

IS YOUR LIBRARY PREPARED?

A RESOURCE FOR MICHIGAN'S PUBLIC LIBRARY LEADERS
PROTECTING COMMUNITY SPACES **PEOPLE DEPEND ON.**



Prepared by BAE Networks, a Michigan-based managed IT and cybersecurity provider helping organizations strengthen security, resilience, and long-term technology planning.



TABLE OF CONTENTS

SECTION ONE: WHY LIBRARIES ARE INCREASINGLY TARGETED	PAGE 2
SECTION TWO: PUBLIC WORKSTATION RISKS	PAGE 3
SECTION THREE: PROTECTING PATRON PRIVACY	PAGE 4
SECTION FOUR: CYBER INSURANCE & TECHNOLOGY EXPECTATIONS	PAGE 5
SECTION FIVE: HUMAN RISK: PHISHING & AWARENESS	PAGE 6
SECTION SIX: BACKUP, RECOVERY, & RESILIENCE	PAGE 7
APPENDIX: LIBRARY CYBERSECURITY SELF-ASSESSMENT	PAGE 8

Prepared by BAE Networks, a Michigan-based managed IT and cybersecurity provider helping organizations strengthen security, resilience, and long-term technology planning.

SECTION ONE:

WHY LIBRARIES ARE INCREASINGLY TARGETED

Today's public libraries are highly digital environments. Libraries rely on public computers, cloud applications, digital collections, payment systems, online programming, and staff collaboration tools to serve their communities.

At the same time, many libraries operate with limited technology resources and lean staffing models. This combination can make libraries attractive targets for cybercriminals looking to disrupt services or gain access to sensitive information.

Cybersecurity incidents don't just affect technology: they can impact community trust, access to resources, and the essential services libraries provide every day.

What This Means for Libraries

- **Public computers** increase the number of devices that must be secured.
- **Digital services** have expanded the library's technology footprint.
- **Limited staffing** can make proactive cybersecurity challenging.
- **Service disruptions** may affect patrons who depend on library resources.

Questions to Ask

Could our library **continue operating** if key systems became unavailable?

Do we understand where our **greatest technology risks exist**?

Are cybersecurity responsibilities **clearly defined**?

Does **leadership regularly discuss** technology risk?

Libraries have become increasingly digital organizations, making cybersecurity an essential component of protecting community services and maintaining public trust.

SECTION TWO: PUBLIC WORKSTATION RISKS

Public computers are one of the library's greatest strengths and one of its most unique technology considerations.

Unlike traditional offices, libraries intentionally provide technology access to thousands of patrons each year. These devices often support job searches, financial activities, government services, and personal communications.

Because public computers are used by many individuals throughout the day, libraries should regularly evaluate how these systems are managed and protected.

What This Means for Libraries

→ **Public workstations** require different security considerations than staff computers.

→ **Session data** should not remain on devices between users.

→ **Clear policies** improve consistency and security

→ **Updates and security monitoring** are critical.

→ **Network segmentation** helps reduce risk..

Questions to Ask

Are public computers **separate from** internal systems?

Is **patron information removed** between sessions?

How **quickly** are **updates applied**?

Who is responsible for managing public workstations?

Public access is part of the library's mission. Protecting the technology that enables that access should be part of the strategy.

SECTION THREE:

PROTECTING PATRON PRIVACY

Public libraries have been trusted stewards of information and intellectual freedom. Today's libraries also handle a growing amount of digital information, from library card registrations and online account credentials to room reservations, event registrations, and digital resource usage.

While libraries may not retain highly sensitive information like healthcare providers or financial institutions, patrons still expect their personal information to be handled responsibly and securely.

Protecting patron information is not simply a technology issue but rather an extension of the trust libraries work hard to build within their communities.

What This Means for Libraries

- **Review** what patron information is collected and stored.
- **Limit** access to patron information based on job responsibilities.
- **Evaluate** third-party vendors that may handle patron information.
- **Include** privacy considerations in technology planning discussions.

Questions to Ask

Do we know what patron information our library stores?

Who has access to that information?

Are our vendors following appropriate security practices?

Does staff understand privacy expectations?

Protecting patron information is ultimately about protecting community trust.

SECTION FOUR:

CYBER INSURANCE TRENDS

Cyber insurance has evolved significantly over the last several years. Organizations of all sizes, including public entities and nonprofit organizations, are increasingly being asked to demonstrate basic cybersecurity practices before obtaining or renewing coverage.

Libraries may find that cyber insurance applications include questions about multi-factor authentication, backups, staff training, and incident response planning.

Preparing for these conversations ahead of time can make renewals smoother and help identify opportunities to strengthen cybersecurity readiness.

What This Means for Libraries

- **Cyber insurance expectations** continue to evolve.
- **Insurance questionnaires** can help identify security gaps.
- **Documentation** of security practices is increasingly important
- **Leadership** should understand insurance requirements before renewal periods.
- **Cybersecurity planning** and insurance planning go hand-in-hand.

Questions to Ask

When is our cyber insurance **renewal date**?

Do we know **what security controls** our carrier expects?

Could we **confidently answer** our application today?

Have we **reviewed our coverage** lately?

Cyber insurance is increasingly seen as a measure of cybersecurity maturity rather than simply a financial safeguard.

SECTION FIVE: HUMAN RISK: PHISHING & STAFF AWARENESS

Cybersecurity incidents often begin with a simple interaction: clicking a link, opening an attachment, or responding to a convincing email.

Libraries are especially collaborative environments. Staff routinely communicate with patrons, vendors, volunteers, community partners, and one another. That openness and accessibility can create opportunities for malicious actors attempting to gain access to systems or information.

Technology alone cannot prevent every incident. Building awareness among employees remains one of the most effective ways to strengthen resilience.

What This Means for Libraries

- **Staff awareness** is a critical security control.
- **Phishing** attempts continue to become more sophisticated.
- **Training** should occur throughout the year, not only during onboarding.
- **Incident reporting** procedures should be simple and well understood.
- **Leadership participation** reinforces the importance of cybersecurity.

Questions to Ask

Would staff know how to recognize a phishing attempt?

Do employees know how to report suspicious emails?

Have we conducted training recently?

Do we encourage employees to ask questions when something seems off?

Cybersecurity awareness is about helping people recognize and respond to potential risks with confidence.

SECTION SIX:

BACKUP, RECOVERY, & RESILIENCE

Even organizations with strong security practices can experience technology disruptions. Equipment failures, accidental deletion, severe weather events, vendor outages, and cybersecurity incidents can all affect access to systems and services.

The question is not whether information is backed up, but whether the library can recover quickly and continue serving its community.

Resilience planning helps ensure libraries can respond thoughtfully and recover with confidence.

What This Means for Libraries

- **Backups** should be protected from unauthorized changes.
- **Recovery procedures** should be tested periodically.
- **Leadership** should understand restoration expectations
- **Critical systems** should be identified and prioritized.
- **Recovery planning** should include people, processes, and technology.

Questions to Ask

How quickly could we **restore our critical systems**?

Have we **tested our backups** recently?

Do we know which systems should be **restored first**?

Who would **coordinate recovery efforts**?

Resilience is not measured by whether an incident occurs. It's measured by how effectively the organization responds and recovers.

APPENDIX: LIBRARY CYBERSECURITY SELF-ASSESSMENT SCORECARD

Use the following checklist to evaluate whether your organization is *prepared for today's cybersecurity challenges*.

If the statement is true, check the box!

Unsure? No worries - you can circle the box instead.

At the end, you'll tally your responses to get a snapshot of your library's cybersecurity readiness.



NEXT STEPS:

Complete the self-assessment and bring your scorecard to **Booth 15 at the MLA Annual Conference** (October 28 - 30, 2026, at Vibe Credit Union Showplace).

Our team will talk through your results and discuss what comes next.

Prepared by BAE Networks, a Michigan-based managed IT and cybersecurity provider helping organizations strengthen security, resilience, and long-term technology planning.

SECTION ONE: IDENTITY & ACCESS MANAGEMENT

- ☐ Multi-factor authentication is enabled for staff email accounts.
- ☐ Former employees' accounts are disabled promptly.
- ☐ Staff have unique logins and do not share accounts.
- ☐ Administrative privileges are limited to authorized personnel.
- ☐ Password requirements align with current best practices.

SECTION TWO: PUBLIC COMPUTER SECURITY

- ☐ Public-use computers are separated from internal systems.
- ☐ Public computers automatically remove patron data between sessions.
- ☐ Software updates are applied regularly.
- ☐ USB usage is restricted or monitored appropriately.
- ☐ Public computers have antivirus and endpoint protection.

SECTION THREE: STAFF AWARENESS

- ☐ Staff receive cybersecurity awareness training annually.
- ☐ Employees know how to report suspicious emails.
- ☐ Leadership participates in security discussions.
- ☐ Staff understand basic phishing warning signs.
- ☐ Security reminders are shared throughout the year.

SECTION FOUR: BACKUP & RECOVERY

Critical systems are backed up regularly.

☐

Backups are tested *at least* annually.

☐

Backup copies are protected from ransomware.

☐

Leadership understands how long restoration would take.

☐

Recovery responsibilities have been assigned.

☐

SECTION FIVE: INCIDENT PREPAREDNESS

☐ The library has an incident response plan.

☐ Leadership understands who to contact following a cyber event.

☐ Key vendors and partners are documented.

☐ Cyber insurance information is readily available.

☐ Role and responsibilities have been identified.

SECTION SIX: STRATEGIC PLANNING

Technology risks are discussed with leadership, and/or the board.

☐

Technology investments are planned proactively.

☐

Cybersecurity responsibilities are clearly defined.

☐

The library conducts periodic technology reviews.

☐

Technology initiatives align with organizational priorities.

☐

HOW DID YOU DO?

25 - 30 Checked Boxes

Your library appears to have a **strong foundation in place!** Continue reviewing your practices regularly to adapt to changing risks.

15 - 24 Checked Boxes

You may have some **opportunities to strengthen your cybersecurity** readiness and improve resilience.

Fewer than 15 Checked Boxes

Consider **prioritizing conversations around technology** planning, staff awareness, and incident preparedness.

REQUEST A LIBRARY CYBERSECURITY READINESS REVIEW

BAE Networks offers **complimentary readiness reviews** to help Michigan's public libraries identify opportunities to **strengthen cybersecurity** and **support long-term planning**.

*This includes a **dark web exposure scan**, a review of your **cyber insurance policy requirements** for cyber liability, and a discussion of **backup and recovery best practices**.*

REACH OUT TODAY:

 (248) 707-1040

 events@baenetworks.com

 1250 Stephenson Hwy, Troy, MI 48083

Meet our Michigan Library Security
team at **Booth 15!**

BAE
NETWORKS

MLA
MICHIGAN LIBRARY ASSOCIATION

ANNUAL CONFERENCE
OCTOBER 28 - 30, 2026
VIBE CREDIT UNION SHOWPLACE