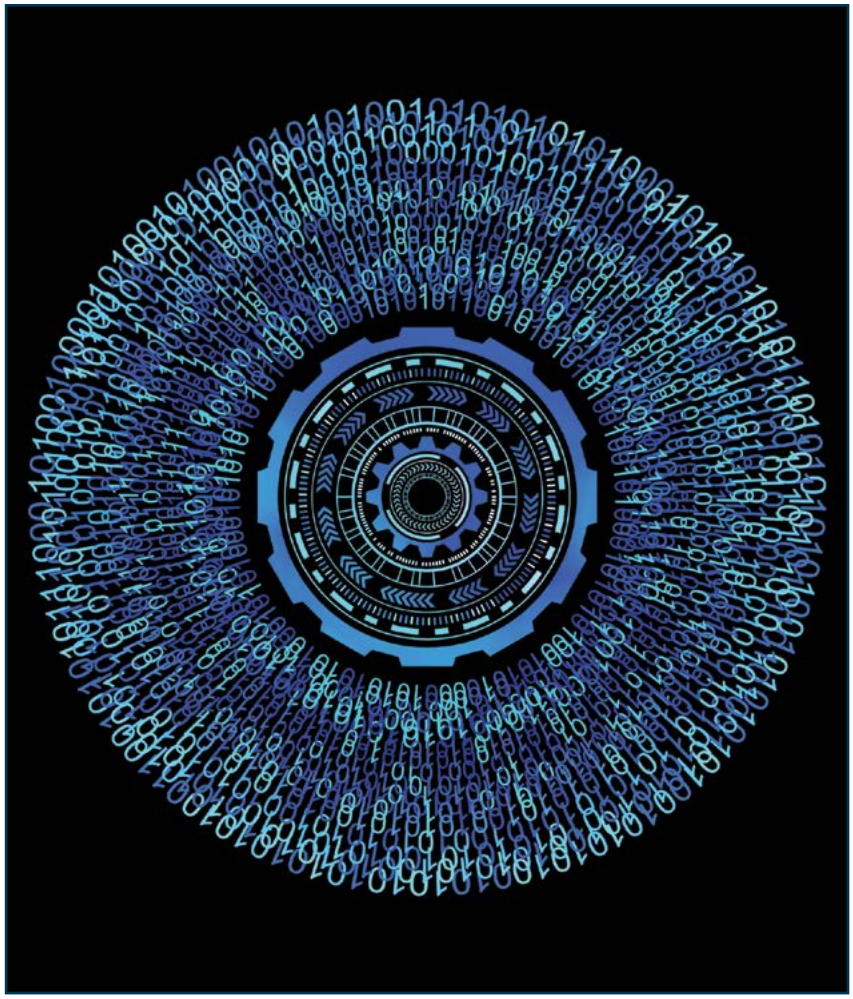
Privacy and Security Potpourri

By John Bell

Status of pressing security and privacy issues to be addressed in the next year, including GDPR, ransomware, payment processing, transparent layer security and risk.



Let's look forward and examine some of the security and privacy issues the industry will be facing between now and the next HITEC in 2019. This article covers a potpourri of security and privacy issues the reader may encounter or want to address in the next year.

Privacy and GDPR

The big gorilla in the room regarding privacy is the European Union's General Data Protection Regulation best known as GDPR. GDPR impacts the data being held on European citizens both inside and outside of Europe. The potential penalties, up to 4 percent of global annual revenue has gotten the attention of many companies who are now starting to pay serious attention to privacy issues. It is impossible to begin to cover all of the intricacies involved in a regulation as complex as GDPR in an article this short, so consider these principles:

- Companies are responsible for protecting the data they collect and process about individuals,
- The person (data subject) must give consent for data collected about them to be used for specific purposes,
- The data subject has the right to see or examine all of the data about them held by a company,
- The data subject has the right to ask for the data about them to be corrected if it is inaccurate or incomplete,

John Bell (jtbell@ajontech.com) is a founding leader and technology solutions consultant at Ajontech LLC, a consulting company which focuses on the hospitality and lodging industries.

- The data subject has a right to ask that data be removed when no longer needed for the purpose it was collected, and
- The data subject has the right to data portability allowing the data to be moved to another processor.

Many companies and the systems they use are not prepared to collect consent or provide easy access to customers so the customer can easily view, modify, erase or download their information, so I expect this will be a major effort for IT and privacy organizations within companies for the next couple of years.

Security and Ransomware

Security issues pop up frequently and quickly. Sometimes they impact even those that try their best to be secure as in the recent exploits on Pretty Good Privacy (PGP) and Gnu Privacy Guard (GPG) and some popular e-mail clients. One of the most serious concerns many companies have faced this past year and will probably continue to see in the years to come is ransomware. Ransomware is malicious software that infects a computer and encrypts the files making them inaccessible until a ransom is paid in Bitcoin or some other digital currency. The best way to protect against ransomware is to assume that you will be hit, and make certain you have regular backups of the files you need to recover. Also periodically test the recovery process to make certain it can be completed and systems made operational in a timely fashion. Also check to assure the backups are intact and operable. Consider performing these recovery tests at least quarterly if not more frequently.

Security and Payments

EMV is the chip on card system that was originally specified by Europay, Mastercard and Visa. In the United States a mandate was issued by the card companies that all merchants should have EMV in place by October 15, 2015. To be fair, the card industry wasn't ready to meet the needs of the hotel industry at that time. Today, this is no longer true and if a company hasn't updated their systems to support chip cards they should be planning to do so now. EMV primarily protects against counterfeit cards, but does not automatically provide point-to-point encryption (P2PE) between the card collection device and the processor or other points in the process. P2PE encrypts data at the source in a manner that can only be decrypted or understood at the destination computer. Any computers that may pass the data in between are unable to decrypt or see the data. So the recommendation is when you implement EMV, also implement P2PE at the same time. It will save money since payment collection terminals will only need to be configured once.

Security and the Transport Layer

Transport Layer Security (TLS) is how Internet pages are sent securely. On your browser you may see a green lock icon that indicates that TLS is being used. Over the years several of these secure protocols have been retired and should no longer be used. The Payment Card Industry (PCI) Council requires that all Secure Socket Layer (SSL) protocols and TLS 1.0 be retired by June 30 this year. It is a good idea and best practice to disable these old protocols on your servers now. It will not impact modern web browsers.

Unfortunately, on some Internet of Things (IoT) environments like point-of-sale terminals there is no ability to update the protocols on the web client. These systems are stuck with the old insecure protocols that have been retired. For these systems, if possible, P2PE is the best approach.

> " Risk is the product of what can be lost and the probability that it will be lost. The value in understanding risk is that it determines how much investment is needed to protect against that risk."

P2PE breaks the need to depend on the Internet security protocols for security. There are other approaches that can be explored using secure virtual private networks (VPN), but the details could be an entire article in itself.

Risk

My personal issue for the industry this year is risk. Risk is the product of what can be lost and the probability that it will be lost. The value in understanding risk is that it determines how much investment is needed to protect against that risk. Since many of the risk elements are the same in most companies in the industry, it makes sense to me for hoteliers to work together and create an industry-wide risk model that can be used as a starting point for each company to determine their own risk. Hopefully this will lead to more rational investment into security and less loss for the industry. ✷