**EMCS2600: The Future of Cybersecurity: Technology and Policy**

Assignment: 2nd Short Response Paper for Modules 4-5 (Final)

Brian Russel Davis, brian\_davis@brown.edu

*Develop and justify a plan to respond to a serious penetration of your computing infrastructure assuming that it appears to have begun in the last few days. Explain and justify training that preceded the break-in and how playbooks will be consulted. Whom do you notify and when?*

Organizations need to be confident that their data, their infrastructure and most importantly their people are safe. When a computing infrastructure breach occurs it affects the organization in a multitude of ways, however, the greatest impact may be centered around the loss of trust. In order to shore up confidence in leadership, the computing infrastructure, and the people, the security council should prepare clear and regular communication to the organization coupled with proactive actions. Any serious breach should be treated as a crisis, not with the intention of triggering fear, but with the intention of setting in motion a prepared response that shows how the organization is synthesizing information and working to preempt any future damage or harm to its users, systems, and employees. We may not be able to overcome the emotion that people feel while experiencing the crisis, but we can acknowledge their emotions and respond with emotional intelligence when we find our selves in the midst of a crisis. Dealing with a breach like any other crisis is an exercise in resiliency. No one can plan for a breach or a crisis but you can be prepared to respond by fostering a culture that places an emphasis on readiness.

Being “Response Ready” during a breach means creating a culture that fosters the ability to:

1. Identify problems in real-time
2. Be action-oriented
3. Rely on mind-set and experience to formulate responses
4. Be strategically proactive instead of reactive

Once a breach has been identified the security council, a cross-functional team of security-minded individuals should work together to work through 5 distinct steps:

1. Anticipate … issues, problems, challenges.
2. Mitigate … against these problems, issues, and challenges.
3. Prepare … by setting up a crisis response team that formulates strategy.
4. Implement … new software, policies, and practices.
5. Monitor … the infrastructure using the new information gained from the breach.

In the anticipate step the team should think through all the parts of the business that will be affected by the breach, i.e. privacy implications, if the breach requires a report to the state, local or federal government, legal liability and most important how does the breach affect users and employees. What will customers expect, what fears will they have once the news gets out to the public, and how will the breach impact the organization’s relationships and reputation. Each one of the points mentioned may be a part of or trigger a domino effect. The security council should additionally categorize these concerns as short-term, mid-term and long-term according to their impacts, potential timelines and whether the concerns affect any thresholds. By thinking through these issues ( in parallel to taking action ) the team will make better decisions and have the ability to communicate in a more comprehensive way that demonstrates credibility. From this point forward, any actions taken by the organization should be paired with clear direct communication.

The mitigate step for this type of crisis starts mainly with the security team. Servers, routers, switches, desktops, laptops, printers, fax machines and anything connected to the network need to be reset and restored from back-up. Many times there is a fear that resetting hardware will result in data loss, and it might, but data few hours worth of data loss in most cases might be less consequential that dealing with an Advanced Persistent Threat.

Preparation, the next step, seems like a step that should have happened before the crisis, and it should. But, in crisis preparation is also important. A breach doesn’t just happen and get solved all in one day. A breach triggers a series of events that will involve weeks and maybe months of strategic responses. The organization should create a cross-functional crisis response team ( one that maybe includes the members of the security council ) that meets twice a day to discuss new developments and to craft communication. In some high stakes situations, a 24-hour crisis war room may need to be created.

Implementation of mid-term and long term mitigation should be the results of mitigation and preparation. Short mitigation like resetting the hardware should make way for mid-term mitigation like finding the source of the breach, patching vulnerable software, services or hardware and formulating new policies and practices so the same breach doesn’t happen again.

Monitoring should have been already taking place, however, in light of the new information derived from the breach forensic analysis, improved monitoring should be implemented to shore up the controls.

Responding to breach doesn’t have to be a business ending event. There is no written plan that can stop a business from experiencing a cyber attack. There is no playbook that can provide all the answers on what to do when a breach happens. Every organization will face different challenges depending on the nature of their business and the circumstances surrounding the breach. However, creating a team that is ready to respond to the crisis with a level-headed experience bred strategy is better than any static playbook.

#### Bibliography

Pearson, Christine M., and Judith A. Clair. "Reframing crisis management." Academy of management review 23.1 (1998): 59-76.

Goldberg, Ed. "Preventing a data breach from becoming a disaster." Journal of business continuity & emergency planning 6.4 (2013): 295-303.

Brown, Hart S. "After the data breach: Managing the crisis and mitigating the impact." Journal of business continuity & emergency planning 9.4 (2016): 317-328.

Ruefle, Robin, et al. "Computer security incident response team development and evolution." IEEE Security & Privacy 12.5 (2014): 16-26.

Lind, G. Ö. R. A. N. "Crisis exercises make for crisis readiness." SVERIGES RIKSBANK ECONOMIC REVIEW (2003): 5-24.