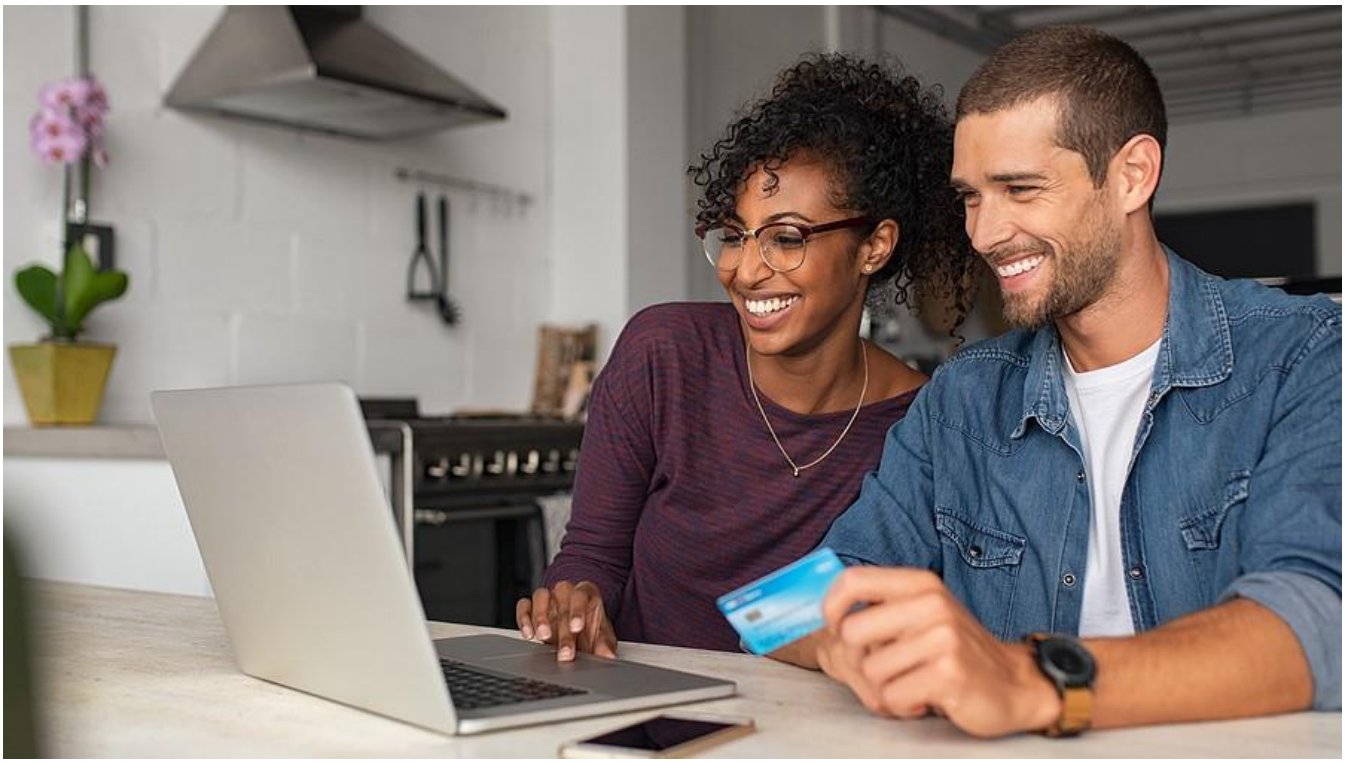
What is the Role of Cyber Security in Protecting Personal Data?



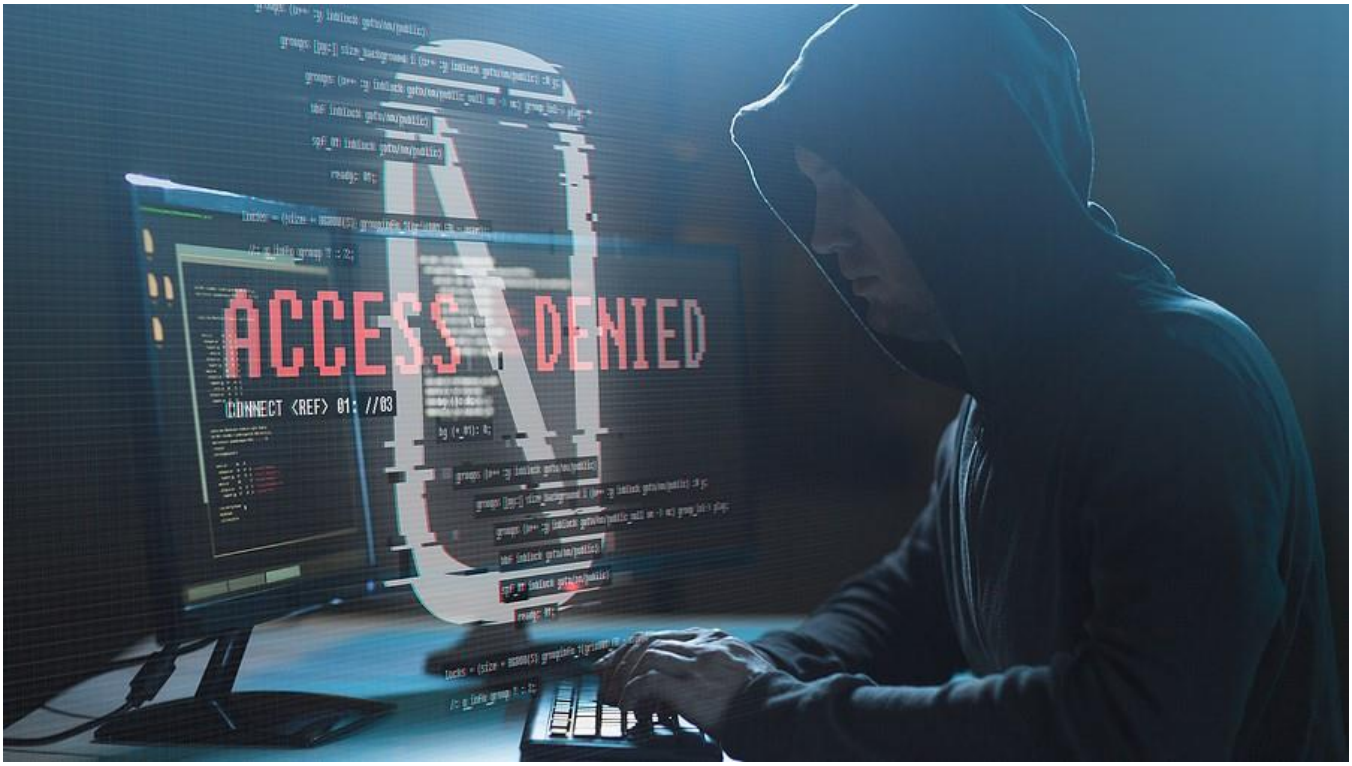
Businesses and public organizations depend on big data to provide personalized services, to innovate, and to guide business strategy. But they also have a legal and ethical responsibility to keep sensitive data safe. Business leaders cannot afford to underestimate or under-resource the role of cyber security in protecting personal data.

The average business or municipal organization manages an astonishing amount of personal data. This includes health, financial, and employment data, of course. It also includes names, biometrics, Social Security numbers, contact information, and other identifiers.

While individuals surrender personal information as a matter of course when transacting business, they expect organizations to keep that data secure from unauthorized access. Evolving cyber threats and an increasingly complex regulatory environment mean high stakes for business leaders. To stay ahead, companies must revolutionize their cyber security efforts.

Personal Data Under Threat

As the volume of personal data rises exponentially, it becomes more and more difficult to keep it safe. In the first place, the expansion of mobile devices, the IoT, and online services means that sensitive data comes from a wide variety of sources and in numerous formats. Security teams cannot protect data unless they know where it lives and where it travels.



Secondly, personal data represents a highly valuable commodity for cyber criminals, and cybercrime has grown into a lucrative business. Ransomware and phishing remain prime attack methods, but they use more sophisticated tools than ever before. Hackers continue to devise new ways around security measures, often aided by AI-powered tools such as deepfakes.

Privacy Laws Increase Pressure on Businesses

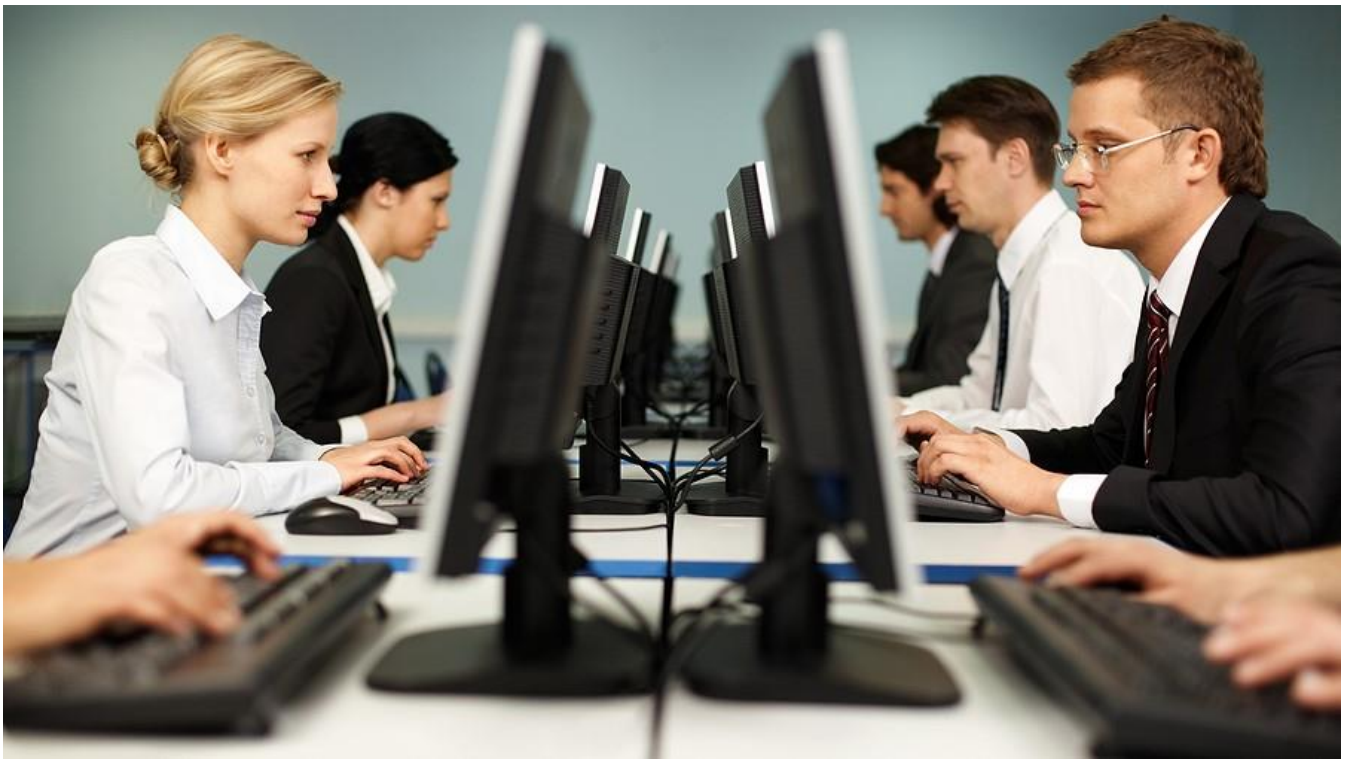
Meanwhile, complex privacy regulations enacted at the industry, state, and global level set stringent standards for data protection. Companies must be able to demonstrate that they have taken steps to prevent unauthorized access and data breaches.

For example, most privacy laws require companies to conduct regular risk assessments and implement "reasonable security procedures" to protect personal data. Additionally, they typically require companies to develop and maintain plans for responding to data breaches and cyber incidents.

Understanding the Role of Cyber Security in Protecting Personal Data

Implementing certain cyber security best practices will help ensure regulatory compliance while building consumer trust. Building a comprehensive compliance program takes time, and detangling the mass of requirements can be challenging. However, prioritizing some basic security measures will help. For example:

- Data encryption – Encryption serves as a critical barrier against data theft. You probably know that data should be encrypted both at rest and in transit. But not all encryption methods provide the same protection. Security teams may need to update encryption, particularly for the most sensitive data.
- Regular risk assessments – Security audits and risk assessments help organizations achieve regulatory compliance. More importantly, they highlight vulnerabilities, guiding security teams in creating a security strategy and identifying priorities.
- Patch management – Poor patch management leaves the door open for hackers to expose known vulnerabilities. Keep systems and software updated with the latest security patches, automating the process where possible.
- Review and update access controls – Strengthen password policies and implement multi-factor authentication (MFA) for an additional layer of protection. Ensure that employees and vendors have only the access they need to do their job.



- Invest in quality security awareness training – 95 percent of successful cyber attacks result from human error. Target training to employees' specific circumstances for maximum results.
- Develop an incident response plan – Have a well-defined response plan in place to ensure quick action and mitigation in the event of a data breach.

Implement Data Security Strategy with Expert Guidance

More than just an IT issue, cyber security plays a critical part in protecting sensitive personal data, and it involves commitment on all levels. Smaller organizations that find it difficult to hire the necessary security skills in-house will find it beneficial to partner with security experts.

Bringing a dedicated cyber security provider to the table gives businesses the benefit of enterprise-grade solutions to complex problems. Additionally, by accessing the expertise of leading information experts like Messaging Architects, businesses can gain control of wayward data and safeguard sensitive information.