Security Contingency Planning: Private Recovery and Public Response

Michelle N. Aninye and Dr. Humayun Zafar

Cyber Institute

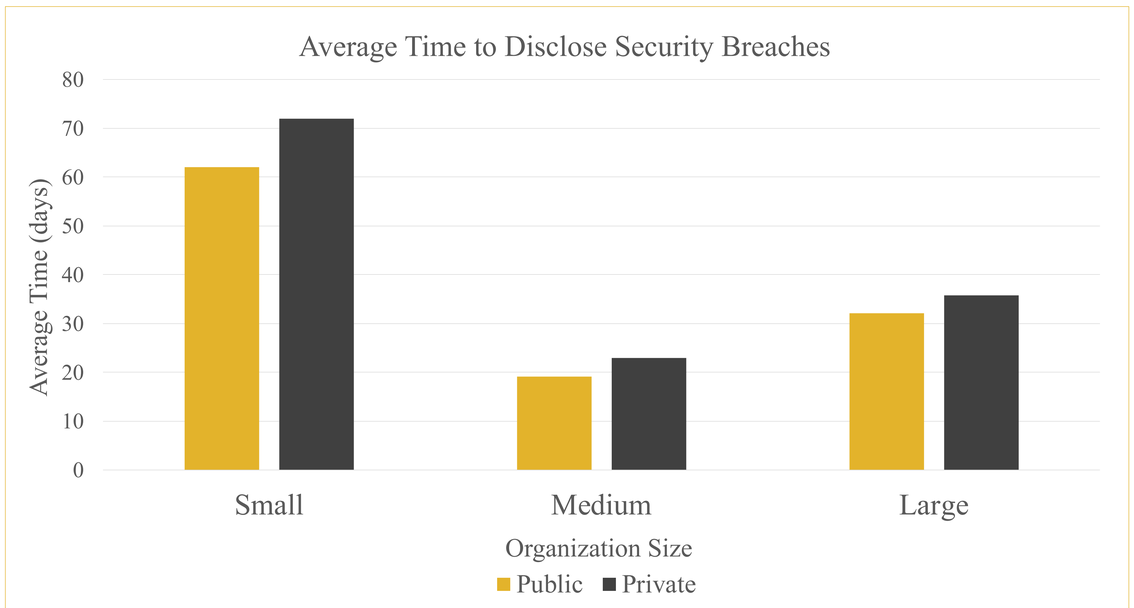
KENNESAW STATE UNIVERSITY

INTRODUCTION

Contingency planning is a common business practice used to protect an organization and recover information technology, IT, services in the event of an emergency, disaster, or disruption. Security contingency planning places an emphasis on an organization's cybersecurity assets and functions. With the rise of security breaches, security contingency planning is becoming an increasingly vital business function. However, security contingency planning remains underregulated and understudied. This study considers two major criteria:

- Organizations take 55 days to contain breaches (*private recovery*)[1]
- The amount of time taken to disclose breaches (*public response*)

This study examines correlations between various types of organizations and their response times. The resulting evidence is used to make suggestions for creating effective and comprehensive security contingency plans.



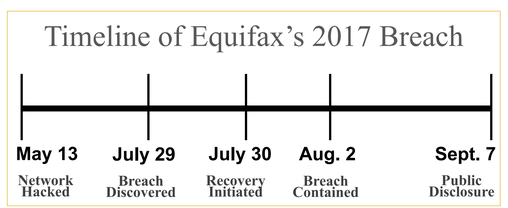
METHODOLOGY

This study analyzes 260 security breaches from 2004 to 2018 taking into account the amount of time between recovery and disclosure.

- For companies that experienced multiple breaches, each breach is included as a separate event
- Data collected from news reports and public notices
- Included 39 small organizations, 64 medium organizations, and 164 large organizations
- Small organization: 99 employees or less
- Medium organization: 100-299 employees
- Large organization: 300 employees or more

RESULTS

- Average amount time to publicly disclose breaches is 40.68 days
- 36% of organizations included disclosure as part of their security in their contingency plans
- 29% of organizations offered assistance to affected parties



CONCLUSION

- Individual security frameworks are not publicly accessible
- Public organizations follow federal regulations such as the General Data Protection Regulation (GDPR)
- Organizations should adhere to the security frameworks from external sources, such as the National Institute of Standards and Technology (NIST)
- Supports previous research by Goode et al. (2017) suggesting that organizations with stronger security postures respond to breaches more effectively
- Future research should investigate the impact of federal regulations on both phases

REFERENCES

[1] Ponemon Institute. 2013. "2013 Cost of Data Breach: Global Analysis," Research Report, Ponemon Institute.

CONTACT

Michelle N. Aninye

Kennesaw State University

maninye@students.kennesaw.edu

michelleaninye@gmail.com