**EMCS2200: Global Cyber Challenges: Law, Policy, and Governance**

Post-Work: Industry Solutions

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

*After the board meeting, your CEO contacts you to inform you that the board agrees that the cyber threats you identified (in your pre-work brief) pose great risk to your industry. The board is also willing to allocate money in the budget to address these challenges.   
  
Your CEO now asks you to come up with three recommendations for what your organization should do in the face of these cyber challenges. Think of ways your company could minimize disruptions of its operations and prepare for cyber challenges.*

**Live, Regular, Mandatory Training**

It’s a well observed fact that the most of vulnerable parts of our organizations are the people. One podcaster on the Cyberwire said “a castle with a moat doesn’t mean much when one of the people inside let the drawbridge down”. Live training, where people can engage with the instructors, is important not only to ensure the material is received, but to offer a forum where people can have their questions answered. The objective of the training should be teach and not lecture, engage and not present. The most valuable asset in terms of security is well trained staff. Here is a list of the most important topics:

*Strategies for Creating Strong Passwords*

*Strategies for Protecting Sensitive PII*

*Understanding When and How to Report Suspicious Activity*

Armed with good common sense and basic knowledge about CyberSecurity hygiene, the people in most organizations can see and stop over 90% of CyberAttacks.

**Read Industry Based Threat Assessments and Software Patch Management**

Intrusions are reported, found and dissected by experts on a daily basis. Not only that, but threat groups often repeat attacks month after month, sometimes continuing for years before they become inactive. Russian vote meddling was practiced in the Ukraine before it came to the US. We have information on how and who before it ever came to our shores. Having a keen sense of the types of attacks that may be targeting the company based on the industry will help the security team understand where to focus their attention. Services like “Record Future’s” Daily Threat Assessment briefings provide real time information of the types of schemes threat actors are employing and provides an opportunity for security teams to interrupt the kill chain in the early stages.

A list of threat actors and their malicious activity is usually accompanied by a list of vulnerabilities that emanate from unpatched vulnerable software. Engineering Teams and Security Teams need a well defined SLA ( Service Level Agreement ) in place so they can respond to vulnerability reports in timely fashion and triple verify every patch, hotfix and upgrade. Without an SLA, Engineering and Security may not cooperate effectively or efficiently, leaving the organization and the user open to attacks that may have been easily averted.

**AI Based Antivirus, Channel Monitoring and Endpoint Protection**

Traditional virus protection that relies on malware definitions provides pretty weak protection these days, especially for industries that have a lot of valuable data. Intruders rarely depend on one piece of malware to break in. Furthermore almost all modern day kill chains include disabling the antivirus and gaining access to elevated privileges ( ie running actions and commands as a root user ). Instead of looking for a predefined piece of malicious software, virus protection powered by artificial intelligence and machine learning look for patterns outside the norm. This includes data moving through endpoints at irregular times or in irregular quantities; Users logging in from strange locations and elevating their privileges, or the privileges of others outside of the normal domains. These types of actions should be flagged in a dashboard where the security team can review them, and better yet the administrator should be able to define automated responses, so the security team is not overwhelmed with false positives. The dashboard should also be customizable so the security team can define what’s normal and what’s abnormal activity. There are many companies that offer this type of end to end protection. Although it’s not foolproof, when layered with all the other measures it does provide a high level of security above and beyond traditional means.

**Conclusion**

Three points summarize the approach here: Train, Patch, Monitor.

***Train*** the users to practice good CyberSecurity hygiene, spot threats and report issues.

***Patch*** vulnerable software in agreement with the Engineering Department.

***Monitor*** the activity on the network with state-of-the-art ML and AI tools.