COMPUTER LAW & SECURITY REVIEW 000 (2018) 1–22

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Patching the patchwork: appraising the EU regulatory framework on cyber security breaches

*Maria Grazia Porcedda**

School of Law, University of Leeds, Leeds, UK

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Data breaches
Security breaches
Cyber security
Data protection
Network and information security
Cloud computing
Data security breaches

ABSTRACT

Breaches of security, a.k.a. security and data breaches, are on the rise, one of the reasons being the well-known lack of incentives to secure services and their underlying technologies, such as cloud computing. In this article, I question whether the patchwork of six EU instruments addressing breaches is helping to prevent or mitigate breaches as intended. At a lower level of abstraction, the question concerns appraising the success of each instrument separately. At a higher level of abstraction, since all laws converge on the objective of network and information security – one of the three pillars of the EU cyber security policy – the question is whether the legal 'patchwork' is helping to 'patch' the underlying insecurity of network and information systems thus contributing to cyber security. To answer the research question, I look at the regulatory framework as a whole, from the perspective of network and information security and consequently I use the expression cyber security breaches. I appraise the regulatory patchwork by using the three goals of notification identified by the European Commission as a benchmark, enriched by policy documents, legal analysis, and academic literature on breaches legislation, and I elaborate my analysis by reasoning on the case of cloud computing. The analysis, which is frustrated by the lack of adequate data, shows that the regulatory framework on cyber security breaches may be failing to provide the necessary level of mutual learning on the functioning of security measures, awareness of both regulatory authorities and the public on how entities fare in protecting data (and the related network and information systems), and enforcing self-improvement of entities dealing with information and services. I conclude with some recommendations addressing the causes, rather than the symptoms, of network and information systems insecurity.

© 2018 Maria Grazia Porcedda. Published by Elsevier Ltd. All rights reserved.

1. Introduction

News of public and private organizations being breached proliferate. While not all breaches of security are caused by cybercrime,[1] the term generally refers to the unauthorized access to network and information systems, which can lead to further cybercrimes, notably the 'exfiltration' of data, i.e. the creation of unauthorized copies for dissemination, sale, or for blackmailing through the information contained in such data. Breaches of security affecting personal data, usually referred to as 'data breaches', have on average increased in size in 2017,[2] and are almost a daily occurrence, so much so that it has become difficult to keep track of them. The security firm

* Corresponding author: The Liberty Building, School of Law, University of Leeds LS2 9JT, Leeds, UK.
E-mail address: m.g.porcedda@leeds.ac.uk

[1] Other causes include human error, system glitch and natural disasters: David Wall, 'Enemies within: Redefining the insider threat in organizational security policy' 26 Security Journal 107–124; Larry Ponemon, *2017 Cost of Data Breach Study. Global Overview* (2017).

[2] Ponemon (2017), 2017 Cost of Data Breach Study. Global Overview.

https://doi.org/10.1016/j.clsr.2018.04.009
0267-3649/© 2018 Maria Grazia Porcedda. Published by Elsevier Ltd. All rights reserved.

Please cite this article as: M.G. Porcedda, Patching the patchwork: appraising the EU regulatory framework on cyber security breaches, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.04.009

Gemalto[3] boldly suggests that the question is not whether one's network and information system will be breached or not, but rather when the breach will take place.

Such a bleak scenario may not fully reflect reality yet, but could provide an accurate description of the (near) future, if the root causes of breaches remain unaddressed. A well-known root cause of breaches is the underinvestment in network and information security, which is often seen as a burden, rather than an asset.[4] Hence, in addition to attaching criminal liability to perpetrating, or aiding and abetting, breaches, several jurisdictions,[5] including the EU, have opted for the imposition of legal obligations to protect one's systems and data. These have been coupled with the adoption of legal devices such as the notification of breaches to a supervisory authority and, possibly, to the (affected) public.

In its Impact Assessment accompanying the proposed General Data Protection Regulation (hereafter GDPR), the European Commission identified three advantages of notification. In detail, "breach notifications provide a systematic feedback about the actual risk and the actual weaknesses of existing security measures; they enable authorities and consumers to assess the relative capabilities of data controllers with respect to data security; they force data controllers to assess and understand their own situation regarding security measures".[6] I dub the three advantages of notification as 'mutual learning', 'public awareness' and 'self-improvement' respectively. However, notification is not without faults: Burdon and others submit that it is conceptually incoherent, because it tries to balance conflicting concepts, "namely the provision of effective consumer protection and the prioritisation of corporate compliance cost mitigation."[7] Instead of being included in one overarching instrument, provisions on the notification and mitigation of breaches have been inserted in separate instruments. Hence, I refer to the ensemble of EU laws on breaches, as a regulatory framework or 'patchwork'.

In this article, I question whether the EU regulatory framework is helping to prevent or mitigate breaches as intended. At a lower level of abstraction, the question concerns appraising the success of each instrument separately – to the extent feasible with respect to the availability of data and state of implementation of the rules. At a higher level of abstraction, since, as I will demonstrate, all laws converge on the objective of network and information security (one of the three pillars of the EU cyber security policy[8]), the question is whether the legal 'patchwork' is helping to 'patch' the underlying insecurity of network and information systems – thus contributing to cyber security. To answer the research question, I will look at the regulatory framework as a whole, from the perspective of network and information security, rather than focussing on the distinction between breaches concerning personal/non-personal data. To refer to all breaches, I use the expression 'cyber security breaches'.[9] This is in agreement with the suggestion advanced by Burdon et al.[10] I appraise the regulatory patchwork by using the three goals of notification identified by the European Commission as a benchmark; I further enhanced them with policy documents, legal analysis, and academic literature on data and security breaches legislation,[11] to which I endeavour to contribute.

I begin by illustrating the EU regulatory patchwork on cyber security breaches, which is composed of six instruments emerging through three regulatory waves. I subsequently illustrate the 'state of the framework', by focussing in particular on the definition of breaches, the rules on the notification and mitigation of breaches, and provisions on inventories, sanctions and liabilities. In the next section, I appraise the regulatory framework. The only instruments that can be appraised individually and hence lead to answering the research question at a lower level of abstraction, are those relating to the first regulatory wave. Based on the (unsatisfactory) evidence gathered, I propose a method to evaluate the regulatory framework as a whole at the higher level of abstraction. I then reason on the implications of my findings with reference to the case of cloud computing, which is addressed in both the second and third regulatory wave. There, I propose to reflect on the possible consequences of the state of the art with reference to the scenario of universities with teaching hospitals. I must warn the reader that the analysis is specu-

[3] See at: http://breachlevelindex.com/data-breach-risk-assessment-calculator (last accessed on 19th December 2017). Some commentators go in the same direction, suggesting that the focus should be on harm reduction rather than prevention. Ioannis Agrafiotis and others, *Cyber Harm: Concepts, Taxonomy and Measurement* (Saïd Business School WP 2016–2023, 2016).

[4] Ross Anderson and Tyler Moore, 'The Economics of Information Security' (2006) 314 Science 610–661; Mark Burdon, Bill Lane and Paul von Nessen, 'Data breach notification law in the EU and Australia - where to now?' 28 Computer Law & Security Review 296–307.

[5] The first law was passed by the State of California. Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - where to now?'. See also at: https://iapp.org/news/a/eu-data-breach-notification-rule-the-key-elements/.

[6] European Commission, Commission Staff Working Paper SEC(2012) 72 final. Impact Assessment Accompanying the General Data Protection Regulation (2012), p. 100.

[7] Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - where to now?', p. 302.

[8] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* ((Joint Communication)JOIN(2017) 450 final, 2017); European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Cyber Security Strategy: An Open, Safe and Secure Cyberspace* ((Joint Communication) JOIN (2013) 01 final, 2013).

[9] The term cyber security breaches does not have legal significance, but, as I hope to illustrate in section 3, nicely captures the gist of the problem. It is currently used in the UK yearly official statistics on breaches (see at: https://www.gov.uk/government/collections/cyber-security-breaches-survey).

[10] Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - where to now?'

[11] Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - where to now?'; Apostolos Malatras and others, 'Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities' 33 Computer Law and Security Review 458–469; Rachel M. Peters, 'So You've Been Notified, Now What? The Problem with Current Data Breach Notification Laws' (4) 56 Arizona Law Review 1171–1202; Rosa Barcelo, 'EU: Revision of the ePrivacy Directive.' (2009) 31 Computer Law Review International 31; Rebecca Wong, *Data Security Breaches and Privacy in Europe* (Springer 2015).

Please cite this article as: M.G. Porcedda, Patching the patchwork: appraising the EU regulatory framework on cyber security breaches, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.04.009

Download English Version:

https://daneshyari.com/en/article/10225860

Download Persian Version:

https://daneshyari.com/article/10225860

Daneshyari.com