

the *Availability Digest*

www.availabilitydigest.com
[@availabilitydig](https://twitter.com/availabilitydig)

HPE Cyber Risk Report 2016

March 2016

HPE has released its 2016 Cyber Risk Report.¹ Prepared by the HPE Security Research team, it is an extensive report (96 pages) that examines the vulnerabilities that leave organizations exposed to data breaches. It is no longer a question of 'if' an organization will be attacked but 'when.' The report provides insights into how security funds and personnel can be better allocated to counter the threats and to prepare a better breach response.



The report focuses on seven key themes:

- Theme #1: The year of collateral damage.
- Theme #2: Overreaching regulations push research underground.
- Theme #3: Moving from point fixes to broad impact solutions.
- Theme #4: Political pressures attempt to decouple privacy and security efforts.
- Theme #5: The industry didn't learn anything about patching in 2015.
- Theme #6: Attackers have shifted their efforts to directly attack applications.
- Theme #7: The monetization of malware.



Theme 1: The Year of Collateral Damage

Anthem, Inc., is the second largest health insurer in the United States. In late 2014, hackers stole almost 80 million health records from Anthem. It was the largest data breach to date of any U.S. health insurer.²

If this made 2014 the Year of the Breach, 2015 has become the Year of Collateral Damage. Certain attacks affected people who never dreamed that they would be the victims of a data breach because they did not knowingly have their personal data stored anywhere. However, they were affected by data as it related to someone else.

¹ HPE Security Research Cyber Risk Report 2016, *HPE Security Research*; 2016.
http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/index.html?jumpid=va_kxdmr1h9cv
² Anthem Loses 80 Million Records to Hackers, *Availability Digest*; March 2015.
http://www.availabilitydigest.com/public_articles/1003/anthem_hack.pdf

In April, 2015, the U.S. Government's Office of Personnel Management (OPM) discovered that its database had been breached.³ The data theft had been going on for almost a year. The government determined that the information of over 21 million people had been compromised. The victims included anyone who had worked for the government or who had tried to work for the government.

The data for each victim included a 120-page employment application that included sensitive information on virtually every aspect of the victim's personal history needed for security clearance, including extensive lists of relatives and friends. It was these relatives and friends that suffered collateral damage. Some of their personal information now had been exposed, including names, addresses, email addresses, and social security numbers.

A more sordid example was the data breach of Ashley Madison.⁴ Ashley Madison is the premiere website for the married who wanted to cheat on their spouses. The worst happened for members of the web site. Its database was hacked and was posted online for all to see. The data stored in the Ashley Madison membership database included names, email addresses, street addresses, phone numbers, and sexual fantasies.

With a quick search of an email address, spouses could find out if their "better" halves had been trying to cheat on them. Divorces and suicides followed. Even more embarrassing for those victimized by adultery was that friends and neighbors could find out who they were from the information posted about their cheating other halves.

Theme #2: Overreaching Regulations Push Research Underground

When massive data breaches occur, legislation frequently is introduced hastily to "correct" the problem and protect data. However, too often the legislation has unintended consequences that can push legitimate security research underground. To be effective, regulations impacting security must protect and encourage research that benefits everyone.

The recent overturn of the U.S./E.U. safe haven by the European courts can be a problem for many. The safe haven allowed U.S. companies to store data in the European Union so long as they followed U.S. security regulations and vice versa. However, now U.S. companies must follow E.U. regulations when storing data in the E.U.; and European companies must follow U.S. regulations when storing data in the U.S. One major difference is that in the E.U., the storage of a person's sensitive data requires an opt-in from that person, whereas in the U.S. an opt-out procedure is followed.

Another example is the Wassenaar Arrangement, which has been implemented by more than forty countries. This agreement uses export controls as a means to combat terrorism by promoting transparency and greater responsibility in the transfer of conventional arms and dual-use technology. However, the recent inclusion of "intrusion software" in the Wassenaar Arrangement may be a backlash in response to malicious security offerings aimed at compromising systems.

We can expect to see further extensions of the Wassenaar Arrangement and other legislation that may make protecting against data breaches harder. This, in turn, promotes the likelihood of successful breaches; as the environment increasingly favors those operating in the black market.

³ [The Government OPM Hack Gets Worse](http://www.availabilitydigest.com/public_articles/1007/OPM_attack_2.pdf), *Availability Digest*, July 2015.
http://www.availabilitydigest.com/public_articles/1007/OPM_attack_2.pdf

⁴ [Ashley Madison Cheats Exposed](http://www.availabilitydigest.com/public_articles/1008/ashley_madison.pdf), *Availability Digest*, August 2015.
http://www.availabilitydigest.com/public_articles/1008/ashley_madison.pdf

Another example of over-regulation was a submission for public comment by the U.S. Department of Commerce's Bureau of Industry and Security (BIS) to impose an incredibly broad set of controls related to intrusion software. These controls were so broad that they would make much of today's defensive cybersecurity research untenable, if not criminal. The outcry from the community helped sway BIS into withdrawing its proposed changes.

Theme #3: Moving from Point Fixes to Broad Impact Solutions

In 2015, Apple and Microsoft both released more patches to their software than at any prior point in their histories. It is not clear if this level of patching is sustainable, either by the vendors or by the users who must install the patches.

Patches were successful at breaking the common exploit techniques of the time, but attackers worked their way around the defenses. The cat-and-mouse game between software vendors and exploit writers continued with new exploit-specific mitigations being released and new malicious techniques quickly following. While these mitigations evolved, new vulnerabilities continued to be discovered and patches deployed.

Recently, vendors that receive hundreds of vulnerability reports began taking a different approach to software mitigations. As an example, rather than focusing on specific vulnerabilities, Microsoft now is making headway with defensive measures that correct entire classes of vulnerabilities in its browser. It and other vendors must invest in these broad fixes that knock out many vulnerabilities at once.

Theme #4: Political Pressures Attempt to Decouple Privacy and Security Efforts

The revelations of Edward Snowden and other whistleblowers have led to a difficult year for the balance between privacy, encryption, and security. Privacy issues gave the security world much to discuss and ponder throughout 2015.

Many lawmakers claim that security is only possible if fundamental rights to privacy are abridged. There are some in the U.S. Congress who want to give their national security agencies a blank check. These members feel that any attempt to protect privacy somehow makes the country less safe. Others suggest a framework of 'balancing' privacy rights and national security. Still others argue that privacy rights are pre-eminent. Protecting basic privacy rights and protecting the country are not part of a zero-sum equation. Both can be accomplished.

Given this ongoing debate, those evaluating the security of their enterprises would do well to monitor government efforts such as adding "backdoors" to encryption and other security tools.

Theme #5: The Industry Didn't Learn Anything About Patching in 2015

Almost 50% of the top ten vulnerabilities exploited in 2015 are over five years old. Microsoft Windows vulnerabilities account for 50% of all discovered vulnerabilities.

While vendors continue to publish patches to correct discovered vulnerabilities, the patches do little good if users do not install them. A major problem is that applying patches in an enterprise can be risky and expensive, especially when the patches cause other problems. The most common rationale given by those who disable automatic patch updates or who fail to install patches is that patches break things.

A major challenge for software vendors is that it is nearly impossible to completely test a patch's ability to have no adverse effect on some function, given the complexity of today's software products. However, it is incumbent upon software vendors to win back the trust of their customers in order to help restore faith in their patches.

Theme #6: Attackers Have Shifted Their Efforts to Directly Attack Applications

It used to be that attackers would attempt to enter the perimeter of a system's network and attack the system software. However, with the wide use of mobile devices, the attackers have moved to mobile applications. They see this as the easiest route to accessing sensitive enterprise data.

From the perspective of applications and platforms, Android is second only to Windows as a targeted platform. Of interest, Android's main threats are potentially unwanted applications and advertising frameworks collecting private and potentially identifiable user information.

Today's security practitioner must understand the risk of convenience and interconnectivity to adequately protect enterprise data.

Theme #7: The Monetization of Malware

In 2015, malware took on a new focus. Moving from its use to execute data breaches, malware now is producing revenue. This has led to an increase in ATM-related malware, banking Trojans, and ransomware.

Attacks targeting ATMs generally fall into one of two categories:

- Stealing credit card information. These attacks may use hardware such as skimmers, software loaded onto the ATM, or a combination of both.
- Directly dispensing cash. These attacks rely on directly bypassing card authentication and are performed at the software level.

While there is no definitive answer as to what contributes to the rise of ATM malware, it is likely that an aging ATM fleet plays a significant role. The ease of access to the inner workings of certain ATMs and their locations contribute as well. What is certain is that cybercriminals attacking ATMs are well-organized and operate internationally.

Banking Trojans continue to use Microsoft Office Word documents and Excel spreadsheets as the favored means of infection. Many businesses use these programs to conduct day-to-day operations, which provides a broad user base for attackers to target.

Ransomware wreaks havoc by encrypting files of private and corporate users alike. Once encrypted, the malware author typically demands ransom, often in the form of Bitcoins for anonymity, in exchange for the decryption keys required to restore the files.

The best protection against ransomware is to frequently back up all important files on the system. By default, Windows keeps shadow copies of all files in the user's home folder. Sometimes the system can

be recovered from a ransomware attack by restoring shadow copies, but ransomware authors will try to disable shadow copy restores by deleting them.

Bug Bounties

A flip side of malware monetization is bug bounties. Security researchers now have a multitude of options available to benefit from their discoveries of vulnerabilities:

- The White Market – Bug-bounty programs and hacking contests provide responsible disclosure opportunities to the software vendors who often will pay a researcher for newly discovered bugs. Companies who provide bug-bounty programs include Google, Facebook, Netscape, and United Airlines.⁵
- The Gray Market – Some legitimate researchers operate in a legal gray zone by selling their newly discovered vulnerabilities to governments and law-enforcement agencies in countries around the world.
- The Black Market – Vulnerabilities can be sold to the highest bidder and used to disrupt private or public individuals and groups.

A major entry into bug bounty programs is the Zero-Day Initiative (ZDI) program. A zero-day vulnerability is one that has been newly discovered, leaving the software vendor with zero days to fix it.

ZDI is the world's largest vendor-agnostic bug-bounty program. It compensates researchers for submitting their vulnerability finds. Founded in 2005, ZDI has disclosed over 2,000 vulnerabilities and has paid out USD \$12 million in cash awards.

Summary

The HPE Cyber Risk Report 2016 provides a wealth of information to help defeat data breaches and other malware attacks. It should be studied by every security specialist who is tasked with defending the data and systems of his enterprise.

⁵ United Airlines' Bug Bounty Program, *Availability Digest*; July 2015.
http://www.availabilitydigest.com/public_articles/1007/UA_bug_bounty.pdf