RESEARCH PAPER

Submitted by

Arvind Ponnarassery Jayan

(aponnar1)

Johns Hopkins University

Information Security Institute (JHUISI)

Michael Dean Kociemba Sr.

Johns Hopkins University Information Security Institute (JHUISI)

April 2020

The views expressed in this paper are those of the author and do not reflect the official policy or position of the Johns Hopkins University Information Security Institute

Correlation of Business Maturity and Cybersecurity Table-Top Exercises

Abstract — The cybersecurity leadership maturity for a company defines how it responds to cybersecurity threats and issues. The higher the maturity state, the stronger the company is in the cybersecurity front. This paper attempts to find whether there is a correlation between this business maturity and cybersecurity table-top exercises.

***Index Terms* — Cybersecurity leadership maturity model, table-top exercises, cybersecurity**

I. Introduction

A. *Purpose of the Study*

This topic was chosen to understand how to increase business maturity states with the minimal financial expense for securing its assets using a specific technique. The business mentioned here includes all types of companies from various industries like finance, health, technology, etc. I have included all businesses at a macro level because most of the businesses in the current era use digitized data with the advent of the internet. Business maturity in the scope of this paper refers to the growth of any business from a reactive group to a proactive group in the Cybersecurity Leadership Maturity Model. The table-top exercise is chosen as one of the cost-effective and efficient methods to optimize the cybersecurity implementations within a company. The paper focuses on how this simulation training ensures business continuity and growth in business maturity with a minimum financial cost. The sources for establishing the effectiveness of a complete and proper table-top exercise are hard to come by but in general, all table-top exercises or simulation training applied in various domains including training for cybersecurity was simple, efficient and cost-effective.

B. Problem Statement

From reviewing the papers it is found that existing table-top testing even though limited has been cost-effective and partly realistic. Iterative application of this system could be used for improving the compliance guidelines and helping the company be prepared for real disasters or cyber incidents. A company that is an Influencers in the Business Leadership Maturity Model can ensure its business continuity and cyber defence. So my research question is: Can any company of a lower maturity reach the ideal business maturity by implementing Cyber Security Table-top exercises? Is there a correlation between Business Maturity and Cyber Security Table-top exercises?

II. LITERATURE REVIEW

A. Business and IT

With the emergence of high-speed communication, businesses are more dependent on digitized storage of information and hence they have more to lose than just infrastructure when a disaster befalls. The proportion of digitized data will be different depending on the industry in focus, but for any industry, it is important that their information is secure. Many businesses also operate in a “24/7” environment (such as the health industry) and many businesses are global in their scope of operations (any IT service industry). A large percentage of small businesses are also Internet-based or have a significant portion of income derived from the Internet.

Consider the following facts:

(a) 80 percent of businesses affected by a major “incident” close within18 months,

(b) 90 percent of businesses that lose data as a result of a disaster close within two years, and

(c) 58 percent of UK businesses were disrupted by a manmade disaster over 3,000 miles away in another country (the World Trade Center terrorist attacks of September 11, 2001, in New York).

It is clear that all businesses, from large multinational corporations down to the local business selling services on Internet,
must develop a disaster recovery (DR) plan and prepare for business continuity (BC) following an incident that affects business operations. [1]

B. Business Continuity

In a survey of 94 Australian organizations in 1999-2000, the majority of organizations stated that the longest time they could be out of action was less than 24 hours. Moreover, 30% of these organizations said that their longest out-of-service time was less than 8 hours. Business Continuity Management states “the objective of business continuity management is to ensure the uninterrupted availability of all key business resources required to support essential or critical business activities”. In “A business continuity management simulator” by William J. Caelli, Lam-For Kwok and Dennis Longley, it is clearly stated that Australian Standards HB292-200 provides comprehensive guidance in the establishment of effective business continuity management by closely relating it to risk management. I believe this is generally true and BCM cannot address the problem of risk analysis for the systems in the post disruption phase since mere conformance to a guide never ensures perfect security. This is where it is important to resolve this issue by conducting tests and using the results as an input to update the comprehensive compliance guide. This is a continuous process and should not be terminated in one iteration, the tests should be conducted periodically with the newly updated rules to obtain a better system that can enforce business continuity in different situations. One of the best ways to conduct this process of iterative testing with cost-effectiveness in attention is by using simulations or table-top testing. [2]

C. Table-Top Testing

The table-top testing considered here is both basic and advanced table-top exercise. Where basic table-top exercises is just discussions and advanced table-top is a simulated interactive exercise that helps test an organization's capability of responding to a simulated event. It is a coordinated response to a situation in a time-pressured, realistic simulation that involves several agencies. This focuses on the coordination, integration, and interaction of an organization's policies, procedures, roles, and responsibilities before, during, and after the simulated event. It heavily emphasizes communication among all the agencies participating in the exercise. [3]

One of the scenarios where simulated training was used is in preparing for disasters by the organization St. Paul Regional Water Services (SPRWS) when it hired AECOM Technical Services to prepare an Emergency Response and Recovery Preparedness Manual for the McCarron's Water Treatment Plant. It was SPRWS's intent to reinforce the staff members' skills and familiarity with their current positions and training, and then apply those skills during disaster response and recovery drill. I believe the steps followed by this organization is the foundation for table-top exercises. SPRWS initially interviews with key staff members and developed an activation chart that considers all possible risks and outcomes. 3 teams were assembled, one for handling a type of incident, one for considering the logistics and finance and the last for planning. This was followed by conducting tabletop exercises to help familiarize team members with their responsibilities during a recovery and response scenario. After each iteration, the staff debriefed and compiled ideas on how to improve response and recovery efforts. Through this process and continual practice, the organization can be prepared whenever a disaster strike. [4]

D. Table-Top Exercises and Cybersecurity

The cyber incidents can cause pertinent damage to critical infrastructures of an industry or a region (e.g. water, gas, electric power). Each company must have some training to respond to IT security incidents since shutting down its service would be very costly. The available tabletop security that I found interesting are discussed below. [8]

The paper "Environment for Cybersecurity Tabletop Exercises" by Brilingaite, Agne, Linas Bukauskas, Virgilijus Krinickij, and Eduardas Kutka talks about a game-based exercise called "TableTop eXercise Web Environment" (TTXWE), which enables cyber incident scenario simulation for available roles, RG, and time limitations. TTXWE supports essential table-top exercise social aspects but enables usage of online web-based software for incident reports (incident solving, delegation, and information) instead of paper forms. The learning objectives of the game are:

- ability to identify, understand, and classify the cyber incident,
- ability to make decisions individually and in a group,
- ability to interpret legislative documents,
- ability to link the cyber incident to the organization’s purpose and activities.

The players must gather together in groups of roles and solve cyber incidents with respect to team discussion results. This simulator is simple to use (due to its web interface), fast and has a qualitative response when taking action. But it has its limitations, it has not been tested with professionals, there is a limitation to the number of people who can take the test and also the cyber incident realism is not fully simulated (stress-level). [5]

Another table-top exercise that I wanted to highlight was from the paper “Network Oriented Cyber Security Model (NOCS-M)” by Hein, Carl, Mike Stebnisky, and Ambrose Kam. The initial implementation of NOCS-M explored basic classes of abstractions needed for capturing cyber effects. It demonstrates faster than real-time operation, high-fidelity, low-cost, and ability to scale to arbitrary networks rapidly. New and hypothesized threats may be quickly modelled in this approach. Though this simulator is limited to network security, according to me this is a better system for conducting table-top testing compared to the previous one because of its effectiveness, realism, and cost-effectiveness. [6]

The benefits of table-top exercises can be observed from the above examples, especially the cost-effectiveness and simplicity in simulating realism and providing training. A company can initially start from basic and existing guidelines and iteratively produce stronger ruleset as well as trained employees through cost-effective and simple simulative training. But at the same time, we can observe that existing cybersecurity table-top exercises are not perfect and are always lacking in some way. The paper “Table-top Exercises for Emergency Management-

Tame Solutions for Wicked Problems" by Edzen, Svante discusses the shortcoming of table-top exercises. It defines the concept of the wicked problem, which has six characteristics:

1) The problem is not understood until after the formulation of a solution - The information needed to understand a problem is based on the idea of a possible solution.

2) Wicked problems have no stopping rule - Because the problem is not defined, it is not possible to set criteria that indicate when the problem has been resolved.

3) Solutions to wicked problems are not right or wrong - Solution quality cannot be determined objectively.

4) Every wicked problem is essentially novel and unique - No two problems are identical, though there may numerous similarities.

5) Every solution to a wicked problem is a "one-shot operation" - Each solution implemented will have consequences (may spawn new wicked problems).

6) Wicked problems have no given alternative solutions - There may be no solutions, or there may be a number of possible solutions or a range of solutions that no one has yet considered.

I completely agree with this paper, we believe everything can be secured if we identify the problem and map it to an existing problem. Following a compliance guide or using existing solutions to patch whatever incidents that occur may not be satisfactory for when the problem is "wicked". The company after being secured with iterative table-top exercises can still be attacked with completely new and unknown malware and face interruptions in business continuity. In the end, table-top testing should also factor in cases where an impossible situation has occurred and how the Business Continuity can still be ensured with minimum or no compromise to any assets or resources. I also believe the CISO (Chief Information Security Officer) of the company (if present) and his decisions will make a great impact in these situations. By factoring in these wicked problems and executing the iterative table-top exercises the company can ensure its business continuity and also its growth. [3]

E. Cybersecurity Leadership Maturity Model

A company could be among one of the three Business Leadership Maturity: Responders, Protectors, Influencers.

Responders: This group is very reactive and is working headway to be compliant with regulations and may not have the appropriate resources or business influence to drive significant change.

Protectors: This group recognizes the importance of information security but lack insight or budget to incite the necessary transformations.

Influencers: They have both the security insight as well as business influence and authority to drive a change.

I believe a company with the best security system in place would have a maturity level of "Influencers" and companies on the other maturity level should try to obtain this ideal state. [7]

III. RESEARCH METHODOLOGY

A. Survey Preparations

For this research, I have conducted a survey[1] with security professionals from 8 different companies present in various industries and I was able to collect data regarding the business maturity as well as the overall security of the company. Since the data collected is sensitive, the name and other specific details of the companies will not be referenced throughout this report for privacy issues.

The information collected using the survey is the following:

1. The industry of the company
2. The size and popularity of the company
3. The amount of digital data that the company handles
4. The various clients that the company handles
5. The different security threats faced by the company
6. The different security controls placed before and after being hacked (if hacked)
7. Is there a CISO in place?
8. How strong is the power of CISO (if present)?
9. Is basic table-top testing being conducted?
10. Is advanced table-top testing being conducted?

Through this survey, we can identify the following:

1. What is the business maturity of the company?

[1] The survey was difficult to conduct due to the current conditions. Also, the survey demands very sensitive information from the company, many security professionals were not willing to reveal this information due to its security implications.

2. What is the influence of placing security controls and whether they look forward to moving up in the cybersecurity leadership maturity model?
3. Whether the company had security controls initially or later?
4. Whether table-top exercises are being used for the improvement of the overall cybersecurity?
5. Whether cybersecurity table-top exercises helped in the improvement of the company’s business maturity?

B. Aggregated Information

The information collected from various industries are present below in detail, where the answers for each question in the survey is answered in order:

1. Company T1
   - This is a company from the IT Industry.
   - This is a small-sized company that contains 50 employees and only one branch is present.
   - The company handles a huge amount of digital data, but the data is not highly sensitive.
   - The clients are not international.
   - The company has not faced any security threats.
   - The company has minimum security controls in places such as Firewall, Anti-virus. Minimum security compliance is enforced as per requirement.
   - There is no CISO in place. The security team contains just 2 people that overview the security of the whole company.
   - Not applicable.

- Basic table-top testing is not conducted, where there is a relevant discussion of improving security controls.
- Not applicable.

2. Company L2
    - This is a company from the Medical Industry.
    - This is a medium-sized company with 200-300 employees.
    - The company handles normal amounts of digital data, which are sensitive in nature.
    - The clients are not international.
    - The company has faced security breaches (ransomware attack 20XX)
    - Before the security breach, the company had minimum security controls - firewall, antivirus, black box. After the security breach, the company had more security controls added along including anti-ransomware, honey pot, IDS, and security awareness for the employees. Security compliances such as FDA compliance, 21 CFR part 11, and other relevant security compliances were enforced.
    - There is no CISO in place. CIO is the acting CISO.
    - The acting CIO did have discussions with the security team of 6 on exerting the importance of placing an IDS, honey pot, etc for strengthing the security controls before the security breach. These new security improvements were flagged down by the CFO, even though approved by the CEO, due to "Budget Constraints". After the security breach, the acting CISO was provided the power to place the extra security controls to prevent being hacked again.
    - Basic table-top is being conducted where several scenarios of threats and its mitigations were discussed even before the security breach.

- Advanced table-top testing applicable to this specific company includes intensified security awareness programs that occurred after the breach.

3. Company K3
   - This is an international airline company from the Transportation Industry.
   - This a large-sized company that has bases internationally.
   - The company hash to handle international flight details which are digital as well as sensitive.
   - The clients are international.
   - The company faces a lot of security threats constantly.
   - The company provides huge importance to security and has several important security controls in place and several compliances including Federal Aviation compliance.
   - The CISO is present.
   - The CISO is provided strong power to take the required actions, as the whole company is risk-driven.
   - Basic table-top exercises are conducted, where there are security discussions daily, weekly, and monthly.
   - Advanced table-top exercises are conducted as well, where simulators of threats and mitigations are performed with a strong awareness of security among the employees.

4. Company Q4
   - This is an international banking company from the Finance Industry.
   - This is a large-sized multi-national company.
   - The company handles a lot of digital as well as sensitive data.
   - The clients are international.

- The company faces huge security threats due to involvement with investment firms and the stock market.
- The company provides huge importance to security and has several important security controls in place and several compliances including Financial Compliance.
- There is a CISO in place.
- The CISO is provided strong power to take the required actions, as the whole company needs to compliant and ready for regulatory inspections.
- Basic table-top exercises are conducted, where there are security discussions among the different managers of the same level that report to the CISO.
- Advanced table-top exercises are conducted minimally for setup.

5. Company N5
    - This is a company from the Manufacturing Industry.
    - This is a large-sized multi-national company.
    - The company handles a minimum amount of digital, most of the IT appliances are only accessible internally.
    - The clients are international.
    - The company faces security threats such as phishing emails. The breach is successful 90% of the time due to human errors.
    - The company had minimum security controls in place before 2016. After 2016 the company realized the importance and requirement of security and hired a 3rd party security provider for cybersecurity.
    - The manager from the 3rd party security provider acted as the CISO (CISO as a service).

- The acting CISO was supported by the CEO and CFO for financial investments for security infrastructure.
- The 3rd party company conducted sufficient basic table-top testing.
- They were also responsible for conducting advanced table-top exercises by hiring a 3rd party vendor for simulations of attacks in the company.

6. Company U6
   - The company is from the IT Industry.
   - This company is large-sized.
   - The company handles a huge amount of digital data and it depends on the customer.
   - The clients are international.
   - The security threats faced by the company depends on the customer it handles.
   - The security control placed by the company depends on the client it handles. The company sets up infrastructure that has to be compliant with the customer requirement. For example, the client requires encrypted laptops for confidentiality, the client will only communicate using VPNs, etc.
   - There is a CISO in place.
   - CISO is bound to the work within limits and is restricted to be compliant with the clients.
   - The table-top exercises are not applicable since the company setups infrastructure as per the client requirements.
   - Not applicable.

7. Company T7
   - The company an international bank from the Finance Industry.

- The company is large-sized.
- The company handles a huge amount of digital as well as sensitive data.
- The clients are international.
- The company faces huge security threats due to involvement with investment firms and the stock market.
- The company provides huge importance to security and has several important security controls in place and several compliances including Financial Compliance.
- There is a CISO in place.
- The CISO is provided strong power to take the required actions, as the whole company needs to compliant and ready for regulatory inspections.
- Basic table-top exercises are conducted, where there are security discussions among the different managers of the same level that report to the CISO.
- Advanced table-top exercises are conducted minimally for setup.

8. Company B8
    - The company is from the Medical Industry.
    - The company is small-sized.
    - The company handles simulation data that is being tested inside the facility by researchers. The data stays internal to the company and is not exposed.
    - The clients are not international.
    - The company does not face many security threats.
    - The company has minimum security controls and compliances in place.
    - There is no CISO in place.
    - Not applicable.
    - Basic table-top exercise is not being conducted.

- Not applicable.

The above information in a glance is the following:

The columns represent each survey answers for the 10 survey questions mentioned before and the rows represent each company.

Company/ Survey Answers	1	2	3	4	5	6	7	8	9	10
T1	IT	Small	Large	Non-international	No Security Breaches	Minimum	N	NA	N	NA
L2	Medical	Medium	Large	Non-international	Security Breaches	Moderate	N	Weak	Y	N
K3	Transport	Large	Large	International	Security Breaches	Maximum	Y	Strong	Y	Y
Q4	Finance	Large	Large	International	Security Breaches	Maximum	Y	Strong	Y	Y
N5	Manufacturing	Large	Less	International	Security Breaches	Minimum	N	Strong	Y	Y
U6	IT	Large	Large	International	Security Breaches	Relative	Y	Weak	N	N
T7	Finance	Large	Large	International	Security Breaches	Maximum	Y	Strong	Y	Y
B8	Medical	Small	Less	Non-international	No Security Breaches	Minimum	N	NA	N	NA

IV. RESULTS AND DISCUSSIONS

A. Conclusion

By going through the survey responses, we can understand why different companies from various industries place security controls and whether they were able to improve the these controls by following cybersecurity table-top exercises.

From the survey we can conclude the business maturity for each company as discussed below:

1. Based on size of the company:
   - A company that is small, that is not popular, doesn't handle sensitive information or doesn't expose its IT infrastructure can be seen to not place appropriate security controls. These companies don't get any security breaches and don't plan to expand, hence they will not plan on placing a security officer nor provide any significance for cybersecurity. From the survey, we can see that companies T1 and B8 fall under this category. These companies tend to have the business maturity "Responders" since they are reactive and crisis-driven. These companies will not know when they will get hacked or if they were already hacked.
   - A company that is medium-sized or large-sized will be popular and well-known. These companies will be facing security breaches. If the company was previously having the maturity group "Responders", then either the company can go bankrupt or will have to jump to the business maturity group "Protectors" or "Influencers". In the survey, it is observed that the companies L2 and N5 revised their plans: if any chief officers were against security investments before the breach, the decisions for security investments were supported completely after the breach since it is realized as a necessity for moving forward. It can be also observed that several table-top exercises from basic table-top

exercises to advanced table-top exercises were performed for the company to improve its business maturity.

2. Based on data handled by the company with security threats:
    - A company from any industry that handles a limited amount of sensitive digital data, will not be focusing on maintaining a strong cybersecurity officer for ensuring cybersecurity for the company. But since these companies are popular and face a lot of security threats, these companies need to have strong cybersecurity in place. For solving this issue, a company can hire 3rd party to provide security as a service or maintain strong client-compliance. From the survey, we can see that companies N5 and U6 fall into this category. These companies tend to have the business maturity “Protectors” since they are compliance-driven.
    - A company from any industries that handle international affairs will be required to be compliant to the international standard, which implies that these companies have a mature process in place. Being exposed and the need for maximum security, forces the companies to place a strong CISO to ensure company’s cybersecurity. From the survey, we can see that companies K3, Q4, and T7 fall into this category. These companies tend to have the business maturity “Influencers” since they are risk-driven.

B. Implications

From the conclusions we can derive at the following implications:

- Many companies from different industries including the IT industry does not provide significance to cybersecurity.
- Companies that are in the “Influencers” Business Maturity in the survey are present in that state mainly because of the compliance the company had to follow as well as because of the highly sensitive nature of the data that the company is handling. These companies cannot start from a lower maturity state and start off as a Influencer because

of the same reasons. These company statistics does not help with establishing the required correlation.

- The companies that do want to improve their business maturity for many reasons including client compliance, regulations, or security breaches do follow at least a basic table-top exercise for improvement. The companies that expand without cybersecurity even with several breaches tend to shut down at the end.
- Cybersecurity table-top exercises do help in improving business maturity. But companies that want to mature do not focus on being “Influencers”, they only want to be appropriately compliant with a minimum investment in security through these exercises. Hence these companies stop improving after reaching the business maturity of “Protectors”.

In summary, we can find that a company can raise their maturity from Responders to Protectors through cybersecurity table-top exercises; these exercises are adopted due to its cost-effectiveness and efficiency. This drive to improve business maturity will happen when 2 condition are met by the company:

1. The company has sufficient funds to invest in security infrastructure.
2. The company is planning on expanding its business and is at risk of security breaches.

This is so that company can be client compliant, regulatory compliant, and also wants to be protected from minimum security breaches. These companies at the same time do not plan to jump to the ideal maturity state “Influencers” since the company is satisfied by being compliant-driven as it only requires minimum security investment for maximum profit. Hence we can establish that there is a correlation between the business maturity and cybersecurity table-top exercises since companies were able to jump from “Responders” to “Protectors” with these iterative practice.

C. Future Work

This survey only captures 8 specific companies from various industries to understand the correlation of business maturity and cybersecurity table-top exercises[2]. This survey can be expanded, for example considering the exact ROSI or ROI that the company uses with respect to security other investments. The survey can also be applied to more companies to understand and infer a more accurate description on how companies consider cybersecurity and whether cybersecurity table-top exercises can raise any company from the lowest maturity state to the highest maturity state.

REFERENCES

1. Brilingaite, Agne, Linas Bukauskas, Virgilijus Krinickij, and Eduardas Kutka. 2017. "Environment for Cybersecurity Tabletop Exercises."Academic Conferences and Publishing International Limited, 17.

2. Caelli, William J., Lam-For Kwok, and Dennis Longley. 2010. "A Business Continuity Management Simulator."Springer New York LLC, 10. doi:10.1007/978-3-642-15257-3_2. http://dx.doi.org/10.1007/978-3-642-15257-3_2.

3. Edzen, Svante. 2014. "Table-Top Exercises for Emergency Management: Tame Solutions for Wicked Problems."IEEE Computer Society, 14. doi:10.1109/HICSS.2014.250. http://dx.doi.org/10.1109/HICSS.2014.250.

[2] Only 8 out of the several security professionals from different companies were willing to provide this information.

4. Ghormley, Yvette. 2008. "Business Continuity and Disaster Recovery Plans." In , 308-319: IGI Global. doi:10.4018/978-1-59904-855-0.ch026. http://dx.doi.org/10.4018/978-1-59904-855-0.ch026.

5. Hein, Carl, Mike Stebnisky, and Ambrose Kam. 2014. "Network Oriented Cyber Security Model (NOCS-M)."SISO - Simulation Interoperability Standards Organization, 14.

6. Krebs on Security. "What’s Your Security Maturity Level?", https://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/.

7. Pearson, R. M. 2011. "Disaster Preparedness through Simulation Training." *Journal / American Water Works Association* 103 (1): 30-32.

8. Subau, Georgiana, Livia Rou, and Ion Bdoi. 2017. "Modeling and Simulation Architecture for Training in Cyber Defence Education."Institute of Electrical and Electronics Engineers Inc, 17. doi:10.1109/ECAI.2017.8166396. http://dx.doi.org/10.1109/ECAI.2017.8166396.