GALLOWAY

Galloway Johnson Tompkins Burr & Smith

Texas | Louisiana | Mississippi | Alabama | Florida | Georgia | Missouri

Cybersecurity matters to small and medium-sized businesses (SMBs)

"Fifty percent of small to medium-sized businesses have been the victims of cyber attacks and over 60% of those attacked go out of business."

Dr. Jane LeClair, Chief Operating Officer, National Cybersecurity Institute

******

******

50% of all SMBs were hacked within the last 12 months.

******

59% of SMBs fail to monitor employee network activity.

******

65% of SMBs fail to manage employee/vendor access credentials.

******

Cybersecurity planning for your small or medium-size business

No company is immune to a data breach. The dynamic rise in digitized information has allowed companies to gain unprecedented access to the global marketplace. This surge in access is accompanied by significant cyber risk due to malicious hacks or user error (the most prevalent form of breach in the U.S.). This escalating threat has received mixed responses from U.S. companies, many of which believe they are too small or globally insignificant to fall victim to a breach. In fact, the opposite is true; though much attention is given to incidents involving Fortune 500 companies, small and medium-sized businesses (SMBs) are the most vulnerable due to limited resources and lack of cyber preparedness.

Increasing your company's cybersecurity preparedness is a necessary cost of doing business in today's marketplace. Breaches can lead to considerable fallout for any company, including data loss, inability to conduct business, harm to your company's reputation, and costs associated with responding to applicable breach notification laws, law enforcement, regulatory inquiries, and defending tort claims. According to Dr. Jane LeClair Chief Operating Officer National Cybersecurity Institute, a cyber event could be the death knell for an SMB: "Fifty percent of small to medium-sized businesses have been the victims of cyber attacks and over 60% of those attacked go out of business." So the question is, *how prepared is your company if a breach occurs?*

"I have an IT professional. Isn't that enough?" No, cybersecurity now extends across multiple professional disciplines. Legal counsel is now essential for companies to mitigate the wide-ranging tapestry of industry standards and state, federal, and international laws governing data security. This typically involves preparing breach response plans, security-conscious corporate policies, vendor agreements, notification procedures, providing onsite counsel during a breach, and litigation defense services when a lawsuit is filed.

GALLOWAY
Galloway Johnson Tompkins Burr & Smith

Is your business prepared for a breach ?

- Does your company have cybersecurity-conscious employee policies?
- Does your company conduct routine employee training regarding cybersecurity?
- Does your office space display cybersecurity best practices?
- Does your company have cybersecurity-conscious vendor and client agreements? If so, do these agreements include defense and indemnity language?
- Does your company routinely update its network with the latest security updates and software patches?
- Does your company know what sensitive data it possesses, where it is located, and who has access to it?
    - Is your company hardware physically secure?
    - Is your data routinely backed up?
    - Is unneeded data routinely disposed of?
    - Does your company manage data access credentials and passwords?
- Does your company have a breach response plan in place? If so, does it designate a breach response team?
- Does your company have a legally informed cybersecurity strategy to guide future business decisions?
- Does your company regularly conduct penetration testing, evaluate/update its cybersecurity policies, and practice its breach response plan?
- Does your board discuss cybersecurity preparedness during each board meeting?
- Do your corporate officers and board members know whether the company's current insurance policies cover data breaches?

GALLOWAY
Galloway Johnson Tompkins Burr & Smith

Steven M. Bucher
Attorney
Lafayette Office

Steven's practice focuses on insurance defense litigation and assisting small and medium-size businesses with cybersecurity-related corporate planning matters.

About us. For over 30 years, Galloway, Johnson, Tompkins, Burr and Smith has aggressively represented its clients' interests in thousands of cases and dozens of industries worldwide. We are easily accessible with eleven convenient office locations: Houston, Texas; Dallas, Texas; Lafayette, Louisiana; New Orleans, Louisiana; Mandeville, Louisiana; Gulfport, Mississippi; Mobile, Alabama; Pensacola, Florida; Tampa, Florida; Atlanta, Georgia; and St. Louis, Missouri.