Risk Analysis for Boys and Girls Clubs of Southeastern Virginia

Isaiah Bristol, Ryan Reaves, Asher Embry

Old Dominion University

COVA CCI Cyber Clinic

Spring 2026

CYSE368: Cybersecurity Internship

Professor Teresa Duvall

Apr 21, 2026

Table Of Contents

Introduction

Old Dominion University's School of Cybersecurity offers students the opportunity to apply cybersecurity principles in real-world environments by working with client organizations through the Cyber Clinic. Through this program, students perform cybersecurity evaluations and offer recommendations to improve an organization's cybersecurity posture.

The purpose of this risk assessment is to identify, analyze, and evaluate potential security risks facing a small business or nonprofit in Hampton Roads, specifically those affecting its systems, assets, and operations. This includes looking at vulnerabilities in infrastructure, policies, and user practices that external threats could exploit. By assessing the likelihood and potential impact of these risks, the Cyber Clinic team aims to provide actionable recommendations that align with industry best practices and frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The ultimate goal of this assessment is to help better understand the organization's current security posture, prioritize risk mitigation efforts, and strengthen its ability to protect sensitive data and reduce the likelihood of cybersecurity incidents.

Members of the Boys & Girls Clubs Team

- **Isaiah Bristol**: Cybersecurity Major, class of 2026, was responsible for the following sections: Overview of the Industry, Common Threats in the Industry, and SWOT Analysis. He was also in charge of formatting the report to reflect the feedback from our TAs. Isaiah spent a lot of time familiarizing himself with the most common threats that nonprofits face, to accurately apply them to the Boys and Girls Clubs.
- **Ryan Reaves**: Cybersecurity Major, class of 2026, was in charge of writing the report introduction, conducting the Valor's Top 10 Digital Security risk assessment, taking notes on the company's assets, risk, and controls, applying it to the NIST framework, keeping notes of client questions, and providing suggestions.
- **Asher Embry**: Cybersecurity Major, class of 2027, was responsible for the following sections: Company Description, Company History, Social Media Presence, parts of Client Suggestions, and the Appendix. He also assisted with taking notes during meetings, gathering company information, conducting research, designing the final presentation slide deck, and checking for grammar and formatting consistency.

Overview of the Industry

The Boys & Girls Clubs of Southeast Virginia (BGCSEVA) is a charitable organization operating within the youth development and social services industry. Organizations within this industry focus on providing mentoring programs and support services to the youth in local communities. Many organizations use Positive Youth Development (PYD) to approach their interactions with young people. PYD is designed to develop and strengthen young people's leadership skills, their ability to build and maintain interpersonal relationships, and to access opportunities they otherwise might not have had. The support does not stop after graduation. Many programs aim to guide their members as they enter adulthood. This kind of support can change the lives of children from all walks of life.

The Boys and Girls Clubs of America (BGCA), and subsequently, the BGCSEVA, fit into this industry by providing educational programs that promote health, fitness, and leadership. It is their mission to develop young individuals into capable leaders by providing safe places for children to grow, equipping students with life skills via their educational programs, and connecting them with mentors committed to their well-being. Organizations like BGCSEVA play an important role in shaping the futures of young people. As a result, the youth that they serve have the opportunity to not only better themselves, but also the world around them.

Common Threats

Likely, a non-profit like the BGCSEVA is not what most people would consider a high-value target for cyber attackers; however, non-profits were the second-most-targeted business sector in 2021, accounting for 31% of successful attacks (Lazar 2024). A year later, Cisco reported that small businesses were the targets of 70% of cyberattacks (Gross 2022). Attackers commonly attempt extortion via ransomware, employ social engineering strategies like phishing, and exploit vulnerabilities in systems shared with third-party vendors. Two-thirds of small businesses have experienced an attack to varying degrees. An alarming 60% of those businesses close their doors permanently after a data breach, according to PreVeil Cybersecurity. These statistics should spark urgent responses to prevent this growing trend from affecting more businesses. To ensure proper mitigation of such risks, we must explore them in greater depth. The following sections will dive into ransomware, social engineering/phishing, and the exploitation of third-party vulnerabilities.

Phishing is a form of social engineering that uses fake emails, texts, and websites to obtain login credentials or install malware. Attackers will often send emails and text messages with links to websites that look like reputable companies. Once someone has followed the link, they may be asked to log in to their account. Afterwards, the threat actor uses those credentials to gain unauthorized access to the account and information. Links in phishing emails and texts may install malware directly onto the device that accesses it. In this scenario, the victim may still be directed to a fake website. However, even if they do not use their login information on said website, the attacker has already started doing damage. Threat actors can also make phishing phone calls and request login credentials, credit card numbers, and more. It is important to train employees to avoid any email or message that can not be verified. Without the proper training, a

small business can be exposed to an attack that it has not allocated the resources to prevent, contain, and recover from.

Malware that encrypts data or blocks access to computers and information is called **ransomware**. Attackers will often use "double-extortion," meaning they have stolen and encrypted data, to demand a payment. Attackers often threaten to release the information publicly if the ransom is not paid. As mentioned previously, malware can be installed through links sent by phishers. Critical systems can become infected if a device is connected to the same network or if infected hardware is installed (ie, a USB stick, external hard drive, etc.). It is important to implement threat detection and keep all software updated to help prevent and contain any possible threats.

Nonprofits outsource many of the services that help their organization run. This in itself is not bad; however, it exposes them to attacks from a new front. An organization that has done this must ensure that **third-party vendors** can access only the information necessary to provide their services. This could include implementing least-privilege access controls for vendors who need digital access to systems and ensuring that all offices, computers, and other physical access points to the network are secured, if a vendor is physically present on site. Role-based access controls (RBACs) can reduce the likelihood of exposure. RBAC could allow an organization to assign vendors to specific roles that limit what systems and data they can access. Organizations can track which information users have attempted to access. Regular monitoring of vendor activity is essential to ensuring they comply with all policies. Some of the biggest concerns come from what is out of the nonprofit's control. If a vendor has a vulnerability in their network and also has access to an organization's systems or data, a breach in the vendor's system could create a security risk for the nonprofit.

Nonprofits must not only control what vendors can access, but also keep in mind that third-party connections increase their risk of an attack. Network segmentation can further mitigate this risk. Strict onboarding and offboarding processes should not be limited to employees. Organizations must ensure that new vendors are given secure, role-based access to necessary systems and information, and promptly revoke said access when a service is no longer needed. Network segmentation divides the network into smaller sections to limit movement between each system. This means that even if a vendor's access is compromised, they cannot move to other parts of the network without going through more security. Even though outsourcing is often a necessary part of running an effective nonprofit, protecting the organization from further risks requires strict oversight. Combining RBAC with other techniques will best protect critical systems and sensitive information.

Company Information

Company Description

The Boys & Girls Clubs of Southeast Virginia (BGCSEVA) is a youth development organization dedicated to providing safe and educational spaces for youth ages 6 through 18 across the Hampton Roads area. Operating nine clubs in Chesapeake, Norfolk, Suffolk, Franklin, Virginia Beach, Portsmouth, and the Eastern Shore, the organization focuses on three primary outcomes: academic success, good character and citizenship, and healthy lifestyles. Through offering after-school and summer programs, BGCSEVA aims to enable all young people "*to reach their full potential as productive, caring, and responsible citizens*" with mentorship, career preparation, and leadership development.

Company History

Beginning in 1919, the precursor to BGCSEVA was founded by the Rotary Club of Norfolk as the *Boys Club of Norfolk*. For decades, it operated as a single-site location providing a positive environment for boys to learn and grow. In 1974, a new era of growth began with the opening of a location in Virginia Beach. Joining the national movement toward greater inclusivity, the organization expanded its services to include both boys and girls in 1993, renaming itself the Boys & Girls Clubs of South Hampton Roads to better reflect its broader mission and the diverse youth it serves.

Between 1998 and 2004, BGCSEVA experienced rapid growth, expanding its service as far west as Franklin and north to the Eastern Shore of Virginia. In 2003, it adopted its current

name, Boys & Girls Clubs of Southeast Virginia, to better represent its larger geographic footprint. In recent years, BGCSEVA has continued to modernize and expand its operations, notably consolidating sites in Portsmouth in 2021 to create a more central hub and partnering with the Norfolk Redevelopment and Housing Authority in 2023 to open two new clubs in the Grandy Village and Young Terrace neighborhoods. Currently, there is ongoing construction and development of a new teen center in Chesapeake. Today, with over 100 years of impact, BGCSEVA remains a vital community partner serving thousands of youth members annually.

Social Media Presence

BGCSEVA maintains an active social media presence to share club news, success stories, and community events. They utilize platforms such as Facebook, Instagram, and LinkedIn to showcase member achievements, such as the annual “Youth of the Year” winners, and to highlight local partnerships. They also maintain a YouTube channel featuring videos that highlight their impact on the community, including recaps of major fundraising events and testimonials from club members and staff.

While staying active online helps them stay connected to the community and promote their mission, it also introduces them to more risks. Photos, videos, and stories that include the youth require special attention to ensure that identifying information is not revealed. Unwanted interactions, such as inappropriate comments or messages from outside users become a risk. Social media accounts also broaden the attack surface of the organization. The account could become compromised if the login credentials are weak or repeated across platforms. There is also the possibility of someone impersonating the BGCSEVA by creating an identical account or by claiming to be affiliated with them. Both account compromise and impersonations can

negatively impact the BGCSEVA brand and reputation. As mentioned above, phishing attempts and malware attacks are common threats to nonprofit organizations. The frequency of such attacks can increase because of active social media accounts. Staff responsible for managing the accounts must be vigilant so that the organization can avoid becoming a victim of cyber criminals.

Risk Assessments

Valor's Top 10 Digital Security Checklist

For the Boys and Girls Clubs' Risk Management Report, we were able to work with Valor Cybersecurity as a trusted partner to the Cybersecurity Clinic. Valor Cybersecurity (CEO Greg Tomchick) is a small business owner who provides scalable, adaptive cybersecurity protocols to other business owners. Based on our clinic meetings with Greg, this is our suggested write-up based on the Valor Cybersecurity Digital Checklist Assessment. Greg Tomchick developed a "Top Ten Digital Security Checklist" for businesses to use to grade themselves on their cybersecurity posture. The grading scale is from 0 to 50, and while answering the ten questions, you grade yourself on a scale of one to five, with a score of one meaning that the objective is not implemented and a score of five meaning that the objective is implemented in some way.

Cybersecurity Risk Assessment Summary Chart

#	Assessment Area	Description (Short)	Score (1–5)
1	Annual Digital Risk Checkup	Regular cybersecurity risk assessment	5
2	Access Control & Permissions	Review and limit access to systems/data	5
3	Data Backup & Testing	Backup data and test recovery	5
4	Multi-Factor Authentication (MFA)	Require multiple login verification methods	5
5	Network Firewall	Protect the network from unauthorized access	5
6	Incident Response Plan / Security Policy	Established cybersecurity policies and response plans	5
7	Employee Training	Cybersecurity awareness training	1
8	Onboarding/Offboarding Processes	Manage user access lifecycle	5
9	Monitoring & Surveillance	Monitor systems for suspicious activity	5
10	Email Security Configuration	Secure and updated email protections	5

In our assessment, we were able to grade the Boys and Girls Clubs a 46 out of 50. With that being said, the Boys and Girls Clubs are in the green in terms of current cybersecurity risk. The only area of concern is the lack of employee training on cybersecurity best practices. Incorporating some kind of cybersecurity awareness training, large or small, could lower the chances of a cyber attack via phishing or other human-connected methods. Awareness training significantly reduces cyber attacks by transforming employees into a "human firewall," cutting employee chances of being phished by up to 86% (Daly, J., 2021). Effective programs can lower overall organizational risk from 60% to 10% in the first year, with 80% of organizations

reporting fewer security incidents (Daly, J., 2021). It directly addresses the human element present in 60% of breaches (Verizon, n.d.). By addressing the gap in employee training, the organization can greatly reduce its exposure to common attack methods and strengthen its overall security posture. Implementing even a modest awareness program would not only complement existing safeguards but also make sure that staff members play an active role in protecting the organization against evolving cyber threats.

NIST Assets, Risks, and Controls

The National Institute of Standards and Technology (NIST) is a non-regulatory U.S. government agency in the Department of Commerce. It promotes innovation and competitiveness in the industry by advancing measurement science, standards, and technology, including important cybersecurity frameworks. The NIST Cybersecurity Framework (CSF) 2.0 is used by all businesses, regardless of size, to manage and reduce their cybersecurity risks. The framework is comprised of six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. In 2024, the CSF 2.0 was released with the new *Govern* function to emphasize executive oversight of cybersecurity and align with business objectives. As described by NIST, “The structure of the Core is intended to resonate most with those charged with operationalizing risk management within an organization” (NIST, 2024).

NIST CSF 2.0 At a Glance

- **Govern**: Provides ways to inform what an organization may do to achieve and prioritize the other outcomes of the other 5 functions in the context of its mission and stakeholder expectations. (e.g., establishing rules for the staff to follow concerning sensitive data)
- **Identify**: Understanding the organization's assets (e.g., student data, software, systems, facilities, staff) and other related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs found by the governance.
- **Protect**: Focuses on implementing safeguards to secure systems and data. Its goal is to reduce the likelihood and impact of cybersecurity incidents by controlling access, protecting information, and maintaining secure operations. (e.g., multi-factor authentication and limited access to certain sensitive files.)

- **Detect**: Focuses on identifying cybersecurity events promptly. Its goal is to quickly discover potential threats or anomalies so organizations can respond before significant damage occurs. (e.g., email filtering, monitoring login activity)
- **Respond**: Focuses on taking action after a cybersecurity incident is detected. Its goal is to contain the impact, mitigate damage, and communicate and manage the response effectively. (e.g., notifying Mode5 about any suspicious activity, locking any infected accounts)
- **Recover**: Focuses on restoring systems and operations after a cybersecurity incident. Its goal is to return to normal operations and improve resilience based on lessons learned. (e.g., restoring data from backups and learning from the mistakes made)

SWOT Analysis

A SWOT analysis is a tool that can be used to assess an organization's position and plan for the future. It highlights the strengths and potential opportunities for the organization to grow, while giving honest feedback about its weaknesses and threats that could exploit vulnerabilities.

- Strengths - Internal advantages that give the company an edge.
- Weaknesses - Internal imitations or challenges that harm performance.
- Opportunities - External conditions that can be used for growth.
- Threats - External risks that could negatively impact the organization.

SWOT Analysis Table

Strengths ● Implementation of multi-factor authentication. ● Desire to grow. ● An openness to new ideas ● Well-informed about the operations across club locations. ● Awareness of an upcoming policy change. ● Looking to improve daily check-in processes.	**Weaknesses** ● Paper Files are not stored in locked cabinets. ● Lack of uniformity across all club locations. ● Informal cyber IRP. ● Lack of physical security at the Eastern Shore location. ● Hands-off approach to managing their security. ● Lacking knowledge about the upcoming policy changes. ● Need a process for buying and connecting new assets to the system. ● Unapproved and insecure devices on the internal networks.
Opportunities ● Could learn how to manage security. ● Could gain staff training programs. ● Could implement a uniform incident response plan across clubs. ● Could get ahead of future policy changes. ● Resources and support from third-party vendors.	**Threats** ● Unauthorized access to PHI files. ○ Violating HIPAA policies. ● Falling out of compliance with the national BGCA policies. ● Increased threat to non-profits.

Next Steps

Client Questions and Recommendations

How do we implement a cybersecurity incident response plan?

We recommend that BGCSEVA implement a cybersecurity Incident Response Plan (IRP) to effectively manage and mitigate potential cyber threats while protecting sensitive information such as youth records, donor data, and employee information. This plan should apply to all staff, volunteers, and any systems used within the organization. This would include computers, networks, and cloud-based services. One of our suggestions is to have a designated incident response team, with defined roles such as an incident response lead to oversee decision making, IT personnel to handle technical investigation and containment, and a communications coordinator to manage internal and external communications. The IRP can be broken down into the following sections:

Preparation

Preparation involves making sure the organization is ready to respond effectively to cybersecurity incidents. This includes maintaining up-to-date security tools such as antivirus software and firewalls, establishing incident response procedures, and ensuring system backups are regularly performed and securely stored. Preparation also includes defining roles and responsibilities for the incident response team and ensuring communication channels are in place.

Identification

The identification phase focuses on detecting and confirming potential security incidents. Indicators may include unauthorized access attempts, unusual system behavior, or alerts from security tools. Once an incident is suspected, it should be promptly reported and documented, including the time of detection, affected systems, and observed activity. Accurate documentation is very important for an effective response and later analysis.

Containment

During containment, the goal is to limit the spread and impact of the incident. This may involve isolating affected systems from the network, disabling compromised user accounts, or restricting access to critical resources. Short-term containment actions should be implemented quickly to prevent further damage while preserving evidence for investigation.

Eradication

Eradication involves removing the root cause of the incident. This includes eliminating malware, closing vulnerabilities, applying security patches, and resetting compromised credentials. The objective is to ensure that all traces of the threat are removed and that the system is no longer vulnerable to the same attack.

Recovery

The recovery phase focuses on restoring affected systems and returning operations to normal. Systems should be restored from clean backups, tested to ensure they function correctly, and closely monitored for signs of recurring issues. Recovery should be performed cautiously to avoid reintroducing vulnerabilities.

Lessons Learned

After the incident is resolved, a lessons-learned review should be conducted. This includes analyzing what occurred, evaluating the effectiveness of the response, and identifying areas for improvement. The organization should update incident response procedures, security controls, and training based on these findings to strengthen future response efforts. **See the appendix for example cybersecurity IRP.**

What basic cyber risk management practices should we implement?

Implementing employee cybersecurity awareness training is very important in protecting the company and reducing cyber risk. It should be simple, continuously ongoing, and focused on real-world risks. All staff and volunteers should receive basic cybersecurity training during onboarding, followed by regular refreshers to keep those good cybersecurity practices in their heads. Key topics covered should include recognizing phishing emails, using strong and unique passwords, and the importance of enabling multi-factor authentication, which has already been implemented. Employees should also be trained on protecting sensitive data, especially youth and donor information, by only accessing what they need and handling it securely. Basic device security, such as logging out of computers when not in use and avoiding joining public Wi-Fi networks, should also be discussed.

Employees also need to know how to report suspicious activity quickly, like strange emails or system behavior. Creating a culture where reporting is encouraged without fear of punishment can help stop incidents early. Using short videos, quick quizzes, and occasional simulated phishing tests can keep the training engaging and effective while reinforcing good cybersecurity habits.

How do we configure content filters and manage our Cox Internet blacklist?

We were able to find how to access the Cox Malblock Dashboard and make changes as needed. First, sign in to the Cox Business portal with your user ID and password. Once you sign on, find the “Services” section and click the “Internet” icon. Then, from the “Internet” page, click the “MalBlock DNS Security” icon. Lastly, from the “MalBlock DNS Security” page, click the “MalBlock Dashboard”.

Now that you have accessed the MalBlock Dashboard, you will be able to apply your own website filters without Cox having to do it for you. You can do this by clicking the “Settings” tab from the MalBlock Dashboard and selecting “Block & Allow Lists”. From the “Block & Allow List” page, select the user group for which you want to block certain websites. In the case you do not have any user groups, we provided directions on how to do so in the packet we gave you. Once you click on the user group you want to configure, you should see a “URL Check” section. In the Check URL to add Block or Allow list field, enter a domain name, then click “Check.” Select “Whole website” or “Specific URL” and click “Block” or “Allow”. As a result of doing so, in the “Lists” section, the domain name displays in the “Block” or “Allow” list column. Now, if you want to add websites in bulk, we provided directions for that in the packet as well.

How can we secure the use of AI at the administrative and club locations?

One of the concerns that was brought to our attention was Mode 5 introducing Hatz AI to the company. We were asked to do some research on Hatz and look at other alternatives on AI tools BGCSEVA could use. Hatz is a secure AI-as-a-service platform designed for managed service providers and small to medium businesses to build and manage custom AI agents.

The protection provided by Hatz is System and Organization Controls 2 (SOC2) certified. SOC 2 is a compliance standard designated for service providers to help manage client data. There are 2 types of SOC reports. A Type 1 report is when an auditor assesses whether the system they use is safe or not, and if it follows the data safety guidelines. The Type 2 report goes a step further by evaluating the operational effectiveness of these systems over a six to twelve-month time frame. It gives details on whether the controls in place are functioning as intended and effectively maintain the data safety guidelines throughout that timeframe.

Alternative AI tools would be Microsoft Copilot, which is good for daily office use. The pros of this AI tool are that it is typically free or is heavily discounted via the company TechSoup. It integrates into your workflow, living inside of Microsoft Word, Microsoft Excel, and Microsoft Teams. It has great security measures since it inherits Microsoft's massive security infrastructure and General Data Protection Regulation (GDPR) compliance. Microsoft Copilot is also SOC2 Type 2 certified. The drawbacks would be that you are not able to tailor it to your liking as well as you could with Hatz. Another downside would be that it only works best when all the files on the computer are stored in OneDrive/SharePoint. Box AI is another AI tool that you could potentially use if you want to focus more on protecting sensitive data than the AI's ability itself. The pros would be that it has top-tier security, it is approved by the Health Insurance Portability and Accountability Act (HIPAA) and Federal Risk and Authorization Management Program (FedRAMP), so at its core, it is made to protect sensitive data. They guarantee private educational data is never used to train public AI models. And they, too, are SOC 2 Type 2 Certified. The cons for Box AI are that it is a file storage platform first, and the AI is an add-on, not a standalone assistant. Another con would be that it can be more expensive than Microsoft Copilot if you are not already using Box AI for storage.

AI Tools Comparison Chart

AI Tool	Pros	Cons
Hatz AI	• Highly customizable (build specific AI agents like tutoring) • Multi-tenant (manage multiple sites in one dashboard) • White-label branding for nonprofit use • SOC 2 certified security	• Time-intensive setup and configuration • May require technical expertise to fully implement
Microsoft Copilot	• Low cost (often free/discounted via TechSoup) • Integrates with Word, Excel, Teams • Strong security (Microsoft infrastructure + GDPR) • SOC 2 Type 2 certified • Easy to use within existing workflows	• Limited customization compared to Hatz • Works best with OneDrive/SharePoint • Less flexibility for specialized AI agents
Box AI	• Top-tier security focus • HIPAA & FedRAMP compliant • Does not use private data to train public AI • SOC 2 Type 2 certified	• AI is secondary to file storage • Not a strong standalone AI assistant • Can be more expensive if not already using Box

How can we implement policies to prevent inappropriate cellular data usage while on the property?

To prevent inappropriate cellular data usage while on the property, BGCSEVA should implement policies that establish clear expectations, consistent supervision, and education rather than complete restriction. Because a complete restriction on members using their phone data isn't possible without breaking any laws. The BGCSEVA should establish guidelines that limit phone use to designated times, such as before or after programs, and prohibit use during instructional/group activities. Members and staff should be required to avoid accessing inappropriate content and to refrain from recording or photographing others without permission. Because cellular data can bypass Wi-Fi filters, the policy should discourage its use during program hours. BGCSEVA should encourage connecting to the club's monitored Wi-Fi when devices are permitted, and require devices to be stored during activities. Staff supervision is crucial for this policy to work. Devices should be limited to visible areas, and there should be a progressive discipline system that could include warnings, temporary confiscation, and parent involvement if necessary. Also, involving parents through signed agreements when new members join or have parents sign the agreement, even if they are already members. While it is not possible to eliminate misuse of cellular data, implementing these measures that establish strong rules, supervision, and education can reduce inappropriate behavior and support a safe and positive environment.

Conclusion

Overall, after reviewing the Boys and Girls Clubs over the past few weeks, we came to the conclusion that, currently, BGCSEVA is not in immediate danger. From Cox and Mode 5, they have good cybersecurity practices in place. Unfortunately, due to unknown changes from the Boys and Girls Clubs of America, it is difficult to predict what policies BGCSEVA will need to implement or change. Despite this uncertainty, BGCSEVA remains in a strong, cyber-secure position and only needs minor changes to further strengthen its stance. To strengthen your cybersecurity posture, we recommend that you implement an ongoing employee cybersecurity awareness training for all employees and volunteers. We also recommend that you also look into establishing an incident response team to carry out the incident response plan we provided and adjust it as necessary.

References

Berlove, O. (2024, November 27). *Facts and stats about cybersecurity and compliance*. PreVeil. https://www.preveil.com/blog/cybersecurity-statistics/

Cybersecurity and Infrastructure Security Agency. (2025). *Cross-sector cybersecurity performance goals*. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Cybersecurity and Infrastructure Security Agency. (2026, March 20). *CISA CPG checklist*. https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist

Daly, J. (2021). *How effective is security awareness training?* usecure. https://blog.usecure.io/does-security-awareness-training-work

DGCG Support. (2024, October 29). *8 cybersecurity concerns for nonprofits & how to address them*. Nonprofit Leadership Center of Tampa Bay. https://nlctb.org/tips/8-cybersecurity-concerns-for-nonprofits/

Gross, A. (2021, July 13). *The essential guide to cybersecurity for the small business*. Cisco Umbrella. https://umbrella.cisco.com/blog/cybersecurity-for-small-business

Karpsen, G. (2025, October 24). *Security awareness training statistics 2025 [100+ studies]*. Brightside Technologies SA. https://www.brside.com/blog/security-awareness-training-statistics-2025-100-studies

Lazar, A. (2024, March 25). *Cyber-poor, target-rich: The crucial role of cybersecurity in nonprofit organizations*. CyberPeace Institute.

https://cyberpeaceinstitute.org/news/cyber-poor-target-rich-the-crucial-role-of-cybersecurity-in-nonprofit-organizations/

National Fund for Workforce Solutions. (2024, March 15). *How positive youth development approaches can inform your business choices*. https://nationalfund.org/how-positive-youth-development-approaches-can-inform-your-business-choices/

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (Version 2.0). https://doi.org/10.6028/nist.cswp.29

SOC 2 Type 2 certification: What it is and why it matters. (2026). Gallagher. https://security.gallagher.com/en/Blog/SOC-2-Type-2-certification-what-it-is-and-why-it-matters

2025 data breach investigations report: Executive summary. (n.d.). Verizon. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

Appendix

Example Cybersecurity Incident Response Plan

This is an example of a Cybersecurity IRP for BGCSEVA. This is generalized and will require modifications as necessary for staff responsibilities to ensure effective usage of this response plan. Other resources can be used for modification, such as NIST *Incident Response Recommendations and Considerations for Cybersecurity Risk Management* https://csrc.nist.gov/pubs/sp/800/61/r3/final or SANS *Incident Handler's Handbook* https://www.sans.org/white-papers/33901.

1. **Preparation - The Response Team**

   Define key roles and responsibilities ahead of time and clearly.

   - Incident Commander: Executive officer or IT Lead.
   - Technical Lead: External managed service provider (Mode5) and internal staff lead.
   - Communications Lead: Handles notifying staff, parents, and (if applicable) the board of directors or media.
   - Legal/Compliance: Consults on state reporting requirements regarding member data.

2. **Identification - Is it an Incident?**

   Train staff to recognize signs of a compromise and report them immediately to the Technical Lead. Signs of trouble include:

   - Unusual login activity (logins from different countries).
   - Files being encrypted.

- Staff receiving “urgent” emails asking for gift cards or to log in to a different site (phishing).
- Inappropriate content bypassing network filters.

3. **Containment - Stop the Bleeding**

   The goal is to prevent the threat from spreading further across the network. This includes short-term and long-term containment.

   Short-term Containment:

   - Disconnect affected devices from Wi-Fi/Ethernet (**DO NOT** power them off, as this may erase evidence in the device memory).
   - Disable compromised user accounts.
   - Change passwords for **all** administrative accounts.
   - If members are directly involved, ensure they are safe, and parents are notified promptly.

   Long-Term Containment:

   - Patch the vulnerabilities that allowed the entry (ex. Updating a firewall).

4. **Eradication and Recovery - Clean and Restore**

   Once the threat is contained, remove it and return to normal club operations.

   - Eradication: Run deep antivirus scans and wipe/reinstall operating systems on infected machines.
   - Recovery: Restore data from the most recent clean backup.
   - Testing: Verify that systems are back online and that content filters are functioning correctly before allowing full staff access.

5. **Notification - Protecting Members**

   Notification of members and staff is crucial.

Audience	When to Notify	Method
Staff	Immediately	Internal meeting/Email
Parents/Guardians	If member data is accessed	Direct letter/phone call
Board of Directors	Within 24 hours	Formal briefing/Email
Law Enforcement	If it involves a crime or PII theft	Local authorities, FBI, IC3

6. **Lessons Learned - Post Incident Review**

   Within one week of the incident, hold a post-mortem meeting to answer the following;

   - Exactly what happened and at what time?
   - How well did the staff follow the IR plan?
   - What one change to our content filtering or security training would have prevented this?