Student Perception of Cyber Resilience vs Prevention

Frank H. Katz

Georgia Southern University

Preventing Every Attack

- Is that really possible?
- Not according to Mr. Dan Greer, called the “elder statesman and philosopher of Cybersecurity”
- He is a fervent believer in analog backup ***systems***, not just backups.
- Rather than place emphasis on preventing attacks, Mr. Greer is “determined to figure out how to recover quickly and limit an attack’s damage”
- In the book **Sandworm**, Greer stated to author Andy Greenberg that “It may be time to no longer invest further in lengthening time between failures, but instead on shortening the meantime to repair”

Discussion Question

- Given to the students – requiring them to read an excerpt from Andy Greenberg's book, and then either agree, disagree, or suggest another opinion on Greer's premise about what could be called Cyber Resiliency
- Students had to back up their conclusion with reasoning based on a source search analysis & evaluation of those sources

Definition of Cyber Resilience

- A relatively new term, related to ability of organizations to recover quickly from deliberate attacks; or incidents involving the use of information and communication technologies
- Its aim is to strengthen cybersecurity practices to achieve an approach that goes beyond attack prevention
- As a result, organizations can develop strategies that enable the rapid recovery of their essential services; by reducing the magnitude of the impact of any incident or attack

The Survey

- Was based on a graded exercise in three consecutive terms of IT 3530, Fundamentals of Information Systems Security
- Students were graded in terms of their ability to determine a response to a situation or scenario and defend their conclusion.
- Grades were scored by a standard discussion rubric which scored the:
  - Logic behind their answers
  - Completeness of their answers
  - Participation (i.e., responses to other students)
  - Reference to sources
  - Mechanics (spelling, grammar, & composition of posts)

Results, over three terms

Term	Agreed w/Greer	Disagreed w/Greer	Prevention & Resilience Treated Equally
Summer 2020	22	5	4
Fall 2020	10	1	13
Spring 2021	24	1	7
Total	56	8	32
As Percent	58.3%	8.3%	33.3%

This question has been asked in each subsequent term of IT 3530, the data from those terms is not included

Sample Student Posts

Agreed with Greer

- A student gave an analogy of her greenhouse
- Despite all her efforts to keep out pests from the plants she is growing, she could not keep out the small white lacewing.
- Although not harmful to the plants, this pest brings with it “traces of mycelium and fungus that thrives off the unprotected plants.”
- She has since stopped “using all my time and resources to defeat them, but rather now focus on their recovery and overall resilience.”
- Consistent monitoring of the leaves, stems and ambient conditions allows her to recognize & resolve issues before they destroy the entire plant

Even-Handed Approach

- 33% of the students felt that organizations should take an even-handed approach between preventing an attack and correction after an attack
- Student F wrote: “I believe that MTTF (prevention) and MTTR (resilience) should both be emphasized equally because I think that they are dependent on each other.”
  - “Focusing on MTTF means that the company works to make sure that every security measure is in place before an attack takes place.”
  - “Focusing on MTTR means focusing on putting a plan together to repair the system after an attack occurs and bring everything back up as quickly as possible. However, MTTR would depend on how much damage was caused by the attack, which could be minimal if equal time is taken to focus on MTTF.”

Disagreed With Greer

- This student's reason for emphasizing prevention over resilience was convincing
- "I do not think this emphasis should come at the expense of putting resources into effectively preventing attacks. While getting systems back online is crucial, it does not roll back some of the effects that happen during a cyberattack."
- Some cyberattacks leak data into the public – example given was the Sony Pictures hack.
- "Even with a low 'mean time to repair', this information cannot be magically wiped from public memory. In conclusion, while resilience is a noble goal, attack prevention is still the most effective option to limit damage."

Primary Method Proposed by Students to Promote Resilience

- ***BACKUPS*** – fall more in the realm of recovering from an attack than preventing one
- ***Immutable*** backups:
  - "Immutability refers to the property, which, once applied or given to an object, prohibits any subsequent changes to that object. In file systems, immutability refers to preventing any changes or modifications to the contents of the file".
  - "Once you have stored an immutable backup it cannot be altered or changed, and this is particularly important when it comes to malware or ransomware. If your backup is immutable then it is impervious to new ransomware infections and/or deletion."

Conclusion

- While most students felt Mr. Greer was correct, this discussion should not be an either-or situation.
- Rather than take Mr. Greer's position, organizations should consider raising their efforts at cyber resilience to the level of their cyber prevention efforts & treat both equally