DATA ERASURE CASE STUDY

Securely Erasing Company-Owned SSDs Prevents Theft of Employee Data

Statistics

85% Japanese & ASEAN organiza ons feel their company is at risk of an insider attack*

¥274 million average cost of a data breach in Japan**

¥13,788 average cost of a stolen record in Japan**

The rise in the number of connected devices, or the Internet of Things (IoT), as it is more commonly known, has led to businesses equipping employees with a whole host of smart devices, allowing them to stay connected whilst on the go. For businesses, this means employees are equipped to perform at optimal levels of productivity and efficiency. On the other hand, the proliferation of sensitive company data across these connected devices heightens the risk of falling victim to a data breach, imposing both financial and reputational damage to the business. If data isn't adequately erased before these devices are reused, recycled or resold this can have devastating consequences for both employees and their employers.

Samsung Japan

Samsung Japan was established as the Japanese retailer for the semiconductor division of Samsung Electronics, specializing in semiconductor components, including memory, system LSI, TFT- LCD and organic EL products.

> **Because the work is automated, we managed to reduce the human error associated with manual operations and release resources for other document creation and in-house audits. I would say that management of data deletion now requires about a sixth of the man-hours that it used to, so we have managed to improve efficiency."**
>
> – Hiroki Uno, Business Innovation Partner, Samsung Japan

Challenge

As the retailer for a cutting edge semiconductor manufacturer, Samsung Japan has introduced its own products, such as smartphones, tablets and PCs with internal SSDs, for its staff. As these devices often contain

*Vormetric Insider Threat Report, 2015
**PwC Global State of Information Security Survey, 2015

Results

- ✔ **70% faster than previous erasure method**
- ✔ **3 working days gained per employee, per year**
- ✔ **84% reduced working-hours than previous erasure method**

confidential information, such as classified technical specifications and customer data, the company needed to find a secure and efficient solution for completely wiping data from the internal SSDs. The solution previously being used by Samsung Japan required disassembling the devices following the erasure process to record serial numbers for auditing purposes, which could often take significant amounts of time and resources to complete.

Solution

To securely erase data from SSDs across a wide array of IT assets, from desktop computers and laptops to smartphones, and tablets, Samsung Japan relied on a holistic data erasure management approach.

Using Blancco Drive Eraser, the company was able to quickly and effectively perform multiple SSD erasures, across a range of devices, without disturbing or damaging the operating system. Samsung Japan also required a more efficient way of recording proof of erasure. With Blancco Management Console, the company can get a centralized point of view of all data erasure licenses, create and modify users, monitor activities and collect 100% certified, tamper-proof audit reports.

About Blancco

Blancco Technology Group is the de facto standard in data erasure and mobile device diagnostics. The Blancco Data Eraser solutions provide thousands of organizations with an absolute line of defense against costly security breaches, as well as verification of regulatory compliance through a 100% tamper-proof audit trail. Our data erasure solutions have been tested, certified, approved and recommended by 18 governing bodies around the world. No other security firm can boast this level of compliance with the most rigorous requirements set by government agencies, legal authorities and independent testing laboratories.