MURPHY & McGONIGLE
A Professional Corporation

10 Practical Steps to Protect Your Firm from Cyber Threats

1. **Know Your Data and Systems.** Know what data you possess, where it's stored, whether it's encrypted, and who has access to it. Know how your computer network is configured and what devices are connected to it, including your employees' personal devices. This information will help you make informed decisions on how to protect your data and systems.
2. **Know Your Vulnerabilities.** Understanding your vulnerabilities allows you to effectively manage your cyber risk. Conduct risk assessments at least annually or prior to making significant changes to your business model, software, or equipment. Monitor your network for threats and intrusions and engage outside consultants to conduct periodic penetration testing.
3. **Cybersecurity Policies and Procedures Should Be Tailored to Your Business.** Your cybersecurity policies should be drafted to address the specific risks and circumstances of your business and should be updated as the cyber landscape changes. And once your policies are drafted, they must be enforced and validated – a policy that looks great on paper won't protect your business if it's not put into practice or isn't effective in the real world.
4. **Put the Right People in Charge of Cybersecurity.** Whoever is responsible for cybersecurity at your firm should have the right qualifications and sufficient seniority and resources to be effective in their role. Make sure that cybersecurity issues are on the agenda of senior management and the board. And assemble an interdisciplinary team to tackle cybersecurity issues that includes the perspectives of the business, IT, legal, security, compliance, audit, HR, public relations, and others, as appropriate.
5. **Watch Your Employees.** A single employee clicking on a malicious link might result in your entire system being compromised. Ensure all employees are trained at least annually on how to spot phishing emails and other cyber attacks likely to affect your business and how to escalate them to your cybersecurity team. Document the training for each employee. And create an insider threat program to identify suspicious behaviors by employees who may be planning to steal confidential data.
6. **Manage Your Third-Party Vendors.** Your cyber defenses are only as good as your weakest link, which is sometimes your third-party vendors. Conduct initial and periodic due diligence for each vendor regarding certifications, encryption practices, and incident response plans. Ensure that vendors are accountable by including cybersecurity requirements in your service agreements, including audit rights, indemnification clauses, and duties to notify you if the vendor experiences a breach.
7. **Control Access to Your Systems.** Control access to your systems and data so that only those employees, vendors, and customers who need access for a legitimate purpose will be granted access. Immediately terminate access rights for employees when they leave your firm and for vendors when their engagement ends. Use multi-factor authentication when appropriate.
8. **Prepare for Incidents Before They Happen.** It's not a question of *if* your firm will be attacked, but *when*. Be prepared by maintaining written incident response plans. Designate key persons to be part of an incident response team and have their contact information available so they may be reached if they are out of the office. Have external counsel and experts identified in advance. Have a plan in place to quickly inform law enforcement, your regulators, customers, and the public, if necessary. Maintain backups of your data and systems. And test your incident response plan by conducting "tabletop" exercises so all team members are clear on their roles and responsibilities.
9. **Stay on Top of the Latest Developments.** Ensure that your cybersecurity staff keeps current with the latest threats and technologies. Join industry cybersecurity threat sharing groups such as the Financial Services Information Sharing and Analysis Center (FS-ISAC).
10. **Implement Critical Software Patches Immediately.** When heretofore unknown software and hardware vulnerabilities are announced publicly, you should expect that hackers will seek to exploit them. Implement any available patches for those vulnerabilities immediately. Ensure that non-critical updates are made routinely and that all cybersecurity software and network monitoring systems are kept up-to-date.

Learn more about the Murphy & McGonigle
Cybersecurity, Cybercrime & Incident Response Practice