Taylor & Francis
Taylor & Francis Group

Journal of Organizational Computing and Electronic Commerce

ISSN: 1091-9392 (Print) 1532-7744 (Online) Journal homepage: https://www.tandfonline.com/loi/hoce20

Should executives go to jail over cybersecurity breaches?

Dave Chatterjee

To cite this article: Dave Chatterjee (2019) Should executives go to jail over cybersecurity breaches?, Journal of Organizational Computing and Electronic Commerce, 29:1, 1-3, DOI: 10.1080/10919392.2019.1568713

To link to this article: https://doi.org/10.1080/10919392.2019.1568713

Published online: 17 Feb 2019.

JOURNAL OF ORGANIZATIONAL COMPUTING AND ELECTRONIC COMMERCE
2019, VOL. 29, NO. 1, 1–3
https://doi.org/10.1080/10919392.2019.1568713

Taylor & Francis
Taylor & Francis Group

Should executives go to jail over cybersecurity breaches?

Dave Chatterjee

Department of Management Information System, Terry College of Business, The University of Georgia, Athens, Georgia, USA

ABSTRACT

The Consumer Data Protection Act, a new bill introduced by Senator Ron Wyden, is proposing "jail time of up to 20 years for executives who knowingly sign off on incorrect or inaccurate annual certifications of their companies' data-security practices." The bill also recommends that companies be fined "up to 4 percent of their annual revenue." While the critics consider the penalties too harsh and severe, the proposed legislation reflects two key realities – a) active involvement and commitment of senior management is essential to achieving a high level of cybersecurity preparedness; and b) legislation and fear of severe penalties (such as Sarbanes-Oxley Act of 2002 and European Union's General Data Protection Regulation) is often necessary to motivate desired organizational behavior. In an increasingly digital ecosystem characterized by high levels of electronic connectivity, vulnerability to cyberattacks is growing. Organizations are in a perpetual state of breach with rapidly expanding attack surfaces and evolving threat vectors. Protecting confidential data and related digital assets is becoming critical to survival and success. Senior management must come to terms with this new business reality and give strategic priority to cybersecurity preparedness and investments. Research finds active involvement of top management in cyber risk mitigation initiatives to be a critical success factor and best practice. The onus is also on senior management to create a high-performance security culture founded on three key cornerstones – commitment, preparedness, and discipline. They also must lead the charge in establishing a cybersecurity governance structure characterized by joint ownership, responsibility, and accountability.

KEYWORDS

Cybersecurity; High-Performance Security Culture; Cyberattacks; Cybersecurity preparedness; Top Management Commitment

A discussion draft of a new bill introduced by Senator Ron Wyden, the Consumer Data Protection Act (CDPA), is proposing jail time of up to 20 years "for executives who knowingly sign off on incorrect or inaccurate annual certifications of their companies' data-security practices." The bill also recommends that companies be fined "up to 4 percent of their annual revenue" (Wolff 2018). The critics consider these proposed penalties to be too harsh and over-the-top reactions to data breaches. Though security is an important priority, they feel it cannot be a company's only priority.

While most organizations are not in the business of securing data and digital assets, protecting such assets is critical to survival and success in today's highly digitized and connected environment. With rapidly expanding attack surfaces and evolving attack vectors, organizations are in a perpetual state of breach and have to deal with this existential threat (Ray 2017). No industry or organization is being spared. Data breaches in the healthcare industry are being reported on an almost daily basis. Cyber attacks increased by more than 70% in the financial services industry in 2017. The Ponemon Institute global study finds a rising trend in all key cybersecurity measures –

CONTACT Dave Chatterjee dchatte@gmail.com Department of Management Information System Terry College of Business, The University of Georgia Athens, Georgia 30602, USA

between 2017 and 2018, the average total cost of a data breach increased by 6.4 percent from $3.62 to $3.86 million, the average size of data breaches increased by 2.2 percent, and the average cost of each lost record increased by 4.8 percent from $141 to $148 (2018 Global Cost of a Data Breach Report).

From a big picture standpoint, the possibilities of a bank failure, a national power outage, contamination of the water supply, and collapse of the financial market cannot be ignored. Cyber-attacks are becoming an epidemic. The hacker community is getting increasingly aggressive and innovative, and organizations are having difficulty playing catch-up and trying to fend off attacks (Fuhrmans, 2017).

Cybersecurity preparedness is a critical and distinctive competency, and senior management has to accept this business reality. Investing in cybersecurity defenses must be given strategic priority even though such investments cannot be associated with revenue generation activities. The traditional view of strategic endeavors has to be altered – investment in any activity focused on reducing cyber threats is as strategic and significant as any other traditional value creation and market development activity. After all, if a business ceased to exist, of what good would be any revenue generation investments?

Developing robust cybersecurity defense is no easy task and requires, among other things, a well-thought-out plan and a sustained commitment of resources. Senior management attention and active involvement are critical success factors. The proposed CDPA legislation with harsh executive-focused penalties is designed to get top management attention and commitment and increase accountability. Unfortunately, it takes legislation and the threat of severe penalties for organizations to seriously commit to issues of significant social consequence. Sarbanes-Oxley Act (SOX) of 2002 was enacted in response to accounting scandals in companies such as Enron and Worldcom. When these companies went under, not only did employees lose their jobs, but shareholders lost a significant portion of their investment value, and for many their entire retirement nest egg was gone. While the SOX legislation is not perfect, it does serve as a deterrent to financial and accounting frauds and thereby helps maintain investor confidence in the stock market. The recent introduction of the European Union's (EU) General Data Protection Regulation (GDPR) to protect personal data is also intended to deter misuse and abuse of customer data by companies. None of these legislations would be necessary if organizations acted responsibly and proactively on their own. Unfortunately, fear and threats continue to be the most effective motivators for desired corporate behavior.

The cybersecurity phenomenon presents an interesting dilemma and challenge in that compliance with legal requirements does not ensure the company is relatively immune to different forms of attacks (Benz and Chatterjee 2018). In fact, no amount of spending or investing guarantees a high level of immunity from impending attacks. Not surprisingly, senior leadership are willing to look the other way and focus on primary value-creating activities and take their chances with cyberattacks. The chief administrator of a major hospital advised the leadership team to focus on providing best possible care and not worry about cyber threats. Another senior leader of a large healthcare organization wished for an attack, as that would help identify security weaknesses (Abraham, Chatterjee, and Sims, 2019). The intent of the Consumer Data Protection Act and similar legislations is to discourage a reactive and low-priority cybersecurity mindset among executives.

Without active involvement and engagement of senior leadership, it is impossible to motivate all organizational members to do their part in protecting the organization. The cyber war cannot be fought effectively by just a team of security professionals. It requires an organization-wide initiative and effort to protect the numerous enterprise vulnerabilities and endpoints. Humans continue to be the strongest and weakest link in the cyber security chain and need to be adequately equipped with training and tools. Security training and awareness programs need to be customized and sustained over a prolonged period of time (Burns, Johnson, and Caputo 2019; Disparte and Furlow 2017; Khan and Alshare 2019).

Top management commitment and support is also key to creating a high-performance security culture that embodies three key traits: commitment, preparedness, and discipline (Chatterjee 2018). Whether it is to

mobilize organization-wide support or commit adequate resources, establish formal governance procedures, require security audits and drills, continuously monitor performance, or enforce security policies, the senior leadership plays a key role (Chatterjee 2018; Kabanda, Tanner, and Kent 2018). They must be hands-on in their commitment and effort to not only understand the organizational vulnerabilities but also what it takes to deal with the challenges. Outsourcing cybersecurity responsibility to a team of security professionals and then blaming them for failure is a cop out, a symbolic check-the-compliance-box approach that is unlikely to produce substantive results. Led by top executives, every organizational member must share joint ownership, responsibility, and accountability in the security preparedness initiative. The proposed CDPA legislation seems to encourage such a holistic approach to dealing with cyber threats.

Ideally, an organization should be proactively and sincerely committed to taking all possible steps and measures to secure sensitive data. Then, and only then, can the organizational representative satisfactorily respond to the question that stakeholders are likely to ask after a successful attack: "What did this institution do to prepare?" If every reasonable effort was made to prevent data breaches, then executives shouldn't have to go to jail over cyberattacks.

References

2018 Global Cost of a Data Breach Report, Ponemon Institute

Abraham, C., D. Chatterjee, and R. Sims. 2019. Muddling through cybersecurity: Insights from the U.S. healthcare industry, *Business horizons* Accepted for Publication, July 2019.

Benz, M., and D. Chatterjee (2018) Reducing Cybersecurity Risks in the Midmarket: A Unique Methodology for Pinpointing the Highest-Value Improvements, under review, submitted on December 24, 2018.

Burns, A. J., E. M. Johnson, and D. D. Caputo. 2019. Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce* 29 (1), 24–39.

Chatterjee, D. (2018) High Performance Culture is Essential in Cyber Warfare under review, submitted on December 13, 2018

Disparte, D., and C. Furlow. May 16, 2017. The best cybersecurity investment you can make is better training. *Harvard Business Review* 2–4.

Fuhrmans, V. October 12, 2017. New Worry for CEOs: A career-ending cyberattack; corporate chiefs get more involved in defense against hackers, fearing a breach could cost their jobs, hurt their businesses. *Wall Street Journal*.

Kabanda, S., M. Tanner, and C. Kent. 2018. Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce* 28(3): doi:10.1080/10919392.2018.1484598.

Khan, H. U., and K. A. Alshare. 2019. Violators versus non-violators of information security measures in organizations – A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce* 29 (1), 4–23.

Ray, M. C. September 2017. *The new cyber reality: A perpetual state of breach*, New York: Nardello & Co.

Wolff, J. 2018. Don't get carried away with cybersecurity. https://slate.com/technology/2018/12/marriott-data-breach-wyden-consumer-data-protection-act.html

Notes on contributor

Dr. Dave Chatterjee is tenured professor at the Terry College of Business, The University of Georgia. An accomplished scholar and technology thought leader, Dr. Chatterjee's interest and expertise lie in the various facets of technology management – from technology sense-making to implementation and change management, data governance, internal controls, information security, and performance measurement. His work has been accepted for publication in prestigious outlets such as The Wall Street Journal, MIT Sloan Management Review, California Management Review, MIS Quarterly, and Business Horizons. Dr. Chatterjee is a noted speaker, delivering talks around the world, moderating CXO panel discussions, conducting corporate training and workshops, webinars, providing consulting and advisory services, and authoring papers. He has appeared on radio and TV interviews and is frequently quoted by news media on major technology related development. Dr. Chatterjee is Senior Editor of the Journal for Organizational Computing and Electronic Commerce. He also serves on the Corporate and Community Leadership Council of Cybersecurity Collaborative, a confidential forum and resource for chief information security officers (CISOs).