Southwest Audit Committee Network

September 2019

SWACN

SUMMARY of THEMES

Cyber breach response

Members of the Southwest Audit Committee Network (SWACN) gathered in Dallas, Texas on September 11, 2019 for a conversation about cyber breach response, a lunch discussion on the future of cybersecurity, and a tour of the EY Cyber Center. This *Summary of Themes* synthesizes the discussion on cyber breach response with Roy Mellinger, former Chief Information Security Officer (CISO) at Sabre Corporation and Anthem.[1] At the request of the lunch guest, the discussion on the future of cybersecurity was off the record. *For a list of meeting participants, please refer to page 5.*

Lessons learned for improving preparedness and response

During the meeting, Mr. Mellinger and members discussed past experiences with cyber-attacks and recommended practices for improving preparedness and response.

Practicing the breach response plan is critical

Many companies have breach response protocols in place, and regular practice can be critical to maintaining vigilance and enhancing preparedness. For health insurer Anthem, the strong execution of a well-practiced plan was critical to the company's response and recovery in 2015, when it became the victim of one of the largest data breaches ever recorded. Several members noted that their organizations practice breach response protocols on an annual or semiannual basis. Mr. Mellinger outlined the rigor of Anthem's practice approach: *"We did a quarterly tabletop that involved all of the incident response teams, including the general counsel, human resources, and the communications teams. We would do a big annual exercise with my department and those teams as part of the Health Information Trust Alliance (HITRUST) with all the nationwide healthcare providers. And then my team would do an ad-hoc monthly drill, as a way to make sure we were staying fresh in response.*" Though many companies have yet to experience a major breach, it is important to conduct post-mortem reviews for even minor attacks or incidents. Mr. Mellinger said, *"Anytime we had an incident the team would sit down and talk about what we would have or could have done differently and conduct a root cause analysis. We were used to that process."*

The crisis communications strategy must be thoughtful and nimble

Once a company has learned it is the victim of a major cyber breach, the communications strategy can play a significant role in determining reactions from authorities and regulators,

media, and customers and clients. Mr. Mellinger described an intensive communications campaign that the firm embarked on in the wake of the breach:

- **Authorities and regulators.** In the immediate aftermath of the breach—having already begun work with the FBI—Mr. Mellinger and Anthem's government affairs team notified the necessary regulators and political constituents: *"We let them know first…That helped us get a lot of goodwill; we let them know in person and they didn't find out in the press. We did a lot of pre-work in the four days before going public with the Wall Street Journal."*
- **Media.** Once the necessary law enforcement authorities and regulators had been briefed on the situation, Mr. Mellinger, Anthem's general counsel, and a few others met with selected reporters to share the story about the breach: *"So we broke the story and then we held off from other media releases…We were prepared from that perspective and wanted to make sure we controlled how the story came out."*
- **Customers and clients.** When a company is the victim of a major data breach, the greatest risk is often to brand trust and reputation. Mr. Mellinger said, *"In the end it's about brand loyalty and the relationships with your customers and your clients, it's about if they trust how you carry yourself."* Many of Anthem's major clients wanted to speak with the CISO to discuss the breach, so that's what Mr. Mellinger did: *"I went out and met with all the major clients. I didn't do anything over the phone but actually went on the road and sat down with any client who needed it, [and] said, 'Here's what we know, here's what's classified, and here's what we're doing about it".* In the three years after the breach, Mr. Mellinger said he met with 56 clients for such discussions, adding that no major client left the company as a result of the breach.

Mr. Mellinger highlighted that many of these actions were not in Anthem's original response plan and instead evolved with the situation. Though it is critical to have a thoughtful and well-practiced response plan, the circumstances of every breach are different, and companies must be nimble enough to adapt, as necessary.

Subsidiaries and M&A activity may represent a cyber risk

The Anthem breach stemmed from successful phishing attacks on the company's subsidiaries.[2] Members discussed the challenges of governance and oversight in this area, particularly as it relates to mergers and acquisitions (M&A), when due diligence may need to be conducted in a tight timeframe. One member asked, *"A lot of companies are doing joint ventures today, including with companies from other nations such as China. What kinds of checks should companies have in place when doing M&A or entering those joint ventures to wall it off?"* In an M&A situation, Mr. Mellinger recommended having the CISO conduct a review of the other company's systems, saying, *"If the systems are going to be interconnected, that's the big risk. Start doing vulnerability scans, penetration testing, look at their security of their own systems."* It is useful to conduct such reviews even if a new acquisition is not going

to have its systems connected, as a lack of due diligence in this area could represent a reputational risk down the road.

The board provides helpful oversight

Members discussed the challenges of determining the appropriate role of the board and audit committee in overseeing cyber breach preparedness and response. Some directors feel unprepared from a technical angle, and others are concerned that they have not spent adequate time addressing the topic or have not done enough. One member asked, *"We're all looking at dashboards and working through NIST frameworks, what else can we do to help?"* Members and Mr. Mellinger discussed several tactics that boards and audit committees may use to help management prepare for future attacks:

- **Ask detailed, in-depth questions.** Boards or audit committees often receive periodic updates on the status of the organization's cybersecurity, typically using dashboards and reviews of key metrics. However, Mr. Mellinger said, *"Every organization has scorecards and metrics; my experience is those numbers don't necessarily mean anything. Management tells the board what they want them to hear."* As a result, he recommended that boards ask more pointed questions: *"For the board to understand what's truly happening they need to ask more granular questions."* He provided an example, *"Say you were penetrated and there's malware trying to send data out, but it was stopped. Sure, you stopped it that time, but what about if you don't next time? A lot of the time the board would never know it happened if they don't ask the right questions."*
- **Find different ways to evaluate cyber preparedness.** A few members asked about the viability of having an outside firm assess the company's cyber posture. Though Mr. Mellinger said these types of assessments can offer some value, there are also drawbacks: "*It's a snapshot in time, it's expensive, and they only see what they're shown. Unless they do a real deep dive and a long engagement, IT professionals are very hesitant to show too much."* He recommended leveraging the internal audit department to help benchmark cyber preparedness, adding, *"I've always look[ed] at the audit programs as friends, not foes. They can really help you improve your cyber programs."*
- **Ensure the board and management are aligned on the escalation approach.** Boards should assist management in putting in place clear leadership and reporting lines and making clear to management when the board expects to be notified of a breach. Mr. Mellinger opined that the CISO should not report to the Chief Information Officer (CIO) and recommended that boards meet with their CISOs regularly and in private, as they do with the head of internal audit. Members discussed who on the board should be notified in the event of a breach, and what should trigger that sort of escalation. One member said, *"It shouldn't just be [the] audit chair, it should be full board notification if it's high risk to the company. Of course, some companies are getting attacked a million times per day, so I don't want to know every time, but I do want to know if it's significant and could have*

reputational significance." Another added, *"I agree it should be the full board because it is reputational. Knowing the data is in someone else's hands or involving outside authorities should be a trigger to notify the board."*

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc. and EY and the associated logos are trademarks of EYGM Ltd.

Meeting participants

- Mark Buthman, Alumni
- Barbara Duganier, Buckeye Partners and MRC Global
- Paulett Eberhart. Cameron
- Tom Glanville, Itron
- Bella Goren, MassMutual Financial Group
- Bruce Hanks, CenturyLink
- Steve Johnson, Torchmark
- Don Kendall, SolarCity
- Jennifer Kirk, Republic Services
- Teresa Madden, Peabody
- Gil Marmol, Foot Locker
- Don Robillard, Helmerich & Payne
- Dunia Shive, Trinity Industries
- Valerie Williams, DTE Energy Company
- Billie Williamson, Cushman & Wakefield

EY was represented by the following:

- Scott Hefner, Global Client Service Partner
- Frank Mahoney, Vice Chair and Regional Managing Partner – US West
- Sandra Oliver, Partner, US West Audit Leader
- David Pond, Principal, Southwest Region Business Development Leader

Endnotes

[1] *Summary of Themes* reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Italicized quotations reflect comments made in connection with the meeting by network members and other meeting participants.

[2] Marianne Kolbasuk McGee, "A New In-Depth Analysis of Anthem Breach," *Bank info Security*, January 10, 2017.