Software Darwinism

Maintaining Software to Mitigate Security, Legal, and Compliance Risks

Chris Mermigas
Head of Legal, RSA

RSA

When Conditions Change, Software Must Evolve

In the rapidly evolving landscape of technology, staying up to date with software is not merely a matter of convenience or efficiency; it is increasingly becoming a legal imperative. Software permeates nearly every facet of modern life, powering critical infrastructure, facilitating communication, and driving business operations.

As in nature, software must continue to adapt to new conditions and evolve to survive new vulnerabilities. And as in nature, software represents only one component of a wider ecosystem. With the proliferation of software comes a myriad of legal considerations that must be addressed by both developers and users. One such consideration is the obligation to keep software up to date, which extends beyond mere convenience or performance optimization to encompass a host of legal benefits and multifaceted ramifications of failing to keep software up to date.

From compliance obligations to security concerns and intellectual property considerations, maintaining current software can mitigate legal risks and enhance overall legal posture.

Compliance with Laws and Regulations

One of the foremost legal benefits of staying up to date on software pertains to regulatory compliance. Numerous industries are subject to stringent regulatory frameworks governing data privacy, security, and consumer protection. Many of these regulations explicitly mandate the use of up-to-date software to safeguard sensitive information and mitigate cybersecurity risks.

For instance, the General Data Protection Regulation (GDPR) in the European Union and Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations requires organizations to implement appropriate technical and organizational measures to ensure the security of personal data. Failure to update software may result in vulnerabilities that expose personal data to unauthorized access, potentially leading to non-compliance penalties, fines, and reputational damage.

Similarly, industries such as healthcare (HIPAA), finance (SOX, PCI DSS), and telecommunications (CPNI) have specific regulatory requirements that necessitate the use of current software to protect confidential information and ensure operational integrity. By adhering to software update protocols, organizations can demonstrate compliance with regulatory mandates and mitigate legal risks.

Security Enhancement

Software updates play a pivotal role in bolstering cybersecurity defenses and mitigating security vulnerabilities. In an era marked by escalating cyber threats and sophisticated attacks, maintaining current software is imperative for safeguarding against data breaches, ransomware, and other malicious activities. Look no further than the Verizon 2024 Data Breach Investigations

Report, which “witnessed substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years. It almost tripled (180% increase) from last year.” Breaches beginning with this tactic “were primarily leveraged by Ransomware and other Extortion-related threat actors."

Failure to install security patches and updates leaves systems susceptible to exploitation by cybercriminals, potentially resulting in data breaches, financial losses, and legal liabilities. From a legal standpoint, negligence in securing software can expose organizations to lawsuits alleging inadequate security measures and breach of duty to protect sensitive information.

Moreover, in the event of a security incident, regulatory authorities and courts are likely to scrutinize an organization's adherence to best practices, including timely software updates, as a factor in determining liability and culpability. By proactively addressing security vulnerabilities through software updates, businesses can mitigate legal exposure and demonstrate a commitment to data protection and cybersecurity.

Intellectual Property Protection

Software updates also play a crucial role in preserving intellectual property rights and mitigating infringement risks. Intellectual property law grants exclusive rights to software developers and vendors, encompassing copyrights, patents, and trade secrets. However, outdated software may inadvertently incorporate third-party code or infringe upon existing patents, exposing users to legal challenges and litigation.

By staying current with software updates, organizations can avail themselves of the latest features, bug fixes, and legal safeguards provided by software vendors. This includes licensing updates, indemnification clauses, and patent infringement mitigation measures designed to protect users from legal disputes and intellectual property infringement claims.

Furthermore, timely updates can help organizations avoid inadvertently using pirated or unauthorized software versions, thereby mitigating copyright infringement risks and potential legal consequences. By ensuring compliance with software licensing agreements and terms of use, businesses can safeguard their intellectual property rights and mitigate legal exposure arising from unauthorized software usage.

Enhanced Contractual Protections

Many software agreements, including end-user license agreements (EULAs) and service level agreements (SLAs), contain provisions requiring users to maintain up-to-date software versions as a condition of continued support and services. Non-compliance with these contractual obligations may result in the termination of services, loss of warranty or indemnification protections, or other adverse consequences. By adhering to contractual requirements and keeping software updated, organizations can preserve their rights under software agreements and avoid disputes with vendors or service providers.

In conclusion, the legal benefits of staying up to date on software are manifold and far-reaching. From compliance obligations to security enhancement and intellectual property protection, maintaining current software is essential for mitigating legal risks, safeguarding sensitive information, and preserving business integrity.

By prioritizing software updates and upgrades, organizations can demonstrate regulatory compliance, strengthen cybersecurity defenses, and protect intellectual property rights. In an increasingly interconnected and digitized world, the legal imperative of staying current with software cannot be overstated. Software that doesn't adapt doesn't survive; likewise, businesses that don't reach a new evolutionary will be selected against. It is not merely a technological best practice but a fundamental legal requirement for the fittest businesses seeking to survive and thrive in an increasingly digitized world.

About RSA

The AI-powered RSA Unified Identity Platform protects the world's most secure organizations from today's and tomorrow's highest-risk cyberattacks. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For more information, go to RSA.com.