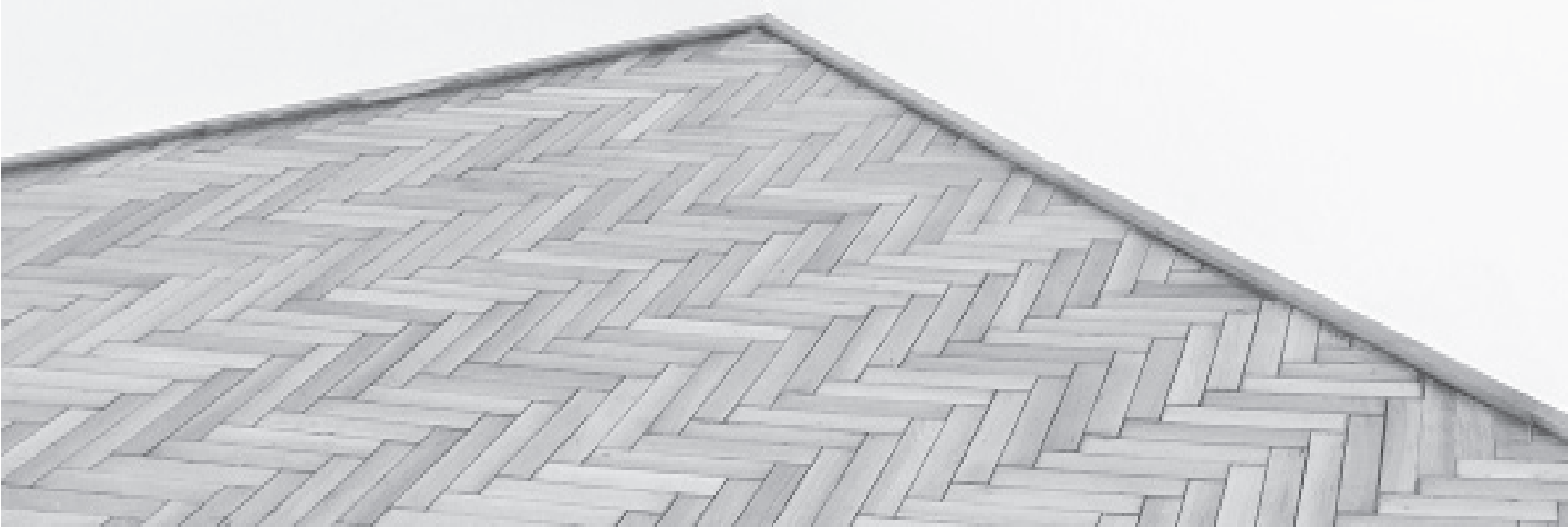
Gallery Fuel

Checklist

Cyber Preparedness



Cyber attacks will continue to occur. Keeping your gallery's information secure will require continued diligence. There are many things your business could do to get cyber battle-ready and keep sensitive information of your clients, artists, and employees safe.

Taking some time, even on just an annual basis, to check the health of your gallery's online security could *literally* save your business if you are attacked. Critical to the process is having employee policies in place and asking smart questions of your vendors regarding their security measures. Also consider in advance how you will communicate with clients, artists and business partners should your gallery become a victim of an attack.

Use this checklist to regularly audit the basic cyber security of your gallery.

©2018

✓ Inventory all areas of vulnerability

Create a comprehensive list of all devices (computers, laptops, tablets, cell phones) and what security software is employed on each device. Include when it was last updated. Note what information is on each device as well so you can prioritize risks. Include in your inventory all passwords and systems such as gallery inventory and payment software that can be accessed on each device. Should there be an attack or security breach, an inventory of this information will help you act more quickly.

✓ Understand risks and response procedure with third-parties with whom you share data

It is wise to have regular conversations with your third-party vendors regarding 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.

✓ 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 what anti-virus software vendor you are using and make sure it is still the best option. Once top rated, Symantec and Norton security software were recently found to have several critical vulnerabilities.

©2018

✓ Install an SSL certificate on your gallery website

Google and other major web browsers are requiring websites displayed in their search results to be secure with an SSL (Secure Socket Layer) certificate. You will be better protected with improved encryption, data integrity and prevention of cyber criminals replicating your website and funneling personal information from site visitors

✓ Secure your internet Wi-Fi connections

Safeguard your Internet connection by using a firewall and encrypting information. Your Wi-Fi network should be password protected and hidden.

✓ Regularly backup the data on all computers

Data would include sales and inventory histories, employee records, vendor contacts, accounting documents and customer and artist files. Ransomware attacks have become too familiar. Being able to retrieve essential files from backup will save you both time and money. It is also a good idea to put a process in place for regularly deleting sensitive information you no longer need.

©2018

✓ Limit physical access to computers

Computers and mobile devices are easy targets for theft. Make sure they are not left unattended in the gallery or left out overnight. Assign separate user logins for each employee who needs to access a gallery computer.

✓ Secure mobile devices

Mobile devices can cause significant security challenges depending on how your gallery uses them. The biggest threats are if lost or stolen, malware and viruses. Because these devices connect to WiFi and Bluetooth, hackers can easily connect and steal information. Require staff to password protect their devices and install security apps to prevent criminals from taking information while the phone is on public networks. Always keep software updated. They often include important security patches and upgrades.

✓ Establish company security practices and policies to protect sensitive information

Develop procedures on how gallery employees and possibly vendors should handle and protect personal information and other sensitive data. Include policies on the strength of password creation and how often they are changed. Clearly define the consequences of violating your gallery's cyber security policies.

Document your policies and ensure all employees understand what is expected.

©2018

✓ Stay informed about cyber threats

Be knowledgeable about online threats and how to protect your data on your computers, network clouds and even social media usage. You can sign up for alerts from US-CERT.gov.

✓ Employ best practices on payment cards

Review what you use to process credit cards currently and ensure it is still the best and most secure option available. Make sure you are Payment Card Industry (PCI)-compliant. PCI certification provides you with assurance that the processor your gallery uses follows and has passed a strict set of best practices for securing credit card payments.

This is checklist is not exhaustive and your gallery's cyber security needs will be unique to your business's systems, user requirements and data.

It is critical to stay vigilant by preforming an annual review of all your security vulnerabilities. Use this checklist to help guide your review to ensure it is comprehensive.

With all your many responsibilities, your days get busy and you have many time-sensitive priorities. Cyber preparedness can to often be put on the back burner, but many have paid the price for doing that. Don't be one of them.

©2018