**Westlaw Today**
*powered by Reuters*

# Who is minding the store (online)? Considerations for owners, managers and c-suite executives

**By Adam Bialek, Esq., and Jana Farmer, Esq., Wilson Elser Moskowitz Edelman & Dicker LLP**

**MAY 1, 2023**

Investments, from purchasing a home to leasing a building to acquiring a business, require independent third parties contracted to provide reassurance on safety and compliance, and to identify issues that could be red flags. However, stepping out of the real world into the virtual, when it comes to digital compliance, most businesses either fail to have independent inspections or they choose to rely on service providers to self-certify their work. While digital interaction is now a significant part of business strategy, logistics and operations, there is a lack of standardized observance of the same governing principles.

*It is the owners' or C-suite executives' responsibility to ensure that a business is legally compliant.*

Corporate governance is a critical component of business management, and businesses need to recognize that it's time for a change in their governing principles to ensure that digital compliance becomes a regular part of business operations.

## Where to start — assigning accountability

Before assessing a business's compliance with digital risk mandates and guidelines, first identify who will monitor compliance and how. Without accountability, a business may not have the requisite ownership of the risk to ensure it is properly addressed. The responsibility for digital risk varies by organization and is often fractured, with certain aspects being watched by different managers. Some duties have fallen to the information technology (IT) department within a business, while others may fall to marketing, public relations (PR) and sales.

While IT may report to a chief information officer (CIO), a chief technology officer (CTO), a chief security or chief information security officer (CSO or CISO), a director of technology, an IT manager, a general manager or an operations officer, those individuals are rarely supervised by a "risk manager," a director of risk management or legal counsel. The marketing, PR and sales staff rarely have the understanding of what is legally permissible and their interaction with the IT staff may be limited to ensuring that their desired content is reaching the target audience. The marketing, PR and sales staff likely will report to a national sales manager, a marketing executive or an operations manager. On occasion, those individuals may consult with an in-house or outside attorney. However, the compliance obligations are typically viewed as an operational function, rather than a risk mitigation function.

Ultimately, however, it is the owners' or C-suite executives' responsibility to ensure that a business is legally compliant and is not exposed to unnecessary financial risk. Accordingly, a business needs to determine who will be charged with the responsibilities for ensuring that the online exposure is kept to a minimum, and the owners and C-suite executives need to determine who at the upper ranks of the business will monitor the performance of such individual(s) and hold accountable those in charge of the various points of risk.

## Identifying the risks

Once accountability for compliance is assigned, that individual or team must determine where the risks are and from what activities they emanate. Risks can be general, industry-specific, location-specific or company-specific. At the very least, a business should recognize the following among other concerns:

- Registration of Touch Points/Accounts — It is critical for an organization to have a clear understanding of the role of titleholder for an account. This may impact liability, reputational risk and legal control. For example, if a business owner or related entity registers a domain name in his/her/its own name, rather than the business's name, that individual or business entity may have risk for what appears at the website where the domain resolves.

  If the business has numerous corporate entities, and the domain or account is in the name of an entity that becomes embroiled in a public relations mess, such title holding could risk the reputation for both the business involved and the business holding title to the account.

  If the account is registered or owned by an in-house IT professional or an outside IT services company, and the relationship sours, the business may have a difficult and costly fight trying to regain control of the account (while typically the business will prevail, apart from the money spent on lawyers, there can be intermediate actions taken by the scorned

individual to damage the business — e.g., a disgruntled former IT employee could redirect a domain to a porn site or another highly toxic or divisive site).

- Content Management Risks — Websites and social media are primarily focused on content — the information or impression a business wants to convey and how. There are numerous risks associated with content including, but not limited to the following:
  - Copyright
  - Trademark
  - Trade Dress
  - Trade Secrets
  - Rights of Privacy and Publicity
  - Web Accessibility
  - Content Collection
  - Content Transfer
  - Language/Translation
  - Child Protection
  - Storage and Content Stability
  - Expandability and Technical Concerns
  - False Advertising, False Endorsement, False Affiliation
  - Defamation/Trade Libel
  - Brand Integrity
  - Government Concerns — Laws, Rules and Regulations.

  It is critically important for a business to understand where the risks are present and how best to avoid exposure and mitigate the risk. For example, businesses are sued regularly for infringement on uses of images and music, violations of rights of publicity, false advertising and the lack of web accessibility, among other claims. Apart from the costs associated with defending these claims, the distraction from core business operations when defending claims, as well as the reputational damage that may be caused, support the expenditure of resources to avoid such claims.
- Data Security and Privacy/Cyber Risks — It is critical for a business to ensure its systems are secure, and that internal actions (e.g., opening attachments to emails) or the introduction of third-party programs, code and functions do not adversely impact the control that a business has over its data. Exposures can include, but are not limited to:
  - Malware, including redistribution to clients, customers and others
  - Data Loss
  - Data Tampering
  - Ransomware
  - Phishing and Smishing
  - Credit Cards and Financial Data
  - C-Suite Fraud (e.g., targeting executives to authorize financial transfers)
  - Trade Secrets
  - Failure to Function
  - Denials of Service
  - Vandalism and Reputational Damage
  - Falsified User Identities
  - Right to Be Forgotten, Right to Correct Information, Limitation on Use of Data
  - Human Failures
  - Governmental Compliance — Laws, Rules and Regulations.

  Over the past several years, cyber claims have grown despite the awareness of such risks and the expenditure of resources to prepare for and prevent such exposures. While businesses may be spending more money to secure their systems and avoid exposure, they often lack oversight of the person accountable for such activities and their success. It is not sufficient that an internal IT professional self-certifies the actions they are taking to secure the business's systems.
- Functionality/Experience Failures, such as:
  - Accessibility (the ability for individuals with disabilities to be treated fairly)
  - Code Compliance
  - Privacy, Cookies, Tracking Technologies
  - System Controls
  - Broken Links
  - Outdated Email Addresses.

Every business will have unique risks and, depending on their geographic location and industry classification, there may be additional factors to consider (for example, privacy law compliance, minimum age for use and disclosure of specified health or financial information). Businesses also may view their social impact and the reputational issues that can arise (such as the carbon footprint to operate a website with duplicative or outdated content, political or sensitive societal preferences).

Each business owner, manager and C-suite executive who has supervisory and accountability responsibilities will need to determine the issues that are particular to their business, and the importance of compliance in each area. Vendors and lawyers offer audit services, but, ultimately, information provided by the business must be the determinative factor in compliance, and a business needs to have a resource that is educated on the risks and the requirements for compliance.

## Unknown or unrecognized risks — threats posed by third parties

While a business's responsible individual may identify the risks posed by its online operations, there are other risks that are not readily known or recognized by the business. Many of these risks occur due to operations delegated to a third party, often in the context of third-party software. Most businesses have websites that incorporate third-party software code to aid in the user experience.

Developers leverage third-party code to be efficient, to limit the costs of development and to speed the time it takes to develop a website or an application. Developers leverage external code for functionality such as font delivery, payment processing, customer login, ad service, employee acquisition, chatbots, analytics and more. According to the 2021 Web Almanac,[1] "a staggering 94.4% of mobile sites and 94.1% of desktop sites use at least one third-party resource." And, close to half of the requests made on such sites are third-party requests.

*A business needs to have a resource that is educated on the risks and the requirements for compliance.*

While there certainly are benefits from using such third-party resources, there also is risk. Third-party resources in this context are typically those included in the site's functionality, where the resources are hosted on a public or shared server, are widely used by different sites and are not influenced by the individual site owner. Rather, they are included by developers to ease their burden in including certain operations. The gratuitous use of an image or the use of a widget to provide a login to a secure area of a site can expose a business to impacts to performance, privacy and security that third-party developers and internal IT professionals often overlook.

These risks are real and should be considered by someone other than the individual who made the decision to include them. The use of cookies is one example of how a website can circumvent the business's stated position on data collection and usage. By the time a web page loads, and even when confronted by a "cookie banner" or permissive use tracker, there are numerous pieces of code that are part of the delivery of the webpage. These pieces of code and the functions embedded within them could pose a risk to a business if the business promises the user that it will not track or use its information, or if it does not disclose the use of such technology.

Highlighting the risk, lawsuits have been filed regarding the consequences of such third-party software, including but not limited to:

- Trespass
- Web accessibility violations under the Americans with Disabilities Act (ADA)
- The unauthorized disclosure of sensitive information through the use of technology embedded during the inclusion of these third-party resources.

For example, lawsuits have been filed claiming that the use of cookies without consent trespasses on the user's computer. When websites use plug-ins from third-party vendors, there often are consequences such as the inclusion of technology or content that does not comply with the web content accessibility guidelines (WCAG) that have been promulgated by the World Wide Web Consortium (WC3) and have been adopted by legislative acts (see, e.g., California) or courts presiding over such claims. Website operators can use best efforts to ensure that their web content is compliant with the WCAG standards, yet use third-party plug-ins that make their site noncompliant.

Recently, two of the largest hospital networks in Louisiana were subjected to class-action lawsuits alleging that their websites used a tracking code that shared sensitive patient information with Facebook and Instagram through the incorporation of the "Meta Pixel" website code, which allegedly gathered, analyzed and shared protected medical data in violation of privacy laws. In these cases, the common element causing noncompliance may be the inclusion of third-party software.

The use of third-party software is not likely to end. As such, it is imperative that businesses try to protect themselves against claims by ensuring that they obtain representations and assurances that the provision of third-party software will not cause the website or application to be noncompliant. Businesses may seek to include indemnity clauses in their agreements with vendors and developers to ensure that steps will be taken to make the site compliant.

*Businesses often adopt new technologies or follow trends without recognizing the potential risks.*

While such provisions may not always be available (such as when using a common plug-in issued by a major software developer, or a free or inexpensive plug-in), a business can attempt to gain such assurances from the developer. In addition, a business should discuss with its insurance broker whether such claims would be covered under its existing insurance policy, or whether there are specialized policies that might provide coverage for such claims.

## New technologies may lead to new risks

Businesses often adopt new technologies or follow trends without recognizing the potential risks. Embedding content from other sites could expose a business to claims of copyright infringement. While Instagram allows for a business to embed content on a third-party site, the original content creator may claim that such display of the content on a business's site is unauthorized. The ability to use content created by others has been made easier due to technological advances, but the traditional intellectual property laws, such as copyright and trademark law, as well as rights of privacy and publicity must be taken seriously.

Recently, the use of artificial intelligence (AI) plug-ins by businesses has been increasing. The legal ramifications of using AI for various

functions, however, are still being explored. Copyright infringement claims have already arisen out of the use of AI to create new images. More AI risks are likely to emerge, and new technologies may be adopted before the full risks are calculated. Businesses must be aware of the potential risks and take steps to mitigate them.

## The need for accountability

Over the past two decades, and accelerated by the impact of the COVID-19 pandemic, business has migrated from traditional brick and mortar, localized commerce to a borderless online experience. Forbes Advisor[2] recently reported that in 2023, approximately 71 percent of businesses have a website, 28 percent of all business activity is now conducted online, and the use of mobile devices for accessing the web is over 51 percent.

Yet, many businesses have not attained the same level of supervision and accountability for online operations as for their brick and mortar operations. With online operations posing as much, if not more, legal risk for businesses, it is imperative for a business owner, manager and C-suite executive to recognize the potential exposure for not taking such risks seriously. A business may wish to consider delegating a point person who has accountability for compliance.

When considering who to appoint and which third parties can assist in compliance oversight, leadership should recognize that independence from the process is critical. For example:

- Having the IT director in charge of reporting on compliance may be insufficient to get an impartial view of the real exposure.
- Self-certification may gloss over significant risks.
- Vendors should not be able to sign off on their own work without oversight and an impartial review of the work.
- Similarly, a business may not want the employee who oversees technology risks to be able to report compliance without independent verification.

Until business owners and C-suite executives insist on unbiased and independent clarity regarding the risks and accountability, digital compliance will be more difficult and businesses will have greater exposure.

### Notes

[1] https://bit.ly/40NumrK

[2] https://bit.ly/42121il

## About the authors

**Adam Bialek** (L), a partner at **Wilson Elser Moskowitz Edelman & Dicker LLP**, is co-chair of the firm's intellectual property and technology practice, a member of its information governance leadership committee and a founding member of its virtual privacy officer service. He is experienced with all facets of intellectual property law, internet law, art law, data security and privacy, and cyber/media risk matters, including insurance coverage pertaining to these areas. He can be reached at adam.bialek@wilsonelser.com. **Jana Farmer** (R), a partner at the firm, is one of the leaders of its consumer privacy practice and a member of its intellectual property and technology practice. She advises clients on emerging legal issues in the technology space, including those involving internet law, non-fungible tokens, artificial intelligence and blockchain technology. She can be reached at jana.farmer@wilsonelser.com. The authors are both based in New York.

**This article was first published on Westlaw Today on May 1, 2023.**