NCCoE Hosts Hospitality/Retail Community of Interest Webinar
Thursday, February 28, 2019 | NCCoE

The National Institute of Standards and Technology’s (NIST) National Cybersecurity Center of Excellence (NCCoE) recently hosted and moderated an online panel discussion with cybersecurity experts from both the retail and hospitality sectors allowing them to share their views on cybersecurity challenges and opportunities in 2019.

Bill Newhouse, a security engineer at the NCCoE, moderated the discussion. The panel featured:

- David Coley – Owner, Dominion Tea
- Patrick Dunphy – Chief Information Officer, Hospitality Technology Next Generation
- Paul Lanzi – Chief Operating Officer and Co-Founder, Remediant
- Jake Necessary – Chief Information Security Officer, Interstate Hotels & Resorts

Over the course of the hour, the panelists offered their insights about where they could see advances in cybersecurity happening this year. Below are a few areas touched upon during the discussion.

**Application of Cybersecurity Standards**

Standards help to provide a common cybersecurity foundation for an industry. To date, the application of cybersecurity standards specific to retail and hospitality industries is inconsistent, and panelists agreed that to improve cybersecurity, this needs to change. The European Union’s General Data Protection Regulation fundamentally reshapes the way in which data is handled across every sector. Retail and hospitality organizations will be looking to apply cybersecurity standards for protecting data. The panelists all noted a need to coalesce around and come to consensus on baseline cybersecurity standards that will help organizations adhere to GDPR and to show customers that cybersecurity risk is being addressed. Progress in this direction was noted by Patrick with the creation of the Travel Information Sharing and Analysis Center, a trusted environment for security professionals in the travel industry to share threat information and cybersecurity best practices and to collaborate on standards created at the request of several hospitality Chief Information Security Officer.

**Third-Party Vendor Risk Is Real**

Retailers and hospitality organizations rely heavily on third-party vendors for digital services and data storage. The means by which a third-party vendor interacts with you can increase your risk. For example, a vendor with access to your network may also have a path for unauthorized access to confidential customer, company, and employee information. If your vendor’s network has exploitable vulnerabilities, your data may also be at risk. Panelists noted that it is not enough to rely on service level agreements (SLA) to reduce risk. Implementing additional cybersecurity technologies to mitigate risk is needed alongside those SLAs.
Fortunately, our panelists have seen an uptick in the sophistication of requests for security products and services from within the retail and hospitality sectors in the past 12–18 months. Vendors are being challenged by industry adopters of cybersecurity advances, and this bodes well for improved cybersecurity.

**Cybersecurity Is Everyone’s Job**
Panelists agree there is a shortage of good cybersecurity talent. It’s a familiar lament that is pervasive across all industries, and retail and hospitality are no different. Panelists noted that more and more high schools are incorporating cybersecurity in their curricula, and online courses offering foundations in cybersecurity are proliferating.

Younger generations are more accustomed to enhanced security too. For example, colleges and universities are moving toward adopting multifactor authentication for students to access a school’s network and resources, and this points to a future where those students will become customers who welcome greater security as part of their online activities.

**Will Username/Password Ever Go Away?**
Customers have been using usernames and passwords for decades, and that will likely continue in the near term. There remains concern in the hospitality and retail sectors that asking customers to use stronger authentication may result in those customers taking their business elsewhere. There are new and innovative authentication approaches that can help move the industry to more secure, passwordless future, such as FIDO standards and WebAuthn. The ongoing hospitality project at the NCCoE will include FIDO authentication techniques.

**References for Further Exploration**
The National Initiative for Cybersecurity Education (NICE) at NIST is working to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. Even if your job title doesn’t include the word “cybersecurity” and your tasks are not focused on your organization’s cybersecurity risk posture, your employer should offer you cybersecurity awareness and training programs that prepare you for the challenges of operating on enterprise systems and offering digital services to customers. NICE’s Workforce Management Subgroup drafted a Workforce Management Guidebook titled Cybersecurity is Everyone’s Job that offers information about what each member of an organization should do to protect it from cyber threats, based on the types of work performed by the individual.

The Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, and Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References, such as existing standards, guidelines, and practices for each Subcategory. NIST recently celebrated the Framework’s 5th anniversary in February, and is hosting a webcast on April 26 to look back and ahead at the Cybersecurity Framework.
Stay Connected with the NCCoE

NCCoE cybersecurity practice guides for retail and hospitality offer useful insights and act as a foundation for businesses interested in creating a more secure environment for their customers.

To join the Hospitality Community of Interest, email hospitality-ncco@nist.gov.

To join the Consumer/Retail Community of Interest, email consumer-ncco@nist.gov.