Luxury Daily®

The News and Intelligence You Need on Luxury

LUXURY MEMO SPECIAL REPORTS

Privacy and security – Luxury Memo special report

January 3, 2019

Privacy and security are top concerns for both brands and luxury consumers. Image Credit: Unsplash

By JOE MCCARTHY

In the aftermath of the massive data breach at Marriott's Starwood Hotels, it has become abundantly clear that while luxury brands have exclusive price points, services and products, their operations are just as vulnerable to cyber crime as any other company.

Numerous high-profile security breaches have been reported over the past several years, exposing the personal information of potentially billions of consumers, and social media platforms have similarly hemorrhaged the data of their users via behind-the-scenes transactions and reckless expansions that leave gaping security holes. Altogether, these events underscore how much work has to be done to shore up privacy and security in the luxury business, and hint at the massive investments that are already underway to earn back the trust of consumers.

"With all the data breaches and violations of privacy, luxury consumers, who have the most to lose from privacy threats, have lost trust in vulnerable social media and brazen databases," said Milton Pedraza, CEO of the Luxury Institute, New York. "This is becoming a crisis and affluent consumers' wealthy donors are beginning to demand action from brands and regulators.

"Besides plain vanilla solutions, brands and their agencies have done little to get ahead of the issue," he said. "It has not been taken as seriously to the level of the threat requires by any brand as far as we are aware."

Top five privacy and security trends in luxury

- Digital responsibility of brands

  The onus of cyber security ultimately falls on companies that are handling massive amounts of consumer data. Although customers should take basic safety precautions such as enrolling in cyber protection services and maintaining strong passwords, it's up to companies to earn back consumer trust through airtight security measures.

- Banking and wealth management

  Inherently risk-averse, the banking sector has generally been ahead of the curve when it comes to cyber security, enacting various reforms to shield the privacy of high-net-worth individuals. At the same time, rapid

adoption of mobile services and the ever-evolving nature of cyber risk have left the industry exposed.

- Emerging technology

  With technologies increasingly relying on biometric information such as face or fingerprint scans, consumers and companies have to take cyber security more seriously than they ever have before. This often means putting security ahead of innovation and ensuring that a solid foundation for protecting data is in place before a new product or service is rolled out.

- Security measures

  As security risks escalate around the world, a suite of security tools promising peace of mind have sprouted up and luxury consumers would do best to become informed of their options. Many of these tools require high-net-worth consumers to become versed in the vocabulary and basic dynamics of cyber security.

- Social media

  Social media is often intensely intimate and users participate on platforms with the presumption that their information, messages and interactions are protected from prying eyes. This implicit understanding has come under grave scrutiny in recent years, following a seemingly endless parade of data breaches on major platforms such as Facebook, LinkedIn and Twitter.

Digital responsibility of brands

Beginning in 2014, hackers gained access to the guest database of Starwood Hotels, gradually gathering the information of an estimated 500 million customers (see story).

The breach exposed home addresses, email addresses, passport information, payment details and more. Security experts warn that those exposed are at higher risk of cyber fraud and criminals in possession of their information could open accounts in their names.

It was a dizzying revelation that could not have come at a worse time — right around the holidays, when consumers are getting ready to travel and open up their wallets to buy presents.

And the worst part of the ordeal is that it was not even out of the ordinary.

The new Starwood Luxury card. Image credit: American Express

In recent years, scores of companies have had the private information of their customers siphoned by cyber criminals (see story). In fact, an interactive feature by *The New York Times* shows how much personal information the average American has likely lost to cyber criminals, from credit history to credit card numbers to fingerprints, and reveals how hard it has become to remain untouched by cyber crime.

Rather than wait for cyber crime to interrupt their bottom line, brands should proactively institute reforms throughout their operations to protect consumers (see story). As time goes on, lack of preparation will be enough to deter consumers from spending money on a brand.

“In 2019 trust will become key currency for brands,” said Michael Becker, managing partner at Identity Praxis. “People will increasingly choose between brands based on trustworthiness, with privacy, security and compliance being key attributes for establishing trust.

“Moreover, in 2019, brands will begin to understand the importance of preparing for the emerging personal

information economy," he said. "They will realize that an individual's personal information is an economic asset that increasingly will become a currency of exchange between the brand and the individuals being served."

This process begins with investing heavily in the integrity of company Web sites, point-of-purchase terminals in stores and third-party affiliations.

When safeguarding Web sites, there are a few golden rules companies should follow, according to security experts at Sucuri, including always updating Web sites when new plugins and other tools are available, using trusted servers and Web site extensions and installing encryption services such as SSL.

These are just a few of the baseline steps that should be taken to protect brand Web sites.

When it comes to in-store protections, companies have to ensure that payment info is not being lifted when consumers swipe their cards or from backend payment processing databases.

Although industry-wide precautions have been taken to prevent credit card skimming, companies can still be targeted by point-of-purchase malware. Top-of-the-line security systems, the latest and most advanced terminals and constant monitoring of backend infrastructure can help companies avoid in-store crises (see story).

In recent months, some of the biggest multinational businesses have signed Microsoft's Digital Call for Peace, a movement designed to get world leaders and companies to commit to stronger cyber protections and collaborate to enforce cyber laws.

Microsoft's HoloLens

Companies big and small would do well to join this effort to signal to consumers that they are serious about cyber security.

Further, in the years ahead states throughout the U.S. and elsewhere are expected to roll out more stringent digital regulations that will punish shoddy security measures with hefty fines, according to Mr. Becker (see story). In a world of a higher standards, getting ahead of the curve with early investments makes sense for a company's bottom line.

"Moreover, brands will invest heavily in identity resolution services," Mr. Becker said. "As 2019 closes, brands will begin to understand the need to respect self-sovereign identity and will begin to put identity controls into the hands of the people."

Banking and wealth management

Affluent consumers throughout the world generally have reliable banking and wealth management options that take cyber security seriously (see story).

"The banks are among the most mature industry from a cyber security perspective, due to their historically conservative approach to risk, their consistent, sizable investments in security and privacy safeguards and their tradition of collaboration within the industry and with authorities," said Charlie Jacco, financial services lead, cyber security services KPMG in the U.S., in a report.

Because of the significant amount of assets and transactions handled by banks, they often lead the way when it comes to cyber security. Oftentimes, regulatory frameworks cover banks and wealth management firms before they expand to cover the rest of economies because of the risk levels associated with the industry if vulnerabilities were allowed, according to KPMG.

Hong Kong boasts some of the most wealthy consumers in Asia Pacific and also some of the most expensive real estate. Image credit: Florian Wehde via Luxury Society

Banks have also had to play defense for the full scope of activities that their customers engage in through extensive fraud monitoring departments that specialize in thwarting cyber theft.

Additionally, banking companies also have to work with various third parties and have to ensure that these partners are up to par when it comes to digital security.

“Banks are taking actions to evaluate security controls of third-party providers, scrutinizing what data is being shared with outsiders and even beginning to conduct cyber security simulations that involve testing third-party connections and personnel,” said Henry Shek, head of cyber security services for KPMG in China, in a report.

Banks and wealth management firms also hold vast amounts of private information and protecting this data has become a top priority, especially following major breaches at credit reporting agencies such Equifax, which exposed the information of 143 million Americans.

Many financial institutions are going beyond encryption services and investing in blockchain technology to safeguard consumer data (see story).

In some parts of the world, blockchain has been used in ways that make digital vulnerability seem like a thing of the past.

For example, the government of Estonia has created blockchain infrastructure for holding citizen information and carrying out basic services. In the process, Estonians no longer have to worry about identity theft.

Blockchain can also reduce that old foe of luxury commerce – counterfeits – by significantly improving authenticity and verification measures. Some luxury brands have already adopted blockchain as a way to signal transparency and security (see story).

Emerging technology

While some technologies such as blockchain could improve cyber security in the years ahead, others have the potential to further unravel it.

The Internet of Things (IoT), in particular, is being adopted at a scale that outpaces the quality of its security. Various computer programmers and engineers have shown that smart cars can be overtaken by a remote hacker and made to crash, and the popular television show "Mr. Robot" demonstrated how a home hooked up to the latest in-home technology can be hacked and go terribly awry.

Since affluent consumers are the most likely to adopt smart objects and incorporate them into their day-to-day lives due to high price points, they are often also the most at risk to cyber crime.

Automation may seem antithetical to luxury, but smart brands can integrate it without compromising quality. Image credit: Mandarin Oriental

Steps can be taken to secure smart technology, but some of the flaws are inherent to the technology and can be infiltrated by sophisticated criminals regardless of the safeguards put in place. As a result, many companies have to invest in a new generation of smart objects that are fully secure.

The IoT is also rapidly being incorporated into retail environments in ways that can undermine consumer privacy. For example, devices that detect a shopper's identity and curate a relevant or enhanced experience are being introduced (see store), but many still have security flaws.

And then there are the proliferation of smartphone applications that gain permission to a person's location, contacts and more. As data analysis tools become more sophisticated, a user's whereabouts can be tracked on a minute-to-minute basis, according to a report from *The New York Times*.

These developments roll back gains that have been made to safeguard user privacy, and mounting outrage on the part of consumers is helping to drive a shift in the opposite direction.

Security measures

High-net-worth individuals have a vast array of tools at their disposal to boost their online security and safeguard their privacy.

The first thing that affluent consumers have to do is learn more about the basics of cyber security and the various ways that cyber crimes are launched.

Oftentimes, schemes and scams are easy to spot if an individual knows what to look for. For example, phishing ploys that attempt to gain access to person's computer or smartphone through an email or text message generally contain glaring errors or inconsistencies that signal nefarious intent.

Affluent consumers should invest in security systems that can constantly monitor computers, phones and other devices for intruders and theft. On top of this, individuals can invest in fraud monitoring programs that can identify if and when identity theft occurs.

More online shoppers are turning to smartphones than desktops or tablets. Image credit: Bloomingdale's

Even the best defense systems cannot provide absolute security, so affluent consumers should also purchase cyber liability insurance just in case an event happens at some point.

Many companies offer bundle options to high-net-worth individuals and families, covering security, monitoring, insurance and more. For example, Morgan Stanley's The Magellan Group oversees $2.4 trillion in assets for affluent clients.

Other companies specialize in digital security. In the wake of the Equifax breach, the digital cybersecurity firm Rubica rolled out a cyber concierge for wealthy customers that provides on-the-spot consulting in moments of digital alarm.

Social media

The amount of data that social media and other popular sites have gathered on users is a cause of great alarm, especially for high-net-worth consumers that prize privacy (see story).

Facebook and Google have hundreds of data points that represent a veritable life summary of each user that they then sell to other companies for advertising and other purposes. These companies also track and log every action taken on the sites, including every search, like, comment and more.

For many users, these revelations have come as a stark violation of a tacit feeling of trust, and have encouraged many people to abandon popular platforms.

In fact, there are very few ways for users to safeguard their data on these Web sites, except locating the limited privacy controls available in a platform's settings and checking the most stringent options (see story). These steps, however, do little to pry a user's profile away from the many data mining companies buying and selling information.

Facebook has faced widespread criticism over use of personal data.Image credit: Facebook

Social media platforms are also vulnerable to massive data leaks, as has happened at Facebook numerous times over the past several years, exposing the private information of hundreds of millions of users.

The best option for affluent consumers may be seeking out platforms that prioritize privacy, or limiting social media engagement.

"Privacy and its close cousin security will become one of the most important topics for luxury brands in 2019 and beyond," Identity Praxis' Mr. Becker said.

"In fact, privacy has become a new luxury good," he said. "People will begin to distinguish between brands that provide cutting-edge privacy and maintain state-of-the-art security."

The Luxury Institute's Mr. Pedraza and Mr. Becker both agree that the years ahead could usher in a new paradigm for privacy, with the flagrant overreach and abuse of social media giants and other companies spurring a movement among users to regain control of their personal data (see story).

"Consumers will demand that brands demonstrate that they can protect their data," Mr. Becker said. "Consumers will begin to use legal and political pressure to get companies to act responsibly.

"Consumers will eventually demand to own their own data and brands will have to pay to market to them."

Best practice tips for privacy and security

- Michael Becker, managing partner of Identity Praxis
    - "Luxury consumers should begin to adopt the five-fold path to digital sovereignty: awareness & understanding, intent and behavior, insurance & professional services, social accountability and

adoption of passive and active technologies."

- "Luxury consumers should take accountability for themselves online and take action to product themselves, gain personal insight from their data and then ultimately actively participate in the exchange of their data."
- "Maintaining effective and efficiency privacy and security practices is not enough. Brands must also maintain compliance to and prepare for the latest regulatory frameworks, like the GDPR and California Privacy Protection Act."

- Milton Pedraza, CEO of the Luxury Institute
  - "Store as little of the most potentially harmful personal data as possible."
  - "Create data protection and encryption methods to stay ahead of hackers."
  - "Develop better detection and prevention systems."