Oct 30th, 2:30 PM - 3:00 PM

Resilience vs. Prevention. Which is the Better Cybersecurity Practice?

Frank Katz
Georgia Southern University, fkatz@georgiasouthern.edu

Abstract

Students in multiple cohorts of our 3000 level Fundamentals of Information Systems Security course were given a discussion question where they had to either agree or disagree with the premise that given all the constant threats to our systems, we should dedicate more of our efforts to quickly repairing the damage of an attack rather than dedicate more of our time and energies to preventing such attacks. They were required to give their reasoning and provide sources to back up their analysis of his comment.

This paper will describe and explain the concept of cyber resiliency. It will then evaluate the responses of the students and their sources to determine if they felt that emphasizing bringing systems back quickly over prevention is a cybersecurity practice that more organizations should consider, as well as give some recommendations about both cyber prevention and cyber resiliency methods.

Location

Online Zoom Session

Disciplines

Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

Student participation and responses to Discussion Questions are an integral part of our university's Cybersecurity curriculum. The purpose of these exercises is not only for students to think through a problem or scenario and come up with a possible solution, but for them to respond to each other to challenge what might be pre-conceived or commonly held ideas and concepts regarding Cybersecurity. One of the most widely held dogmas in Cybersecurity is that practitioners should make the attempt to prevent every possible attack on an organization. But is that really possible?

In the final chapter of his book, **Sandworm**, A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, author Andy Greenberg interviewed Mr. Dan Greer, a well-known Cybersecurity expert. Because of his fears of a Cyber meltdown, Mr. Greer is a fervent believer in analog backup systems (not just backups themselves). He also posited an interesting concept regarding the prevention of cyberattacks. Rather than place our emphasis on preventing attacks, Greenberg wrote that "he's (Mr. Greer) determined to figure out how to recover quickly and limit its damage." Mr. Greer was quoted "It may be time to no longer invest further in lengthening time between failures, but instead on shortening mean time to repair." (Greenberg, 2019, p. 305)

The students were given a discussion question on this topic, requiring them to read the excerpt from Mr. Greenberg's book, and then either agree, disagree, or suggest another opinion on Mr. Greer's premise about what could be called Cybersecurity or Cyber Resiliency. Of course, the students could not just state that they agreed or disagreed with his opinion, they had to back up their own conclusion with reasoning based on their own source search analysis and evaluation of those sources.

This paper does not intend to discuss the overall or statistical merits of the students' *grades* on the question. Rather it intends to look at the data of the responses in terms of student agreement or disagreement with Mr. Greer's principle of Cyber Resiliency. It will discuss some of the comments made by the students and the sources they used to support their conclusions. Based on this information, a conclusion will be drawn as to whether the opinions of the students make sense in today's Cybersecurity environment, and recommendations will be made of methods of promoting resilience in an organization.

WHAT IS CYBER RESILIENCE?

What is cyber resilience? "Cyber-resilience is a relatively new term, related to the ability of organizations to recover quickly from deliberate attacks; or incidents involving the use of information and communication technologies. The aim of

cyber-resilience 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." (Cyber-resilience: All you need to know, 2018)

That article pointed out several benefits of adopting cyber resilience as a strategy: giving the company a competitive advantage; reducing the economic impact of a business disruption; and improving risk management. As the student who cited it wrote, "it (cyber resilience) allows a business to return to normal operating procedures much faster and allows a minimal delay of operations for customers. This ties into the second advantage. The shorter downtime decreases the financial impact of an attack, along with decreasing the overall severity of a breach. These measures are what bring risk management, along with a business continuity plan, full circle, limiting the effects of a breach." (Student A, 2020)

Oxford defines resilience as "The quality or fact of being able to recover quickly or easily from, or resist being affected by, a misfortune, shock, illness, etc.; robustness; adaptability." (Oxford, 2021) Consequently, "resilience assessment starts with an assumption that the system is affected and functionality impaired, with emphasis placed on speed of system recovery." Solid, tested business continuity and recovery practices and methods are crucial to promoting cyber resilience in an organization. However, cyber resilience doesn't just relate to an organization's cybersecurity practices, "it also refers to the resilience property of a system or network; sometimes we also use the term as referring to the features or components of the system that enable cyber resilience." Thus, cyber resilience also relates to the computer system itself. "Cyber resilience ensures that system recovery occurs by considering the interconnected hardware, software, and sensing components of cyber infrastructure cyber resilience refers to the system's ability to recover or regenerate its performance after a cyber-attack produces a degradation to its performance." (Kott, Linkov,2019, p 4)

Thus cyber resilience can be defined as the ability of a system, its hardware, software, its data, its network, its people, and its business to recover from the debilitating effects of a cyber-attack.

THE SURVEY, STUDENT RESPONSE DATA, AND STUDENT RESPONSES

The discussion question was included as a graded exercise in three consecutive terms of our 3000-level course, IT 3530, entitled Fundamentals of Information Systems Security: Summer 2020; Fall 2020; and Spring 2021 (two sections). As stated above in the introduction to this paper, students were graded in terms of their

ability to determine a response to a situation or scenario and defend their conclusion. The grades were scored by way of a standard discussion question rubric which scores the logic behind their answers, the completeness of their answers, and their reference to sources used against four categories: Planning (their response to the question, their original post); Participation (responses to other students' posts); Reflection (a summary of their learning based on their original and response posts); and Mechanics (spelling, grammar, and composition of their posts).

With that in mind, there were two constraints in place for this discussion question:

- It was only posed to the same course, IT 3530. For example, it was not posed to students in our Network Security course, of which IT 3530 is a prerequisite.
- It was always given to the students during the course's module on Risk, Response, and Recovery, i.e., Risk Assessment methods.

After evaluating what each student wrote, the following was determined:

- Summer 2020 class: 31 students. 22 agreed with Greer; five disagreed; and four felt that both concepts, prevention, and resilience, should be treated by organizations equally.
- Fall 2020 class: 24 students. Ten agreed with Greer; one disagreed; and thirteen felt that both concepts should be treated equally.
- Spring 2021 class: 41 students in two sections. 24 agreed with Greer, one disagreed, and seven felt that both concepts should be treated equally.
- In total, 56 students, or 58.3% of the total, agreed with Greer; 8 students, or 8.3% of the total, disagreed with his premise; and 32 students, or 33.3% of the total, felt that the two concepts of prevention and resilience should be handled equally by an organization.

Students Agreeing with Greer

Very early in the textbook used by my 3000 level Fundamentals of Information Systems Security course, the Mean Time to Failure (MTTF) and the Mean Time to Repair (MTTR) are defined. In Cybersecurity terms, MTTF would be a failure of defenses to prevent an attack, and MTTR could be considered repairing systems, or bringing them "back up quickly" after an attack. (Kim & Solomon, 2018, p. 18). In effect, MTTR is a measurement of the capabilities of an organization – how quickly can the employees of the organization use the tools they possess to recover from system failure.

Student B provided a defense of Mr. Greer's premise by using an analogy given in "DevOps Metric: Mean Time to Recovery," that organizations would be better served by placing a higher priority on MTTR vs MTTF. In this analogy, perception is paramount, especially the perception of the organization by its customers. "If Amazon.com was down once every three years, but it took them a whole day to recover, consumers won't care that the issue has not happened for three years. All that will be talked about is the long recovery time. But if Amazon.com was down for 3 times a day for less than one second, it would barely be noticeable." ("DevOps Metric," 2016)

Organizations that use DevOps and its agile development concept would benefit from placing a higher priority on MTTR. As the article states, "if DevOps is about build, measure learn, and fast feedback cycles, then it should become an undeniable truth that "whatever can go wrong, will go wrong," and if you embrace that mantra, you can start measuring "mean time to recovery" instead." Consequently, prioritizing, or incentivizing MTTR allows the organization to build "faster feedback mechanisms into the pipeline so that a fix can go through the pipeline faster; add and start using better logging and monitoring systems; and make it just as easy and fast to deploy a fix as it is to roll back a version." This approach would benefit organizations where rolling back versions of software or restoring multiple version-controlled sets of data would be extremely onerous after an attack. ("DevOps Metric," 2016)

Student C used the analogy of her greenhouse, which for that student is a leisure activity. 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 me to recognize and resolve any issues that arise before they destroy the entire plant. These observations are what I believe have driven Dan Greer to also focus on resolution to failure and consistent reevaluation of systems to allow them to evolve to protect themselves." (Student C, 2021) She described a situation where it appears that one of the driving forces behind focusing on resilience as measured by MTTR is that organizations may just accept that they are going to be attacked. Therefore, they conclude that it is better to prioritize recovery by constantly monitoring their systems to rebound from an attack more quickly.

Student D suggested that "in an age when massive corporate security breaches have become part of daily life the only solution is to make data more resilient. The FBI's 2019 Internet Crime Report (2019 Internet Crime Report of IC3, 2019) shows that almost $53.4 million was reported lost due to corporate data breaches. Clearly,

companies have a lot to lose in the event of a breach, but I think too much focus is placed on prevention, and not enough on recovery. I think more robust recovery systems could help to reduce a company's risk in the event of a breach." (Student D, 2020) This concern about the cost to an organization due to downtime after an attack was echoed by Student E. He agreed with Greer because of this (Student E, 2021), posting data from the blog The 20, that according to Gartner, "the average cost of IT downtime is $5,600 per minute. Because there are so many differences in how businesses operate, downtime, at the low end, can be as much as $140,000 per hour, $300,000 per hour on average, and as much as $540,000 per hour at the higher end." (The Cost of IT Downtime, 2021) While this data from Gartner is somewhat old, the cost of downtime could be a major reason why businesses would choose resilience over prevention.

Students Favoring an Even-Handed Approach

As shown above in the statistics, 33% of the student respondents felt that organizations should take an even-handed approach between preventing an attack and correction after an attack. One of the best posts in favor of this approach came from Student F, who wrote "I believe that MTTF and MTTR 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. Doing this could mean the difference between catching an intrusion as soon as it happens or having a major breach occur that could cause major damage to systems or company reputation. 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. Emphasizing the importance of both MTTF and MTTR allows a company to be more proactive instead of reactive." (Student F, 2021) This student used a recent article from Forbes to support his or her position, that "it may take businesses days, if not weeks, to identify security anomalies, suspicious network activity or hacking attempts. An average company spends 197 days to identify and 69 days to contain a security breach." (Yoo, 2021) Given these statistics, the need to promote resilience in an organization cannot be overstated.

Students Disagreeing with Greer

Representative of the 8.3% of the students who disagreed with Mr. Greer's premise was this from Student G: "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. For example, in the wake of NotPetya, quite a bit of produce spoiled because the computers handling transportation infrastructure were offline. While better resilience would have kept as much of it from spoiling, some waste still would have occurred with any "mean time to repair" . . . some cyberattacks leak data into the public. One such attack 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." (Student G, 2021)

This student's point is well-taken, as information once leaked to the public cannot be "unseen". However, as evidenced by the categorized student response data, a plurality of the students felt that, as a minimum, both resilience and prevention should be performed equally, and a majority felt that resilience is slightly more important.

METHODS TO PROMOTE BOTH PREVENTION AND RESILIENCE

The discussion question itself only asked students whether they agreed, disagreed, or neither agreed or disagreed with Mr. Greer's position, and why. A shortfall of the question itself is that it did not ask for the students to provide specific methods to prevent or recover from a cyber-attack. Nonetheless, multiple students did provide some methods for both.

In terms of prevention, many students stated that since so many attacks are a result of people making mistakes, Security Education, Training, and Awareness, or SETA programs would be invaluable to prevent attacks. Employees should not only know proper password creation methods but be able to recognize when an attack is possibly and probably underway. Several mentioned the use of technical methods such firewalls to prevent dangerous packets from entering a network and the use of VPNs to ensure that persons entering a network were properly authenticated.

Nonetheless, no matter how much technology we employ to prevent attacks, we cannot remove people from the system. People don't practice good cyberhygiene, falling for phishing attacks, willingly giving up their credentials to attackers. People ARE the "weakest link". It is why the Colonial Pipeline Company was hit by one of the most notorious ransomware attacks in May 2021. (Vishwanath, 2021) It is why the Oldsmar, FL water treatment facility was hacked by an attacker who tried to raise the level of lye in the plant's underground water reservoir in February 2021. (Collier, 2021). Using the same password on multiple systems; not using strong passwords; never changing passwords; and most egregious for system and security administrators, leaving

the accounts of former employees on a system. All of these are mistakes that can be prevented by training and educating users and security personnel alike. (Hunter, 2021)

Several students mentioned using backups – these fall more in the realm of recovering from an attack than preventing one. And one backup methodology, more than others, would be instrumental in recovering from an attack – what is known as an "immutable backup." "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". (Tucek, et al, 2005) "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. In addition, some cloud services will also offer deletion protection. If a backup set is deleted by the backup client, the file is moved to a 'trash' area for a predefined period before actually being fully deleted. This enables the quick recovery of deleted backup sets by the cloud provider". (Young, 2021)

Immutable backups are often set on timers, so that the backup is unchangeable for a given period, such as one day, but more likely for one week. Using versioning to create a full immutable backup on Monday, then Tuesday, etc. is one method of doing this. Even though that would require only the most recent backup to restore a system, it would require a lot of storage. A more reasonable method would be performing one full immutable backup, for example, on Sunday night, and then one immutable differential backup each subsequent day of the week. Of all the possible methods of promoting resilience, using immutable backups may provide the greatest benefit. It ensures that a system can be rapidly restored in case of an attack.

CONCLUSION: THE WORLD WE LIVE IN

In 2021 to-date we have seen multiple security breaches, some of which have reached national and international exposure, such as the ransomware attack against the Colonial Pipeline Company. Others have only been made public locally, such as the ransomware attack against Savannah's St. Joseph's – Candler Hospitals and health system. There is no denying that as these attacks become more frequent, and the ransom demands increase, the discussion of whether we, as cybersecurity professionals, should emphasize prevention or resilience is going to continue.

While most of the student respondents felt that Mr. Greer was correct – that promoting resilience after a cyber-attack is important, a smaller plurality felt that both prevention and resiliency should be treated equally by organizations. Consequently, the discussion mentioned above 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 and treat both equally.

REFERENCES

2019 Internet Crime Report of IC3 (n.d.) Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

Collier, Kevin (2021, February 9). Lye-poisoning attack in Florida shows cybersecurity gaps in water systems. Retrieved from https://www.nbcnews.com/tech/security/lye-poisoning-attack-florida-shows-cybersecurity-gaps-water-systems-n1257173

Cyber-resilience: All you need to know about this security approach. (2018, August 3). Retrieved from https://www.gb-advisors.com/cyber-resilience-security-approach/

DevOps Metric: Mean Time to Recovery (MTTR) Definition and Reasoning (2016, October 20). Retrieved from https://pipelinedriven.org/article/devops-metric-mean-time-to-recovery-mttr-definition-and-reasoning

Greenberg, Andy (2019), *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (p. 305). New York, NY: Doubleday

Hunter, T. (2021, July 8). Don't be THAT Employee: How to Avoid Ransomware Attacks at Work. Retrieved from https://www.washingtonpost.com/technology/2021/07/08/ransomware-attack-avoid/

Kim, D., & Solomon, M. (2018). *Fundamentals of Information Systems Security* (3rd ed., p.18). Burlington, MA: Jones & Bartlett Learning.

Linkov I., Kott A. (2019) Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: Kott A., Linkov I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham.

Oxford English Dictionary (n.d.) Retrieved from https://www.oed.com/view/Entry/163619?redirectedFrom=resilience#eid

Student A, July 13, 2020, DQ4 – Failure vs. Repair, https://georgiasouthern.desire2learn.com/d2l/home/552997

Student B, July 13, 2020, DQ4 – Failure vs. Repair, https://georgiasouthern.desire2learn.com/d2l/home/552997

Student C, July 13, 2020, DQ4 – Failure vs. Repair, https://georgiasouthern.desire2learn.com/d2l/home/552997

Student D, October 16, 2020, Module 08 Discussion – Risk Assessment, https://georgiasouthern.desire2learn.com/d2l/home/571621

Student E, March 13, 2021, Module 08 - Resilience vs. Prevention, https://georgiasouthern.desire2learn.com/d2l/home/607884

Student F, March 10, 2021, Module 08 - Resilience vs. Prevention, https://go.view.usg.edu/d2l/home/2220322

Student G, March 13, 2021, Module 08 - Resilience vs. Prevention, https://georgiasouthern.desire2learn.com/d2l/home/607884

The Cost of IT Downtime. (2021, July 14). Retrieved from https://www.the20.com/blog/the-cost-of-it-downtime

Tucek, J., Stanton, P., Haubert, E., Hasan, R., Brumbaugh, L. and Yurcik,W., "Trade-offs in protecting storage: a meta-data comparison of cryptographic, backup/versioning, immutable/tamper-proof, and redundant storage solutions," 22nd IEEE / 13th NASA Goddard Conference on Mass Storage Systems and Technologies (MSST'05), 2005, pp. 329-340

Vishwanath, Arun (2021, May 13). The Failures that Led to the Colonial Pipeline Ransomware Attack. Retrieved from https://www.cnn.com/2021/05/13/opinions/colonial-pipeline-ransomware-attack-was-stoppable-vishwanath/index.html

Yoo, G. The Importance of Time and Speed in Cybersecurity (January 22, 2021). Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/01/22/the-importance-of-time-and-speed-in-cybersecurity/?sh=9c4640636a92

Young, Stephen, “When ransomware strikes, what's your recovery plan?” Network Security, Volume 2021, Issue 7, Pages 16-19. Retrieved from https://www.sciencedirect.com/science/article/pii/S1353485821000775