If my review of the top hospitality technology headlines of 2016 taught me anything (see the January edition of Siegel Sez on Hotel-Online), it clearly demonstrated that some large, sophisticated hotel operators with lots of security resources are still struggling to effectively protect sensitive information from theft. And the theft of customer credit card data is not the only information security threat facing our industry.

A 2014 Deloitte survey of 1,000 frequent travelers indicated that only 33 percent believed that their loyalty account information was adequately secured, but 75 percent expected travel companies to secure their personal information to the same — or even higher — standard as a financial institution.

This study followed a 2014 Krebs on Security report that stolen Hilton HHonors points were being sold online. And in 2015, Krebs reported that hackers had compromised numerous Starwood Preferred Guest customer accounts.

Employee personally identifiable information (PII) in HR systems is also a target for theft, whether by hackers or scammers. The beginning of 2017 saw a flurry of fraudulent email attempts to trick trusted employees into handing over employee W-2 records, some of which resulted in breaches. Courts in several states, including California, have ruled that employers have a legal duty to protect the personal data of their employees. And, as if we didn’t collectively have enough to worry about, it was reported a few days before this writing that hackers had infected a resort hotel in the Austrian Alps with ransomware that disabled the hotel’s electronic key locking system, locking guests out of their rooms and preventing new keys from being made until the hotel paid the ransom.

POINT MADE: We know we have significant exposure to risk.

I’m sure that many of the leaders in our industry charged with improving or maintaining information security constantly feel like Michael Keaton in the movie Mr. Mom — you’re just trying your best, and all these random people are yelling at you, “You’re doing it wrong!” So, how do you do it right?

TALK TO A LAWYER

This may seem counter-intuitive to some people, and blindingly obvious to others. But at the end of the day, security is about risk and liability. You must understand what your legal and contractual status is. If you are a merchant who accepts credit cards, then your merchant services contract with the acquiring bank requires you to be compliant with Payment Card Industry Data Security Standards (PCI DSS). Chance are, that contract also places all financial and legal liability on you, the merchant, even if the bank or card company cannot prove you are at fault. Is that just a contractual obligation, or is there a regulatory requirement? That used to be a simpler question until the FTC started fining hotel operators for failure to protect customer data.

If the owner and operator of a hospitality establishment are two different entities, who is “the merchant”? Generally, it is the owner of the business, as the merchant account is tied to financial ownership of the asset and the bank accounts of the business. If the establishment is operated by a separate entity, the typical management agreement indemnifies the operator from liability except in cases of gross negligence by the operator. But wouldn’t some owners consider mismanagement of information security “negligence”? The legal relationship and liabilities of the various parties should be clearly defined in the respective contracts. PCI DSS, for example, requires that the responsibilities of service providers for the protection of cardholder data be clearly addressed in the contract between a merchant and service provider — and third-party hospitality operators are service providers in this scenario.
Hotel brands are also service providers. Does your agreement with the brand – either for management or a franchise – include the specific language required regarding information security and PCI compliance responsibilities? Is the brand providing you with documentation of its compliance posture, and how that overlaps with your branded operations? Are they required to?

Do you have business locations -- or customers -- in the United States and in multiple states? Forty-seven states now have some type of law regarding the protection of the personal data of their citizens. These laws have differing requirements for businesses, depending on the state and the type of data disclosed. Does your information security plan have provisions for managing the legal requirements in the event of a breach or disclosure?

### HAVE A PLAN

In the U.S., the Super Bowl is now over. Do you think that either of these two highly effective football teams went into the Super Bowl without a detailed game plan? Of course not. Do you have a detailed game plan for information security? What are the elements of a good information security plan?

<table>
<thead>
<tr>
<th>It must address your legal requirements and responsibilities (see above).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>It must be based on documented facts.</strong> Have you performed a formal information census? Do you have current documentation showing what types of information your organization stores, whether it is considered “sensitive,” which specific laws or regulations apply, where it is stored, who is responsible for its management and security, how long you must keep it, whether it must be encrypted? Do you have current, detailed network diagrams showing all cardholder data flows and all connection points of the cardholder data environment to other networks and the outside world? Not only is this a PCI DSS requirement, but how can you plan security without knowing the details of the environment you are trying to secure?</td>
</tr>
<tr>
<td><strong>It must be based on detailed policies.</strong> Have you read your information security policy recently? Does it establish clear direction on how information security will actually be implemented and managed? Compare your policies and procedures on cash handling and accounting with those for information security. You will probably find the information security P&amp;P’s lacking in detail by comparison. The cash-handling P&amp;P almost certainly goes all the way down to the line staff level, and establishes an auditable trail of custody for cash from customer receipt to bank deposit. Information is an asset, just like cash.</td>
</tr>
<tr>
<td><strong>It must be based on a formal risk assessment.</strong> This is also one of the newer requirements of PCI DSS (v.3.2) that applies equally to all information security planning. Requirement 12.2 states: Implement a risk assessment process that:</td>
</tr>
<tr>
<td>• Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),</td>
</tr>
<tr>
<td>• Identifies critical assets, threats and vulnerabilities, and</td>
</tr>
<tr>
<td>• Results in a formal, documented analysis of risk.</td>
</tr>
<tr>
<td>Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.</td>
</tr>
<tr>
<td>Guidance: A risk assessment enables an organization to identify threats and associated vulnerabilities with the potential to negatively impact its business. Examples of different risk considerations include cybercrime, web attacks and POS malware. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized.</td>
</tr>
<tr>
<td>If you don’t have a formal ongoing risk assessment program that results in a formal, documented analysis of risk, then you don’t have the necessary information upon which to base an effective information security plan (and you’re not PCI DSS-compliant). And you’re doing it wrong.</td>
</tr>
<tr>
<td><strong>It must have an executive.</strong> Football teams are indeed teams, even at the management level. But there is a head coach responsible for building and executing the game plan. When information security became important to your organization, did you create an executive position to build and execute that game plan? Or did you dump it – er, sorry – delegate it to IT. Or worse yet, assign it to a committee. Committees have their place. You probably should have an information security steering committee. But at the end of the day, it is a highly specialized field of management, and you should have someone with the necessary qualifications in charge. Their level in the organizational structure depends on the size of your business, but he or she should be high enough to make and implement policy decisions. This individual may not be the head coach, but he or she should at least be a top-notch defensive coordinator. After all, defense wins championships…</td>
</tr>
<tr>
<td><strong>It must be achievable, with priorities based on risk.</strong> It sounds obvious, but achievability must be a guiding principal at every step of the planning process. If your team was trapped on a desert island with a storm approaching, would you create a shelter with the resources at hand, or start sketching plans for a new beachfront resort? Well, the storm is upon us. And leaning back on the overserved football analogies, your defensive line is beat up and injured, and the opponent has a healthy, top-ranked offense. Do you base your game plan on who you might get in the next draft, or whether the plans for the new stadium get approved? Or do you plan on what you can get done in the next week with what you have? The stuff down the road is important, and must be addressed in the plan, but the coming storm (or the next big game) has the most risk, and plans must be prioritized accordingly.</td>
</tr>
<tr>
<td><strong>It must include a detailed response plan.</strong> Greg Harnish, CEO of Grey Castle Security, was quoted in a recent article, “The key to data breach recovery is preparing a plan of action before the breach occurs, and PCI standards actually require some type of response plan. Statistics show and data proves the more prepared you are, the less impactful an incident is on the merchant, and the less time it takes to resume normal business operations.”</td>
</tr>
</tbody>
</table>
HAVE A PLAN

A good information security plan must be based on legal requirements and built with the assistance of your legal team, it must include detailed policies to form the framework for initiatives and processes, it must be based on a formal risk assessment process, it must have a dedicated executive, it must include a detailed response plan, and it must be achievable. Otherwise, your doing it wrong.

USE EFFECTIVE STRATEGIES AND TACTICS

Feeling overwhelmed yet? You should be. Those are just the high points of what needs to go into an effective plan for information security. But the plan is everything. A wise man once told me, “Plan your work, and work your plan.” Another wise person once said, “Wish in one hand, [poop] in the other, see which one fills up first.” You can’t wish your way to better information security. You must have a detailed, achievable plan. But what strategies and tactics can you use to make your plan workable?

Use a prioritized approach based on your risk assessment. The most frequent type of data breach incident in our industry is the theft of credit card data. The greatest financial and legal liability results from this type of breach. The most frequent target for a credit card data breach is an F&B point-of-sale (POS) system. If your tactical plan to address the risk of a data breach doesn’t address the POS systems in your environment first — and quickly — then you’re doing it wrong.

Eliminate sensitive data. If there is no gold in the vault, then the security you put up around the vault becomes much simpler, and much less expensive. For credit card data, the complementary technologies of tokenization and point-to-point encryption (P2PE) remove the sensitive data — the gold — from the merchant systems and environment. If implemented correctly with hardware payment terminals, these solutions greatly reduce the risk of a breach and reduce the compliance requirements. Many of the products used for tokenization and P2PE also enable acceptance of EMV chip cards, which greatly reduces the merchant’s financial liability for EMV-related chargebacks. For a more detailed discussion, see Jeff Parker’s excellent article in Hospitality Upgrade, “Falling Asleep at the Wheel: The hotel industry and EMV,” or refer to the wealth of documentation on the PCI Security Standards Council website (www.pcisecuritystandards.org). As Parker mentions, there are certainly challenges to effectively implementing tokenization and P2PE in the hotel e-commerce, distribution and PMS world, given the myriad channels by which customer credit card data is collected and transmitted. But POS is a much more straightforward exercise for tokenization and P2PE. If you’re not enabling tokenization and P2PE on all your POS systems immediately (and other payment systems when possible), then you’re doing it wrong.

Use third-party service providers. Let’s be crystal clear: There is no such thing as a magic service provider that eliminates all your risk and makes you fully compliant. However, good service providers, used in a smart, targeted fashion, can improve security, reducing both risk and compliance requirements. Moving payment systems above property is one example — the merchant is still responsible for validating the PCI compliance of the hosting provider, be it an application vendor, a brand company or a private cloud, but many of the detailed requirements for managing the data and the environment shift to the service provider when it is hosting. The trend to move more applications to the cloud also facilitates emerging services such as software-defined wide area networking (SD-WAN), which in turn streamlines how service providers can handle more of the security load and simplify the IT environment at remote sites (where hospitality’s line of business resides).

There are also a great deal of ongoing services related to good information security management: vulnerability assessment, external vulnerability scanning, penetration testing, log and event monitoring, endpoint security, threat detection and the list goes on. These are all items that must be done. Your choices are to either hire qualified staff (and give them adequate tools) to manage and provide these services, or you can contract them out to a managed security services provider. Either approach is workable, but if you don’t already have the in-house resources, going with a third-party service provider is going to yield results faster but maybe not cheaper; you do get what you pay for in many cases. If you are not effectively leveraging good service providers, then you’re doing it wrong.

Use network segmentation. Putting different applications and functions on different, isolated parts of the network is a well-established security practice. It can also reduce the scope of compliance in much the same way as using tokenization, P2PE and moving apps to the cloud. Segmentation can also enable the network to be more manageable and to perform better, in addition to being more secure.

The other strategies mentioned may simplify the extent and complexity of the segmentation required, but won’t eliminate it. If your property networks are not segmented in some fashion, then you’re doing it wrong.

Standardize, standardize, standardize. Put on your auditor hat for a moment. If it’s not managed, it’s not secure. If it’s not documented (or documentable), it doesn’t exist. If it’s not audited regularly, it’s not being done. If it’s not standardized, it’s difficult — if not impossible, to document and manage. If it’s not managed… you see where this is going. We’ve already talked about the importance of detailed policies and procedures — that is where standardization starts. Good information security (and PCI DSS compliance) requires that every device has a documented security configuration that is based on published standards, periodically reviewed and updated, and is based on the roles and functions of the device and the device user(s). That one requirement alone is impossible without a high degree of standardization, and that is just one requirement.
USE EFFECTIVE STRATEGIES AND TACTICS

Do not be tempted by expediency or false economies. If you acquire a new hotel, do not try to retrofit systems or equipment or network architectures that don’t fit your standardized model. The only way to improve security is through management and monitoring, and you (or your outsourced service provider) have built a standardized solution that can manage and monitor. Resist the temptation to deviate from your standards to save a quick buck. For example, if your network management and monitoring solution is based on having one specific brand of network switch (for the sake of discussion; hopefully it isn’t), then it should literally be a company policy that all locations have those network switches. In short, if you don’t have a standardized, managed environment then you’re doing it wrong.

Get better tools. There is the oft-repeated adage of “work smarter, not harder.” That is the underlying theme of all these strategies and tactics for effective information security. You’ve taken the steps above to minimize risk by eliminating sensitive data, segmenting your networks, moving apps and services to third-party providers, and building more standardized environments. You (or your service provider) will still have a lot of managing and monitoring to do. Better tools will not only facilitate that effort, they will move the task needle from “impossible” to “achievable.”

At a minimum, the toolset being used in your environment should include:

SYSTEM CONFIGURATION MANAGEMENT
Since all devices must have standardized security configurations, and all devices must be managed and manageable, the choice is to either do it manually (hint: bad choice), or use configuration management tools such as Microsoft’s System Center Configuration Manager, Quest’s KACE Endpoint System Configuration Manager, LANDesk Service Desk IT Management Suite or Symantec IT Management Suite. And other tools in this category can enforce configuration settings and manage the deployment and updating of software. Most of the vulnerabilities in the typical IT environment are due to missing patches and unauthorized or unsupported software, so the ability to automatically deploy software patches and updates is mission-critical.

SOFTWARE WHITELISTING
This is a technique that only allows specifically pre-approved software to be installed on managed devices. This is both a standardization solution that greatly simplifies the task of supporting and updating the software stack, as well as a crucial security feature that blocks most malware, including ransomware, from being installed. Whitelisting is a feature of some of the system management suites above, as well as security suites such as Carbon Black, which acquired Bit9, one of the pioneers of this application.

ENDPOINT SECURITY
Also a part of many of the larger management and security suites, it is a product bundled with network security appliances as with the WatchGuard solution set. Endpoint security dynamically enforces policies for security and configuration when endpoints – computers, laptops, tablets – try to access a network. These solutions also typically provide bundled anti-virus/anti-malware, software firewalls, web content filtering and file-integrity monitoring, among others.

NETWORK ACCESS CONTROL (NAC)
According to Wikipedia, NAC is an approach to computer security that attempts to unify endpoint security technology, user or system authentication and network security enforcement. You can start to see how there is a lot of overlap between many of the solution suites, so care is needed to avoid duplication of features (and costs). As solutions mature and features are added, the differences become mostly a matter of terminology.

MOBILE DEVICE MANAGEMENT (MDM)
Represented by mobile-specific solutions such as AirWatch and IBM MaaS360, MDM is a type of NAC solution tailored for the common mobile device operating systems – Apple® iOS, Google Android, Windows Mobile. MDM solutions are widely deployed because of the huge growth in mobile devices in the workplace, both user owned and company issued. MDM either wasn’t handled by the organization’s NAC solution, or there was not yet a NAC solution. Increasingly, MDM will be part of a unified endpoint security suite.
RON HARDIN IS AN INDEPENDENT TECHNOLOGY CONSULTANT. HE CAN BE REACHED AT WWW.RONHARDIN.TECH.