PELNIK
INSURANCE

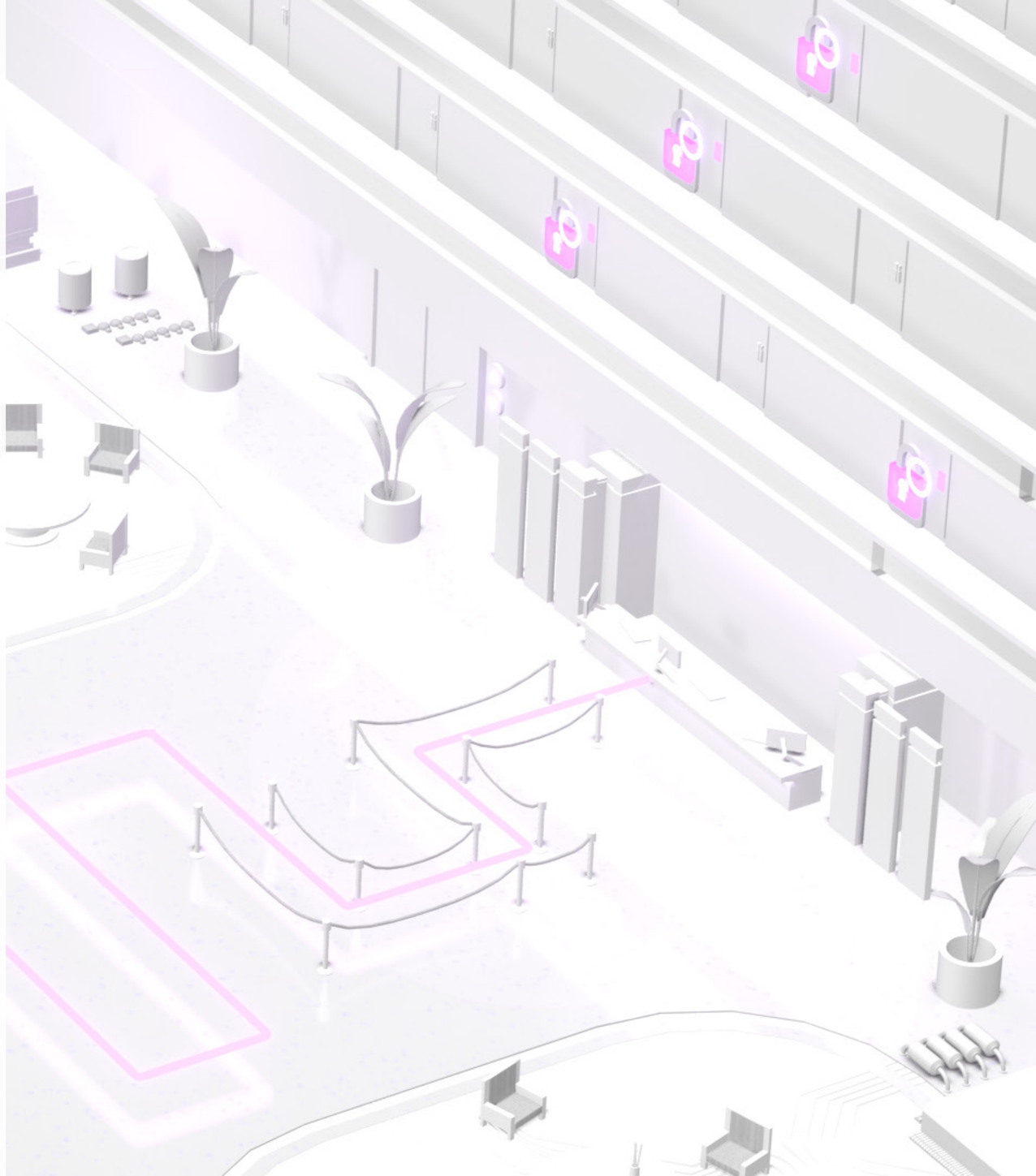
# Cyber Case Study

provided by Pelnik Insurance

## Marriot Data Breach

In the final months of 2018, Marriott International—a hospitality company that oversees one of the biggest hotel chains in the world—discovered that cybercriminals had compromised its guest reservation system. This data breach exposed the personal information of hundreds of millions of customers from various countries who had made bookings with the company's Starwood properties over the past several years. As a result of the incident, Marriott faced significant recovery expenses, legal ramifications and reputational damages.

This breach—which ultimately stemmed from existing security vulnerabilities that carried over during Marriott's 2016 acquisition of Starwood—has since become known as one of the largest cyber incidents the world has ever seen, showcasing the importance of prioritizing cybersecurity during merger and acquisition (M&A) events. In hindsight, there are various cybersecurity lessons that organizations can learn by reviewing the details of this incident, its impact and the mistakes Marriott made along the way. Here's what your organization needs to know.




# The Details

In 2014—two years before Marriott even acquired Starwood—the latter company's guest reservation system was infiltrated by cybercriminals via remote access trojan (RAT). Put simply, a RAT is a harmful computer program that grants the perpetrator unauthorized administrative control of their victim's technology. A multitude of digital vulnerabilities at Starwood's properties could have contributed to the success of the cybercriminals' RAT. Namely, these properties were using outdated versions of Windows Server across their computer systems and had left their remote desk protocol (RDP) ports open to the internet. Despite this intrusion within the guest reservation system, Starwood was unable to detect the cybercriminals' activity—allowing them to remain unnoticed.

Moving forward to September 2016, Marriott officially acquired Starwood. During the acquisition process, Marriott failed to complete a detailed cybersecurity audit of Starwood's networks and technology. As such, Marriott was also unable to identify the cybercriminals' activity within Starwood's guest reservation system—permitting them to stay undetected throughout the acquisition. Additionally, Marriott didn't discover that Starwood had been further targeted by separate attackers in an unrelated incident during 2015, leaving its workplace devices infected with malware.

Rather than adopt uniform networks and technology following the acquisition, Marriott allowed Starwood properties to move forward with their current operations—thus utilizing a compromised guest reservation system and malware-ridden devices. Marriott also began migrating information from several databases housed within Starwood's guest reservation system. This information included a variety of customers' personal details—such as names, addresses, phone numbers, email addresses, passport numbers and credit card numbers.

While the information in these databases was encrypted, the cybercriminals were eventually able to locate their associated decryption keys and subsequently unlock the information. From there, the cybercriminals began exfiltrating the information. After transporting this information, the cybercriminals then re-encrypted it in an effort to remain undetected within the system.

In September 2018—a full two years after the acquisition—Marriott finally identified the breach due to a system security alert. Upon this discovery, Marriott reported the incident to law enforcement officials and consulted forensic specialists to launch an investigation. On Nov. 30, 2018, Marriott revealed the details of the breach to the public in an official statement. At this time, Marriott confirmed that the personal information of nearly 500 million customers around the world—including the United States, Canada and the United Kingdom—had been compromised.

PELNIK INSURANCE

# The Impact

In addition to exposed data, Marriott faced several consequences following the large-scale breach. This includes the following:

**Recovery costs**

Marriott incurred nearly $30 million in overall recovery expenses as a result of the breach. This total includes costs related to investigating the cause of the breach, notifying impacted customers of the breach, providing these customers with year-long access to security monitoring software, developing an international call center related to the breach and implementing updated cybersecurity measures to prevent future incidents.

**Reputational damages**

Apart from recovery costs, Marriott also received widespread criticism for its cybersecurity shortcomings after the incident. In particular, the media and IT experts scrutinized Marriott's failures to perform its due diligence on Starwood's existing security vulnerabilities prior to the M&A process and detect the cybercriminals' activity after the acquisition was finalized—essentially allowing the cybercriminals to access and exfiltrate customers' personal information for nearly four years. Consequently, Marriott's stocks dropped by 5% almost immediately after it announced the details of the breach. What's more, the company is estimated to have suffered over $1 billion in lost revenue due to diminished customer loyalty following the incident.

**Legal ramifications**

Lastly, Marriott encountered costly legal ramifications from various avenues because of the breach. Since the incident affected individuals from the United Kingdom, the Information Commissioner's Office fined Marriott over $120 million for violating British customers' privacy rights under the General Data Protection Regulation. In North America, Marriott was met with multiple class-action lawsuits after announcing the breach—one of which requested $12.5 billion in damages, or $25 for every impacted customer.

Marriott confirmed that the personal information of nearly **500 million customers** around the world—including the United States, Canada and the United Kingdom—had been compromised.

Marriott's stocks dropped by **5%** almost immediately after it announced the details of the breach. What's more, the company is estimated to have suffered over $1 billion in lost revenue due to diminished customer loyalty following the incident.

# Lessons Learned

There are several cybersecurity takeaways from the Target data breach. Specifically, the incident emphasized these important lessons:

**RDP ports require proper safeguards.**

Exposed RDP ports were another potential culprit of this costly incident. Although RDP ports are useful workplace tools that permit employees to connect remotely to other servers or devices, leaving these ports open can allow cybercriminals to leverage them as a vector for deploying malicious software or other harmful programs (including RATs). That being said, RDP ports should never be unnecessarily left open to the internet. Virtual private networks (VPNs) and multi-factor authentication protocols can also be utilized to help keep RDP ports from being exploited by cybercriminals.

**Cybersecurity must be considered during M&A events.**

Marriott neglecting to prioritize cybersecurity amid its acquisition of Starwood proved detrimental in this breach. Primarily, Marriott should have diligently assessed Starwood's IT vulnerabilities throughout the M&A process. Further, Marriott should have ensured an effective cybersecurity infrastructure between the combined companies once the acquisition took place. Especially as cyber incidents continue to surge in both cost and frequency, cybersecurity should be top of mind during any M&A activity. In particular, each company involved in the M&A process should be carefully evaluated for potential cybersecurity gaps. A proper plan for rectifying or—at the very least—mitigating these exposures should be developed prior to the finalization of the M&A event. In many cases, it can also be advantageous for merged companies to adopt shared digital processes and security policies in order to maintain uniform defense strategies against cybercriminals.

**Effective security and threat detection software is critical.**

A wide range of security and threat detection software likely could have helped both Starwood and Marriott identify and mitigate this breach in a much faster manner—thus reducing the resulting damages. Although this software may seem like an expensive investment, it's well worth it to minimize the impacts of potentially devastating cyber incidents. Necessary software to consider includes network monitoring systems, anti-virus programs, endpoint detection products and patch management tools. Also, it's valuable to conduct routine penetration testing to determine whether this software possesses any security gaps or ongoing vulnerabilities. If such testing reveals any problems, these issues should be addressed immediately.

**Proper coverage can provide much-needed protection.**

Finally, this breach made it clear that no organization—not even an international hospitality company—is immune to cyber-related losses. That's why it's crucial to ensure adequate protection against potential cyber incidents by securing proper coverage. Make sure your organization works with a trusted insurance professional when navigating these coverage decisions.

For more risk management guidance and insurance solutions, **contact us today at 919-459-8000 or www.Pelnik.com.**

PELNIK INSURANCE