EPIC®
Insurance Brokers &
Consultants

Mitigating Risks and Ensuring Compliance: Biometric-Based Authentication and Your Business

Biometric-based authentication tools and software solutions are quickly gaining traction with businesses of all sizes, operating in multiple industry verticals. These tools will allow employees to use fingerprints, facial recognition, or iris recognition as an alternative method to unlocking a company device. Biometric devices are also widely used for building access and time clock systems. Biometric authentication tools and solutions are becoming a popular component of network, data, and physical security strategies because they combine a strong authentication method with a low-friction user experience.

While there are significant benefits to the use of biometrics, there is also great potential for exploitation. In addition, as the popularity of these biometric based authentication tools increases, there is also a rising wave of biometric information privacy regulations and associated litigation.

While there are significant benefits to the use of biometrics, there are also challenges and potential risks that come with incorporating biometric-based tools and solutions into your business operations. In addition, organizations should also consider the impact these tools may have on their risk transfer mechanisms – insurance and contractual.

Windows Hello for Business (Windows Hello) is an example of a biometric-based authentication system offered by newer versions of Microsoft Windows desktop and server. It provides facial recognition, fingerprint recognition, or PIN-based logins, eliminating the need for traditional passwords. *Windows Hello* has been growing in popularity in recent months. Below we consider some of the benefits and potential risks associated with *Windows Hello.*

Benefits of integrating *Windows Hello*:

- **Enhanced Security:** Most cybersecurity experts agree that biometric authentication offers a higher level of security compared to passwords, potentially helping to reduce the risk of data breaches and identity theft.
- **Convenience and User-Friendly:** *Windows Hello* provides a convenient and user-friendly authentication process, reducing the burden of password management.
- **Multi-Factor Authentication:** *Windows Hello* supports multi-factor authentication, adding an extra layer of security with options like facial recognition combined with a PIN.
- **Integration with Microsoft Services:** *Windows Hello* integrates well with other Microsoft services, simplifying user identity and access control management.
- **Scalability and Flexibility:** *Windows Hello* can be used on a wide range of devices, making it flexible and adaptable to different environments.

Potential risks associated with integrating *Windows Hello*:

- **Consent, Acceptance and Training:** Users may need time to adjust to the new authentication method, resulting in a learning curve and additional training costs. In addition, privacy laws in certain jurisdictions require organizations to obtain specific and detailed consent prior to collecting biometric information from employees, clients or customers. *Windows Hello* may trigger this obligation. Organizations should consult legal counsel to advise on specific legal obligations that may exist.
- **Multi-Factor Authentication:** As discussed above, *Windows Hello* supports multi-factor authentication, adding an extra layer of security, which is beneficial. However, this level of MFA may not satisfy some cyber insurance carrier requirements. Organizations should discuss this with their insurance broker or advisor.
- **Insurance Risk Transfer:** Commercial insurance products currently available may not adequately protect organizations against claims arising in connection with collection and use of biometric information. Organizations should not assume that any of the insurance policies they have in their portfolio will respond to a biometric privacy claim. Many insurance carriers have elected to proactively limit their exposure to the risk via exclusionary endorsements, enhanced underwriting, and/or sublimits of liability. It is important to consider the impact of implementing a biometric tool or solution on your insurance risk transfer mechanism. A discussion with your insurance broker or advisor would be in order.
- **Biometric Data Privacy Regulations:** Collecting, storing, using and handling biometric data presents a significant privacy risk. This risk has led three states to enact standalone, biometric information privacy laws – Illinois, Texas and Washington. In addition, most recently enacted comprehensive U.S. State Privacy Regulations – California, Virginia, Connecticut, Colorado, Utah, Iowa, Indiana and Tennessee – address biometric information specifically. During the 2022-23 legislative cycle, many additional states have introduced privacy bills that address a range of issues, including protecting biometric identifiers and health data. If your organization does collect biometrics, or is planning to, it will be imperative to constantly monitor the regulations in the relevant jurisdiction, and update any policies and procedures as required.

Although *Windows Hello for Business* may provide enhanced security, convenience, and scalability, it also presents significant challenges related to regulatory/legal liability, insurance coverage, data privacy, user consent/acceptance, single point of failure, as well as other more technical challenges surrounding hardware and third-party application compatibility. Organizations should carefully and thoughtfully evaluate the benefits and the challenges before implementing *Windows Hello for Business* as an authentication solution.

Let’s Talk!

Find out how EPIC Insurance Brokers & Consultants can help your business.

EPIC