	3	4	12	5	4	20
Scalability	3	3	9	3	3	9	4	3	12
Cost									
License	3	4	12	2	4	8	2	4	8
Total Cost of Ownership	2	4	8	2	4		3	4	
Support									
SLA	4	5	20	3	5	15	3	5	15
Training	3	5	15	1	5	5	2	5	10
Overall Scoring		**108**			**67**			**81**	

Interested in partnering with MxD to add to future editions of this Cybersecurity Guide?
Contact Michael Tanji, Director of Cybersecurity at **michael.tanji@mxdusa.org**

We invite you to share this report with others in the industry.
Visit the Cybersecurity Guide Page on the MxD website at **mxdusa.org**.