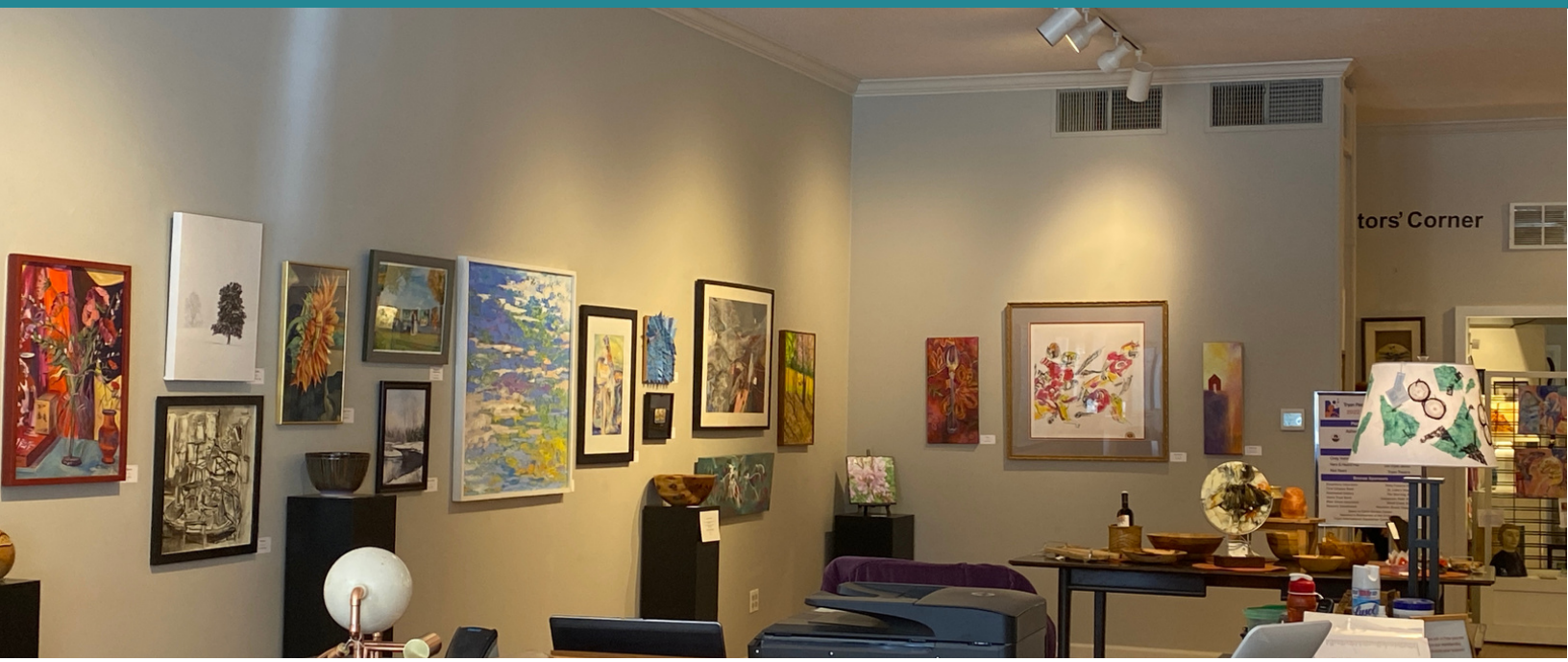
Cyber Preparedness

CHECKLIST

Between 2021 and 2022, there was almost a 200% increase in incidents targeting organizations with fewer than 1,000 employees.

ACCORDING TO VERIZON. DATA BREACH INVESTIGATIONS REPORT. 2022.



Businesses must deal with the risk of cyber-attacks. It's an unfortunate reality. What's additionally worrisome is attacks on small businesses have increased because they tend to be easier targets. Let's make sure your gallery is not a victim. It's super important to stay alert and take action ahead of time to keep your art gallery's info safe. That way, you can be ready for a potential attack and protect your clients, artists, and employees' data.

One smart move is to review your online security every year. This means having policies in place for your employees and asking vendors about their security measures.

It is important to consider how you will communicate with clients, artists, and partners in the event of an attack on your gallery. This can help mitigate any potential damage to your reputation and relationships. Have a plan in place for communicating, including clear messaging about the incident and any steps being taken to address it.

One approach is to be transparent and honest about what happened while also emphasizing your commitment to resolving the issue and ensuring the safety of everyone involved. You may also want to provide regular updates as the situation develops, so that people feel informed and reassured.

In addition to verbal communication, take advantage of other channels, such as email, social media, or a dedicated page on your gallery's website. These can be useful for sharing information quickly and efficiently, as well as providing a platform for people to ask questions or express concerns.

Ultimately, the key is to be proactive and responsive in your communication efforts, demonstrating that you take the situation seriously and are doing everything possible to minimize the impact. This will go a long way towards maintaining trust and confidence among your gallery supporters, even in the face of adversity.

Ok – This may seem obvious, but to help ensure the utmost protection of your gallery, it is imperative to implement robust security measures such as firewalls, antivirus software, and encryption protocols. These measures will help safeguard your gallery against potential cyber threats and unauthorized access.

Regularly updating your software is also crucial in maintaining a secure environment for your gallery. Outdated software can leave vulnerabilities that hackers can exploit to gain access to your system. You can patch any security holes and prevent malicious attacks by keeping your software up-to-date. This also goes for mobile devices too.

Another effective way to enhance your gallery's security is by using multi-factor authentication. This method requires users to provide two or more forms of identification before accessing your gallery's systems or accounts. This extra layer of security can significantly reduce the risk of unauthorized access and protect your valuable data assets.

But it's not just about tech stuff - you also need to teach your employees about cybersecurity best practices. They should know how to spot phishing emails and other tricks that cybercriminals use. Encouraging good password habits and limiting access to sensitive info can also lower the risk of an attack.

By taking these steps, you can protect your gallery from cyber threats and keep everyone's data safe and sound. Just remember that cybersecurity is always changing, so you need to stay alert and adapt to new risks.

Use this checklist annually to help you audit your gallery business's security situation.

"Cyber resilience is much more than a matter of technology. Agility, balance and high level view are indispensable..."

- STEPHANE NAPPO

CHECKLIST

1. Inventory all areas of vulnerability:
    - Create a comprehensive list of all devices (computers, laptops, tablets, cell phones) and the security software employed on each device, including when it was last updated.
    - Note what information is on each device to prioritize risks.
    - Include all passwords and systems, such as gallery inventory and payment software, that can be accessed on each device.

2. Understand risks and response procedures with third parties:
    - Regularly chat with your third-party vendors about their policies and procedures for keeping the data you share with them secure.
    - Vendors would include email marketing providers, payment processors, shipping vendors, and hosted contact management systems.

3. Protection against viruses, spyware, and other malicious code:
    - Ensure all gallery computers and devices are protected with updated software.
    - Configure your security software to update automatically and schedule regular scans.
    - Review the antivirus software vendor you are using and make sure it is still the best option.

Gallery Fuel

"Hardware and software should be treated together, integrated with cybersecurity early and frequently."

— LINDA RAWSON

CHECKLIST

4. Install an SSL certificate on your gallery website:
    - Secure your website with an SSL certificate to improve encryption, data integrity, and prevent cyber criminals from replicating your website and funneling personal information from site visitors.

5. Secure your internet Wi-Fi connections:
    - Safeguard your Internet connection by using a firewall and encrypting information.
    - Password-protect and hide your Wi-Fi network.

6. Regularly backup the data on all computers:
    - Back up sales and inventory histories, employee records, vendor contacts, accounting documents, and customer and artist files.
    - Establish a process for regularly removing sensitive information you no longer need.

7. Limit physical access to computers:
    - Ensure computers and mobile devices are not left unattended or left out overnight in the gallery.
    - Assign separate user logins for each employee who needs to access a gallery computer or database.

Gallery Fuel

"60% of data breaches are caused by a failure to patch. If you correct that, you've eliminated 60% of breaches. And I didn't even have to say AI or Blockchain! See how that works?"

-RICARDO LAFOSSE

CHECKLIST

8. Secure mobile devices:
    - Require staff to password-protect their devices and install security apps.
    - Keep software updated to include important security patches and upgrades.

9. Establish company security practices and policies to protect sensitive information:
    - Develop procedures on how gallery employees and vendors should handle and protect personal information and other sensitive data.
    - Include policies on password strength and regular password changes.
    - Clearly define the consequences of violating your gallery's cybersecurity policies.

10. Stay informed about cyber threats:
    - Stay knowledgeable about online threats and how to protect your data.
    - Sign up for alerts from US-CERT.gov.

11. Employ best practices on payment cards:
    - Review the current processing system and confirm it is the best and most secure option.
    - Ensure the system is PCI-compliant to secure credit card transactions.

Gallery Fuel

This checklist is not exhaustive, and your gallery's cyber security needs will be unique to your systems, user requirements, and data. Staying vigilant by performing an annual review of all your security vulnerabilities is critical.

You likely rely on partners and suppliers. Don't forget to ask them smart questions about their security measures if any information overlaps. Shippers and agencies are good examples of this. It is also essential to consider how you will communicate with clients, artists, and business partners if your gallery becomes a victim of an attack.

By following these guidelines, you can help ensure the security of your personal information online. Remember to adapt the checklist to fit the specific needs of your art gallery and regularly review and update your cybersecurity measures as new threats emerge.

Russia's invasion of Ukraine has had a massive impact on the cyber threat landscape. Since the start of the war, Russian-based phishing attacks against email addresses of European and US-based businesses have increased 8-fold.

In today's fast-paced world, we all have a lot on our plates. Between work, family, and other obligations, it can be easy to let cyber preparedness fall by the wayside. Unfortunately, neglecting this important aspect of gallery management can have serious consequences. Countless small businesses have learned this lesson the hard way.

That's why it's crucial to make cyber preparedness a priority. By taking steps to protect yourself, your business, and sensitive information, you can avoid becoming victims of cybercrime. Educating employees on cyber security, best practices can also help reduce the risk of a successful attack. Regularly auditing your gallery's online security using this checklist can help identify vulnerabilities and prioritize risks.

Whatever step you take, the key is to be proactive rather than reactive. It's far better to invest time and effort into cyber preparedness now than to pay the price later. So don't wait until it's too late - take action today to safeguard your art gallery's digital life.

Your future business will thank you.

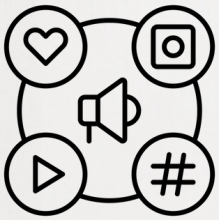
Thank you

NEED PERSONALIZED HELP?

I know you face new challenges every day that might be unique to your gallery business. If you feel working together one-on-one would benefit you in overcoming some of those challenges, I invite you to explore my Art Gallery Business Advisory Services.

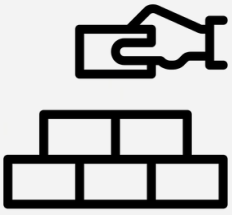
Programs

MARKETING PLAN AND INFRASTRUCTURE



SALES PROCESS DEVELOPMENT

GALLERY BUSINESS FOUNDATIONS



Sessions are tailored to your needs and goals.

Go to GalleryFuel.com to learn more about the advisory services programs and schedule a call to see if we are a good fit.

FUEL FOR RUNNING AN ART GALLERY BUSINESS

Gallery Fuel

www.galleryfuel.com

THANK YOU