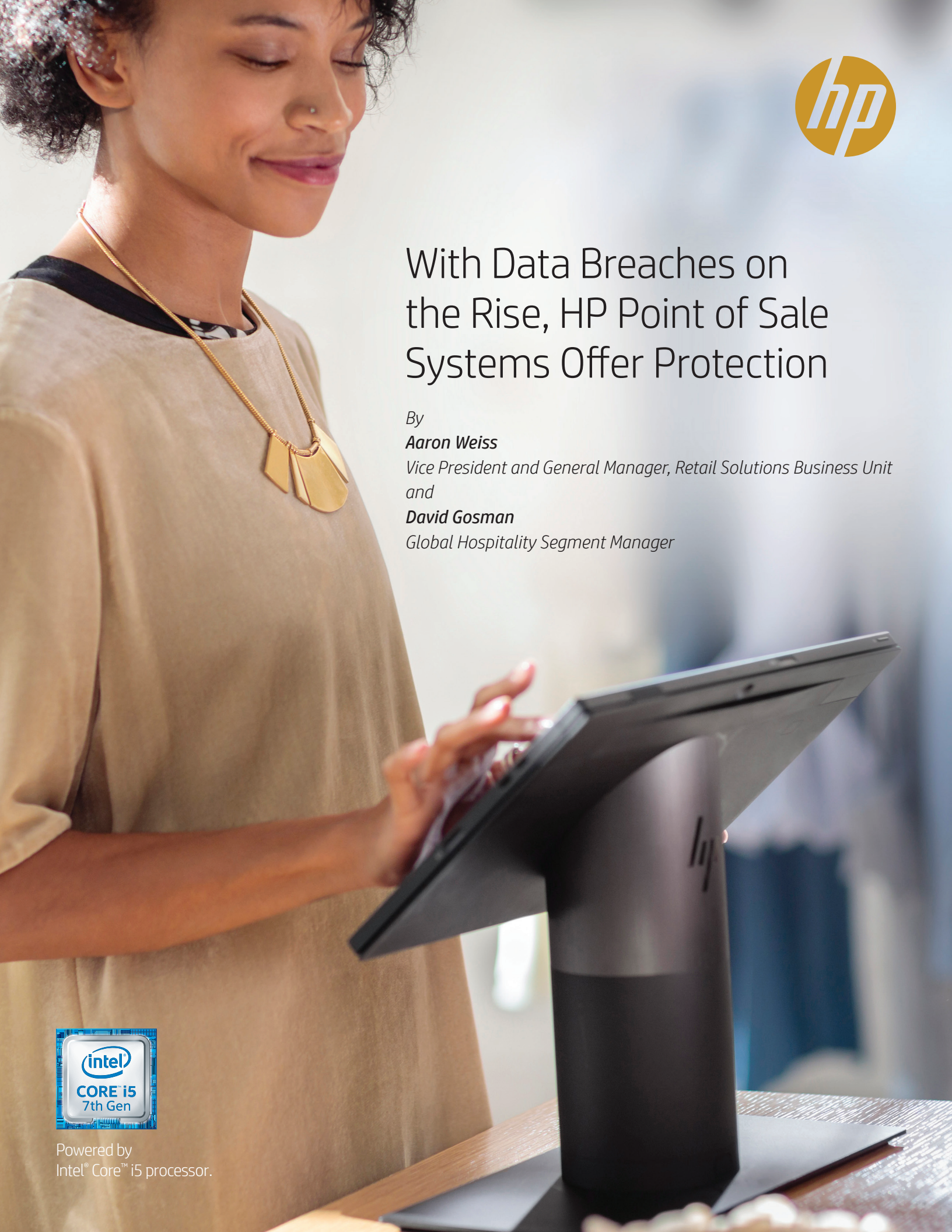


With Data Breaches on the Rise, HP Point of Sale Systems Offer Protection

By
Aaron Weiss
Vice President and General Manager, Retail Solutions Business Unit
and
David Gosman
Global Hospitality Segment Manager

Powered by
Intel® Core™ i5 processor.

A point of sale system is unlike any other piece of technology employed by businesses. It is a sophisticated computer system that manages sensitive customer data in a public space, often accessible by a large number of employees, in addition to customers or anyone else in the area. Because of this, it's a unique target for compromised data. Plus, it's mission-critical nature means compromised systems can bring a business to a halt, resulting in lost business.

"Within the business space, it's estimated that 89 percent of retail data breaches were targeted at point of sale systems[2]."

It is estimated that organizations have a one-in-four chance of experiencing a data breach[1]. Within the business space, it's estimated that 89 percent of retail data breaches were targeted at point of sale systems, according to the 2018 Verizon Data Breach Report[2]. At HP, data integrity is of utmost importance, and we have prioritized advanced security in our technology at every step of the design process.

Point of sale devices are targets for attack precisely because they are so versatile in the business environment. They're instrumental to processing transactions, and multi-purposed to be deployed in multiple locations within a store or placed at any location within a property. That omni-presence makes securing devices and preventing attacks even more important because there is a higher potential for attempted data theft in public spaces that are not always monitored. This is the duality of point of sale systems: they must be versatile enough to be deployed anywhere and interact with a high volume of customers, but also secure enough to safely conduct transactions and repel any attacks.

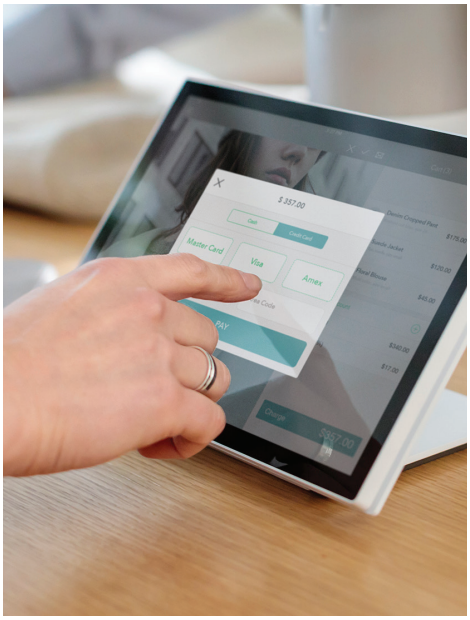
Most importantly, if your devices aren't secure, they can be a major disruption to the business.

Increased Connectivity, Increased Vulnerability

In a modern retail space or hospitality environment, there are more systems communicating than ever—which in turn creates more opportunities for a potential breach. Restaurants take online orders, retail stores receive online orders for click and collect, and hotels hold reservation information that's booked online—while all three of these systems interact with loyalty programs containing historical customer data. This increased cloud connectivity extends far beyond point of sale systems—stores are increasingly embracing IoT technology such as a connected HVAC system—which only increases the number of potential entry points.

" Every business has the responsibility to protect any information it receives from a customer, and the consequences have never been more serious."

If we take the order process for a store as an example, personal information is captured for every online order, whether shipped to home or held for pickup. Online food ordering requires location data and personal information transferred to a machine in-store. Purchases can be connected to loyalty plans or social media, giving retailers access to even more information about customers. This allows for useful personalization, but it also places an increased burden on any business to protect that information. Every business has the responsibility to protect any information it receives from a customer, and the consequences have never been more serious.



The Visible and Hidden Costs of a Data Breach

Breaches cause multiple kinds of damage that can affect businesses. The kind of data used in retail and hospitality spaces—including credit card and payment processing credentials—is both valuable and highly sensitive.

In the event of a breach, there are several serious ramifications. Personal financial data can be stolen, which is a burden for individual customers. Depending on local laws and agreements with financial institutions, businesses must publicly disclose breaches and may be fined after suffering a breach. And compounding those losses, the reputation of any business that gets hit takes a significant drop, losing public trust. Retailers that suffer personal data breaches can see business decline for months to come—in some cases matched by a shift to payment by cash, or customer avoidance altogether.

There is also the possibility of system disruption. A point of sale device is the life support of a retail store or restaurant. If a business is unable to ring up customers due to a breach, even for just a few hours in peak season, it can have a tremendous negative impact on a brand through customer inconvenience and lost revenue. These are the stakes for protecting information and maintaining system integrity—which is why the defense mechanisms are of paramount importance.

"To protect a device, HP delivers physical protection for the actual device and internal digital protection for the system and the information it stores."

Innovative, Evolving Protection

We have three levels of focus when it comes to protecting information on point of sale equipment within a business: device security, identity security, and data security. HP takes steps in each of these areas to help maintain security at the highest level.

To protect a device, HP delivers physical protection for the actual device and internal digital protection for the system and the information it stores. HP point of sale equipment comes with ways to physically attach or bolt down devices. Some systems support Kensington locks, providing the ability to secure devices to a counter. Point of sale systems may also use many different peripherals, from cash drawers and keyboards to printers and touch screens—all connected through ports. HP provides the ability to selectively disable ports to prevent any nefarious attempts to gain access to a system with an unauthorized device. With 7th and 8th generation Intel® processors, HP's devices have power through peak usage adding a layer of durability important to keeping devices up and running.

The HP Engage family of point of sale devices have also inherited quite a few of the advanced features from the HP commercial line of personal computers. For example, a BIOS-level attack could grant access to a machine before other defenses have a chance

to defend at the operating system level. HP has proprietary technology to protect against this - if a BIOS-level attack corrupts the system, the HP Sure Start[3] feature compares the actively running BIOS to a hidden, approved version for inconsistencies, and self-heals in the event of a discrepancy.

HP Engage point of sale systems also have the ability to support and enable features like Device Guard[4], which allows an IT department for a business to whitelist only the applications approved for use on a given device. This prevents any unauthorized application from running on the system.

At the identity security level, HP devices have the ability to support Credential Guard[4] which protects the identity of employees signing into the system, ensuring the security of Personally Identifiable Information. HP has also developed strong multi-factor authentication mechanisms—including biometric fingerprint readers to authenticate employees—making our devices significantly more secure than single, non-hardened "login and password" features.

"Hackers do not rest, and neither do we. We are constantly updating features to create additional security for every generation of HP devices and the information customers store on them."

And at the data security level, there are self-encrypting drives, and many other features across the HP point of sale product lines that are designed to help ensure high data security.

There's no stopping point for these protective measures. Hackers do not rest, and neither do we. We are constantly updating features to create additional security for every generation of HP devices and the information customers store on them.

This is the harsh reality in the new paradigm of data breaches. But it's not all an impending storm—there are new defenses and secure design strategies in new technology geared to repel, protect against and prevent these attacks. The increased vulnerabilities that naturally emerge from a larger, more interconnected business space don't have a single solution. HP can help protect the data that flows through point of sale environments with constantly evolving technology. Businesses using our technology can feel secure knowing that they are taking every precaution while seeking out new and innovative defense strategies to protect customer data and maintain a sterling reputation.

Keep an eye out for more articles from HP covering further aspects of the HP Engage point of sale family, including mobility, service innovation, and more.

Powered by
Intel® Core™ i5 processor.

Learn more at
hp.com/go/engage

Share with colleagues

1 Security Intelligence, 2017 Cost of Data Breach Study, June 20, 2017.
2 Verizon, 2018 Data Breach Investigations Report, April 10, 2018.
3 HP Sure Start Gen4 is available on HP Elite and HP Pro 600 products equipped with 8th generation Intel® processors.
4 Microsoft Device Guard and Credential Guard are available with Microsoft Windows 10 IoT Enterprise 2016 LTSB delivered from HP or to customers with a volume license to use Windows 10 Enterprise. Microsoft Device Guard and Credential Guard are not available with Windows 10 Pro. The installation of Windows 10 Enterprise and Microsoft Device Guard and Credential Guard is available through HP Configuration and Deployment Services.

© Copyright 2018 HP Development Company, L.P. The information contained herein is subject to change without notice. All other trademarks are the property of their respective owners.
Intel, the Intel Logo, Intel Inside, Intel Core, and Core Inside are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

4AA7-3558ENW, August 2018