Association for Information Systems

AIS Electronic Library (AISeL)

SAIS 2020 Proceedings

Southern (SAIS)

Fall 9-11-2020

Cybersecurity Scenario Modeling: Imagining the Black Swans for Digital Infrastructures Risk Management

Atiya Avery
University of Alabama in Huntsville, atiya.avery@uah.edu

COMPLETED RESEARCH: CYBERSECURITY SCENARIO MODELING: IMAGINING THE BLACK SWANS FOR DIGITAL INFRASTRUCTURES RISK MANAGEMENT

Atiya Avery
University of Alabama in Huntsville
atiya.avery@uah.edu

ABSTRACT

The term "digital infrastructures" is used to refer to one or more of a combination of IoT and its artifacts, the cloud, cyber-physical systems, and digitized business architectures. As digital infrastructures become increasingly complex and interdependent, impacts from disruptive events have the potential to be more harmful than mere inconveniences and financial losses. The risk from these catastrophic events to digital infrastructures may leave many organizations unprepared. To predict so-called "Black Swan Events" to increasingly complex digital infrastructures this research in progress postulates that risk management activities should be conducted outside of existing frameworks. In this paper, we argue that qualitative scenario risk modeling exercises utilizing diverse stakeholders may become even more important than other types of risk analysis in the prediction of threats to digital infrastructures. We discuss the importance of diverse stakeholders in developing structured, qualitative, scenario models to predict Black Swan Events to digital infrastructures. We discuss potential issues and solutions for the cataloging and quantification of the use cases developed from qualitative event scenario modeling and the next steps for this research.

KEYWORDS

Cybersecurity, Ontology, Scenario Modeling, Information Security

BACKGROUND

The pace of technological change has made it difficult for any single organization to be able to protect its infrastructure independently because information security is a complex ecosystem of attackers and defenders involved in a perpetual game of cat and mouse (Knapp, Morris, Rainer Jr, & Byrd, 2003). This significantly increases cyber-risks to organizations that do not properly manage threats and opportunities from employees, intermediaries, contractors, partners, suppliers, governments, and even regulators. Currently, negative consequences from threats and missed opportunities in managing cyber-risks can best be described as mere inconveniences and recoverable financial losses to the organizations and the people impacted by them. Consider the January 2016 outage at a Verizon data center, which caused flight delays for airlines and shut down its website, booking, and check-in systems (Sverdlik, 2016). In March 2016, MedStar Health chain of hospital systems was hacked preventing patients from booking appointments in addition to leaving staff unable to check email messages or look up phone numbers. The organization reverted to a paper based system and proclaimed that patient care was not impacted (Gillum, Dishneau, & Abdollah, 2016). Furthermore, the frequency of data breaches has gone from 1 breach every 2 days in 2005 to 2 breaches a day in 2015 to 4 breaches a day in 2019 (Identity Theft Resource Center, 2020). The most common outcome of data breaches is identity thefts (Moore, 2010). However, in 2013, 86% of identity theft victims had personal out of pocket expenses which amounted to less than one hundred dollars (Harrell & Langston, 2013).

In addition, academic researchers are not clear on the market implications of data breaches. It has been difficult for researchers to articulate the full potential impacts and long-term consequences of cyber-risks to organizations; with the research suggesting that there may not be long-term impacts from breach disclosures (Acquisti, Friedman, & Telang, 2006; Gordon, Loeb, & Zhou, 2011; Cavusoglu, Mishra, & Raghunathan, 2004). Many organizations may then perceive that there are no apparent long-term consequences from the mismanagement of cyber-risks. This environment has made it difficult for organizations to understand how to view and manage their cyber-risks. It is apparent that threats and missed opportunities to manage cyber-risks to digital infrastructures within business organizations are not viewed in the same way as those towards physical infrastructures. This is possibly because they are not perceived as being life-altering. However, over the last two decades these cyber-risks have indeed been taken seriously for government-owned and managed digital infrastructures such as SCADA systems; which are at the heart of such operations as power grids, air traffic control systems, and water systems (See Nicholson, Webber, Dyer, Patel, & Janicke, 2012 for a literature review). This research stream while a starting point for business organizations to begin to think about the management of cyber-risks; does not do enough to address the diverse operating environments and competing goals unique to business organizations. In addition, much of the research regarding government-owned and managed digital infrastructures is classified leaving out a large community of researchers and business organizations in which to share findings with, despite business organizations being the largest component of the cybersecurity problems in the United States (Roswell, 2009).

Mismanagement of risks is never inconsequential, even in the long run. Seemingly unrelated risks can be linked together where one consequence has the potential to lead to other unforeseen and exponentially impactful consequences. Consider the events leading up to the devastating September 11, 2001, terrorist attacks. These events had existing elements of risks that when combined created the ‘perfect storm’ for a catastrophe. The potential connection among and between existing elements of risks was not readily apparent to those responsible for managing them. In the cybersecurity space, we already see such a phenomenon in so-called “Advanced Persistent Threats (APT)” where sophisticated cyberattacks are established within the information technology infrastructure of an organization for obtaining information and/or undermining missions, programs, and organizations. APT’s can go on for many years before being detected and are characterized by multiple forms of attacks including physical attacks and acts of deception (Brewer, 2011; Virvilis, Gritzalis, & Apostolopoulous, 2014). Events such as the September 11, 2001, terrorist attacks are examples of “Black Swan " events. Black Swan events can be broadly defined as those extremely impactful, catastrophic events that lie outside the realm of known predictive capabilities; nothing in the past can convincingly point to their possibility (Taleb, 2007; pg.xvii). An interesting aspect of Black Swan events is that despite their surprise factor, these events are easily explainable and predictable after the event has occurred (Taleb, 2007; pg xviii).

There is some debate about whether or not Black Swan Events truly exist. Some experts believe that Black Swan events are nothing more than emerging risks; others view them as physical manifestations of high impact but very low probability events – so-called worst-case scenarios. Emerging risks are defined as new or familiar risks that become apparent in new or unfamiliar conditions whose consequences are not fully understood or appreciated; emerging risks may actually lessen over time or become worse than expected (Flage & Aven, 2015). One example of an emerging risk to an organization is that encountered by the now defunct video retailer BlockBuster. It did not have the ability to manage threats and opportunities from electronic self-service kiosks (Redbox) and online streaming services (Netflix). Mismanagement of these emerging risks led BlockBuster to eventually file for bankruptcy (Abell, 2010; Sandler, 2010; Arnold, 2010). In contrast, Werther (2013), argues however that Black Swan events are simply on the tail end of predictive models and are not a new phenomenon at all. Black Swan events can be considered the manifestation of very low probability but very high impact events that are accounted for but not necessarily describable. With this perspective, we can see how Hurricane Katrina and its aftermath may be considered the physical manifestation of a 1 in 100 year Hurricane event – an event which is modeled but not describable. We argue however that the construct of Black Swan events is still needed. Organizations, whether they would like to admit, have to be ready to manage previously unimaginable worst-case scenarios in order to survive.

We define Black Swan events as those events that are not foreseeable by existing mathematical and logical models; these events have never taken place before. Experts within the domain may be unable to predict these events as they are constrained by prior life experiences and biases (Nafday, 2009). Domain experts have a tendency to focus on the known sources of uncertainty while ignoring the complexity of reality (Taleb, Goldstein, & Spitznagel, 2009). We argue that domain experts do not suffer from the uncertainty about Black Swan events per se but the uncertainty that comes from that lack of deep unknowing knowledge. This is different from a conscious awareness that one does not know. In other words, these events are truly not considered during the course of organizational risk assessment. These are not high impact, low-frequency events. They are not within the imagination of the people responsible for risk management, assessments, analysis (Flage & Aven, 2015; Fischbacher-Smith, 2010; pg 5).

From another perspective, Black Swan events may be viewed as incorrect risk assessments due to the lack of knowledge from the right sources (Aven, 2013). This is our viewpoint of Black Swan events as well. To hedge against the risks of Black Swan Events to emerging digital infrastructures we argue that it is important that as many diverse roles and actors are actively utilized in the practice of cyber-risk management, not just those practitioners within the information systems function. A Black Swan event is best imagined by the collective knowledge, experience, and observations of all people within the organizations. In addition, we argue that management information systems researchers are uniquely positioned to further research in this area in order to assist business organizations.

Business Organizations and Researchers

Business organizations and researchers need to begin to work collectively and independently to imagine the Black Swans to digital infrastructures. In order for this to be realized (1) organizations need to conduct risk management activities outside the confines of traditional governance processes and frameworks., (2) organizations and researchers must utilize divergent experts and collective intelligence, (3) organizations will need to share information with researchers, (4) researchers must attempt to make technical knowledge and findings accessible to the layman and applicable to the field while also advancing theory for future researchers to build on.

Organizations need to conduct risk management activities outside the confines of traditional governance processes and frameworks. Organizations have at their disposal a number of existing governance frameworks and mandates to help manage cyber-risks to their organizations. However, rules and regulations are established to manage risks that are defined and predictable. Future Black Swan events will be unrelated to and fall outside of the context of any current rules (Mclean, 2010). In addition, most information security textbooks, standards, recommendations, and best practices indicate that risks must be properly identified, analyzed and evaluated before the organization can move forward; however many frameworks and methodologies are found not to be applicable in the field (Oppliger, 2015). These systems can get wieldy with their paperwork, approval processes, and general organizational bureaucracy which may disable the organization from quickly responding to emerging threats and opportunities. It is not enough to rely on governance and mandatory compliance measures to manage cyber-risks for business organizations; many organizations do not fully practice their existing governance frameworks (Avery & Cheek, 2015; Jourdan, Rainer Jr, Marshall, & Ford, 2010). This does not mean that they still cannot manage risks to their digital infrastructures. To hedge this, it is important that MIS researchers understand the current gaps in knowledge and that organizations conduct proper event scenario modeling to truly understand gaps in cyber-risk management as well as imagine and articulate Black Swan events on the digital infrastructures.

Business organizations and researchers must utilize divergent experts and collective intelligence to predict (or imagine) Black Swan Events to digital infrastructures. A characteristic of Black Swan Events is that they appear as if they should have been predictable but only after the fact. Just because experts within a domain claim that they will not be able to predict a Black Swan event should not prevent us from trying to understand (a) what the potential worst case scenarios will look like from cyber-risks to digital infrastructures, and (b) how an organization can best respond to these events before, during, and after to minimize the impacts.

There is a great deal of evidence that certain kinds of analysts and experts using the same information and methods available to everyone else are consistently better at predicting extreme events (Werther, 2013; pgs 14-19). To truly understand risks to digital infrastructures there needs to be diverse and divergent experts working together. In organizations, this means having practitioners whose life experiences and biases are somewhat outside of the STEM domains. These practitioners may be able to see connections between risks that classically trained experts may not see. For researchers this means academic domains coming together to make technical knowledge and findings accessible to the layman and applicable to the field while also advancing theory for researchers to build on. The MIS domain is at a unique intersection between organizational science, information science, academic institutions, organizations, as well as the IT industry and various professional groups which encompass it. Benbasat & Zmud (2003), posit that MIS is focused on IT infrastructures and IT business solutions and the immediate consequences and antecedents of these information systems. For this reason, MIS researchers should lead the charge regarding cyber-risks to digital infrastructures. We acknowledge that there are major differences between information security research (In this paper, cyber-risks, information security, and cybersecurity are used interchangeably and refer to the same constructs but in different contexts) and other types of MIS research. The former may have relegated the majority of the research to the hard sciences. Siponen (2008) notes that the major differences between information security research and information systems research is a lack of theory, no focus on management, and no focus on empirical methods and the two operate as different fields with different systems of cultural values. At the time this was attributed to the immaturity of the information security research field. Although progress has been made via calls for action in MIS "special issue" journals (see Mahmood, Siponen, Straub, Rao, & Raghu, 2010; Warkentin & Willison, 2009), it is not clear that enough research has been done in the MIS domain regarding information security in the context of business organizations. This has left the research gap to be addressed by practitioner-oriented whitepapers, typically selling a service or product or has been appropriated to the computer science and engineering domains where the research is often quantitatively and theoretically conceptual with little consideration given to the complexities of people within organizations and the day-to-day business operations. Some of this perhaps is due to the fact that organizations are hesitant to share security related information due to market fears and negative perceptions associated with having to publicly disclose an information security failure. (Jourdan, Rainer Jr, Marshall, & Ford, 2010; Campbell, Gordon, Loeb, & Zhou, 2003; Moore, 2010). These fears are unsubstantiated however in the context of academic research. There are guidelines built-in place to protect the integrity and confidentiality of research data. Academic research has been used to study highly sensitive personal topics such as sexually transmitted diseases and the illicit drug use of private individuals (for an example of such research see Turner et al (1998)). Academic researchers can surely be trusted to study information security within organizations. Without the sharing of information and data, it is difficult for researchers to conduct rigorous empirical research to answer important research questions and advance theory

Business organizations must share information and data with academic researchers. Academic researchers can provide the business community with unbiased empirical research to understand what works, how to save money, and how to optimize risk mitigation measures. A structured literature review in the information systems, computer science, and engineering domains must be conducted to better understand the research gaps regarding organizational guidance on how to manage cyber-risks to digital infrastructures; and this will be the next step for this research. It will be important to articulate the research gaps so organizations can imagine what the Black Swan events may look like for them. Next, we discuss why structured event scenario modeling is important and the unique challenges of developing such a framework.

MODELING DIGITAL INFRASTRUCTURES RISK & CONCLUSION

Scenarios are narratives that use logical implications, assumptions, and forecasts to communicate about a potential future state; it incorporates issues to be resolved, time relations, interactions and consequences (Gray & Hovav, 2014; Kim & Cha, 2011). Scenarios are most powerful when several of them are used together and can allow organizations to take risk management actions such as changing business practices or innovating (Gray & Hovav, 2014). One major benefit of scenario modeling in the context of organizational risk management is that it allows risks to be articulated in the absence of unequivocal clear evidence. It reduces the burden of proof challenge brought about by the organizations' need to balance competing demands of performance and risk management (Fischbacher-Smith, 2010). In addition, divergent experts can easily articulate their knowledge to domain experts. Use-case scenarios generated from qualitative scenario modeling are specific enough to be categorized, archived, and quantified to understand Black Swan risks to an organization's digital infrastructure. This "cataloging" of use-case scenarios may enable organizations to develop risk management playbooks to mitigate losses from these events. Additional research on the utilization of existing cybersecurity risk management framework as potential ontologies for the cataloging of these use cases is needed particularly in the context of business research.

REFERENCES

1. Abell, J. (2010, October 21). Netflix Instant Accounts for 20% of Peak U.S. Bandwidth Use. *Wired*.
2. Acedo, F., Barroso, C., Casanueva, C., & Galan, J. L. (2006). Co-Authorship in Management and Organizational Studies: An Empirical and Network Analysis. *Journal of Management Studies*, 957-983.
3. Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.
4. Arnold, T. (2010, December 27th). Netflix and Redbox gained in 2010 as DVD. *Reuters*.
5. Aven, T. (2013). On the meaning of a black swan in a risk context. *Safety Science*, 44-51.
6. Avery, A., & Cheek, A. (2015). Analytics Governance: Towards a Definition and Framework. *Twenty-first Americas Conference on Information Systems, Puerto Rico 2015*, 1-8.
7. Brewer, R. (2011, Oct 5th). Comment: It's time to take APT's Seriously. *InfoSecurity Magazine*.
8. Campbell, K., Gordon, L., Loeb, M., & Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security, 11*(3), 431-448.
9. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87-92.
10. Dardick, G. S. (2010). Cyber Forensics Assurance. *Security Research Institute Conferences*, 57-64.
11. Farrell, S. (2008). Security Boundaries. *IEEE Internet Computing, 12*(1), 93-96.

12. Fischbacher-Smith, D. (2010). Beyond the worst case scenario: "Managing" the risks of extreme events. *Risk Management*, 1-8.
13. Flage, R., & Aven, T. (2015). Emerging risk-Conceptual definition and a relation to black swan type of events. *Reliability Engineering and System Safety*, 61-67.
14. Gillum, J., Dishneau, D., & Abdollah, T. (2016, March 29th). MedStar Hacked, Virus Attacks D.C.- Area Hospitals. *U.S. News*.
15. Gordon, L., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33-56.
16. Gray, P., & Hovav, A. (2014). Using scenarios to understand the frontiers of IS. *Information Systems Frontiers*, 337-345.
17. Harrell, E., & Langston, L. (2013). *Victims of Identity Theft 2012.* Washington, D.C.: U.S. Department of Justice.
18. Identity Theft Resource Center. (2020). *Data Breaches.* Identity Theft Resource Center. Retrieved from https://www.idtheftcenter.org/2019-data-breaches/?utm_source=web&utm_medium=sitewidenotice&utm_campaign=01282020_2019DataBreachReport . Accessed 27 July 2020.
19. Jourdan, Z., Rainer Jr, R., Marshall, E. T., & Ford, N. F. (2010). An Investigation of Organizational Information Security Risk Analysis. *Journal of Service Science, 3*(2), 33-43.
20. Kim, Y.-G., & Cha, S. (2011). Threat scenario-based security risk analysis using use case modeling in information systems. *Security and Communication Networks*, 293-300.
21. Mahmood, M., Siponen, M., Straub, D., Rao, R., & Raghu, T. (2010). Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue. *Management Information Quarterly*, 431-433.
22. Mclean, R. (2010). The Six Mistakes Executives Make in Risk Management. *Air & Waste Management Association*, 39-41.
23. Moore, J. W. (2010). From Phishing to Advanced Persistent Threats: The Application of Cybercrime to the Enterprise Risk Management Model. *Review of Business Information Systems, 14*(4).
24. Nafday, A. (2009). Strategies for managing the consequences of black swan events. *Leadership and Management in Engineering, 9*(4), 191-197.
25. Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in light of Cyber-Warfare. *Computers and Security, 4*, 418-436.
26. Oppliger, R. (2015). Quantitative Risk Analysis in Information Security Management. *IEEE Computer and Reliability Societies*, 18-21.
27. Peters, S. (2015). *Medical Identity Theft Costs Victims $13,450 Apiece.* Information Week.
28. Roswell, L. (Fall 2009). Targeting the Digital Infrastructure. *netWorker*, 26-31.
29. Sandler, L. (2010, September 22). Blockbuster said to plan bankruptcy tomorrow with loan. *Bloomberg Business*.
30. Sverdlik, Y. (2016, January 14th). Verizon Data Center Outage Delays JetBlue Flights. *Data Center Knowledge Center*.
31. Taleb, N. N. (2007). *The Black Swan.* New York, NY: Random House.
32. Taleb, N., Goldstein, D., & Spitznagel, M. (2009). The Six Mistakes Executives Make in Risk Management. *Harvard Business Review, 87*(10), 78-81.
33. Ten, C., Liu, C., & Manimaran, G. (2008). Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Transactions on Power Systems, 23*(4), 1836-1846.
34. Virvilis, N., Gritzalis, D., & Apostolopoulous, T. (2014). Trusted computing vs. Advanced persistent threats: Can a defender win this game. *Information Security and Critical Infrastructure Protection Research Laboratory*. Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The Insider Threat. European Journal of Information Systems, 101-105.

35. Werher, G. (2013). When Black Swans Aren't: On Better Recognition, Assessment, and Forecasting of Large Scale, Large Impact, and Rare Event Change. *Risk Management and Insurance Review, 16*(1), 1-23.
36. Young, J. (2014, December 26th). *Boxing Day Earthquake 2004: Could it happen again?* Retrieved from Decoded=Science: http://www.decodedscience.org/boxing-day-earthquake-2004- happen/51608