

Sandy B. Garfinkel

Member, Eckert Seamans Cherin & Mellott, LLC



- Founder and Chair – Eckert Seamans Data Security & Privacy Practice Group
- Specializes in privacy/security for the hotel industry
- Breach response and privacy regulation (GDPR, CCPA)

A photograph of the Houston skyline, featuring several prominent skyscrapers. In the foreground, there is a river with a bridge and some greenery. The image is overlaid with a semi-transparent dark grey filter.

Hospitality Cyber Threats Are Alive & Well — Lessons From Recent Incidents

THE HOSPITALITY LAW CONFERENCE: SERIES 2.0 - HOUSTON

APRIL 9 - 10, 2019

“Acquisition” Can Mean Acquiring Cyber Exposure: MARRIOTT / STARWOOD

- Marriott acquires Starwood September 2016
- BUT, database intrusion occurred in 2014
- Discovered 2018; **383 million records**
- name, address, phone no., email, passport no., preferred guest, DOB, gender, arrival/departure, payment card nos. w/ exp. dates.

Marriott/Starwood - KEY TAKEAWAYS

Cyber is a Critical Due Diligence Consideration

Discovery of the issue pre-closing would have had a profound impact on the value of the deal



Cyber Due Diligence Checklist

- ✓ Build in Sufficient time to assess cybersecurity issues
- ✓ Independent penetration test of the target environment
- ✓ Review inventory of cybersecurity products and tech to understand organizational tech differences
- ✓ Review the third-party relationship inventory, data sharing agreements & risk assessments.

Cyber Due Diligence Checklist (continued)

- ✓ Perform a “Dark Web” style investigation: are key assets, IP, user info credentials already out there?
- ✓ attempt to identify infiltration of the target enterprise
- ✓ Research breach databases for recent disclosures
- ✓ Review past breaches re: remediation status, ongoing obligations to any affected parties

Marriott/Starwood - KEY TAKEAWAYS (continued)

Retention of Personal Information Carries Risk

- 25 million passport numbers were compromised over the course of the Starwood data incident.
- Guest data going back to 2014.

Why retain all of this?

Marriott/Starwood - KEY TAKEAWAYS (continued)

Definition of PII is Expanding

- Traditional PII: SSN, financial accounts, credit/debit, state-issued ID, but since GDPR --
- Example – Illinois: email account info, medical information, health insurance info, biometric data
- Example – CCPA: Any information that “*identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.*”
IP address, browser histories, search history, web activity tracking, audio, electronic, visual, thermal, olfactory information, geolocation data.

Marriott/Starwood - KEY TAKEAWAYS (continued)

The PMS Is Vulnerable

- Most hotel breaches in the last decade – POS System Breaches
- 2008/2010 – Wyndham PMS breach
- Use of PMS in franchised hotels is not optional; vulnerabilities can occur on both the franchisor's and franchisee's end of the system

Cyber Threat: Present Even in the Acquisition of a Single Property

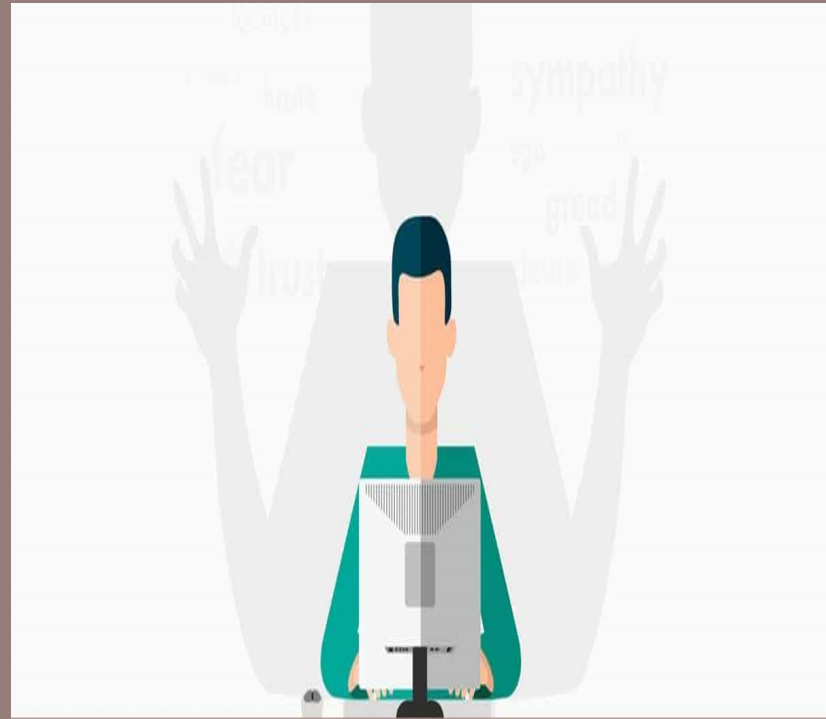
TIMELINE:

EVENT	DATE
Infiltration of Malware	February 2018
Sale of Property	September 2018
Discovery of Malware	December 2018

Don't Forget About Low Tech Attacks!

Hotel employees are susceptible to Social Engineering (just like everyone else!)

2018: Rash of attacks using low-tech methods to fool hotel employees into giving up system credentials. Then they called the guests and tried to fool them, too.



Anatomy of a Social Engineering Scam

Cybercriminal: *Hello, I'm calling from [brand] system support. We're having difficulty with the reservation process on your end, and we need to check it. Can you please log in for me?*

Employee: *Sure. [Logs in]*

Cybercriminal: *We're still having an issue. Can you please give me your username and password so I can try it on our end.*

Employee: *No problem. My username is ... and my password is*

...

Anatomy of a Social Engineering Scam (continued)

[future guest's phone rings]

Cybercriminal: *Hello, I'm calling from the [hotel name] regarding your reservation from [check-in date] to [check-out date]. We're having a problem processing your credit card. The last four numbers are [XXXX]. Could you please provide me with your full credit card information, including security code, so we can get that taken care of?*

How To Combat Social Engineering Scams

- Alert and train employees
- Have a reporting process in place
- Reward employees for reporting these
- Implement multi-factor authentication if possible
- Audit which employees have access to the PMS; disable access for employees who have no business need for it
- Protect payment card information so that it can't be unmasked.
- Change employee passwords regularly

A background image of the Houston skyline, featuring several prominent skyscrapers like the Bank of America Tower and the JP Morgan Chase Tower. The image is overlaid with a semi-transparent dark grey filter. The main text is in large, bold, white, sans-serif font, centered on the image. Below the text is a decorative horizontal line with a repeating white triangle pattern.

FOR QUESTIONS, SEE YOU AT THE DEEPER DIVE ROUNDTABLES

THE HOSPITALITY LAW CONFERENCE: SERIES 2.0 - HOUSTON

APRIL 9 - 10, 2019