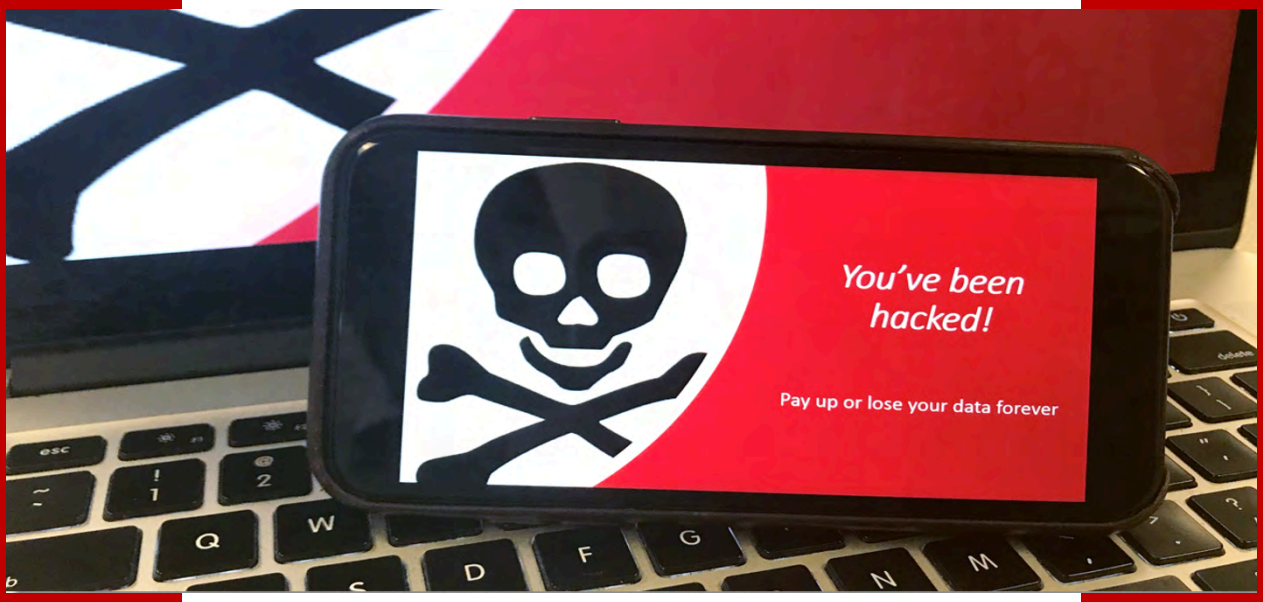


Photo (c) Robert Kang, 2019

Ransomware for the Board & C-Suite

Handout

June 15, 2021

Table of Contents

Description	Why it Matters	Page
Panelist Information	Who we are, and how to find us.	1
List of Key Articles About Cybersecurity & In-House Counsel	Our curated list of cyber-related articles.	2
Ransomware Exercise (fictional scenario)	The exercise used in today's presentation.	3

Panelist Information

Dawn Haghigi
General Counsel
Murcor Real Estate Group
&
Independent Director
Elevate Services

Chris Leigh
Chief Information
Security Office
Eversource Energy
&
Adjunct Professor
U. Conn.

Robert Kang
Chief Counsel –
Cyber & Nat'l Security
Southern California Edison
&
Adjunct Professor
Loyola Law School

Ryan White
Partner
Halpern May Ybarra
Gelberg LLP
&
Former Chief of Cybercrimes
(CD Cal.)

- **Dawn Haghighi**
  General Counsel
  Murcor Real Estate Group
  &
  Independent Director
  Elevate Services

  Email: DHaghighi@aol.com

- **Ryan White**

  Partner

  & Former Chief of Cybercrimes (CD Cal.)

  Halpern May Ybarra Gelberg

  Email: Ryan.White@halpernmay.com

- **Robert Kang**
  Chief Counsel – for Cyber & Nat'l Security
  Southern California Edison
  &
  Adjunct Professor of Technology
  Loyola Law School
  Email: rjk555@ymail.com

- **Chris Leigh**

  Chief Information Security Officer

  Eversource

  & Adjunct Professor

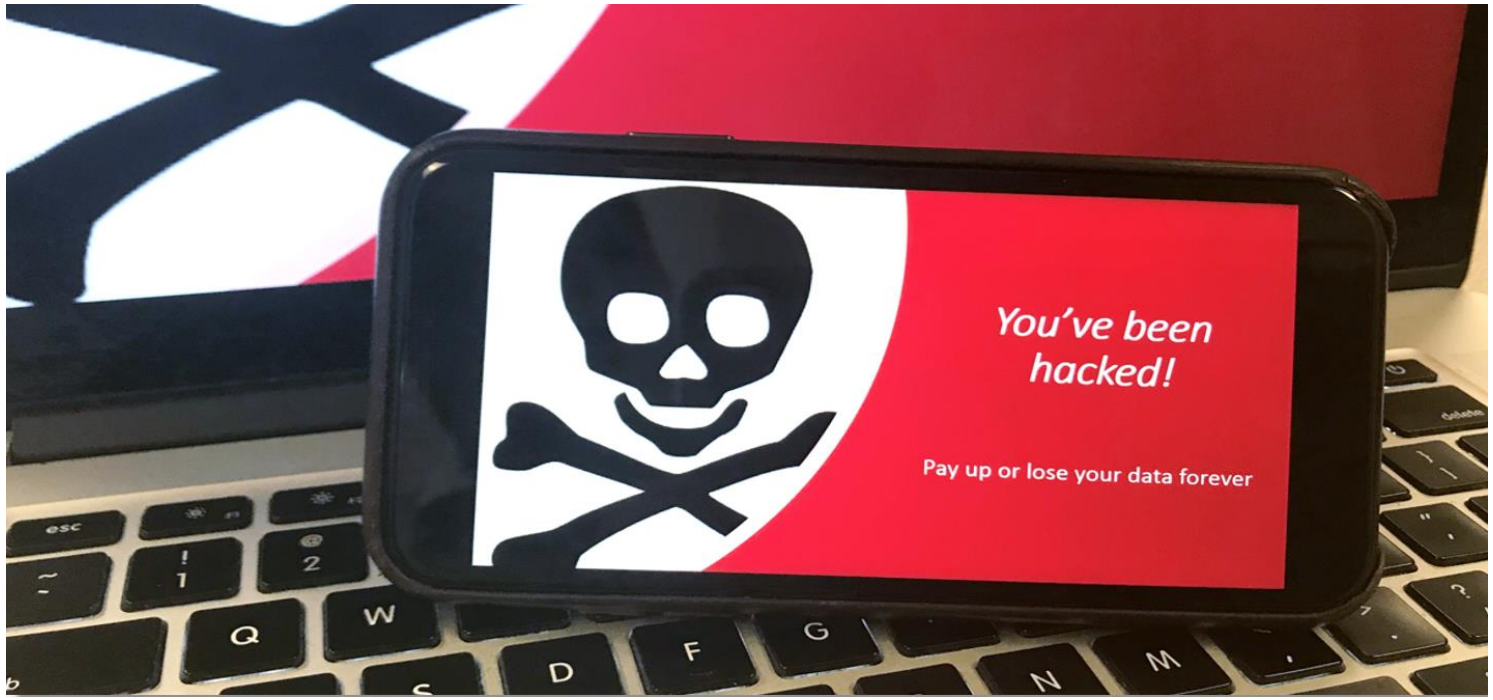
  University of Connecticut

- Email:

  Christopher.Leigh@eversource.com

List of Key Articles
About Cybersecurity & In-House Counsel

No	Description	Why it Matters	Hyperlink
1	**Ransomware Advisory** By US Dept. of Commerce (2020)	Provides guidance for assessing criminal and civil liability for making ransomware payments to US-sanctioned individuals or organizations.	LINK
2	**How Hackers Bled 118 Bitcoins Out of Covid Researchers in U.S.** By Kartikay Mehrotra Bloomberg Businessweek (2020)	Excerpted transcripts of a ransomware negotiation. Details issues that may arise during a ransomware negotiation.	LINK
3	**Best Practices for Victim Response & Reporting of Cyber Incidents** By US Dept. of Justice (2018)	Highlights methods for responding to a cyber incident.	LINK
4	***Thinking of Hiring In-House Cyber Counsel? Here are Some Tips*** By Robert Kang Bloomberg Law (2018)	Growing numbers of in-house legal departments are engaging dedicated in-house cyber counsel. Enclosed are tips for engaging such counsel.	LINK
5	***In the Heart of Technology*** By Danielle Maldonado ACC Docket (2019)	Pathway to becoming an ethical technology lawyer. Featuring Carolyn Herzog.	LINK
6	***White House 2021 Letter re Ransomware*** By Ann Neuberger (Deputy Natl' Security Advisor)	Open letter to business community.	LINK
7	***SEC 2020 Ransomware Advisory*** US Securities & Exchange Commission	Offers cybersecurity & resiliency Observations	LINK



Ransomware

Board & C-Suite Tabletop Exercise

LACBA
PRIVACY AND CYBERSECURITY SECTION

June 15, 2021

ACC Association of Corporate Counsel
SOUTHERN CALIFORNIA

Our Guides

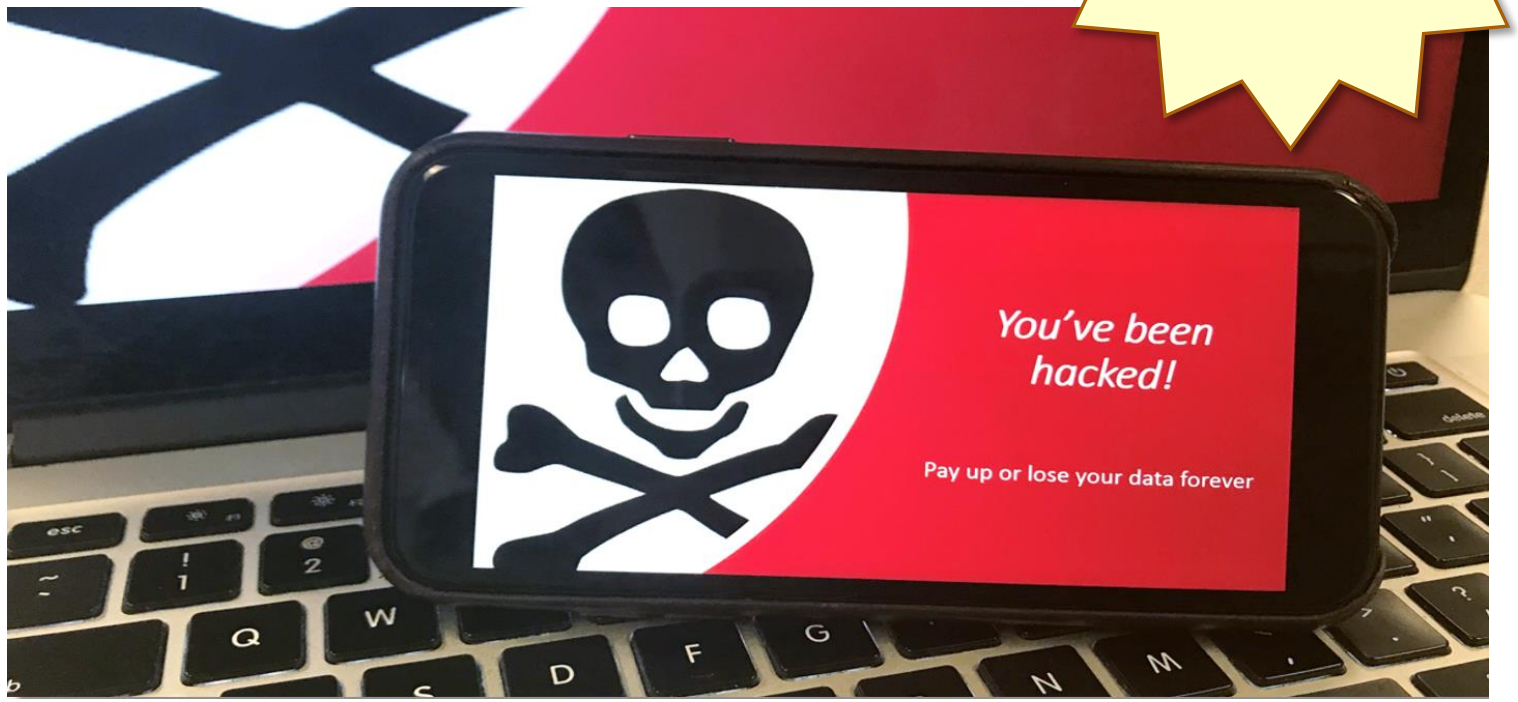
Dawn Haghigi
General Counsel
Murcor Real Estate Group
&
Independent Director
Elevate Services

Chris Leigh
Chief Information
Security Office
Eversource Energy
&
Adjunct Professor
U. Conn.

Robert Kang
Chief Counsel –
Cyber & Nat'l Security
Southern California Edison
&
Adjunct Professor
Loyola Law School

Ryan White
Partner
Halpern May Ybarra
Gelberg LLP
&
Former Chief of Cybercrimes
(CD Cal.)

Abridged



Cyber Tabletop Exercise for the C-Suite No. 1

(ransomware)

By
Prof.
Robert Kang

rjk555@ymail.com

Millennium Link

Telecommunications for the Next Millennium

About Us

1. Fast-Growing Startup. Only a decade years ago it was "five people in a garage."

   Today, it's a major **Telecommunication** Network Provider

2. Has a small incident response team, including some internal data forensic capability.

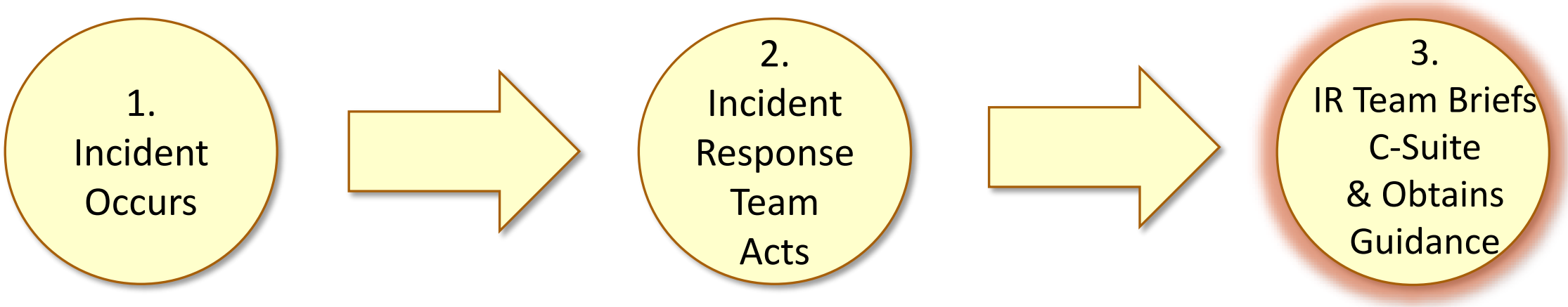
3. Newly publicly traded with an independent Board. Minimal cyber expertise.

4. Has cyber insurance policy with $5mil deductible ($50 mil policy limit)

Incident Response Timeline

Incident Response Timeline

Incident Response Timeline



The Parameters

1. Simulates “end of day” reports to the C-Suite. Tests strategic decision-making, not ”on the ground” response.
2. This is an abridged exercise, designed for short CLEs. Full exercises contain more questions.
3. The simulated IR Team’s actions range include both “good” and “not good” acts. How will the Board & C-Suite respond?
4. This exercise takes creative technical liberties with the specific nature of the incident.

Cyber Tabletop Exercise

No. 1
(ransomware)

By
Prof.
Robert Kang

rjk555@ymail.com

C-Suite Briefing No. 1
June 11 (Fri), 5pm

1. Status

At 10 am today, ML's California Network Switching Staff received word that two workstations were locked up with malware.

- *Could slow down network traffic to/from the state.*
- *Manual workarounds prevented outages. Replaced workstations with backup devices & records by 4pm.*

2. Ransom

Ransom note of $20mil sent by **Spock's Disciples.** Team is researching this entity.

3. Operations Update

- ML engaged a (i) breach coach and (ii) forensic firm/ransomware negotiator.
- Notified FBI, but no other entity.

4. Legal/Risk Update

Attorney opines there is no immediate mandatory reporting requirement

- *Has NOT initiated internal trading hold.*
- *Has NOT yet preparing SEC 8-K.*
- *Has NOT contacted insurance carrier.*

C-Suite Questions

1. This briefing is to the entire C-Suite. Should it be smaller?
2. The ransomware attacker is demanding a huge ransom. However, the incident only involves a few workstations & appears contained. Should ML contact the threat actor proactively?
   - *Who decides – IR team or the C-Suite?*
3. Do we know enough about this ransomware threat actor to make good payment decisions?
4. What about the **Business Impact Analysis**? What else is needed?
5. Do you support the attorney/Risk Dept. actions?
   - *Should ML contact insurance carrier? Who decides?*
   - Do you support refraining from trading hold?
   - How about refraining from 8-K?
   - *Who makes these decisions in your company?*
6. Notify the Board? If so, who on the Board?
7. What other information from the IR Team would be helpful to the C-Suite or Board?

C-Suite Briefing No. 2
June 12 (Sat), 5pm

1. Status

The replacement workstations locked up again. One more also locked up (3 total). Backups are infected. Implemented manual workaround.

2. Business Impact Analysis (Prelim.)

No operational impact yet. Estimated can continue manually to Thursday before impacts felt.

- Most importantly, large part of California will experience temporary outages.
- Economic losses estimated at $5mil/day.

3. Operations Brief

- The forensics firm estimates copies will be ready for analysis by end-of-day June 7, 2021.
- The negotiator has started negotiating with the threat actor.
  - *Negotiator reports Spock's Disciples has good reputation for providing decryption keys after payment.*
- Word of the incident has not spread yet. But internal leaks occur.

4. Legal/Comms. Brief

- Did not initiate internal trading hold; still opines no 8-K report required.
- Team prepared reactive media statement. No inquiries.

C-Suite Questions

1. IR team recommends making no payment yet.
   - *Do you agree?*
   - *Is it time to notify larger segments of the Board? Should the Board have greater involvement in payment decisions? Why/Why Not?*

2. IR team has not initiated trading hold or prepared 8-K.
   - *Do you support or not support?*

3. IR team proposes notifying other telecom companies of the incident. Perhaps even regulators.
   - *What's pros/cons?*
   - *Who decides – the IR team or the C-Suite?*

4. IR team prepared a reactive media statement.
   - *Who approves – the IR team or the C-Suite?*
   - *Why did it take two days to prep the statement?*
   - *How about internal statement?*

5. *What else would be useful to the C-Suite or Board?*

C-Suite Questions

Fictional Scenario

C-Suite Briefing No. 3
June 13 (Sun), 5pm

1. Status

- This morning the York Times issued a report speculating that Spock's Disciples might be associated with North Korea.
- Initial forensic exam results will likely start arriving by Tuesday morning.
- *Note: In response to a COO question, the team reports it considered, but did not, perform in-house forensic analysis of the workstations before sending to the forensic investigator.*

2. Negotiator/Forensic Investigator Report

- Negotiator reports that the threat actor has reduced ransom from $20mil to **$12mil**. Deadline extended to Thursday.
- Investigator reports its clients typically need 15 hours to fully implement decryption key & restart systems.
  - *If ML makes payment today, systems might be up by Monday.*
  - *Some clients needed more than 15 hours to restart.*

3. Legal

- Attorney initiated trading hold. But did not start SEC 8-K filing.

C-Suite Questions

1. IR Team did not perform an in-house forensic analysis, and waited for forensic investigator to provide results.
   - *Pros & Cons?*
2. North Korea may be involved.
   - *How does this impact ML's potential payment?*
3. **Decision time:** pay ransom now, or wait for forensic report on Tues? Deadline for manual workaround is this Thursday.
   - *How does this timing impact payment consideration?*

The negotiator reduced the ransom from $20 mil to $12 mil.

- *What additional information would the C-Suite desire to decide whether to pay/not pay at this point?*
- *Should the Board be consulted?*
  - *Who & what's their role?*

3. Company considers making payment.
   - *Do you know how?*
   - *Is the CFO ready to move that sum of money?*
4. Pls see the attorney's trading/reporting decisions to the left.
   - *Agree with trading hold decision?*
   - *Agree with 8-K decision?*
5. *What else would be useful to the Board or C-Suite?*

C-Suite Questions

Q&A
& Final
Comments