Hewlett Packard Enterprise

# Cyber Risk Report 2016

Executive summary

## The cyber landscape

The 2016 edition of HPE's annual security research Cyber Risk Report details a threat landscape still rife with old problems and known issues. The environment is one in which well-known threat vectors continue to exist in the digital enterprise side by side with the latest attack methodologies to steal unprecedented amounts of corporate and personal data.

The Cyber Risk Report 2016 covers multiple focus areas, drawing from innovative work by HPE Security Research. It examines the nature of prevalent vulnerabilities that leave organizations open to risk, and how adversaries take advantage of those vulnerabilities. The report challenges readers to rethink how and where their organizations can be attacked as it is no longer a question of "if" but "when." This security intelligence can be used to better allocate security funds and personnel resources to counter the threats and prepare a better breach response.

Some of the key findings in this security research report are:

**2015 was the year of collateral damage**

If 2014 was the Year of the Breach, 2015 was the Year of Collateral Damage as certain attacks touched people who never dreamed they might be involved in a security breach. Both the United States Office of Personnel Management (OPM) and the Ashley Madison breaches affected those who never had direct contact with either entity, and whose information resided in their networks only as it related to someone else—or, in the case of the Ashley Madison breach, did not appear at all but could be easily deduced from revealed data. With the OPM breach, the true targets of the breach may be people who never themselves consented to inclusion in the OPM database—and who may be in danger thanks to its compromise. Data compromise is no longer just about getting payment card information. It's about getting the information capable of changing someone's life forever

**Overreaching regulations push research underground**

When horrific events occur impacting the lives of many, there is a natural reaction to do something to try to prevent future occurrences. Too often, the "something" (legislation) incurs unwanted consequences to go along with the intended result. This is the case with various proposed regulations governing cybersecurity. While the intent to protect from attack is apparent, the result pushes legitimate security research underground and available only to those denizens who dwell there. To be effective, regulations impacting security must protect and encourage research that benefits everyone.

**Vendors are moving from point fixes to broad impact solutions**

While it is laudable that Microsoft® and Adobe® both released more patches than at any point in their history, it remains unclear if this level of patching is sustainable. It strains resources of both the vendor developing the patch and the customer deploying the patch. Microsoft has made some headway with defensive measures that prevent classes of attacks. It and others must invest in these broad, asymmetric fixes that knock out many vulnerabilities at once.

**Political pressures attempt to decouple privacy and security efforts**

A difficult and violent year on the global scene, combined with lingering distrust of American tech initiatives in the wake of revelations by Edward Snowden and other whistleblowers, led to a fraught year for data privacy, encryption, and surveillance worldwide. Many lawmakers in the US, UK, and elsewhere claimed that security was only possible if fundamental rights of privacy and due process were abridged—even as, ironically, the US saw the sunset of similar laws passed in the wake of the September 11, 2001, attacks. This is not the first time that legislators have agitated to abridge privacy rights in the name of "security" (more accurately, perceived safety), but in 2015 efforts to do so could easily be compared to the low success of previous efforts made after the attacks of 2001. Those evaluating the security of their enterprises would do well to monitor government efforts such as adding "backdoors" to encryption and other security tools.

**The industry learned nothing about patching in 2015**

The most exploited bug from 2014 happened to be the most exploited bug in 2015 as well—and it's now over five years old. While vendors continue to produce security remediations, it does little good if they are not installed by the end user. However, it's not that simple. Applying patches in an enterprise is not trivial and can be costly—especially when other problems occur as a result. The most common excuse given by those who disable automatic updates or fail to install patches is that patches break things. Software vendors must earn back the trust of users—their direct customers—to help restore faith in automatic updates.

**Attackers have shifted their efforts to directly attack applications**

The perimeter to your network is no longer where you think it is. With today's mobile devices and broad interconnectivity, the actual perimeter to your network is likely right in your pocket. Attackers realize this as well and have shifted their focus from servers and operating systems directly to applications. They see this as the easiest route to accessing sensitive enterprise data and are doing everything they can to exploit it. Today's security practitioner must understand the risk of convenience and interconnectivity to adequately protect it.

**The monetization of malware is the new focus of attackers**

Just as the marketplace has grown for vulnerabilities, malware in 2015 took on a new focus. In today's environment, malware needs to produce revenue, not just be disruptive. This has led to an increase in ATM-related malware, banking Trojans, and ransomware.

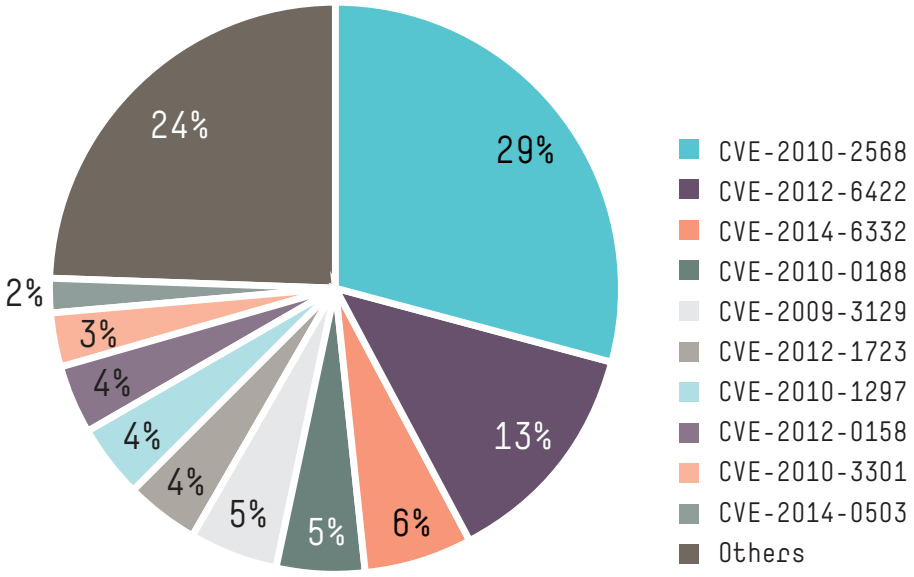


**Figure 1:** Top 10 vulnerabilities exploited in 2015

## Actions and reactions

Faced with increasing threats, software vendors continue to make it more difficult for attackers with the implementation of security mitigations. While these mitigations are not enough to secure the landscape alone, great progress was made this year. Vulnerabilities found in legacy code continued to plague the digital enterprise and prove, once again, that attackers continue to test well-known weaknesses for entrance into the network before turning to new methods. As the quality of exploits continues to improve, they reveal a deep understanding of the nature of the vulnerability and the internals of the target applications.

While the apparent stagnation in the overall growth of malware is an unexpected positive, the slow shift of focus away from Windows® toward Linux, Android, and OS X means the overall attack surface for malware continues to grow. While always disruptive, today's malware has become focused more on money than disrupting services. For these non-Windows platforms, malware often takes the shape of potentially unwanted applications, which could confuse a non-technical user as to what is or isn't malware. This is especially troubling given the first signs that Apple's walled-garden application store approach may not be infallible. While the anticipated flood of attacks on Internet of Things (IoT) devices has yet to occur, attacks on home routers may be a precursor of things to come.

The ever-present ATM has become the focus for many types of attacks, with malware authors targeting the users of ATMs and the machines themselves. While coordinated law enforcement takedowns of banking Trojan infrastructure have been successful, statistics show the attackers can restore services to the botnets in a surprisingly rapid fashion. As more and more of our financial transactions occur online, criminals will continue to target these transactions for profit. Put simply, if there is money to be made, there is money to be stolen. The industry must focus on securing these transactions to deprive attackers of the illicit income they so desire.

Another consequence of the Year of Collateral Damage was the increased scrutiny of privacy issues and encryption. The US federal government struggled to get its privacy house in order, even as the European Union and other entities pressed the accelerator on efforts to bring US companies in line with norms overseas. With geopolitical situations darkening worldwide as the year closed, it seems as if privacy issues will struggle in 2016 to keep their rightful footing side by side with security efforts.

Overall, it has been an interesting year for software security research. Both applications and mobile software pose unique challenges to developers, and various vulnerabilities detected in these platforms support that impression. It was also interesting to note that applications and mobile shared certain trends in vulnerabilities when analyzed by kingdom, thus pointing to common fundamental failures in the software. The rate of vulnerability remediation seems to be increasing, which suggests that technologies are becoming better understood as they mature. Nevertheless, there is room for improvement as shown by the prevalent issues detected.

For the first time our research looks into the world of incident responders in the enterprise and found that many organizations are not keeping pace with attacker trends, including direct attacks on the systems on which enterprises rely. We found evidence that adversaries are taking excellent advantage of technologies enterprises have put in place to serve their customers. Only by learning to treat applications as security entities on the network can defenders hope to adapt to the new adversary landscape.

During the past 20 years, we have witnessed the world change quite a bit. Just 10 years ago when the ZDI launched, most of the population didn't know what a breach was or that there were careers in cybersecurity. We've seen researchers step into the spotlight and we've seen them shun publicity. There have been laws around research, copyrights, exports, and many other topics.

Today, with the "Year of the Breach" just past us, there is more legislation in the US congressional pipeline than ever before, all trying to define "good hackers" and "bad hackers."

The vulnerability white market has had a tremendous positive effect in securing the landscape by bringing researchers and vendors together and setting the standard for coordinated disclosure. We expect the vulnerability market will continue to evolve as more and more vendors announce their own programs to incentivize research. We also expect regulations and legislation to impact the nature of disclosure, and not necessarily in a positive manner. While the environment in which the information security community operates evolves, it is in all of our best interest to continue to find and disclose security bugs in popular software so vendors can fix things in a timely manner. The increasing complexity aside, it continues to be an endeavor worth doing.


**Figure 2:** The vulnerability marketplace

## Conclusion

This year's Security Research Cyber Risk Report details the evolving nature of cybercrime as well as the developing legislation meant to curtail it. The report moves beyond the various techniques used by attackers, still driven primarily by financial interests, to delve into what defenders now face as they look to secure their enterprise.

In the coming years, the complexities of legislation and international events will have a greater impact in the realms of security and privacy. As a result, network defenders need to understand the complexities of privacy issues as thoroughly as they understand the impact of security vulnerabilities. Instead of symmetric responses to threats, tomorrow's network defender must understand how to respond asymmetrically to threats through automated analysis, wide-reaching fixes, and a community-based defense. While the threat of cyberattack is unlikely to go away, thoughtful planning can continue to increase both the physical and intellectual price an attacker must pay to successfully exploit an enterprise. Start by using the information in the 2016 Cyber Risk Report to better understand the threat landscape, and to best deploy your resources to minimize security risk.

For more information on how HPE can help your organization to implement a successful security program, fix the gaps in your environment, or aid you in recovery from a breach, visit **hp.com/go/hpsr**.

Access the full report here
hpe.com/software/cyberrisk

**Sign up for updates**

★ Rate this document

Hewlett Packard Enterprise



4AA6-4178ENW, February 2016