#### Briefing Your “CEO"

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

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

Brown School of Professional Studies

***Background***

Briefing a CEO, President or Head of any organization is a difficult task. Much of the briefing depends on the nature of the business the organization engages in, the types of systems and data the organization is trying to protect and the size of the organization. Working for an organization like mine ( NASA ) adds many layers of concerns to any plan to address CyberSecurity.

##### Targets : People and Things that Need to Be Protected

***Data***

Three types data need to be protected :

* Data at Rest : These are general databases, logs or other data that
* Data in Transit
* Data being Used

***People***

People have three different types of aspects that need to be secured, verified and monitored.

* Identity : We need to make sure we know who is accessing the systems. This includes new employee, current employees,

***Physical Locations and Assets***

Before the was computing it was obvious and natural to secure locations. This doesn’t change that much in the age of

##### Strategy : Planning and Preparing for the Worst

What do we do when … ? Having internal agreement on what to do when something bad happens is just as important as trying to keep it from happening.

**Business Continuity Plans**

If the systems go down what is the plan? How do we serve the users, mitigate against snowballing destruction and safely put things back together?

**HR Policies**

How do you deal with someone who breaks the rules? This should not be “made up” on the spot.

##### Defensive Game Plan

**Managing Vulnerabilities**

Knowing the weakness is of paramount importance. This becomes even more important with multiple platforms, devices and locations. For NASA the surface for an attack is broad and wide. Managing these vectors is not just the job of the security team, it’s the job of every single employee.

**Known Threats**

Focusing on the most recent malware strains in a natural place to start for the layperson. But this is almost last, because there are so many threats, in order to be effective we need to understand our own infrastructure first to make sure we are focusing on the right things.

* Malware
* Data Exfiltration
* Living of The Land Attacks
* Phishing

**Known Actors**

Threats do not appear out of thin air. Unlike natural disasters Cyber Threats are made by someone or some group of people. Understanding the motivations of these persons helps use stay one step ahead of them.

* Skids : Script Kiddies
* Criminals
* State Actors :
* The US Government

##### Dealing with Law Enforcement

Making a decision of how deal with law enforcement is a important discussion that should happen before a crisis. Case in point Apple and the San Bernardino Terrorist iPhone, Google and the NSA tapping the transatlantic cables. Even NASA might have an obligation to keep information out of the sight of law enforcement. Here are some scenarios to consider :

* Verifying the privacy of all the astronauts on the International Space Station
* Ensuring that satellite data resources are being used only by NASA scientist
* Protecting the possible dangerous materials from use in non scientific actions