CUSEUM

Safeguarding Your Membership Data:

How Museums & Cultural Institutions Can Protect Their Digital Assets

As a museum professional or cultural attraction employee, whether a curator, administrator, or membership manager, you play a critical role in preserving art, culture, science, the natural world and history. But today's challenges go far beyond managing and sustaining physical artifacts or exhibits.

As cultural institutions embrace this ever-changing digital age, your expanded responsibilities now include safeguarding a wealth of digital data that can range in utility and risks. From online exhibitions, Big Data to membership records, this information is vital not only to the functioning of your institution but also to its reputation.

In fact, the stakes have never been higher.[1] As museums and cultural institutions increase their digital presence, they face a growing number of cyber threats.

Imagine launching a new digital exhibition and visitors from around the globe are enjoying your collections online, meanwhile, hackers, lurking in the digital shadows, are waiting for the right moment to strike. They're not targeting your physical treasures but, instead of that, are sniffing for your digital data: visitor information, financial records, donor details and more.

Cybercrime is expected to cost the world $10.5 trillion annually by 2025[2], according to Cybersecurity Ventures. Museums and cultural institutions are part of this landscape. A 2021 IBM report revealed that the average cost of a data breach is now $4.24 million, with 66% of companies experiencing a cyberattack in the last year. As museums increasingly digitize their operations, they become prime targets for hackers.

Ransomware attacks, for example, surged by 104% in 2023, according to Security Magazine.[3]

In this paper, we'll explore the cyber threats facing museums worldwide. We'll dive into potential cases where institutions have fallen victim to cyberattacks, breaking down what went wrong and offering practical tools and strategies to defend against these modern day heists. Finally, we'll show how Cuseum is taking the necessary steps to build top-quality software that ensures institutions like yours are able to safeguard their digital assets while continuing their mission to connect people with art, culture, and history.

[1] MIT, "MIT report details new cybersecurity risks," 2024
[2] Business Standard, "Cybercrime costs to hit $10.5 trn by 2025: How insurance may save your biz," 2024
[3] Security Magazine, "Cyberattack attempts increased 104% in 2023," 2024

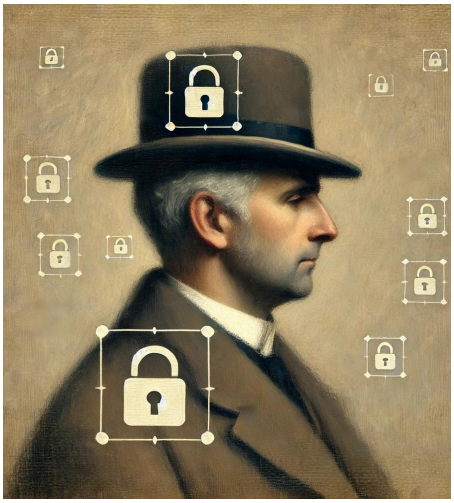
Why Museums & Cultural Organizations Are Prime Targets

While museums and cultural institutions may seem like fortresses of culture, they're also full of valuable digital data, much like any other business that works around a contact or relationship management system. From donor records to financial transactions, museums store valuable information that makes them prime targets for cybercriminals.

According to the 2022 Verizon Data Breach Investigations Report, 82%[4] of breaches involve a human element, often due to phishing or social engineering attacks. Most museums, which hold sensitive personal and financial data, have a lot of human elements attached to them, making them increasingly vulnerable. Additionally, museum databases contain sensitive loan records, provenance documentation, and internal research that, if exposed, could be exploited or sold on the black market.

Adding to the challenge, many museums are perceived as "soft targets." Cultural institutions often have fewer IT resources than sectors like finance or healthcare. A Sophos report revealed that 79% of organizations hit by ransomware lacked proper endpoint security[5] or hadn't conducted recent security audits. This lack of preparedness, coupled with valuable data, makes museums appealing to cybercriminals.

As the digital landscape evolves, museums must prioritize cybersecurity to protect both their physical and digital treasures.



[4] Verizon, "2022 Data Breach Investigations Report: Summary of Findings," 2022
[5] Sophos, "The State of Ransomware 2022," 2022

What Exactly is Cybersecurity for Museums?

Cybersecurity for museums and cultural institutions can be defined as the practice of protecting systems, networks, and data from digital attacks. [6]

But, in general terms, this process, especially for cultural institutions, is much more nuanced. It involves safeguarding not only internal operations but also the digital content that makes museums accessible to the public. Whether it's visitor data, loan agreements, or membership records, securing these digital assets is essential.

Cybersecurity for museums can be seen as both a defense and a strategy. It shields institutions from attacks like ransomware or phishing, but it also ensures smooth operations. Securing museum systems can not be seen as simply an issue about compliance, but more about trust within your members towards their favorite cultural institutions.

Visitors, donors and members need to know that their information is safe. A cyberattack that compromises this trust can do lasting damage to a museum's reputation.[7]

[6] Insurance Journal, "Cyberattacks on Public Entities Rising, Causing Higher Costs," 2024
[7] IMF, "Rising Cyber Threats Pose Serious Concerns for Financial Stability," 2024

Types of Cyber Attacks on Museums: Hypothetical Scenarios

Let's explore hypothetical scenarios illustrating the types of cyberattacks museums can experience. These examples offer insights into potential vulnerabilities and valuable lessons on how to protect against them.

Ransomware Attack on The Heritage Gallery

Scenario:

The Heritage Gallery, known for its historical artifacts and educational programs, is suddenly hit by a massive ransomware attack. Just picture this: one morning, staff members arrive to find their financial systems locked by malicious software, with a hefty ransom demand in cryptocurrency. As ticket sales, membership renewals and donations freeze, online visitors attempting to purchase tickets are bombarded with error messages. Confusion reigns. The front desk staff, stunned by the situation, is also unable to process payments leading to chaos.

Impact:

- **Financial Disruption**: The inability to process transactions leads to significant revenue loss during a peak exhibition season.
- **Operational Paralysis**: Critical internal databases, including exhibition management systems were inaccessible, disrupting day to day operations in multiple ways.
- **Reputation Damage**: Visitors were frustrated by canceled bookings and began to question the institution's technological capability and security.

Lessons Learned:

This type of scenario underscores the importance of maintaining offline backups and having a disaster recovery plan in place. Regularly updating and testing backup systems could have allowed the museum to recover without paying the ransom. Implementing multi-layered protection, such as firewalls, intrusion detection systems, and email filtering, can prevent such attacks from infiltrating the network.

Data Breach at The Contemporary Arts Institute

Scenario:

Picture this. A hacker exploits a vulnerability in The Contemporary Arts Institute's outdated CRM software, gaining access to the personal data of thousands of visitors, including email addresses and credit card details. The breach goes undetected for weeks and by the time it's discovered, the devious attacker has sold the data on the dark web, leading to fraudulent activity for many patrons.

Impact:

- **Erosion of Patron Trust**: Donors and members who trusted the museum with their personal data feel violated, leading to reputational damage.
- **Legal and Financial Repercussions**: The museum is exposed to possible lawsuits and regulatory penalties for failing to protect sensitive data, and must now provide credit monitoring services for affected individuals.
- **Long-Term Damage**: The museum struggles to regain the trust of high-profile donors, who are hesitant to support an institution that compromised their personal information.

Lessons Learned:

Encrypting sensitive data both at rest and in transit is crucial to prevent attackers from reading stolen information. Regular security patches and updates to the CRM system would have closed the vulnerability. Additionally, penetration testing can help identify and fix weaknesses before they can be exploited by hackers.

Phishing Attack on The Global Cultural Center

Scenario:

One day, staff at The Global Cultural Center receive an email appearing to be from a trusted partner, containing a link to a shared document related to an upcoming exhibit. Unknown to them, the link leads to a phishing site where employees, naively, enter their login credentials. The attackers then use these credentials to access donor databases and financial records, wreaking havoc on the museum's finances and operations.

Impact:

- **Data Exposure**: Donor and financial records are exposed, leading to significant data breaches.
- **Financial Losses**: Attackers initiate unauthorized fund transfers, resulting in substantial financial damage.
- **Operational Downtime**: The museum is forced to take its systems offline, delaying ongoing exhibitions and projects.

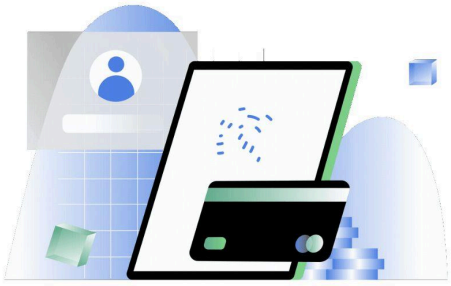
Lessons Learned:

This hypothetical case highlights the importance of conducting ongoing cybersecurity training for staff to be able to recognize phishing attempts. Multi factor authentication (MFA) on critical accounts would have definitely prevented attackers from using stolen credentials. Email filtering systems are also essential in blocking phishing emails before they reach employees.

Distributed Denial of Service (DDoS) Attack on The World Zoological Park Museum

Scenario:

During the launch of a high-profile online exhibition, the World Zoological Park's website is abruptly hit by a DDoS attack. Malicious actors flood the site with traffic, overwhelming the servers and causing them to crash. Visitors attempting to access the online exhibition are met with error pages, leading to widespread frustration.



Impact:

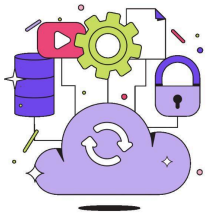
- **Public Frustration**: With the website down, the zoo loses potential ticket sales, donations, and goodwill.
- **Revenue Loss**: The crash resulted in significant financial losses during what should have been a high-traffic period.
- **Reputation at Stake**: The zoo's image as a technologically forward institution takes a hit.

Lessons Learned:

Robust traffic filtering and load balancing systems could have handled the surge in traffic. Partnering with cloud-based security services can help distribute traffic across multiple servers and identify suspicious activity before it causes disruptions. Having a public communication strategy to manage expectations during downtime is also crucial.

Supply Chain Attack on The Fine Arts Museum

Scenario:



A third-party vendor responsible for developing the museum's mobile app is hacked, and attackers inject malicious code into the app's latest update. Visitors who download or update the app unknowingly install malware that collects their personal information, including GPS data and login credentials.

Impact:

- **Patron Security Compromised**: Visitors' personal information is exposed, leading to privacy concerns and potential identity theft.
- **Reputational Damage**: Although the attack originated with a third-party vendor, the museum bears the brunt of the negative publicity.
- **Financial Costs**: The museum must refund app purchases, withdraw the app from stores, and work with cybersecurity experts to patch the vulnerabilities.

Lessons Learned:

Thoroughly vetting third party vendors and ensuring they meet strict cybersecurity standards is essential. Contracts should include cybersecurity requirements and periodic security audits. End to end encryption within the app would have protected their user data in the event of a continued breach.

How to Protect Your Museum's Digital Data

As we can see, cyber threats come in an incredibly diverse array of shapes and forms. Given the rising threat of cyberattacks, museums must take a proactive approach to protect their digital assets.

In order to help with that process, here are some key cybersecurity tools and practices that can help museums strengthen their defenses:

1. Regular Security Audits and Risk Assessments

Museums and cultural organizations should regularly audit their digital infrastructure to identify vulnerabilities. Third-party vendors should also be audited to ensure they meet cybersecurity standards. A 2019 Accenture study found that only 40% of companies conduct comprehensive risk assessments,[8] despite 68% acknowledging rising cybersecurity risks. Proactive risk management is essential for preventing attacks.

2. Data Encryption and Secure Backups

Encrypting sensitive data, whether in transit or at rest ensures that even if it is intercepted it cannot be read by unauthorized users. The IBM Cost of a Data Breach Report 2023 found that data encryption can save an organization $1.25 million in breach costs. Additionally, having secure backups is essential. A Sophos report found that 57% of organizations hit by ransomware were able to recover their data using offline backups, avoiding ransom payments.

3. Multi-Factor Authentication (MFA)

Implementing MFA on all critical systems adds a vital layer of security. According to a Microsoft study[9], MFA can prevent 99.9% of account hacks. Since 81% of breaches are caused by weak or stolen passwords, MFA is a critical step in reducing this risk.

[8] Accenture, "Future Systems Research Reveals Companies That Excel at Scaling Technology Innovation Generate Double the Revenue Growth," 2019
[9] DriveStrike, "Multi-Factor Authentication Prevents 99.9% of Cyber Attacks," 2024

4. Staff Training and Awareness

Human error accounts for 82% of data breaches, according to Verizon.[10] Regular cybersecurity training can reduce the risk of phishing and social engineering attacks. Organizations with strong security awareness programs experience up to 50% fewer phishing attacks, highlighting the importance of staff education.

5. Incident Response Plan

A well-defined incident response plan can significantly reduce the impact of a cyberattack. The IBM Cost of a Data Breach Report 2023[11] found that organizations with tested incident response plans resolved breaches more than two months faster and saved an average of $2.66 million per breach.

By implementing these practices, museums can protect their digital assets, maintain visitor trust, and ensure that their mission of connecting people with culture is not compromised by cyber threats.

[10] DriveStrike, "Multi-Factor Authentication Prevents 99.9% of Cyber Attacks," 2024
[11] IBM, "Cost of a Data Breach Report," 2024

Cuseum - Leading the Charge in Cybersecurity

Cuseum understands the critical importance of cybersecurity for museums and cultural institutions. Our platform, hosted on Amazon Web Services (AWS), uses advanced security measures like data encryption, end-to-end security protocols, and constant monitoring.

We are committed to protecting your institution's digital assets, so you can focus on what you do best: connecting people with art and culture.

To learn more about how we safeguard your digital infrastructure, read about Cuseum's comprehensive security features.

About Cuseum

Cuseum helps organizations drive visitor, member, and patron engagement using digital tools. Cuseum's software platform makes it easy for museums, attractions, and nonprofits to publish mobile apps, generate digital membership cards, and leverage data insights. Headquartered in Boston, the company is backed by leading investors including Techstars. For more information visit **http://www.cuseum.com** or you can request a demo **here**