ADDRESSING REGULATORY NON-COMPLIANCE DUE TO LEGACY OPERATING SYSTEMS

A White Paper

AUGUST 20, 2021

CHIZZY MEKA
[Company Name]

Table of Contents

Abstract

An operating system becomes a legacy operating system when it starts becoming resistant to change and evolution. At which point, these systems usually lose their vendor's support, who often move on to work on newer versions of the operating system. This abandonment leaves these older operating systems without (security) updates. Moreover, legacy operating systems still genuinely constitute a corporate advantage that continually positions them as almost indispensable assets, encouraging many companies to hold onto them. However, with modern data protection legislation, legacy operating systems can be a corporate pandora's box. This white paper considers the regulatory and commercial risks that the use of legacy operating systems inadvertently poses to modern businesses.

1. Introduction to Legacy Operating Systems and Data Protection

A Legacy Operating System refers to an operating system engineered with outdated technology and no longer supported by its vendor. However, it is often the case that due to their extended use, these systems become business-critical. And for that reason, a particular organization may choose to continue running the system to avoid disrupting organizational processes. It is also possible that companies may continue to run legacy operating systems for other viable reasons. Another straightforward reason many organizations continue running legacy operating systems is that they lack the funding to modernize their systems. And many times, even when they can, some other practical obstacle may stop them from doing so, be it logistical, economical, or otherwise (Neumann 1996).

On the other hand, data protection refers to the statutory protection intended to protect the privacy rights of individuals, companies, and governments. Several data protection legislations impose various obligations on organizational entities that handle personal data to encourage these organizations to protect the information entrusted to them by these individuals (Kelleher, D. and Murray 2018).

From a software security perspective, it is fundamental to information security to ensure that the software applications running on our systems comprise the latest updates. However, by definition, legacy operating systems fail on that front from the beginning. We base this inference on the fact that since their vendors no longer support them, it would be improbable that these systems feature the latest patches and updates (Hayhurst 2020). This circumstance leads to an unfavorable position that some companies find themselves in. And even more, many organizations get to that position without even realizing it.

2. Data Protection Regulations and Their Requirements

Social and economic events around the globe have been significant forces in helping to emphasize the importance of data protection and have consequently inspired several data protection regulations on a global scale (UNCTAD 2021). These regulations take various forms, may address different issues, and are predominantly country or region-specific. We briefly introduce and discuss a few of these regulations, highlighting the incongruence between their requirements and the use of legacy systems.

1.1 Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA regulation is a United States regulation developed in 1996. Its fundamental purpose is to modernize the information flow of individuals' health data (Solove 2013).

The HIPAA Security Rules Policies and Procedures address protection from malicious software. In particular, 45 CRF 164.308(a)(5)(ii)(B) stipulates the need to ensure protection from malicious software. It also encourages establishing strict procedures regarding guarding, detecting, and reporting malicious software (United States Department of Health and Human Services 2005).

1.2 General Data Protection Regulation (GDPR)

Over in Europe, the GDPR is a data protection legislation entered into force in 2016 and transposed by EU countries in 2018. The legislation aims to empower individuals' rights to privacy in the modern digital age. The regulation facilitates processes that handle individuals' data by explicitly stating rules that protect people's privacy rights and assigning them to companies that operate these data throughout the European Union (EU) (European Commission 2021).

GDPR features the concepts of the data subject, the data controller, and the data processor. The subject is the individual who owns the data, and the controller is the company, organization, or entity that establishes how to process the subject's data. The processor is the entity that processes the data on behalf of the controller (European Commission 2021). GDPR stipulates that both the controller and the processor must implement adequate technical and organizational controls to safeguard information belonging to their data subjects. The regulation under 'Security of Processing' specifically, Article 32(1), under Section 2, specifically deals with personal data security (European Commission 2021).

1.3 Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Security Standards Council (PCI SSC) came into existence in 2006. They manage PCI DSS, a data security standard that seeks to regulate all organizations worldwide that handle individuals' credit cards. Their main aim is to ensure that these organizations do so in a secure environment (Payment Card Industry Security Standards Council 2021).

3. The Hidden Costs of Using Legacy Operating Systems

Reflecting on the introduction section and reassessing the requirements stipulated by the reviewed data protection regulations yields an invaluable insight. And this insight is the glaring incompatibility between the continual use of legacy operating systems and regulatory compliance. As a result, we further investigate the antagonistic relationship that information security and data protection regulations share with legacy operating systems. The aim is to uncover some of the most significant vulnerabilities and risks businesses expose themselves to in their everyday reliance on these systems.

As addressed in the introduction section, legacy operating systems do not usually receive updates and patches, including updates geared towards software security. This circumstance leaves the systems way more susceptible to cyberattacks (Infonote Datasystems 2020). And it also means that the potential that cybercriminals may steal an organization's customers' data is very high, which increases regulatory violations risks.

Beyond regulatory non-compliance risks, legacy operating systems also embroil operational issues in the problems they cause, as we see in the next paragraph.

Illustrating with GDPR specifically, the legislation requires companies to stay up to date and readily prove what data they have in their possession, their location, and who has access to them (Talend 2021). These requirements are very particular and require a very highly organized and efficient system to handle such obligations. Legacy operating systems are, by definition, inherently old and archaic, and many of them were not purpose-built with modern data protection laws in mind. So, these systems almost always underperform on this front. This susceptibility is two-pronged. In addition to exacerbating the regulatory violations risks, these systems also contribute to inefficiencies in the internal process of an organization as a result of their design which is incompatible with modern business requirements. And this era of big data, where companies are continually amassing more data than ever before, compounds the problems.

Another scenario where legacy operating systems are detrimental is their propensity to be incompatible with other IT systems. A data silo refers to a collection of information groups not easily accessible by another group (Sinani and Edora 2018). Legacy operating systems usually feature a data silo-like design because integrating them with their more modern counterparts is challenging (Talend 2021). The use of legacy operating systems can make it difficult to seamlessly share data and establish inter-departmental or inter-organizational processes with business partners and subcontractors. This position can force an organization to resort to 'clunky' methods, exposing the organization to information security risks. All of these are in addition to the non-compliance risks that legacy operating systems already pose.

4. The Consequences of Data Protection Non-Compliance

We have mentioned non-compliance severally in the preceding sections. However, without directly addressing the ramifications of violating data protection regulations, one may not fully appreciate the gravity and the potential costs of infringing these data protection regulations. So we briefly revisit the data protection laws reviewed in section 2 to highlight the actual consequences they can bring onto organizations that violate them.

Non-compliance with HIPAA regulations may cause the leakage of a patient's private data. In addition to the potential emotional damage to the patient, it can cause reputational damage for medical care service providers (Wu, Ahn, and Hu 2012). Given these potential harms, the punishments that come with such damages can bring an organization to its knees. These fiscal punishments come in four tiers ranging from $100 to $50,000, with a maximum penalty of $1.5 million per calendar year of non-compliance (Karne *et al.* 2021).

On the GDPR front, disclosing a person's private data can severely affect the individual, including anxiety, fear, embarrassment, and other undesirable feelings (Acquisti 2014). And depending on who obtains this leaked information, the harm could go beyond the psychological or emotional realm to something more dangerous like physical harm. For these reasons, legislators try to ensure that companies handling personal data are constantly in tune with their data protection policies by imposing hefty penalties on regulation violators. GDPR penalties include warnings, temporary or permanent organizational bans from handling data, and fines. The maximum fine is €20 million ($23 approx.) or 4% of a company's annual global turnover, whichever amount is higher.

Of all three, the PCI DSS undoubtedly features the most glaring consequence of what may happen to victims who have their data leaked due to an infringement on an organization's part. For clarity's sake, we explicitly state it; financial fraud. Credit card fraud can cause high emotional distress, vulnerability, mental health issues, anxiety, and possibly suicide in individuals. It can also bring on incredible financial difficulty and possibly bankruptcy at individual and organizational levels (International Public Sector Fraud Forum 2020). So the PCI SSC issues enormous penalties to organizations in response to instances of non-compliance. PCI Compliance fines range between $5,000 to $100,000 per month until the subject organization attains a compliant status (GoCardless 2021).

In addition to the steep monetary penalties common amongst data protection laws and standards, there are other potential financial losses that an offending organization could incur following a fine. These include lost business opportunities, damaged reputation, diminished customer relationships (Kalkan, Kwansa, and Cobanoglu 2010). Another subtle point to consider is that it is possible to violate more than one data protection regulation in one action. For example, a company in the EU that inadvertently leaks a customer's financial details could undergo an audit and fall foul of infringing both the PCI DSS standard and the GDPR (IT Governance 2021). This point means that such an organization may deal with penalties from more than one regulatory entity.

5. Eliminating Non-Compliance Risks with [Company Name]

So, what steps can you take to mitigate regulatory violations risks in your organization? The answer to this question is where [Company Name] comes in.

Our professionals at [Company Name] have multiple years of experience in migrating companies of varying sizes from legacy operating systems to modern Windows and Linux solutions. When it comes to modernizing IT infrastructure, our client count is in the hundreds. And when it comes to methodology, our migration approach is simply efficient. Our software automatically reinstalls (and, where applicable, updates) software applications on the new target operating system from your old machines. Our methods consistently yield around 80% efficiency and 70% cost-effectiveness compared to conventional migration methods.

Our migration and IT infrastructure modernization service naturally primes your infrastructure for compliance. Our experts at [Company Name] analyze your situation and implement the necessary controls according to your organization's needs.

We carry out a full assessment of your organization's data protection policies. This assessment includes your data breach reporting procedure to identify elements that could benefit from a review, a readdress, or an update.

We review and identify the changes to your entire IT infrastructure that move your company from the non-compliance and into the compliant zone. Our team also evaluates your data collection processes and their origin. We assess your information security to identify areas for improvement that would bolster your compliance position.

After migrating your IT infrastructure, our solutions ensure that:

- your client's data is intact;
- you have modern tools that help you react promptly in the event of a data breach;
- you can readily manage the infringement;
- and also recover from the breach.

6. Conclusion

We have described what constitutes a legacy operating system, briefly reviewed some modern and current data protection laws and what may constitute non-compliance. We have also considered how legacy operating systems may inadvertently expose companies to violation risks. And, finally, how [Company Name] can help organizations correct that position through our migration service. In the end, it boils down to one viable self-reflection question that IT directors and strategists must ask themselves. The question is, are the benefits involved in retaining our organization's legacy operating systems worth the penalties that come with regulatory non-compliance penalties? And to that end, we assert that the answer would be evident to any business-minded individual. It is not difficult to deduce that the penalties for non-compliance can mean the difference between positive business growth and bankruptcy for an organization.

References

Acquisti, A. (2014) 'The Economics and Behavioral Economics of Privacy', in Lane, J and Stodden, V and Bender, S and Nissenbaum, H (ed.) *PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT*, pp. 76–95.

European Commission (2021) *Data protection in the EU | European Commission*. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (Accessed: 20 August 2021).

European Commission (2021) 'I (Legislative acts) REGULATIONS REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)'. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Accessed: 20 August 2021).

European Commission (2021) *What is a data controller or a data processor? | European Commission*. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en (Accessed: 20 August 2021).

GoCardless (2021) *PCI Fines and Penalties | GoCardless*. Available at: https://gocardless.com/guides/posts/pci-fines-penalties/ (Accessed: 21 August 2021).

Hayhurst, C. (2020) 'ON GUARD: Staying Vigilant Against Medical Device Vulnerabilities', *Biomedical Instrumentation \& Technology*, 54(3), pp. 169–177.

Infonote Datasystems (2020) *GDPR, Legacy Systems and Databases - Infonote Datasystems Ltd*. Available at: https://www.infonote.com/legacy-systems-databases/ (Accessed: 20 August 2021).

International Public Sector Fraud Forum (2020) 'International Public Sector Fraud Forum Guide to Understanding the Total Impact of Fraud'.

IT Governance (2021) *The PCI DSS | IT Governance UK | IT Governance UK*. Available at: https://www.itgovernance.co.uk/pci_dss (Accessed: 21 August 2021).

Kalkan, K., Kwansa, F. and Cobanoglu, C. (2010) 'Payment Card Industry Data Security Standards (PCI DSS) Compliance in Restaurants', *Journal of Hospitality Financial Management*, 16(2), p. 3.

Karne, S. *et al.* (2021) 'Basics about HIPAA for Physicians', *This Inaugural Issue of JAAPI is Dedicated to the following Legendary Indian Physicians*, 1(1), pp. 51–55.

Kelleher, D. and Murray, K. (2018) *EU data protection law*. Bloomsbury Professional.

Neumann, D. M. (1996) 'Evolution process for legacy system transformation', in *IEEE Technical Applications Conference. Northcon/96. Conference Record*, pp. 57–62.

Payment Card Industry Security Standards Council (2021) *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. Available at: https://www.pcisecuritystandards.org/pci_security/ (Accessed: 20 August 2021).

Sinani, S. and Edora, F. (2018) 'Data Quality through Data Integration: How Integrating Your IDEA Data Will Help Improve Data Quality.', *Center for the Integration of IDEA Data*. ERIC.

Solove, D. J. (2013) 'HIPAA turns 10: analyzing the past, present, and future impact'.

Talend (2021) *What is a Legacy System? - Talend*. Available at: https://www.talend.com/resources/what-is-legacy-system/ (Accessed: 20 August 2021).

UNCTAD (2021) *Data Protection and Privacy Legislation Worldwide | UNCTAD*. Available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (Accessed: 20 August 2021).

United States Department of Health and Human Services (2005) 'HIPAA Security S E R I E S Compliance Deadlines What is the Security Series?' Available at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf (Accessed: 20 August 2021).

Wu, R., Ahn, G.-J. and Hu, H. (2012) 'Towards HIPAA-compliant healthcare systems', in *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*, pp. 593–602.