CYBERSECURITY IN THE RHT SPACE: THE NEW IMPERATIVE

MAY 2018 TECH BRIEF FOR THE RETAIL, HOSPITALITY, AND TOURISM INDUSTRY

Ensuring the Safety of the Valued Guest identity

Cybersecurity is defined as the state of being protected against the criminal or unauthorized use of electronic data or the measures it takes to achieve this protection. As internet adoption increases across public and private sectors, more data is being gathered, proliferated, stored and used daily, and therefore, Cybersecurity, as a business imperative, is exponentially increasing in importance.

For the Retail, Hospitality, and Tourism sector, however, Cybersecurity is even more important than it is for almost any other industry group, even financial.

Labor Force Takeaway

Failure to secure sensitive guest data can be not only damaging to RHT industries, but if significant enough, could be disastrous. Numerous opportunities exist in job creation and expansion in the areas of data capture and warehousing, monitoring, and management.

Since new viruses and hacking methods are launched daily, ongoing data inspection and network PEN (penetration) testing through machine tracking and human review and analysis should be routinized. Data savvy personnel should be deployed across the IT teams to ensure the network defense posture remains up and strong.

Certifications/training in widely promulgated software packages, such as Log Rhythm, Virima, or the popular Solarwinds software suite will give associates an edge in seeking roles in this area. Coding skills are also in need this area for the building of API's, data normalization, and ad hoc reports construction..

An understanding of routing/firewalling issues is also viewed as highly beneficial. Any Cisco certifications (CCNA, CCIE) are viewed as a major plus by employers. Knowledge of products by major firewall providers (Barracuda, Juniper, Cisco, FortiNet) lends additional credibility and will return long term advantages.

CYBERSECURITY IMPERATIVES FOR RHT

Why is cybersecurity so essential for the RHT industry? Three major reasons:

(1) Companies in this sector, particularly the Hospitality and Tourism space, hold more types of information about the user, far beyond payment information;
   a. Sensitive personal information, including ordering preferences, likes and dislikes, and even physical location on a property, are often stored for ease of engagement with facilities and services.
   b. Environmental information about the property, at the individual and group level, are now stored and available for potential access, including things like door locks, HVAC, dining in and out of room, and room availability.

(2) Opportunity. Retail is one of the top five industries targeted by hackers, given there are hundreds of system access points across the network of store locations available for breach on a daily basis.

(3) Data breaches in this industry, regardless of size or scope, can effectively kill a brand, and quickly.

These areas of concern, primary among them physical personal security and a hotel's liability for your security, introduce exposure to the property beyond payment systems and credit cards. The areas of legal, law enforcement, insurance, and technical assets are all fair game to the hacker, and therefore businesses in this vertical carry a greater mandate to ensure data safety for themselves as well as for their valued guests and clients.

The dollar volume of this potential exposure is staggering. Consider some of the bigger data breaches of the last decade. EBay saw the exposure of over 145M records. Target had over 70M records compromised, and the dollar volumes of each were upwards of $50M dollars to the company, with ripple effects (in terms of increased spend on prevention, as well as damages) is still being felt.

Although neither of these brands was killed, consumer confidence took a huge hit. According to an IBM whitepaper conducted on the Future of Identity these companies saw double digit drops in profit the quarter after the breach, both due to expense line increases as well as significant downward shifts in top line revenue.

Further, IBM noted, consumers trust in a retailer's ability to handle and protect personal biometric data sunk to only 19%, while remaining in the 40th percentile for similarly entrusted financial institutions. As stated by Mark Yourek, IBM's Global Retail Solutions Lead in an article in Insights on Business, "The financial and reputational damage that can be inflicted on a retailer by a major security breach can be so severe and so destructive as to approach the financial and reputational damage a commercial airline might suffer from a serious accident."

Consumers are also becoming more technically aware, as these breaches proliferate. Identity theft is a major concern, as they realize their data is valuable, and they are demanding more sophisticated methods of data protection be deployed by their preferred vendors. They will stay away if they sense those protections are not in place, or are weak. Evidence shows millennials in particular are savvy enough and are brand agnostic enough to delete accounts held by a known compromised service provider, and will take their business elsewhere.

What creates this environment where this costly data exposure occurs? Studies have consistently shown that security breaches are typically between 90-95% attributable to human error (both client and associate) somewhere in the chain of access and/or control.

There are five major contributing factors that leave data wide open to theft:

(1) End users (guests) accessing malware-laden websites or downloading infected files on private networks or guest terminals
(2) Weak password policies employed for associates
(3) Insecure system configurations deployed by corporate IT teams
(4) Legacy or unpatched/outdated technology in service at host sites
(5) Generally poor network security practices

The onus is clearly on RHT industry members to up their security game to ensure clients have an optimal, secure stay, as well as to protect their bottom line. Clearly, an in-depth security strategy, including the inculcation of a culture of security across all associates is central to securing sensitive data. Other tactics necessary to enhance the corporate security posture include:

(1) A published security defense plan, that proactively addresses the areas of threat identification, containment, vulnerability removal, system patch/upgrade, ongoing monitoring and communication
(2) A strong Point of Sale system, inclusive of state of the art firewalling and perimeter security
(3) Associate training
(4) Thoughtful deployment of analytics-based security tools

Industry standards, such as PCI DSS, are also providing guidance to RHT corporate members on best practices for a secure and certifiable data warehousing standard. Many technology vendors, including Juniper, Windstream, and GTT offer free technology security audits, to help you baseline your posture, and build a plan around defense. Ensure you are dealing with reputable companies on these free audits, however, as network access by unverified sources can result in viruses and malware being intentionally planted on your network.

Numerous software products are also available to log and track events for monitoring purposes, and to aid in PCI-DSS compliance requirements. LogRhythm, Security Innovations, Virima and Solarwinds are but a few of the brands with software specifically created for the RHT industry to give network managers the visibility they need to manage network ingress and egress effectively.

Finally, the importance of a strong POS system is essential. Shopkeep, Revel, TouchBistro, Clover, and Square top the list of the Best POS systems in 2018, ranked by top10bestpossystems.com. From PDA/Mobile usability to inventory management to employee tracking and performance management, in addition to security, a sound POS system in an industry where consumer behavior awareness is fundamental to profitability, is a core component to your security strategy as well as an essential business management tool.

In conclusion, Cybersecurity is and will continue to be a fundamental concern for any profitable business in the RHT sector. Companies should continue to keep this issue at the height of their business planning process, and seek expert consultative advice for best practice leverage and deployment. Your business literally depends on it.