An IDC Signature White Paper, sponsored by Intel

IDC ANALYZE THE FUTURE

Silicon as Code, the Cybersecurity Vulnerability Paradox, and the Transparency Requirements for a 21st Century Processor Vendor

RESEARCH BY:

Frank Dickson
Program Vice President,
Cybersecurity Products, IDC

September 2020 | IDC Doc. #US46787420

Navigating this White Paper

Click on titles or page numbers below to navigate to each.

IDC Opinion

Today's Reality

The modern era of cybersecurity began on December 18, 2013, when news broke that Target was investigating a major data breach "potentially involving millions of customer credit and debit card records." The Target data breach was certainly not the first data breach, but it marks the modern era of cybersecurity as the event moved the impact and awareness of data breaches from Pennsylvania Avenue and Wall Street to Main Street.

It was later revealed that the breach took place between November 27 and December 15, 2013 and that up to 40 million consumer credit and debit cards may have been compromised. Target disclosed that the names, mailing addresses, phone numbers, or email addresses of up to 70 million additional people had also been stolen. If a consumer in the United States was not affected, the odds were that he/she knew someone that was. Organizations now took notice as data breaches had public impacts on business performance and executive job security.

Target also introduced many to the complexity of the cybersecurity task. Terms that were once unfamiliar became known such as compromised credentials and supply chain attacks. Almost overnight, our perceptions were that viruses became a smaller part of a growing family of malicious code referred to as malware.

Vulnerabilities and their known/unknown status create a cybersecurity paradox. Protecting IT architectures from *unknown* vulnerabilities is challenging, requiring sophisticated expertise and large resources. Protecting IT architectures from known vulnerabilities is typically more straightforward; the application of a patch is generally considered the greatest return in security.

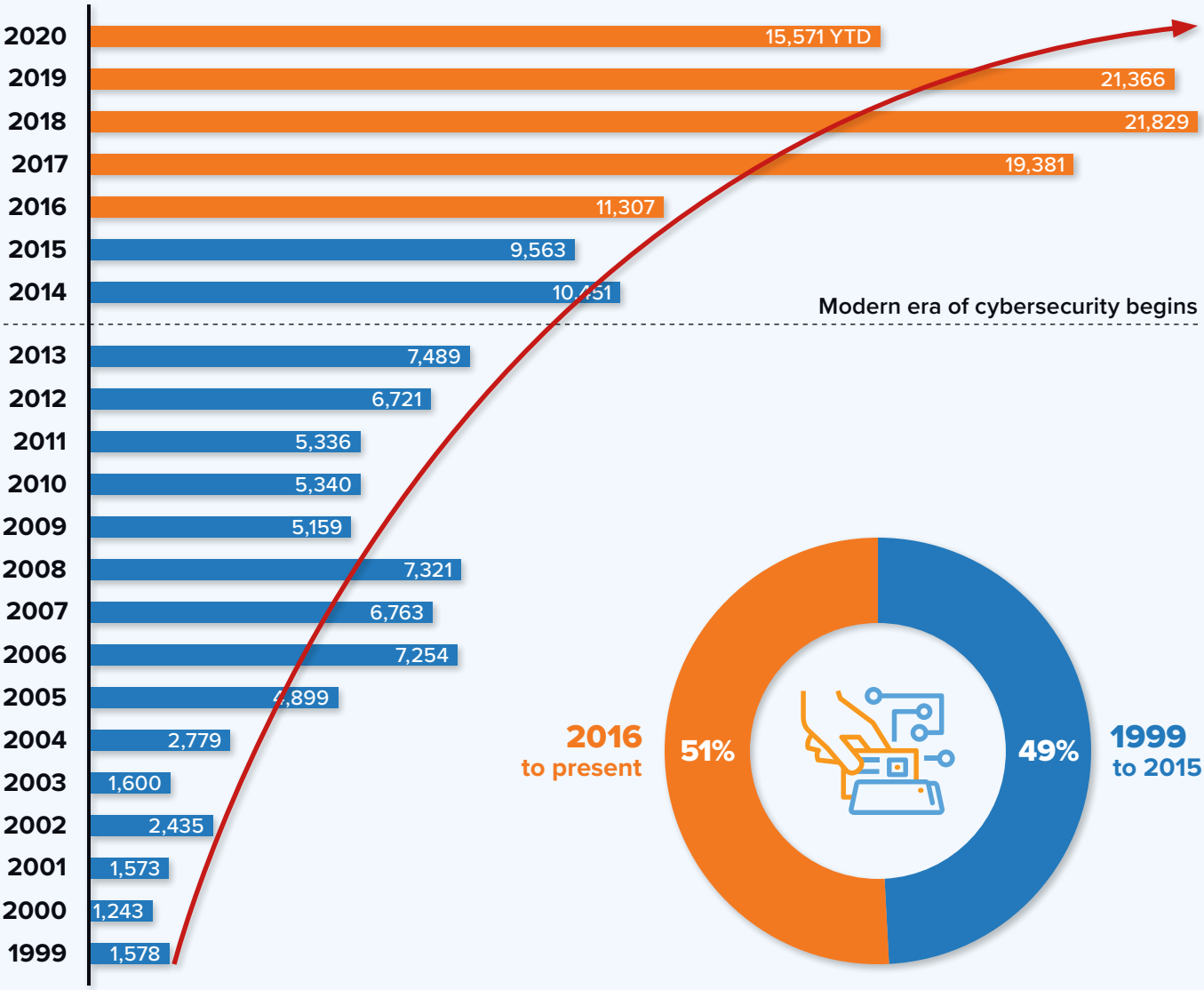
The application of a patch is generally considered the greatest return in security.

Take the Equifax data breach for example. It is reported that Equifax was first compromised via a consumer complaint web portal, leveraging a known Apache Struts vulnerability. The hackers laterally moved from the web portal to other servers compromising credentials stored in plain text along the way. Data was eventually exfiltrated in encrypted form due to failures in handling encryption keys. The sophistication of the hackers and their work were impressive; however, had the available patch for the known vulnerability been applied, the entire attack would have been thwarted almost before it started.

Although the Target breach and subsequent breaches like Equifax raised our awareness of cybersecurity, vulnerabilities, and breaches, the formal logging of vulnerabilities predates the modern cybersecurity era. From 1999 to 2019, over 161,000 vulnerabilities have been documented (see Figure 1). Making the issue especially important is that the rate of vulnerability discoveries is accelerating, with over half of all vulnerabilities being reported within the past five years.

FIGURE 1

Common Vulnerabilities and Exposures Over Time

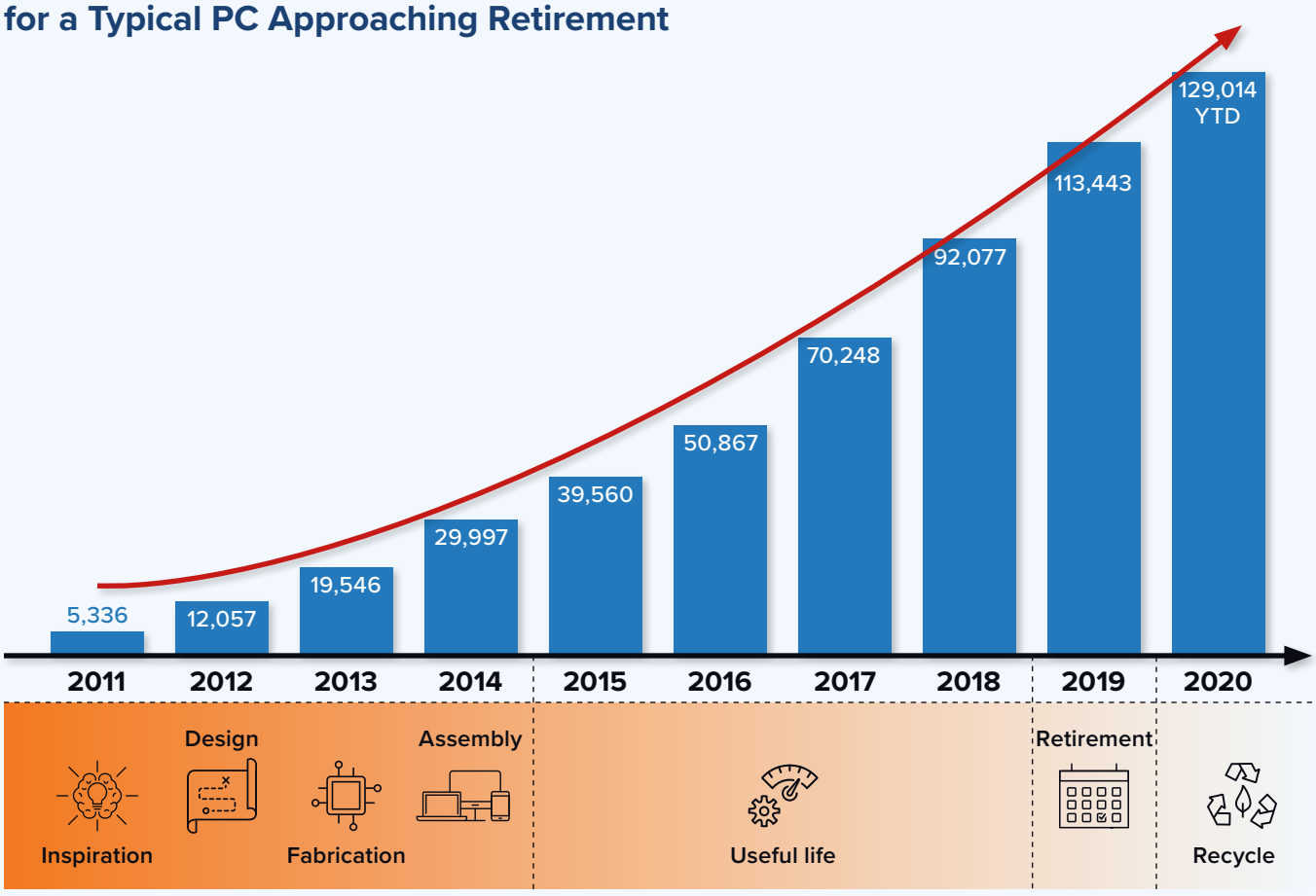


Source: IDC, 2020

Typical systems being retired today will have seen the disclosure of over 130,000 common vulnerabilities and exposures (CVEs). As PC refresh cycles have lengthened and CVE disclosure rates have accelerated, the number of CVEs disclosed over the life of a system will only rise. The discovery of vulnerabilities is to be expected. Just consider the life cycle of hardware. Processor and system development start 4 years before a typical system like a PC is shipped. Where the PC is being utilized often determines the useful life. For U.S. commercial, IDC estimates desktop replacement rates at 5.5 years and notebooks at 4.3 years. For U.S. consumers, IDC estimates desktop replacement rates at 6.1 years and notebooks at 5.4 years. Simple math implies that typical systems have 10-year cycles from program initiation to retirement (see Figure 2).

FIGURE 2

Cumulative Software and Hardware Vulnerability Exposure for a Typical PC Approaching Retirement



Source: IDC, 2020

Situation Overview

Patching and the Myth of the Microprocessor

Why on earth would we need to update and patch a microprocessor? After all, microprocessors are considered physical devices; once fabricated, the device characteristics are forever set in stone, right?

This assertion was certainly true in 1971 when the first Intel processor was launched. The 4004 had 2,300 transistors built on a 10-micron lithography process. The Intel solution was a four-chip set that included the 4004 microprocessors, the 4001 ROM, 4002 RAM, and 4003 Shift Register. You created the software to make it go.

Today's processors are highly sophisticated integrated systems on a single chip. The i9-9900K processor from Intel has a total core transistor count at 1.736 billion on a 14nm process (0.014 micron). The device has 10 cores (each running 16 individual threads), integrated graphics, and 128GB of memory.

The XPU era that we are in now already requires multiple classes of architecture — such as CPU, GPU, FPGA, and artificial intelligence accelerators — to compute the vast array of workloads. These systems on chips additionally have an extended architecture of interconnects including on chip, chip to chip, x computer, x datacenter, x network, memory hierarchies, and caches, all the way to storage.

Most importantly, although the processor is a marvel of engineering hardware, it is a brick without the software. Much like the value of the technology in today's automobiles is much higher than the value of the steel, the value created by the software in a processor is higher than the value of the silicon device.

Vulnerabilities and the Shared Responsibility Model

Absent omnipotent clairvoyance, unforeseen vulnerabilities are a natural outcome. Remember, the modern era of cybersecurity began seven years ago. Systems in the field predate the modern era of cybersecurity.

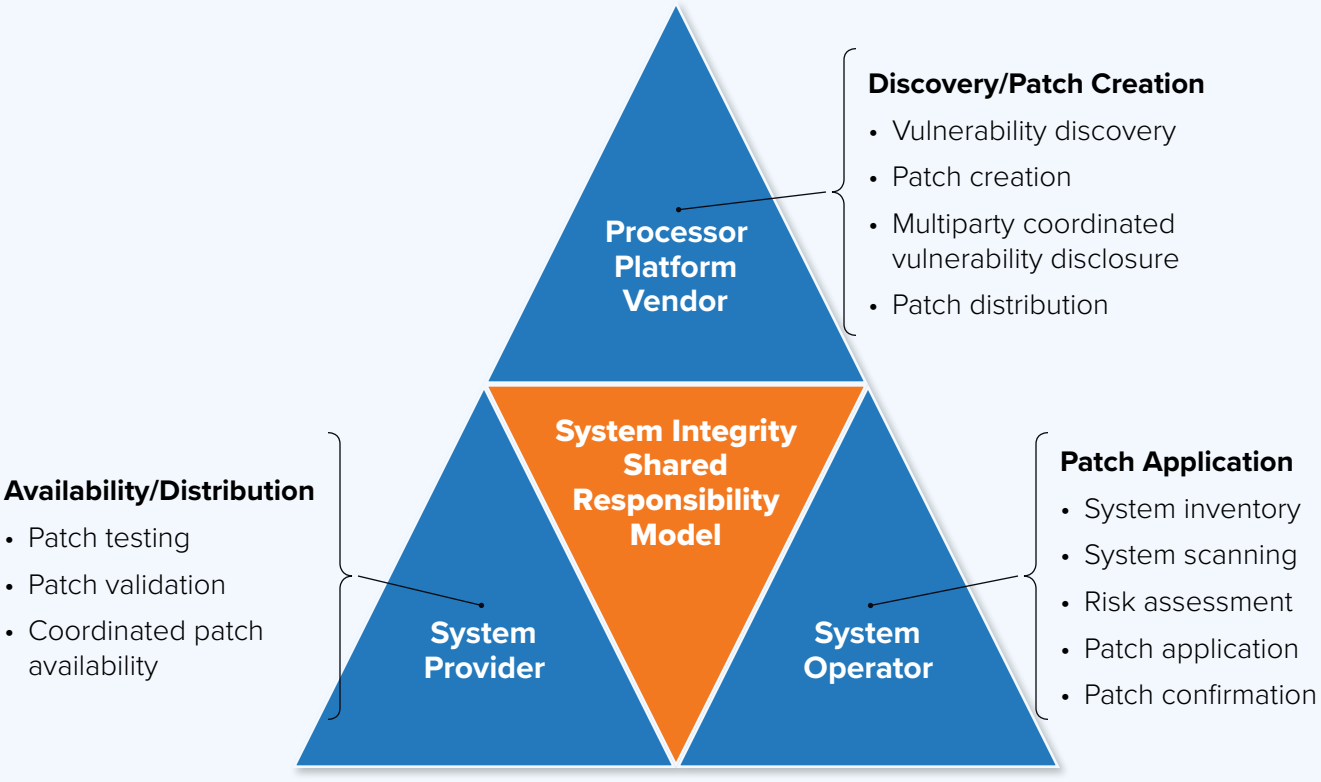
To preserve the integrity of systems, processor platform vendors, system providers, and system operators (end-consuming customers) must participate —it is a shared responsibility model.

The process requires three participants to create a single shared integrity outcome (see Figure 3):

1. **Patch creation** — processor platform vendor's responsibility
2. **Availability/distribution of patch** — system provider's responsibility
3. **Application of the patch** — system operator's responsibility

FIGURE 3

The System Integrity Responsibility Model: Three Participants, One Shared Outcome



Source: IDC, 2020

Known or anticipated threats are rapidly evolving and will certainly change throughout the service/life cycle of hardware. Ongoing research not only helps identify new vulnerabilities but also indicates how to defend against them. OS vendors and application developers have done a good job with regular and consistent updates and have prepared the market for always up-to-date systems. Processor platform vendors have followed suit but can run up against challenges in customer deployment. One of the biggest challenges for processor platform vendors is not having the means to provide updates directly to system operators. In addition, processor platform vendors have to work with a broader ecosystem made up of multiple system, service, and OS providers. Even so, patching hardware is just as critical to help ensure systems stay operational and secure.

It sounds like a really simplistic message, but the best patch is ineffectual if not applied. The Equifax breach was not due to an unknown vulnerability being exploited. It was the result of the exploitation of a known vulnerability to which an available patch was not applied.

The best patch is ineffectual if not applied.

Vulnerability disclosure and management programs are fueled by two components:

Internal offensive security research: The system provider needs to be vigilant in surfacing possible system weaknesses during all stages of the system's life—from inspiration through to useful life.

External offensive security research: Cooperation with academics, partners, integrators, and customers produces a force multiplier to create discovery leverage. Bug bounty programs can complement the external research.

Discovery of vulnerabilities and identification of affected systems are clearly only parts of the solution; patch development is also a critical step. Coordinated notification and patch distribution are paramount as the exploit clock can start ticking once a vulnerability becomes known and malicious actors develop an exploit kit associated with the vulnerability. Proactively sharing internal and external research, developer guidance, and mitigation methods to ease the system operator's burden is as critical as enabling application of the patch. Keys to creating system trust are visibility and transparency.

Considering the 10-year cycles from program initiation to retirement, it is in the best interest of system operators to know how processor platform vendors and system providers are developing and distributing updates as new threats are being discovered.

In the shared responsibility model, IT professionals and security operations teams can improve the security posture of their organizations. They help manage the application of mitigations through a variety of practices, including asset inventory, change management, and dynamic device discovery.

The Final Word

Processors are complete systems on a single chip—think of it as silicon in code. Like any other system, they require regular maintenance and constant hardening for system integrity. The system integrity shared responsibility model brings together the processor platform vendor and system provider to aid in the discovery and management of vulnerabilities and the creation of the requisite patches for remediation. As a result, ensuring the resiliency of IT architectures thus begins with vendor selection. System operators and owners can then be appropriately enabled to address the last portion of the shared responsibility triangle by remediating the vulnerability with the availability and application of the patch.

The most recent Center for Internet Security's CIS Controls V7.1 issued in April 2019 established continuous vulnerability assessment scanning as the third most important cybersecurity control. Proof that a company is adhering to this control satisfies various requirements for auditors and companies offering cybersecurity insurance and is viewed as a condition of compliance. Satisfying regulators and insurers is important, but vulnerability assessment scanning has another vital function. Scanning the most vulnerable endpoints after patches and OS upgrades is the logical conclusion of a remediation cycle.

Vulnerabilities are not malignant by default; they are simply an uncomfortable reality to be addressed. Vulnerabilities don't become malignant until they are maliciously and nefariously exploited. Persistent and aggressive patching can help prevent exploitation and encourages profit-maximizing cybermiscreants to attack other targets.

IDC would implore organizations to remember the cybersecurity vulnerability paradox. Protecting IT architectures from unknown vulnerabilities is challenging, requiring sophisticated expertise and large resources. Protecting IT architectures from known vulnerabilities is relatively straightforward; the application of a patch is generally considered the greatest return in security.

About the Analyst

Frank Dickson
Program Vice President, Cybersecurity Products, IDC

Frank leads the team that delivers compelling research in the areas of Network Security; Endpoint Security; Cybersecurity Analytics, Intelligence, Response and Orchestration (AIRO); Identity & Digital Trust; Legal, Risk & Compliance; Data Security; IoT Security; and Cloud Security. Topically, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.

More about Frank Dickson

Message from the Sponsor

In 2019, Intel managed the coordinated disclosure of 236 vulnerabilities across its product portfolio; 61% were discovered internally, and 30% were reported through the company's public bug bounty program. That means 91% of all vulnerabilities disclosed were the result of Intel's proactive security efforts. Additionally, Intel believes the security of its products is an ongoing priority, not a one-time event, and the level of transparency they provide will only accelerate industry-level progress in security.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701
USA
508.872.8200

idc.com @idc

IDC Doc. #US46787420