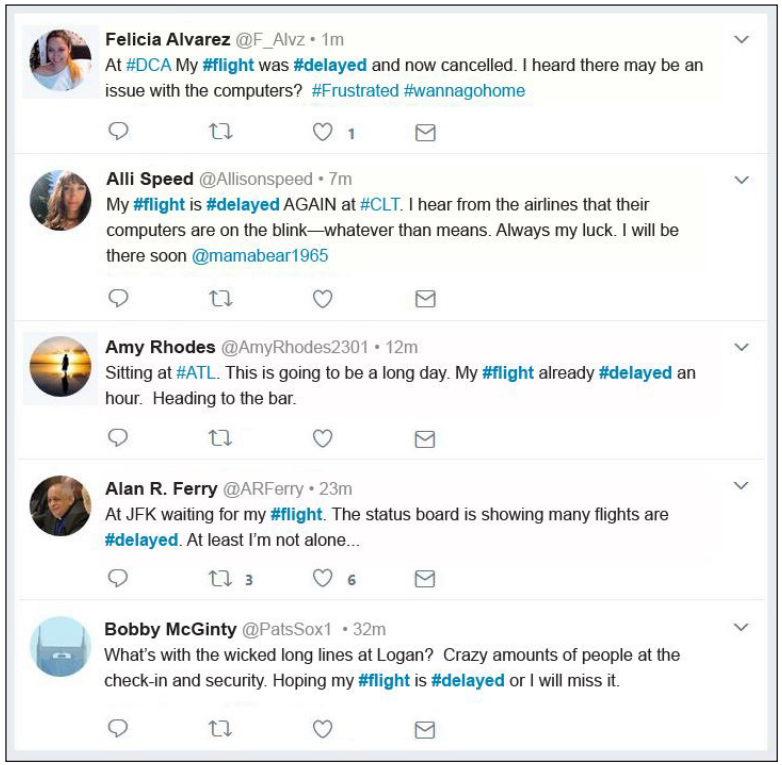
Inject 1.1 - November 19, 4:00 PM

ABC Corporation (ABC) stock share closes on NYSE at $19.70.

Inject 1.2 - November 20, 6:00 AM

Passengers at JFK, Philadelphia, Miami, Atlanta, Charlotte, Washington DC, Providence and Boston airports begin tweeting that airline delays are occurring along the East Coast due to alleged computer problems at baggage and passenger screening areas. Little is known at this time but it is worth watching.



*55 additional similar tweets.

Inject 1.3 - November 20, 6:15 AM

TSA calls ABC to report its IT systems are down across multiple sites and they are assessing the situation.

US Customs and Border Protection calls ABC, reporting IT problems on their network is affecting border screening.

Inject 1.4 - November 20, 7:00 AM

ABC Crisis Management Team (CMT) convenes to discuss problems reported by TSA and US Customs and Border Protection.

Discussion:

1. What are your immediate concerns?
2. What actions are you considering based on the roles and responsibilities defined in your Incident Response Plan?
3. How do you deal with information provided by your customers?

Inject 2.1 - November 20, 8:00 AM

ABC Federal Systems HelpDesk reports they are being inundated with calls from federal government clients (DoD, DHS, USDA, IRS, etc.) complaining that their respective IT systems are down across multiple sites. They are asking for updates on bringing the systems back online.

Inject 2.2 - November 20, 8:15 AM

ABC IT reports that it appears that the Federal Systems' network has been hit with a cyber attack. This is a good news-bad news situation. The bad news it that all clients' networks within the ABC Federal System network are affected. But the good news is that the use of micro segmentation using the ABC Stealth product has limited the attack to the ABC Federal network. Other ABC networks are not affected.

Discussions:

1. What are your immediate concerns now?
2. What are you telling your stakeholders?

Inject 2.3 - November 20, 9:00 AM

ABC Corporation (ABC) stock share opens on NYSE at $18.50

Inject 2.4 - November 20, 3:00 PM

CMT is notified by IT that a unidentified cybercriminal group used a successful spear phishing probe against a senior leadership member of the Federal Group to gain access to the ABC Federal System network and unleash what is determined to be a ransomware, much like the "NotPetya" ransomware used in June 2017 against the global shipping Maersk Group. Once inside Federal Group network, this well-oiled destructive program wormed its way from computer to computer, trashing the infected machines' file systems. It appears that all clients within the Federal Group network have been affected. The forensic investigation is continuing.

Discussions:

1. What are you telling your stakeholders?
2. What are your priorities at this stage?

Inject 2.5 - November 20, 4:00 PM

ABC Corporation (ABC) stock share closes on NYSE at $15.50.

Inject 2.6 - November 20, 6:00 PM

Brian Krebs' blog, 'Krebs on Security,' runs a story on the cyber attack against ABC that virtually shuts down air traffic and U.S. border entry/exit control points. In the article he indicates that ABC has been involved in major cyber breaches before.

Discussions:

1. What are you telling your stakeholders? Has you message changed?
2. Are you responding to social media posts or using social media to covey the positive actions ABC is taking on behalf of their clients?

20 NOV 18 ABC Corporation apparent victim of malicious “NotPetya” type attack.

The country this morning is in the throes of dealing with a malicious cyber attack that has had the effect of bringing air traffic through our country to a virtual crawl. Early this morning, around six o’clock EST, passengers at airports along the east coast began tweeting that alleged computer problems at baggage and passenger screening areas were delaying flights. By eight this morning, every airport across the country was reporting the same network problems, resulting in delays turning into cancelled flights. As you might have correctly assumed, the effects are now being felt throughout North and South America and parts of Asia and Europe. And we had further reports that other government agencies, including Customs and Border Protection, IRS, and departments with the Department of Defense, were experiencing their own network problems. The common thread for all the agencies and sites affected is that ABC Corporation manages their respective IT systems’ network.

The ongoing forensics investigation at this point appears to indicate that an unidentified cybercriminal group used a spear phishing probe within ABC that successfully allowed the criminal group to gain access to the ABC Federal System network and unleash what is determined to be a ransomware much like the “NotPetya” ransomware used in June 2017 against the global shipping Maersk Group. Once inside a corporate network, this well-oiled destructive program worms its way from computer to computer, trashing the infected machines’ file systems.

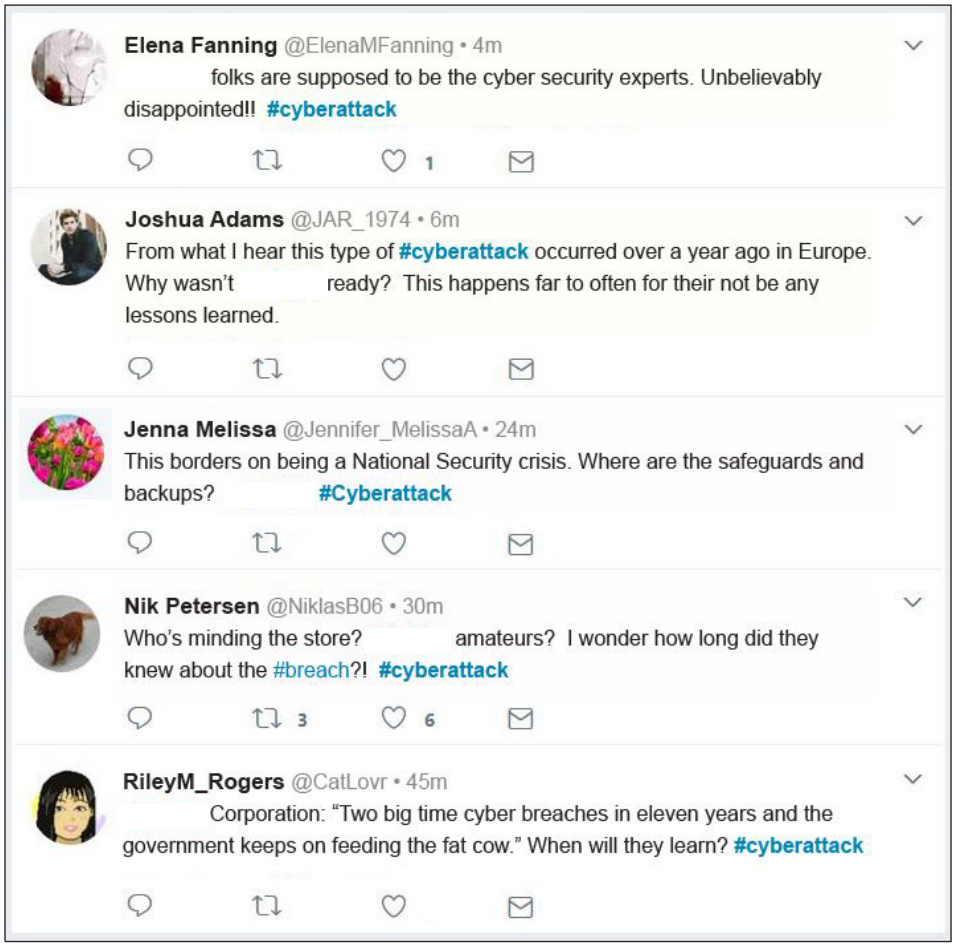
On a positive note, it appears that ABC was able to limit the cyber attack to only government network systems. Other networks managed by ABC have reportedly not been affected.

ABC has been involved in major cyber breaches before. Eleven years ago while working as a staff writer for the Washington Post I uncovered the story that the FBI was investigating a major information technology firm with a $1.7 billion Department of Homeland Security contract after it allegedly failed to detect cyber break-ins traced to a Chinese-language website and according to congressional investigators, they then tried to cover up its deficiencies. The technology firm was ABC Corporation. According to evidence gathered by the House Homeland Security Committee, ABC's failure to properly install and monitor the detection devices meant that DHS was not aware of the breach for at least three months. 150 DHS computers -- including one in the Office of Procurement Operations, which handles contract data, were compromised.

There are a good many best business security practices that, if they were incorporated, would have prevented or limited the severity of today’s attack. ABC promotes itself as a global information technology company that solves complex IT challenges for some of the world’s largest companies and government organizations, including the DHS, TSA, IRS, USDA, and the U.S. military. The company offers outsourcing and managed services, systems integration and consulting services, high-end server technology, cyber security, cloud management software, and maintenance and support services. Just last month Peter Anderson, Chairman and CEO of ABC Corporation, wrote an article on the ABC’s blog entitled “Time to be Audacious in Protecting Cyber and National Security as One.” His message was that cyber security is national security and we must take on cyber security with the same foresight, effort, and intensity once reserved for national security. Peter, I agree, but there is more work to be done and ABC needs to get its house in order before it tries to save the country on its own. The old adage of “Physician, heal thyself” applies.

Inject 3.1 - November 21, 8:00 AM

Overnight and through the early morning hours calls start to come in from clients with the Federal Group network as well as non-government clients. All are concerned about the extent of the cyber hack and steps being taken to get systems back on line.



*86 additional similar tweets.

Inject 3.2 - November 21, 9:00 AM

ABC Corporation (ABC) stock share opens on NYSE at $13.50

Inject 3.3 - November 21, 9:30 AM

Additional social media posts from disgruntled clients:

- How long did they know about the breach before notifying us? Unsat big time!!
- I'm beyond words in trying to describe how disappointed I am with "ABC"
- Right on Krebs. Don't let them off the hook.

*150 more posts by disgruntled clients.

Discussions:

1. How does ABC's communication and marketing teams deal with this situation?
2. What tools does the communications / marketing team use to monitor the chatter on social media as "Krebs on Security" leads with his story?
3. Do you have existing crisis communications responses to stakeholders that could be used in this type scenario?
4. What are your current crisis management resources and protocols and are they effective?

Inject 3.4 - November 21, 4:00 PM

ABC Corporation (ABC) stock share closes on NYSE at $12.10.

Inject 3.5 - November 21, 6:00 PM

GNN Breaking News

This is Tom Kite with GNN Breaking News. This evening's lead story is the cyber attack on the computer networks of TSA and US Customs and Border Protection that effective brought our nation's airports and border crossing to a virtual standstill. Early this morning, around six o'clock EST, passengers at airports along the east coast began tweeting that alleged computer problems at baggage and passenger screening areas were delaying flights. Within the hour we had unconfirmed reports that US Customs and Border Protection were also experiencing network outages—resulting in the closing of borders entry/exit points from Canada and Mexico. By eight this morning, every airport across the country was reporting the same network problems, resulting in delays turning into cancelled flights. And within hours the effects were being felt throughout North and South America and parts of Asia and Europe. And we had further reports that other government agencies, including the IRS and departments with the Department of Defense, were experiencing their own network problems. The common thread for all the agencies and sites affected is that ABC Corporation manages their respective IT systems' network.

Inject 3.5- CONTINUED

Brian Krebs, cyber security expert, reminded us that ABC has been a part of major cyber breaches before. Eleven years ago while working as a staff writer for the Washington Post he broke the story that the FBI was investigating ABC after it allegedly failed to detect cyber break-ins traced to a Chinese-language Web site. According to evidence gathered by the House Homeland Security Committee, ABC's failure to properly install and monitor the detection devices meant that DHS was not aware of the breach on 150 of their computers for at least three months.

On a positive note, it now appears that ABC has contained the cyber attack and government network systems supporting TSA and Customs and Border protection are being brought back on line and should resume normal operations within the next 48 hours.

Krebs, in his blog, Krebs on Security, suggests that there are a good many best business security practices that, if they were incorporated, would have prevented or limited the severity of the cyber attack. Twenty percent of ABC Corporation business is tied up in supporting federal government agencies. ABC purports to be a premier global information technology company that solves complex IT challenges for some of the world's largest companies and government organizations. Some consider that the attack today has serious national security implications. ABC hasn't just sustained a bloody nose, it has taken severe body blows and has its work cut out to stay on its feet and regain its reputation. No doubt damage control is underway at ABC Corporation.

Stay tuned for additional information on this breaking story.

Inject 4.1- November 22, 6:00 AM

ABC Corporation (ABC) opens on NYSE at $11.99.

You are still in the process of damage control, but are also starting to discuss the transition back to normal operations.

As you contemplate your challenges, you receive a call from Chairman Anderson. He would like a briefing by 11:00am on the extent of the cyber attack. He wants you to include the following in the brief:

- How did the attack occur?
- How could it have been prevented?
- What is known about the extent of the attack?
- What have we told our stakeholders? Who, exactly, are our stakeholders?
- What issues have been identified that need to be resolved regarding improved coordination between members of the CMT?
- What are we doing to regain our reputation?
- What are the “lessons to be learned?”