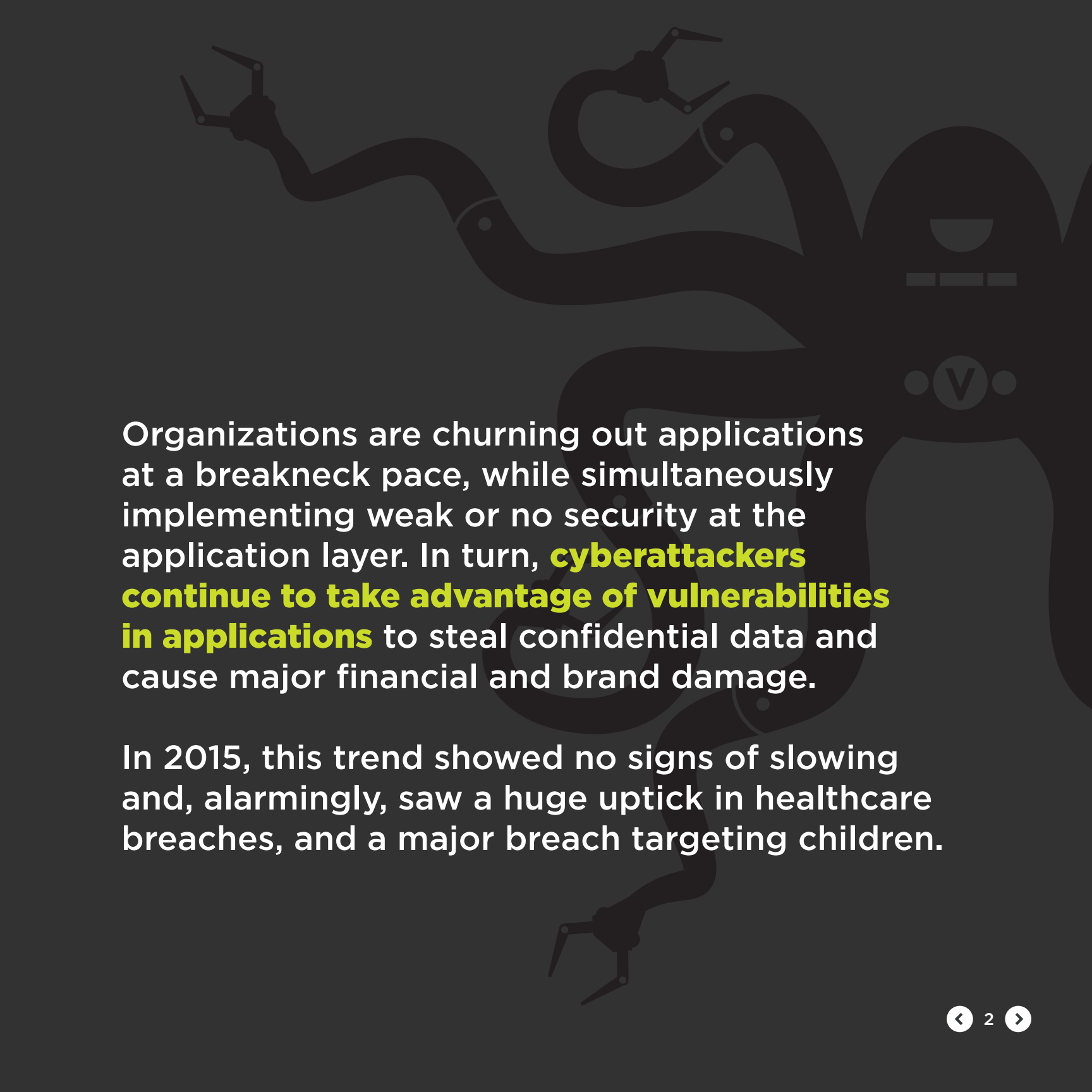


VERACODE eBook

APPLICATION-LAYER BREACHES PERSIST IN 2015

VERACODE



Organizations are churning out applications at a breakneck pace, while simultaneously implementing weak or no security at the application layer. In turn, **cyberattackers continue to take advantage of vulnerabilities in applications** to steal confidential data and cause major financial and brand damage.

In 2015, this trend showed no signs of slowing and, alarmingly, saw a huge uptick in healthcare breaches, and a major breach targeting children.

NOT IF, BUT WHEN

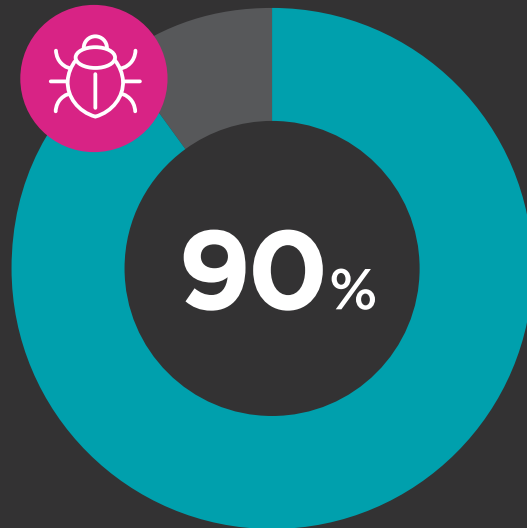
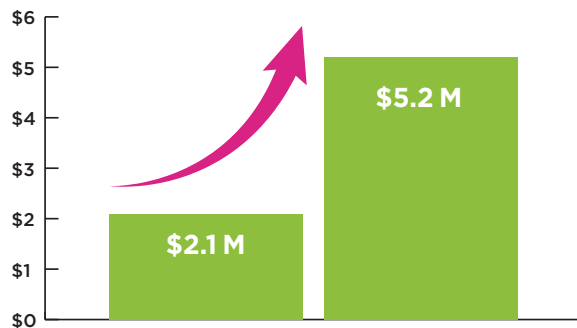
“ It’s not a question of whether or not you’ve been compromised. You will be compromised at some point.”

DONALD GOOD, Deputy Assistant Director of the FBI’s Cyber Division



The cost of a data breach involving 10 million records will fall between **\$2.1 million** and **\$5.2 million**.

Verizon Data Breach Investigation Report



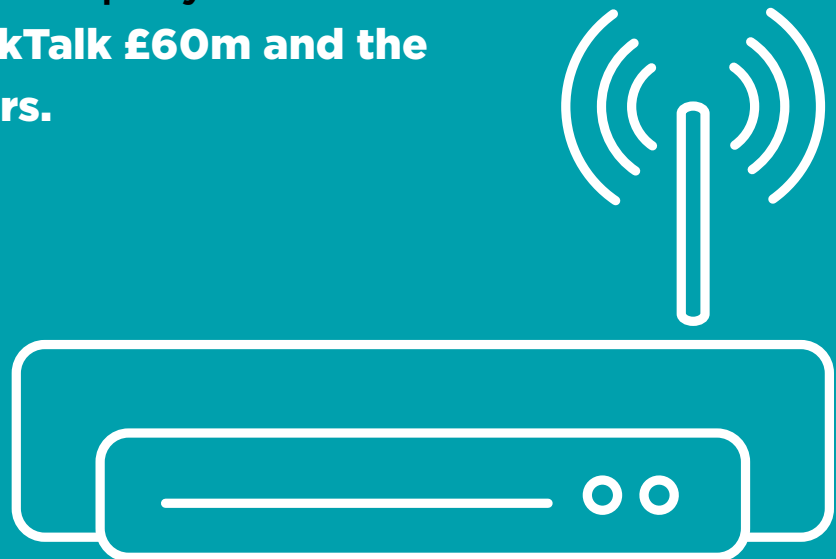
90% of security incidents result from exploits against defects in software.

U.S. Department of Homeland Security

TalkTalk

TalkTalk's intrusion started with a SQL injection (SQLi) attack to abuse an application-layer vulnerability and gain access to its database.

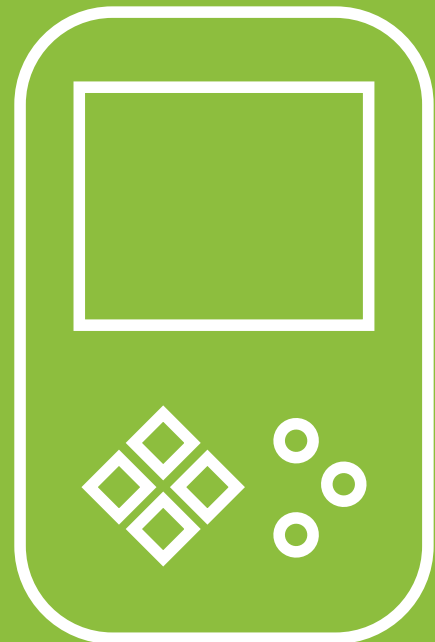
The attack resulted in the theft of names, addresses, birthdays and financial information for potentially all of the company's 4 million customers, and **cost TalkTalk £60m and the loss of 95,000 customers.**



VTech

VTech, a company that makes educational toys aimed at children, suffered a data breach that exposed the data of 6.4 million children in addition to 4.9 million adults. Data compromised included users' names, birthdays and passwords. The cyberattacker accessed customer data through the VTech website, planetvtech.com, which was vulnerable to SQL injection.

In addition to other financial and brand damage related to the breach, **cybersecurity experts subsequently advised parents to boycott or to be wary of VTech's electronic toys.**



The Office of Personnel Management

The OPM revealed in June 2015 that it suffered two apparently separate breaches of its computer system. One breach affected records on 4.2 million people; the other exposed background check data on 21.5 million.

The larger breach involved sensitive personal information gathered for security clearance investigations of current, former and prospective federal employees and contractors.



There was no confirmation on exactly how the breach was perpetrated, but the investigation team evaluating the security of the OPM discovered a vulnerability in the web gateway, which is used to submit materials for background investigations.

“ The government ranks last behind other industry sectors with respect to the security of its software. For example, 3 out of 4 applications fail the OWASP Top 10 when first assessed for risk. The government has the highest prevalence of easily-exploitable vulnerabilities such as SQL Injection and Cross-Site Scripting. Part of the reason for this is that the government still uses older programming languages (such as Cold Fusion) which are known to produce more vulnerabilities.”

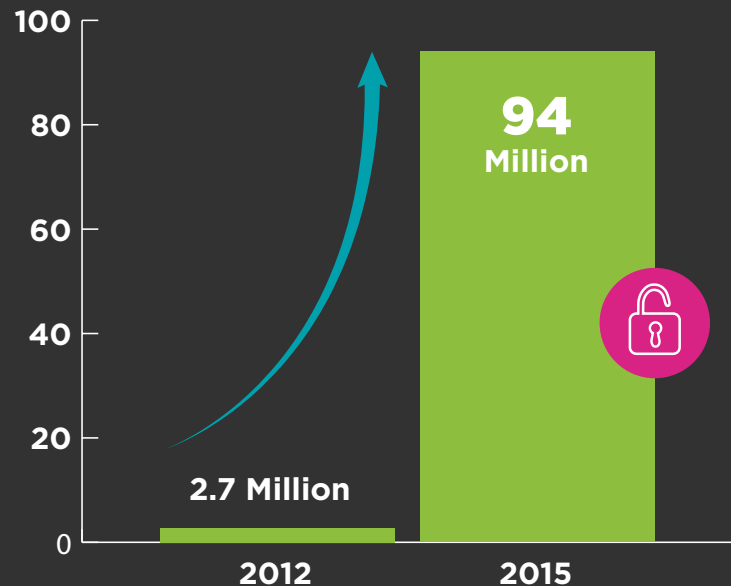
CHRIS WYSOPAL, Veracode Co-Founder

EXPLOSION OF HEALTHCARE BREACHES

2015 saw a marked rise in the number of breaches into healthcare companies.

The number of breaches at healthcare organizations grew from **2.7 million in 2012 to more than 94 million** through the first half of 2015.

U.S. Department of Health and Human Services



WHY THE INCREASE? Healthcare data has become highly sought after by cyber-criminals. The black-market value of an individual healthcare record is up to \$50, 10 times as much as a stolen credit-card number.

Unlike simple credit-card data, criminals can use stolen healthcare data for a wide variety of activities, including committing insurance fraud, purchasing medical equipment and obtaining controlled substances.

Sampling of Healthcare Breaches

SEVERAL HEALTHCARE COMPANIES, including Anthem, Premera Blue Cross, CareFirst BlueCross BlueShield, UCLA Health Systems and Excellus BlueCross BlueShield, suffered data breaches in 2015.

Several attack methods seem to have been deployed, including phishing attacks and taking advantage of flaws and unencrypted data in electronic health record (EHR) systems.



ANTHEM'S breach resulted in the theft of approximately 78.8 million highly sensitive patient records, in addition to 8.8 to 18.8 million non-patient records that included names, birth dates, Social Security numbers, addresses and employment data.

The **PREMERA** data breach compromised the names, dates of birth, addresses, telephone numbers, email addresses, Social Security numbers, member identification numbers, medical claims information and financial information for 11 million customers.

“ While some electronic health record (EHR) systems claim to encrypt data at rest or in transit to prevent breaches of PHI, many such systems have ‘broken’ encryption. That’s why it’s essential to test EHR software to determine if encryption functions are properly implemented.”

CHRIS WYSOPAL, Veracode Co-Founder

REDUCE YOUR RISK BY SECURING APP LAYER



Any organization, of any size, can develop an application security program that reduces the risk of a breach through the application layer.

FIND OUT HOW WITH
**The CISO Kit
for Application
Security**



The Veracode logo is displayed in white and blue text. The word "VERACODE" is in white, with the "O" in blue. A large, stylized black snake graphic is positioned behind the text, winding across the top and right side of the page. The snake has a head with a circular eye containing a white 'V' and a black body with several pairs of mechanical-looking limbs or sensors extending from it.

VERACODE

SOURCES

TalkTalk: www.computerweekly.com/news/4500272314/TalkTalk-loses-100000-customers-in-cyber-attack?utm_medium=EM&asrc=EM_EDA_52968419&utm_campaign=20160202_TalkTalk%20loses%20100,000%20customers%20in%20cyber%20attack_&utm_source=EDA

Vtech: www.bbc.com/news/technology-35532644

OPM: arstechnica.com/tech-policy/2015/06/opm-shuts-down-background-investigation-portal-because-of-vulnerability/
www.nbcnews.com/tech/tech-news/opm-finishes-mailing-notification-letters-data-breach-victims-n478721

Anthem: www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/
www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html

Premera: www.darkreading.com/two-more-health-insurers-report-data-breach/d/d-id/1319511?