# The Fast-Forward Tech Stack for 2024

The Hotel Yearbook Technology 2024

HYB

HYB

# Future Shifts in Cybersecurity Focus

Data & Security

**Lynn Goodendorf**
*Cybersecurity Advisor and Author*

**Synopsis**
Amid rapid tech advances and the shift to remote work, cybersecurity has become a pressing concern. Recent incidents, such as Toyota's 2023 data leak, highlight the vulnerabilities of cloud-based data storage. Ensuring software security through thorough vetting, transitioning to password-less technologies, and enhancing endpoint security are essential to counteract threats. Specialized training for staff and strengthening network resilience against potential failures are also crucial. As we adapt to this evolving technological landscape, a proactive approach to cybersecurity is indispensable.

We have seen some remarkable and rapid changes in technology architecture and strategies in the past few years. The pandemic accelerated the use of cloud services. And we have seen many hotel jobs move to a remote working arrangement either at home or to support multiple locations. On top of this, travelers are using their mobile devices extensively and expecting high availability and performance in Wifi and Internet connections. At the same time, we are developing innovative new ways to serve our guests using mobile devices connected to cloud platforms that are Internet dependent. Meanwhile, cybercriminals are well organized and moving fast to adapt their attacks to this changing environment. What are the implications for cybersecurity in all of these changes?

First of all, we need to shift our focus to safeguard our Confidential data in cloud-provided services. As an example, there are some lessons to be learned from a serious data leak suffered by Toyota reported initially on May 12, 2023. Customer data of 2.15 Million people in Japan was leaked from cloud-connected platforms for over 10 years. The leak was due to human error in a misconfiguration of the database settings from “private” to “public”. The cloud platforms involved provided customers with in-car entertainment, assistance in the event of car accidents, and the option to sign up for the new AI (Artificial Intelligence) driver assistance. This type of vehicle connectivity and cloud-based data management is considered essential for the future of autonomous driving and other AI features and as such was a strategic priority.

Toyota committed to taking these actions as a result of this distressing data loss: 1) auditing all cloud settings; 2) implementing a system to monitor these cloud settings, and 3) educating employees on data handling rules. In addition to those remediation actions, penetration testing of the cloud platforms is recommended to identify this type of exposed data on the Internet. If it had been done, the exposed data leakage would have been identified quickly.

But this is only one small aspect of cloud security. From a cyber attacker's perspective, ***software is the target.*** Jason Schmitt, general manager of Synopsys Software Integrity Group, recently said in an interview with CSO Magazine, “The risks include poor software hygiene, security, and reliability, and they arise because companies do not prioritize security when developing, procuring, and managing their business-critical software.”

We cannot afford to sign contracts and implement new technologies without thoroughly testing and vetting the security of the software. It is a disgrace to see how known coding errors are repeated over and over again in new software or in new versions or updates of software in reputable and established companies. No matter how buttoned down security is in the cloud infrastructure and network of a system, hackers can go straight to target data through vulnerabilities in the application code.

And then there is our long-standing first line of defense: passwords. In the future environment, we can expect the adoption of password-less authentication technologies and those changes have already begun. On World Password Day, May 5, Google announced that it is moving forward with passkeys that allow a fingerprint ID, facial ID or a PIN on the phone or device you use for authentication. Apple is rolling out this type of technology in iOS16 compatible devices and Microsoft is using it through its Authenticator app.

Stronger and new types of authentication for logins require focus because theft of login credentials is expected to continue as a primary attack method. This is in fact, the root cause of many large-scale data breaches. So it is vital to embrace these new password-less technologies.

Today and going forward, a robust end-point security strategy and defense system is critical.

Many of the breaches suffered in the hospitality industry have been due to the infiltration of malware. And these paths for malware will still be open in endpoint devices. The proven technique and best practice are to deploy application whitelisting to all endpoints including smartphones, laptops, desktops, tablets, and servers. Antivirus is not enough due to the rapid number of zero-day viruses, malware, and the difficulty of keeping all devices patched quickly.

In addition, mobile device management is mandatory. The essential functionality of a mobile device platform includes asset management, the ability to remotely wipe/delete lost or stolen devices, the ability to manage software updates and patches, the ability to monitor security features to ensure they are in place and working, etc.

As another shift in focus, we can expect criminal hackers to continue to exploit human behavior. This element of defense is called the human firewall and without it, all the investment you make in security tools and systems can be bypassed by hackers. Trends are indicating that this type of cyber attack technique will escalate in the coming years. Consider having additional specialized training for finance, human resources, sales, and catering teams, anyone using POS devices, and IT staff.

And finally, we need to strengthen network resilience as we are more and more dependent on cloud-provided services and remote working. The action to take is a review of potential network failures or outages which can reveal failure points and mission-critical applications or systems that need to remain on-premises. Outage points can occur with a router and WiFi equipment or cabling, both interior to a building and exterior cable routes. Electrical power failures and network software misconfigurations or errors are examples of other failure points.

There are ways to mitigate these risks but how long has it been since such a review and risk analysis has been conducted?

We can be encouraged that many of these tools and techniques are already available. We can surely expect them to evolve and develop further but it is really a matter of shifting our focus for the future.

**Lynn Goodendorf** — Cybersecurity Advisor and Author
Lynn Goodendorf is a cybersecurity expert whose previous roles include Group Information Security Officer with Mandarin Oriental Hotel Group and Corporate Risk and Chief Privacy Officer with IHG. She currently serves as VP of the Information Systems Security Association's (ISSA) Metro Atlanta chapter.

**Lynn Goodendorf** — linkedin.com/in/lynn-goodendorf-716669
Lynn Goodendorf is a cybersecurity expert whose previous roles include Group Information Security Officer with Mandarin Oriental Hotel Group and Corporate Risk and Chief Privacy Officer with IHG. She currently serves as VP of the Information Systems Security Association's (ISSA) Metro Atlanta chapter.