IT SECURITY RISKS:

Overlooked Vulnerabilities & Best Practices

An EPC White Paper

December 2014

Introduction

Over recent years, there has been an increasing awareness of "total IT security," focusing not just on in-network systems and devices but rigorous asset disposition as well.

Indeed, from HIPAA/HiTech to Gramm-Leach-Bliley and state-specific regulations, estimates are there are over 550 data and environmental security laws on the books carrying penalties that can range into the millions of dollars. In fact, the average per incident liability of a data breach is more than $7 million[1] while environmental fines can easily top $30,000 per day.[2]

In addition, of course, there is the damage to a company's reputation, customer relationships, competitive position and brand reputation that often comes about through the accidental release or deliberate theft of the thousands of pieces of personal, customer and private corporate information stored on the on thousands of PCs, laptops, servers, flash drives, mobile devices and more throughout every layer of the typical organization.

Despite the risks, "compliance" with and even awareness of the security vulnerabilities with on-network devices is often spotty. Potentially more damaging is the fact that off-network asset disposition protocols within many organizations can range from marginally adequate to non-existent. This is surprising since companies are legally responsible for any data recovered from devices they dispose of. Nonetheless, here's what some recent findings have shown:

- The Ponemon Institute reports that 70% of data breaches come from offline computers.[3]
- A study commissioned by BT Group and conducted by the Faculty of Advanced Technology at the highly regarded University of Glamorgan in the UK shows that 34% of computers recirculated back into the marketplace contain personal or proprietary information, including[4]:
    - Confidential business plans
    - Private patient information
    - PII (personally identifiable information)
    - Corporate financial data
    - Internal security policies
    - Employee information
    - National defense secrets

The BT Study organizers said, "This is the fourth time we have carried out this research and it is clear that a majority of organizations and individuals still have no idea about the potential volume and type of information that is stored on computer hard disks.

For a very large proportion of the disks we looked at, we found enough information to expose both individuals and companies to a range of potential crimes....“ Of significant concern is the number of large organizations that are still not disposing of confidential information in a secure manner.”[5]

Overlooked Vulnerabilities

With that as background, the primary focus of this White Paper is on newer and increasingly ubiquitous technologies and devices that can present special and often unanticipated vulnerabilities.

They include the exposure of personally identifiable consumer information ... confidential customer, financial and third-party data ... private corporate information ... trade secrets and intellectual property ... contract details ... employee records and more.

Vulnerability #1: Mobile Devices

Phones and tablets are probably the #1 security threat organizations face these days. While we’re all familiar with the most common vulnerabilities such as device ownership issues, downloading malware-containing apps, accessing corporate information from unsecure sites and so forth, potential new threats are also on the horizon.

For example, security issues are rarely considered when performing everyday activities such as charging a device. However, a recent experiment showed that despite all the defense mechanism in iOS, arbitrary software was successfully injected into current-generation Apple devices.[6]

The experiments show that despite protection in the hardware, malware designed to take over the device can be introduced through trojan power sources. Researchers also showed how the malware infection can remain undetected by using the same technology Apple uses to hide its own built-in applications.

Batteries in laptops have also been cited as potential attack vectors. Other vulnerabilities include:

SIM Cards

This generally considered safe data storage data center of mobile handsets is facing a critical hacking risk according to some experts, especially among older units. One critical risk: the ability to surreptitiously re-direct and record sensitive calls as well as paving the way for targeted attacks. Of greater potential concern is a hack that was able to bypass encryption in more recent cards, allowing the hacker to assume the victim’s mobile identity and receive his calls and text messages.[6]

SD Card Storage

Security researchers, Andrew "bunnie" Huang and Sean "xobs" Cross disclosed in a blog post and talk at the Chaos Computer Congress (30C3) that they have found a way to hack SD Cards and create the perfect setup for man-in-the-middle attacks. Maliciously applied, these hacks can intercept, scrutinize and modify sensitive data.[7]

Best practices

- Plug devices directly in an electrical outlet for charging. If that option isn't available, use a USB device that blocks data transfer. (Visit http://portpilot.net/)
- Remember that, unlike secure data erasure, factory resets can leave remnant and even fully intact data behind increasing the risks of a data breach. Mobile erasure tools such as Blancco Mobile (http://www.blancco.com/us/products/total-data-erasure/mobile/) work well.
- Remove all SIM cards and corporate apps prior to resale.
- If your company has BYOD policies, ensure those policies have clear guidelines on device replacement that cover data erasure responsibilities.

Vulnerability #2: SSD Hard Drives

DoD 3 erasure standards are not designed for SSD devices. Even more worrisome: Secure Erase procedures are correctly implemented by manufacturers less than 35% of the time. For example, researchers discovered[8]:

- ATA and SCSI command set features for securely destroying data on SSDs (ERASE UNIT) were only successful on 4 of 12 drives tested.
- Repeated overwriting of SSDs is far more complicated and time-consuming than with traditional hard drives.
- Degaussing erases no data stored on SSDs. (While SSDs do not contain magnetic storage, researchers hoped that perhaps the electromagnetism might destroy the electronics in the flash chips.)

Physical destruction must reduce residual material to the smallest fraction of that of platter drives—based on current manufacturing processes, less than 8mm.

Best practices

- Use whole disk encryption to reduce data loss risk. Even if the drive is lost, encryption provides protection against most attacks.
- Ensure erasure methods are specifically designed for solid state storage devices.

Vulnerability #3: USB Devices/Flash

USB devices, including thumb drives, flash drives, pen drives and other similar devices are a major security concern to every organization. Threats range from simple loss—left in a pocket, tossed into a desk drawer and so forth—to deliberate insider attacks and data thefts. Further malware from untrusted machines can be introduced into the entire company network.

Compromising these devices is simple and can be serious. Further, like SSDs, DoD 3 pass standards don't guarantee full erasure and many physical destruction solutions still leave recoverable data.[8]

Best practices

- Employ disk Encryption software such as TrueCrypt.
- Clearly define IT security policies on USB devices.
- When not needed, disable USB storage (Group Policy or 3rd party tool).
- Consider whitelisting trusted devices.
- As with SSD, use erasure methods designed and tested against USB storage media.

Vulnerability #4: Printers & Copiers

Many printers and copiers store all information printed or copied on them. Additionally, because they are generally housed in public areas and often networked within the organization, that data is subject to hacking by both internal and external actors. Information typically subject to compromise includes confidential reports, client information and presentations, employee information, internal financial and operational information as well as strategic, product and trade secret reports. In addition, those vulnerabilities can be exacerbated by out-of-date security patches.

Best practices

- Make sure printers and copies are included in an overall patch management strategy.
- Limit network access. For example a networked printer generally should not be connected to a financial data base server. Instead, place units in a segmented VLAN that lets print/management traffic in and limits traffic out.
- Ask your ITAD vendor for data erasure policies on printers and copiers.

Vulnerability #5: Network Appliances

Despite the problems presented by poorly designed patches, responsible organizations implement and rigorously follow sound patch management strategies. That strategy should always include backing up, testing and installing patches intended to fix security vulnerabilities.

Perhaps because they run in the background, network appliances tend to get overlooked when it comes to patch management—leaving the organization vulnerable to hackers through remote access and backdoors.

Best practices

- Understand what vendor's security and patch management prior to purchase. Ask about dependencies and if patches are deployed as dependent libraries are updated.
- Integrate network devices into your patch management strategy.
- Ask vendors what support mechanisms exist in the product. Trust their word—but verify using netflow tools.
- Follow vendor's recommended data destruction processes. In addition, ask your ITAD vendor for data erasure policies on appliances.

Vulnerability #6: Fax Machines

Like printers and copiers, fax machines often store every document ever sent to or from that device. Default passwords are almost never reset and are easy for hackers to buy, sell or guess at.

Best practices

- Never deploy devices with default administrative passwords in place.
- Consider replacing dedicated machines with a fax to email gateway service.
- Follow the vendor's recommended data destruction process.
- Follow vendor's recommended data destruction processes. In addition, ask your ITAD vendor for data erasure policies on appliances

Vulnerability #7: Phone Systems

Phone systems can operate as virtual espionage agents, capturing all manner of sensitive personal and corporate intelligence. A typical point of entry for hackers: the weak or default pins found at companies across the country.

For many companies, the least painful consequence is the loss of tens of thousands of dollars in phony long distance and international calls. (Often to suspicious locations that draw the attention of Homeland Security.)[9]

Of more concern is the fact that phone systems can be used in social engineering attacks, listen to voicemails, as reconnaissance tools to gain access to administrative features and more. Further, VoIP sniffers can silently intercept calls from the network and record the conversations of both parties.[10]

Best practices

- Don't overlook the basics: keep systems up to date, avoid default passwords, and make sure new passwords are strong.
- Limit access to VoIP systems from untrusted networks.
- Audit voicemail pins for easy to guess passwords (1111, 1234, 9876, etc.).
- Never deploy devices with default administrative passwords in place.
- Include phone systems in your patch management strategy, including the phones themselves.
- Follow vendor's recommended data destruction processes, especially as they regard Network Configurations, PIN and VMail erasures. You may also want to speak with your ITAD vendor about their policies and procedures.

Vulnerability #8: Teleconferencing Devices

Often, video conferencing equipment is located where the most sensitive meetings take place. "Lazy habits and sloppy security settings" have brought about a "perfect storm" potential in the view of researcher HD Moore.[10]

Because so many of these devices are, "naked on the Internet," Moore was able to access video conferences held in corporate boardrooms and meetings in research facilities, law offices and venture capital firms. In one case, he was able to dial into an ongoing conference and operate the camera for 20 minutes, zooming in on one participant as he entered a password into his laptop, all without detection.[11]

It's estimated that 150,000 video conferencing setups could be similarly vulnerable.

Best practices

- Disable auto-answering features.
- Place teleconferencing devices behind a firewall that understands video protocols such as H.323.
- Follow vendor recommendations and speak with your ITAD vendor about secure data destruction processes.

Vulnerability #9: Networking Hardware (switches, wireless)

Networking is a critical part of any company's infrastructure. They can no more manage without it than they can without products to sell. However, vulnerabilities can expose the devices to remote attacks, man-in-the-middle (MITM) eavesdropping and other forms of information and data theft.

However, networking hardware is notoriously difficult to patch, so too often it gets shunted off into a "get to it later" silo. While understandable from a resources/time allocation perspective, it can nevertheless leave companies vulnerable to the complete compromise of their network with devastating financial and legal implications.

Best practices

- Include networking hardware in your patch management strategy.
- Follow vendor's recommended data destruction policies.
- In addition, ask your ITAD vendor about their data erasure policies and recommendations.

Vulnerability #10: POS Credit Card Reader

In late 2013, Target, Neiman Marcus and other retailers suffered the largest data breach in history as the personal information of over 110 million shoppers was compromised. Other attacks have affected similarly large numbers of consumers at both the transaction and card data storage level. The effects of a data breach can be almost too costly to calculate, ranging from loss of trust, reputation and share price to the total collapse of the business.

Best practices

- Train employees to be on the lookout for hardware modification and unauthorized maintenance.
- Ensure Point of Sale hardware and software are up to current PCI Standards. Systems older than 3-4 years may not be compliant. For more information visit https://www.pcisecuritystandards.org/
- Limit network access to and from the Point of Sale network to trusted ports and maintenance devices. (This has the secondary benefit of limiting PCI scope.)

Conclusion:

Most technology security is focused on devices rather than people. That said, people mistakes can also be pivot points that compromise the entire network.

For example, the late 2013 Target breach may be traceable to an overlooked point of access to customer data through a third-party HVAC vendor. Neither Target nor the vendor was aware of the vulnerability and there was clearly no need for a company responsible for maintaining heating and cooling equipment to have access to customer data. Nonetheless, according to current information, the vulnerability went unnoticed most probably because IT resources were occupied with other priorities.

Just as every experienced pilot goes through a pre-flight routine before taking off, every IT department should follow these simple rules:

- Patch every deployed device every time.
- Make passwords tough and change them regularly.
- Dispose of data properly according to manufacturer policies and the recommendations of your ITAD vendor.

It's easy to let convenience or the urgency of other priorities overshadow these basics. But, as the Target breach and others like it illustrate, the financial, reputational and legal penalties for lack of diligence can be catastrophic.

IT Asset Disposition (ITAD) 101

In the same way that data compromises can lead to crippling fines as well as the loss of customers, business, revenues and reputation, lack of proper environmental disposition can lead to similarly damaging consequences.

Yet once again, recent studies show companies are falling well short of mandated standards.

The component parts of virtually every electronic device are deemed "hazardous waste" by state, federal and international law-markers. Penalties for violations can range from $32,500 per day to prison sentences for corporate executives deemed negligent. Yet over 82% of the computers, laptops, tablets, mobile devices, printers, copiers and other electronic devices disposed of each year find their way into a landfill somewhere in the world.

Even among companies which take their e-waste to a recycler in good faith, 70% to 80% is still shipped to overseas landfills. Indeed, only 11%-14% of e-waste is sent to responsible recyclers.[4]

Those statistics indicate that as much as 86% or more of corporations are leaving themselves vulnerable to environmental and data security risks that can compromise the entire organization. Accordingly, we recommend that every company with 25 or more employees consult with a firm specializing in IT asset disposition that carries e-Steward Certification. In this way, you can be reasonably assured that sensitive data will be reliably destroyed before redeployment with appropriate documentation and a certificate of recycling for the indemnification of your firm and that all e-waste will be handled in a responsible and compliant manner.

Glossary of Important Terms

- **Asset disposition**: The Corporate disposition of any IT or related company owned asset for further use (re-deployment), removal from company books via outright sale, disposal via proper asset recycling, etc.
- **ATA command set**: Series of functions and commands built in to desktop hard drives.
- **BYOD**: Otherwise known as "Bring Your Own Device", this policy allows employees to use personal electronics to access corporate data and applications
- **Default passwords**: Passwords provided to a user at the time of initial setup.
- **Degaussing**: The purging of magnetic media through the exposure of a strong magnetic field to disrupt the magnetically encoded information.
- **Disk encryption software**: A technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people.
- **DoD 3**: Department of Defense (DoD) three pass overwrite from the DoD specification 5220.22-M – at one time the industry norm for data eradication via software overwrites with verification reporting.
- **Encryption**: The process of encoding information in a way that only authorized individuals can read it.
- **e-Waste**: Electronic waste as generated by any Corporate entity, typically non-serialized assets which might be gathered and processed in bulk, such as peripheral technology, cabling and other miscellaneous electronic mechanisms.
- **Factory resets**: Bringing a unit's software to original factory settings.
- **Flash drives**: Any drive that uses flash memory to store information.
- **Gramm-Leach-Bliley**: A US Congress passed regulation in 1999 which attempts to update and modernize the financial industry, in part providing guidelines within the financial industry regarding the proper handling of consumer information which is largely held within electronic media. Penalties for violating provisions, no matter how inadvertently can be as high as $10,000 per instance.
- **H.323 protocols**: A standard for voice communication across packet networks, such as TCP/IP.
- **HIPAA**: The Health Insurance Portability and Accountability Act became federal law in 1996, restricting access to individuals' private medical records. Penalties for violating HIPAA regulations can reach $50,000 per violation up to $1.5 million.

- **HITECH**: The Health Information Technology for Economic and Clinical Health Act was signed into law 2009 to promote the adoption and more meaningful use of heath information technology. Several provisions strengthen the civil and criminal enforcement of the original HIPAA rules. The legislation is now more commonly referred to as HIPAA/HiTech within the medical industry and by the IT community which services its technology requirements. Without going into details on various violation possibilities, it's important to keep in mind that violations, often through data breaches, carry an average liability of over $7 million.

- **ITAD**: Information Technology Asset Disposition – an acronym utilized by service providers and technology users alike to define the Corporate disposition of assets, specifically those from within the information technology arena.

- **Malware**: Software: designed to disrupt computer operations, gather sensitive information, or gain access to private systems.

- **Man-in-the-middle**: A computer attack achieved by relaying messages between victims without either victim knowing.

- **Mobile erasure tools**: A software or hardware tool designed to permanently erase information stored on cellular devices or tablets.

- **Naked on the Internet**: A device connected to a public network node without a firewall.

- **Netflow tools**: Tools designed to analyze network traffic by using data gathered by Cisco routers.

- **Network appliances**: A typically inexpensive piece of hardware that allows access to the Internet and other utilities, but lacks features of fully equipped IT equipment

- **Networking hardware**: Devices that facilitate the use of network.

- **NIST:** National Institute of Standards and Technology (NIST) is an agency of the United Stated Department of Commerce responsible for establishing standards for testing and implementation of technology equipment in the United States.

- **Patch management strategy**: The set of policies and procedures that cover installation of security updates from software and hardware manufacturers.

- **PCI standards**: Payment Card Industry standards are widely accepted policies meant to protect the security of credit, debit and cash card transactions.

- **Remnant data**: Bits of files that remain after an operating system has marked the file for deletion

- **SCSI command set**: Features Similar to ATA command set – a collection of functions or commands available to SCSI, Small Computer System Interface, hard drives.

- **SD card storage**: Secure Digital storage is nonvolatile memory, typically used in portable devices.
- **SIM Cards**: A portable memory chip, used in cell phones to store personal information for use on the Global System for Mobile Communications network.
- **Social engineering**: Psychological manipulation of people into performing actions or divulging confidential information.
- **SSD hard drives**: Data storage devices that utilize memory chips for storage instead of magnetic platters.
- **Targeted attacks**: A computer attack in which the target was selected, rather than random.
- **Trojan power sources**: A device that represents itself as a power source, like a USB charging station for cell phones, but also attempts to extract information from connected devices.
- **Unsecure sites**: Servers communicating with your browser utilizing unencrypted data.
- **USB devices**: A computer peripheral that connects via the Universal Serial Bus industry standard, which provides a common ground for both communication and power.
- **VLAN: (Virtual Local Area Network)**: a method of isolating devices into separate networks while going through a common network router or switch.
- **VoIP sniffers**: Software or hardware tool used to capture and analyze Voice over IP network traffic and a potential security threat.
- **Whitelisting**: Allowing certain objects unobstructed access.
- **Whole disk encryption**: A form of disk encryption that encrypts the entire user-addressable portions of a hard drive.

Citations

1. e-Week / March 2011
2. “Environmental fines can top $30,000 per day” / ACG News 2014
3. e-Stewards. Basel Action Network / 2008-2010
4. “U.S. Missile Defense Secrets, UK Medical Records Accidentally Sold on eBay” DailyTech / May 2009.
5. “Public Charging Stations Could Steal iPhone Data.” PC Magazine - Security Watch / June 2013.
7. “SIM Card Hack a Wakeup Call” Security Dark Reading / July 2013.
8. “New malware rooting place: Inside your SD Card?” C/Net / December 2013.
9. “SSDs prove difficult to securely erase” Naked Security / February 2011.
10. “Toll Fraud: Protection Your Phone System and Your Business.” Phone system Insight / 2011
11. “Security Tool Cain can successfully capture and replay VOIP traffic...” odix.it/cain / 2001-2014.
12. “Video conferencing mistakes make espionage easy, say researchers.” Computer World / January 2012.