SIMULATION FACILITATORS

Aravind Swaminathan
Partner
Global Co-Chair Cybersecurity and Data Privacy
Orrick, Herrington and Sutcliffe, LLP (Seattle)

Leigh Nakanishi
Senior Vice President
Data Security and Privacy
Edelman (Seattle)
Objectives

- To offer a window into the mindset of effective crisis management
- To demonstrate how today’s media landscape can cause the rapid escalation of crises and necessitates swift response
- To demonstrate the belief that preparedness is vital in today’s complex risk environment
- To teach how effective communication goes well beyond the traditional news media across a wide range of stakeholders
Introduction And Focus

Today, you take part in a simulated crisis that could occur in today’s world.

Though the exercise will last two hours, the series of events in this simulation are meant to unfold over a period of 3 – 5 days.

In this simulation, everyone will play the role of the incident response team and will be asked to participate.

Consider each table as your incident response team for a fictitious company. At different stages, each incident response team (i.e. each table) will be asked to work through the scenario, and a representative may be called on to report to the larger group:

- Actions taken in response to the events that transpire throughout the simulation
- Key considerations and needs as part of the response process
Injests

How will the injests work?

• The facilitators will continually supply you with new information and developments to move you through the exercise

• Each escalation is modeled off of information that you would experience if this were a real crisis (e.g. news articles, voicemail messages, social media, legal documents, websites, etc.)
Do's and Don't's

**DO:**
Act as if this simulation is actually happening in the “real world”

**DO:**
Think big, high-level and forward-looking

**DO:**
Ask the facilitators questions as you go; use us as resources

**DON’T:**
Contact anyone outside of the team here unless instructed by facilitators – this is NOT a real crisis

**DON’T:**
Get bogged down or side-tracked; the exercise is designed to be fast-moving and you will need to keep pace

**DON’T:**
Assume the facilitators have “the answers;” the exercise focuses on the process
Do’s and Don't’s

And lastly—have fun!
Crisis Simulation
Simulation Begins
Day 1: Tuesday, November 22, 2016 – 1:00 p.m. PT

From: Hackd (hackd@gmail.com)
Sent: November 22, 2016 at 1:02 P.M. PT
To: Samuels, Amy; Cross, Kyle
Subject: Do you value your customers’ privacy?

Charlottesville Clothing Company, we have access to data for millions of your customers—including personal information of all your loyalty members. This is not a hoax—we are serious and suggest you do not ignore or underestimate us.

We will protect this data for the price of 11,500 Bitcoin. However, if you do not pay, we will release all the information. We are reasonable people and will give you 48 hours to collect the 11,500 BTC. Find the best exchanger on howtobuybitcoins.info or localbitcoins.com and pay to 16HIiExzh5G39D–Yg6r. If you fail to transfer us the money in 48 hours, we will begin selling to the highest bidder. Is that a risk you are willing to take?

To prove our credibility, this file contains the data of 100,000 CCC customers. This data is less than 5% of the records we have, and we will start leaking or selling these files every hour until you agree to pay the money or until the deadline passes. If you need to contact us, use Bitmessage: BM NJCjjhuwe5HGluyxtAAEYPjix3.

If you don’t pay on time, you will have bigger problems than leaked data. A global DDoS attack on Black Friday would be pretty bad, wouldn’t you agree?

IMPORTANT: You don’t have to reply directly to e-mail—simply pay us. As soon as the money comes through, you will never hear from us again. Thank you.
Simulation Begins
Day 1: Tuesday, November 22, 2016 – 1:00 p.m. PT

SITUATION UPDATE

- Today is the Monday before Thanksgiving and Black Friday
- CEO Amy Samuels is traveling and not immediately reachable until approximately 9 p.m. PT today
- Other individuals may be out of the office for the Thanksgiving holiday; unknown as to specifically who
Simulation Begins

Day 1: Tuesday, November 22, 2016 – 1:00 p.m. PT

• First responders must decide who to contact within the organization

• The company must decide who to contact outside the organization and when
Key Considerations

- Who should be involved in responding to this threat/demand? Who needs to be involved in the decision-making process at this stage, and what actions do each of these groups have at this point?

- Based on the information we have so far, are we characterizing this as a confirmed cybersecurity incident, or something else?

- How legitimate do you feel this threat is at this point, and are you willing to pay this extortion attempt?

- What are the technical investigatory considerations? Forensics? Evidence preservation? Attribution?

- Will you notify law enforcement at this point, and if so, who?

- Who else are you going to notify, if anyone, and when?

- What communications steps would you take at this point?

- Have you called in any external parties to help manage and respond to the situation at this point? If so, who?
Escalation 1
Day 2: Wednesday, November 23, 2016 – 8:15 a.m. PT

SITUATION UPDATE

• Analysis of the sample data file confirms the data is legitimate CCC customer data, including personally identifiable information (PII)—names, DOBs, credit card numbers (plain text), addresses, username information, and MD5 hashed account passwords

• The precise extent of impacted customer data is unknown at this time; minimum 100,000 records based on sample file. Total customer records possessed is estimated at 50 million records

• Service to CharlottesvilleClothingCo.com and external customer sites currently remain unaffected

• IT has implemented increased security measures to company servers. Legal is analyzing obligations to notify customers, etc. of data breach
Key Considerations

• Who is directing your investigation, and what functional groups from the organization are now involved?

• Where is the evidence you need for your investigation, and have you been able to obtain it from those sources or external partners?

• Based on the information we have so far, are we at a point to declare that CCC has experienced a breach?

• What obligation do you have to notify individuals impacted by this incident?

• What questions or issues would you ask your forensics teams to look into at this point?

• From a communications perspective what do you need to start preparing at this point?

• What messages would you want to have prepared at this point?
Hi,

I’m writing after seeing some unusual activity online concerning a data file that appears to contain CCC user data. A text file began circulating this morning on a dark web forum. This file contains about 100,000 records that appear to be a user database populated with PII consistent with a web payment service, in addition to linked payment account details.

I’ve been contacted by the group that claims to be responsible for the hack, and they claim to have 250 million records. They’ve shared a sample of the information with me. From what I can tell, the data appears to be credible.

Can you confirm this breach, and do you know at this time the extent of the compromised data? When will you be notifying customers? I’m planning to go live with a story in the next two hours, with or without a statement from CCC. Hope to hear from you soon.

Thanks,
Brian
Key Considerations

• Would you respond to Krebs’s media inquiry? How? What would you tell him at this point in the process? Would you agree to submit to an interview?

• What can you anticipate happening following a Krebs article and what do you need to do now to prepare?

• Has the possibility of Krebs running a story changed any of your timelines? If so, which ones and how have they changed?

• Does this affect your investigation?

• Does the composition of your incident response team need to change, and, if so, how? Who would you need to notify internally at this point knowing that the issue is likely to be made public shortly?

• What guidance, if any, do you need to provide to front-line employees?

• What do you need to do in preparation for confirming an incident?

• What decisions, if any, are you revisiting and reconsidering?
Escalation 3
Day 2: Wednesday, November 23, 2016 – 11:00 a.m. PT

23 CCC Investigating Data Breach, Ransom

CCC looks to be the latest victim of a major data breach. A large cache of data stolen from CCC has been posted online by an individual or group that claims to have compromised all of the company’s user databases, including username information, passwords and linked payment account details with over 250 million records. The still-unfolding leak originated on the Deep Web via Tor, an anonymity network, and appears to be just the tip of the iceberg for CCC. Deep Web activity suggests that CCC has been asked to make payment in the form of BitCoin or risk all 250 million records being published.

While the origin of the hack is unknown, it is possible that a situation of this extreme nature could involve a current or former employee acting on behalf of a third party individual or group. Indeed, sources within the Deep Web suggest that there may be an international connection—evoking a similar story from 2011 when Russian payment company ChronoPay attacked a competitor via third party hackers.

CCC could not be reached for comment by Krebs on Security. We will update this story as it develops.
Hi Courtney and Trey,

The publication of the Krebs story at approx. 11:30 a.m. PT and subsequent traditional media coverage reporting the data breach has driven a significant increase in social media conversation related to CCC. Mentions are currently increasing at a rate of at least 500 every 30 minutes. We expect this rate to continue increasing as media coverage and speculation surrounding details of the breach continue.

Additionally, #CCCBreach has begun trending on Twitter in the United States. I’m looking for your direction on what can, and should, be shared on social media. This may be necessary on our Facebook page—it is currently being flooded with customers asking if their data is compromised and what CCC is going to do to make it up to customers.

Note that there are some tweets that suggest a recent dip in CCC stock is linked to the Krebs piece.

Thanks,
Dave
Escalation 3 (cont.)

Day 2: Wednesday, November 23, 2016 – 12:30 p.m. PT

---

**Social Media Analytics**

*Twitter posts*

**JCampbell @JCampbell25** · 4m
Another day, another breach. THanks a lot @CCC. Looks like I’m never shopping there again.

**Sydney Norheim @sydneyvoodoo** · 1m
Are you kidding me @CCC? I hate you!!!! This is unacceptable #CCCBreach
Escalation 3

Day 2: Wednesday, November 23, 2016 – 12:30 p.m. PT

SITUATION UPDATE

• Certain logs are not available; the ones that are appear in proprietary format and there are issues loading them into Splunk to conduct the analysis.

• Relevant servers are in a data center on the East Coast and IT is still trying to contact service provider, but appears to be working with a skeleton crew given proximity to the holidays.

• Law enforcement has contacted company through physical security lead, and is asking to meet with CISO and relevant first responders.
Key Considerations

- How do you plan on addressing the significant amount of incoming attention related to the issue?
- What details are you planning to share about the incident at this point? Who are you asking to supply those details?
- Assuming that the reports are legitimate, what steps should you be taking to mitigate potential damage?
- What are you telling corporate leadership and the board?
SITUATION UPDATE

• Origin of data exfiltration may be an insider, coordinating with external actors. Cannot validate reports of 250 million customer profiles

• No indication malware was used; current hypothesis is that individual responsible was able to steal admin privileges from someone in IT

• Confirmed the 100,000 record dump is completely legitimate

• The Board is demanding an update

• The extortion deadline is tomorrow
Key Considerations

- Do revelations of an insider change your approach? If so, how?
- Will this change your messaging at all?
- What legal action are you taking? What legal obligations do you have?
- When will you be ready to notify individuals? What’s a reasonable timeline, and what is required?
- How/what are you communicating to the C-suite and Board regarding the incident? What do they want to know, and who is providing them with (regular) information?
- Beyond providing formal legal notification letters, are there other communication steps that need to take place at this point?
- What are you doing in response to rising demands by customers for “compensation”? Who is handling these requests and escalations? What are you doing about increased strain on current customer service resources?
Notification Logistics

Days 1-30 – External demands for information heighten need for prompt action

SITUATION UPDATE

• CCC determines which individuals and entities to notify

• CCC coordinates credit monitoring and identity theft resolution services for impacted customers

• CCC prepares and coordinates logistics of notifications to individuals, regulators, credit agencies, and media

• CCC coordinates and prepares call centers and develops internal and external post-notification communications plan

FOR TRAINING PURPOSES ONLY
Debrief Questions

1. What challenges did the crisis present?
2. Did there tend to be agreement or disagreement within your teams regarding how to respond to each drop?
3. What did your overall communication strategy aim to achieve?
4. How difficult was it to agree upon a response strategy and craft a statement in the allotted time?
5. What were your biggest takeaways from the exercise?
Contact Information

Leigh Nakanishi
Leigh.nakanishi@Edelman.com
Work: (206) 268-2278
Mobile: (206) 234-5318

Aravind Swaminathan
aswaminathan@orrick.com
Work: (206) 839-4340
Mobile: (206) 639-9157
Orrick Cybersecurity Incident Hotline

800.972.9306
Toll free

Suspect you have a cybersecurity or data breach incident? Call Orrick’s 24/7 Cybersecurity Incident Response Team.
Trust Anchor

An established point of trust in a cryptographic system from which a process of validation can begin

Blog: blogs.orrick.com/trustanchor
Twitter: @Trust_Anchor