BrassValley.com

Embedded Data: Your “Hidden Secret” to Stopping a Major Data Breach

A call for awareness to the security threat of embedded data

BRASSVALLEY
THE OTHER FIREWALL™

Embedded Data, the Hidden Threat inside Off-Network and End-of-Life Device

Executive Summary

Organizations spend most of their IT security budgets on devices that are on-network and protected by firewall technologies; however, over 70% of data breach events come from off-network devices. This indicates that there is a huge disconnect between perceived and actual threats to data security. Exacerbating this problem is the fact that many companies have no visibility into the root cause of a cyber-attack. A study released by the Ponemon Institute in June reported that 45% of organizations have no way of knowing what the root cause of an attack was.

Historically, organizations focus most of their attention regarding off-network data security on securing the hard drive. They focus the data eradication and erasure tools, encryption, tracking, reporting, and the security services available on securing the hard drive because that is where the data resides. Distributed intelligence has created a world where devices have embedded data i.e., not necessarily on a hard drive, with the potential to cripple any business. Historically, if a hard drive was lost or stolen, damage could, for the most part, be compartmentalized and managed. However, embedded data can allow access to your organization's network and in the wrong hands, has the potential to inflict damage on a business in new and very dangerous ways, financially and reputationally.

Although the data security measures undertaken by companies and the number of data security laws on the books are increasing,

Over 70% of data breach events come from off-network devices.

we still encounter shocking gaps in data security simply because of lack of knowledge. At Brass Valley, we want to help educate our customers and the public at large on the potential exposure from some of the hidden dangers.

The purpose of this whitepaper is to give you examples of embedded data, so you know where it may reside in your environment, and share with you some of the data security gaps we found in looking at devices from companies across the U.S.

What is Embedded Data?

There is a general lack of awareness and understanding around what comprises embedded data, where it resides, and the threat (financially and reputationally) that it potentially poses for companies.

Embedded data is data that is contained in some type of media buried within a system, usually not on a hard drive, and overlooked when it comes to finding and destroying data during the decommissioning process. Embedded data is in hard drives, memory, tape, CD/DVD, flash memory, battery backed cache, and more though you may not be aware of its existence! Embedded data may also be a component of embedded intelligence devices such as embedded microprocessors and computers.

Overlooking embedded data when assessing a security risk posed by a particular device is easy! This means that every device, including servers, computers, Smartphones, tablets, etc., used by your employees may have sensitive information stored on them in a place where you are not looking. These devices pose a security risk to both your company and your customers if you do not decommission and dispose of the devices and associated embedded data properly.

Embedded Data is the enabling technology of the “Internet of Things”

Concerns About Embedded Data

Distributed Intelligence is the Driving Force Behind Embedded Data

Everything is getting smarter, which is great! Smartphones, cars, industrial sensors, smart PDU's, HVAC systems, household appliances, medical equipment, and much more are now connected to the internet 24 hours a day, seven days a week, enabling intercommunication between our devices to make our lives easier. This is the Internet of EVERYTHING that we hear about on a daily basis! However, it also puts the organization and clients potentially at risk. This constant interconnectedness also means that data from all these devices is constantly being collected, stored, and monitored, which is where the danger lies. If the organization does not properly manage, protect, and destroy this data when they decommission these devices, there is a huge opportunity for unauthorized access to the organization and clients' sensitive information.

Best Practice

Think outside the hard drive for places where embedded data may be found but do not overlook the hard drive either. An example would be hard drives on copiers or on data center networking devices and other media-storing appliances.

Why Security Experts are Concerned about Embedded Data

In July 2014, at the "The Future of Warfare" at the Aspen Security Forum, Dawn Meyerriecks, the Deputy Director of the CIA's Directorate of Science and Technology cited concerns about the looming geo-security threats posed by the Internet of Things, i.e. the embedding of computers, sensors, and Internet capabilities into more and more physical objects:

> *"Smart refrigerators have been used in distributed denial of service attacks. Last year at least one smart fridge played a role in a massive spam attack, involving more than 100,000 internet connected devices and more than 750,000 spam emails. Even smart florescent LEDs that are communicating their need to be replaced are also being hijacked for other things."*

Why is Embedded Data Important?

In August 2014, at Black Hat USA and DEF CON 22, the dominant and overarching conversation was about the discovery of embedded hardware weaknesses, hardcoded credentials, and intentional backdoors. These weaknesses were on display by researchers who found them in cars, TSA checkpoints, networks, security systems, to name only a few.

In an interview with *60 Minutes*, Dick Cheney said that he had a wireless pacemaker installed that would allow his doctor to monitor his heart online. However, he refused to enable the Bluetooth broadcasting feature for fear that it could be hacked.

These are only a handful of examples of what security experts are concerned about when it comes to embedded media and the data security risk it can pose.

Why is Embedded Data Important?

Embedded data is important due to the nature of the data itself. IP addresses, passwords, login information, device information, company information, confidential information, and other bits of information can now find their way deeply embedded in a device where you would not expect it.

We recommend identifying embedded data sources as new equipment comes into production so it can be inventoried and monitored properly during production and decommissioning.

Client Case Studies: Embedded Data, an Entry Point for a Data Breach

We see examples of companies overlooking hidden data almost on a weekly basis. Some recent examples include:

A client asked us to help them remarket their old phone system, which was comprised of a few hundred phones and a few controller units. When we discussed data security, the client told us the devices were free of any data; that someone had come in and erased all their hard drives. When we brought the equipment into our facility for processing and remarketing, as a normal part of the process, we test all items designated for refurbishment and resale. During the test procedure we found the phones contained IP addresses, passwords, and voicemails, all contained as embedded data.

An example of embedded data showing up somewhere unexpected with the possibility of major negative consequences happened at a well-known box store. They had sent us all their inventory scanners for disposal. They insisted further data security services were not applicable because some other firm shredded their hard drives. Unfortunately, they were a victim of not addressing the embedded data! We found wireless cards in each scanner with complete login credentials to the wireless network of the client. What a find for a nefarious individual attempting to get into their network!

Most of the times when we present embedded data concepts, people naturally tend to think of devices outside the data center. Locating embedded data within the data center is not intuitive and this can be dangerous because data center equipment can contain some of the most devastating forms of information if it falls into

Best Practice Best Practice

Chances are, when you are decommissioning equipment, you won’t be thinking about embedded data.

Unfortunately, the companies you contract for data destruction services may not be thinking about it either.

the wrong hands. A good example of this occurred with a client that was refreshing their switches and we were called in to provide a trade in value. We asked if part of the buy price would include proper erasure of the devices. The client thought for a minute and said, "I'm not sure." We talked further and discovered that he had no idea which switches had media in them and which ones did not. Because he was not aware of it, and he did not track it, he was not sure what devices needed data security processing. This realization made him think about the possible wide-open exposure his company had from previously decommissioned switches that he did not erase properly.

A large financial client was replacing and reselling their multifunction fax machines. They insisted that they flushed the memory buffers and everything was gone. Two months later, the manufacturer showed up at their door looking to fix a fax machine that was dialing home for repairs. The client did not realize there was more than one memory buffer and that it had a call home feature in it and one of the remarketed fax machines used it in its moment of distress. Now the company is distressed!

These are just a few examples of how easily embedded data can slip through traditional decommissioning processes. Some constitute a total breach. Some provide data like IP addresses and passwords that are the point of entry for a data breach. Now you may be asking, how can I be proactive in protecting my company from an embedded media breach?

When you return your copiers after their lease expires, you should not only ask for proof of data destruction for the hard drive, but also proof of destruction for the media containing the IP addresses connecting the copier to the network.

Taking the Steps to Protect Your Company from an Embedded Data Breach

Begin with the end in mind. Proper identification and inventory of embedded data-bearing devices is an essential first step. You need to define, in advance, how you will eradicate data on devices at end of life, including all of the specific process steps and associated costs. You need to ensure that you have a documented, quality assured process in place. This includes making sure that you train and certify the people performing the tasks in this process.

Types of Data whose storage points you need to track

It is important to account for all of the data you may be storing on various devices during the inventory process, so that it can be monitored properly online and erased/destroyed at end of life. For example, you need to know which board on the switch has the drive on it. Is there sensitive information on it that you need to destroy? Chances are the answer to this question is YES. Here are some common types of embedded data that may be stored on your devices:

- IP Addresses
- VLANs
- Administrator userids
- Passwords
- Login information
- Device information
- Company proprietary information

The average cost of an organizational data breach is $5.4 million

Ponemon Institute
June 2014

- Confidential information, such as patient information, social security numbers, financial information
- The list is growing ….

Where do I Find Embedded Data?

- CDs/DVDs
- USB drives
- IP Phones, including Handset and Controller Units
- Networking Devices of any nature
- Portable Devices
- Storage Controllers
- Wireless technologies
- Climate Controllers
- Power Distribution Systems
- Firewalls / Network Intrusion Detection
- Copiers
- Faxes / Scanner / Multifunction Devices
- Medical Equipment
- Banking Equipment
- Cell phones
- Tablets

Implement a strategy to identify where “Embedded Data” may be hidden, and develop the appropriote tactics to manage it.

Conclusion

The IT industry has a focus on electronic attempts to breach their firewalls but a more comprehensive approach includes recognition of the threat that comes from off-network devices as well. This is especially true given the fact that most companies are not able to determine the root cause of breaches. The growing prevalence of embedded data contained in off-network and decommissioned devices, and the people responsible for the decommissioning process and their vendors are, largely overlooking the threat that it represents. Brass Valley is changing that by bringing attention to the impact of the mishandling of embedded data.

Cloud Implications- Transitioning to dumb clients may appear to present little risk since they hold little resident data. However the fact that they have network connectivity rights and login to cloud apps makes them a vulnerability point.

BRASSVALLEY
THE OTHER FIREWALL™

Brass Valley is the leading provider of customized secure IT asset management services using “The Other Firewall”™ tools and methodologies to support some of the most security conscious companies in the world.

For more information, contact us at Brass Valley.

508.545.1200 • BrassValley.com • 425 Fortune Blve., Milford, MA 01757