A NEW GUEST EXPERIENCE REQUIRES A NEW APPROACH TO SECURITY

The Hospitality Industry Faces Risk from New and Old Threats

EXECUTIVE SUMMARY

The hospitality industry is booming, with bookings expected to break another record in 2018. Much of the innovation in the industry is around providing an individualized guest experience, and this means greater reliance on technology. At the same time, new and old threats against hoteliers' IT systems are increasing, and the attack surface is getting larger due to the proliferation of multiple clouds and increasing volumes of data. The threat is real: the number of breaches and incidents at hospitality organizations rose by one-third last year. As a result, hospitality companies must rethink the traditional perimeter-based security strategy in favor of an integrated approach that eliminates architectural silos, enabling transparent visibility and centralized control across the distributed network.

When indirect economic contributions are factored in, the global travel industry accounts for more than 10% of global GDP.[1] The hospitality industry serves as a crucial linchpin in that economic sector, and has seen rapid growth during the post-Great Recession recovery.

Many of the hospitality industry's services are now handled digitally. Studies have shown that travelers strongly prefer to book hotels online versus offline,[2] and that more than one-third of reservations are made using a mobile device.[3] Once guests arrive onsite, technology enhances their stay in many ways. In-room entertainment systems are increasingly sophisticated,[4] and some properties are starting to use artificial intelligence (AI) to improve the guest experience with concierge-style services.[5] Trailblazers are starting to combine AI with the Internet of Things (IoT) and near field communication (NFC) to help create a highly individualized travel experience.[6]

While expansion is cooling in 2018, the growth rate for hospitality is still expected to **exceed 5%** and bookings are projected to reach a record-breaking **$170 billion.**[7]

Beyond these elements of customer experience, digital transformation (DX) at hotels and hotel chains can bring about additional initiatives. Many hotels have introduced microtargeted marketing campaigns, enhanced surveillance and site security, and new products and services that take advantage of the existing point-of-sale (POS) infrastructure. These trends have contributed to the rapid growth and profitability of the industry, but they have also resulted in exploding data volumes, a greatly expanded attack surface, and increased risk.

A DIRE THREAT LANDSCAPE

Today's computing environments are increasingly driven by the desire for DX, resulting in highly distributed implementations. Data is increasingly held in complex on-premises and multi-cloud environments. Hackers are now motivated by everything from nationalism to anarchy to the promise of instant riches. Improving data security must remain a priority for hotel operators. Security breaches are up—and sharply so. More than one-third (36%) of global firms were breached last year, up considerably from 26% in 2017 and 20% in 2016. Results in the U.S. were even worse, with 46% of U.S. firms polled reporting a breach last year—a figure that nearly doubled from the previous year. Two-thirds (67%) of global organizations and 71% in the U.S. have experienced a breach at some point.[8]

The increasingly complex threat landscape and expanding attack surfaces have underlined the need for security that goes far beyond ticking boxes to satisfy regulatory requirements. The aftershocks of a breach on a business can be devastating, with the biggest impacts being loss of reputation and customer trust—which translates to loss of business.

OLD AND NEW THREATS IN HOSPITALITY

Digital evolution leads to an unparalleled and expanding attack surface for all industries, and hospitality is no exception. With personally identifiable information (PII) and financial records having a high value on the black market, hotels are prime targets for opportunistic cyber criminals.

In fact, some experts assert that hotels are an especially attractive target this year due to their diversity of data from a relatively affluent customer base and reputation for lagging behind in security.[9] POS infrastructure is still the most vulnerable system at a hotel, and in some ways hoteliers are more exposed than retailers. Because payment card information is retained throughout the guest's stay—and is often in the system months in advance when the room is booked—cyber criminals have a longer window to access the information.[10]

POS systems still see the most attacks in hospitality—accounting for **65%** of the hospitality industry's security breaches.[11]

Public Wi-Fi networks at hotels are considered table stakes in the industry these days,[12] and this opens an additional threat vector. Hackers can steal both personal information and passwords from the relatively affluent clientele of a hotel. In addition, distributed denial of service (DDoS) attacks on IoT devices are increasing, as are ransomware attacks. Even a few minutes of downtime can prevent a potential guest from booking a specific hotel, and instant reviews mean that an interruption of guest experience amenities can damage future business.[13]

DATA BREACHES AND DOWNTIME AFFECT THE BOTTOM LINE

Data breaches can be costly. In 2017, the average breach cost the hospitality industry $120 per record stolen.[14] For those subject to the EU's General Data Protection Regulation (GDPR), the prospective costs just got even higher. Now, losing the personal data of a European Union resident could result in a fine of up to 4% of a company's annual revenue. In other jurisdictions, the fines may be smaller but could still take a big bite out of tight margins.

Threats such as DDoS attacks have the goal of bringing systems down, and downtime is also costly. Some estimate the cost of downtime as high as $300,000 per hour.[15] But even a few minutes of downtime for a booking system might prompt a consumer to choose another property, and even short periods of downtime for in-room Wi-Fi or entertainment systems can result in negative reviews and angry customers.

Worse, the reputational damage of a data breach or downtime may be even more substantial. For example, one in five consumers (20%) say they will not shop at a retailer that has suffered a cyberattack, even if the company has taken necessary steps to remediate the issue.[16]

In 2017, the **average breach** cost the hospitality industry **$120 per record stolen.**[17]

SECURITY IS NOT KEEPING PACE

Despite potentially serious consequences of data breaches and system downtime, many hoteliers are stuck in a past generation of security. They may use a firewall at the edge of an on-premises network. But if it is dated or its full capabilities are not being employed, it may not successfully detect and mitigate the latest threats. Moreover, with today's distributed on-premises and multi-cloud environments, perimeter protection is no longer sufficient.

The expanding attack surface also taxes legacy security architectures. New technologies prompted by DX bring new clouds, devices, and networks into the infrastructure, which increases risk. Point security products are often brought online to address these new vulnerabilities, but this results in a further fragmented security infrastructure that complicates management and makes automation and centralized visibility impossible. This leads to manual data transfer and analysis, forcing IT leaders into a reactive security posture.

Another challenge emerges when a hotel chain deploys software-defined wide-area network (SD-WAN) technology to accelerate data flow between corporate locations. While sometimes improving network performance, SD-WAN solutions enable some traffic to bypass the security protocols of the corporate data center.

Verizon noted **1/3 more breaches and incidents** at hospitality organizations in 2017 vs. 2016.[18]

SOPHISTICATED SECURITY NEEDS TO BE A TOP PRIORITY

As the hospitality industry increases its reliance on technology for an optimal guest experience, it faces an expanded attack surface and a more complex threat landscape. Verizon noted one-third more breaches and incidents at hospitality organizations in 2017 vs. 2016,[19] and it takes more than six months (197 days) to even detect the typical attack.[20] The majority of these are advanced threats, designed to bypass conventional security measures. This enables the malware to move laterally until it does the maximum damage and yields the most valuable data for cyber criminals.

As the hospitality industry increases its reliance on technology, companies need to reconsider their approach to network, application, and data security. A fully integrated security architecture supports maximum automation of security processes, facilitates transparent visibility, and enables centralized contols, in addition to unlocking automation—from manual security workflows to dynamic threat-intelligence sharing. While it may seem less costly to maintain the status quo with regard to security, the cost of potential data breaches and downtime can easily mean the difference between making a profit and absorbing a loss.

1 "2018 travel and hospitality industry outlook," Deloitte, accessed September 14, 2018.

2 "Distribution of adults in the United States by their preference of hotel booking online or offline in 2017," Statista, accessed September 14, 2018.

3 Steffan Berelowitz, "Important mobile booking stats for hotels in 2018," Travel Tripper, February 6, 2018.

4 Elaine Hendricks, "Trends Directing the Future of In-room Entertainment," Hospitality Upgrade, October 25, 2016.

5 "3 Hotels Using Artificial Intelligence To Improve Guest Experience," Event Manager Blog, December 4, 2017.

6 "2018 travel and hospitality industry outlook," Deloitte, accessed September 14, 2018.

7 Ibid.

8 "2018 Thales Data Threat Report," Thales Security, accessed September 14, 2018.

9 Steve Oates, "Cyber Security Threats Facing Hotel Industry," LinkedIn, February 10, 2018.

10 "2018 Lodging Technology Study: Deconstructing Innovation," Hospitality Technology, December 18, 2017.

11 "2018 Thales Data Threat Report," Thales Security, accessed September 14, 2018.

12 Patrick Nelson, "Wi-Fi most important hotel feature, survey says," Network World, December 16, 2014.

13 "Timeline: The growing number of hotel data breaches," Hotel News Now, January 10, 2018.

14 "2017 Cost of Data Breach Study," Ponemon Institute, accessed September 14, 2018.

15 Jack Oakley, "The Real Cost Of Downtime For Business," 100TB, July 13, 2017.

16 "Consumer Loss Barometer," KPMG, accessed September 14, 2018.

17 "2017 Cost of Data Breach Study," Ponemon Institute, accessed September 14, 2018.

18 "2018 Data Breach Investigations Report," Verizon, March 2018.

19 Ibid.

20 "Advanced Threats in Retail—A Study of North America & EMEA," Ponemon Institute, May 28, 2015.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

October 19, 2018 3:27 PM

247313-0-0-EN

wp-hospitality-new-guest-experience-10-19-18-330pm