SECURITY COMPASS WHITEPAPER

Why Hackers Target Insurance Companies

Security Compass

When hackers select targets for cyber-attacks, insurance companies are often at the top of the list. The reason? The information insurers manage is extremely valuable to criminals. By some estimates, stolen Personally Identifiable Information (PII) from healthcare insurers is worth 100 times more than stolen credit card information.

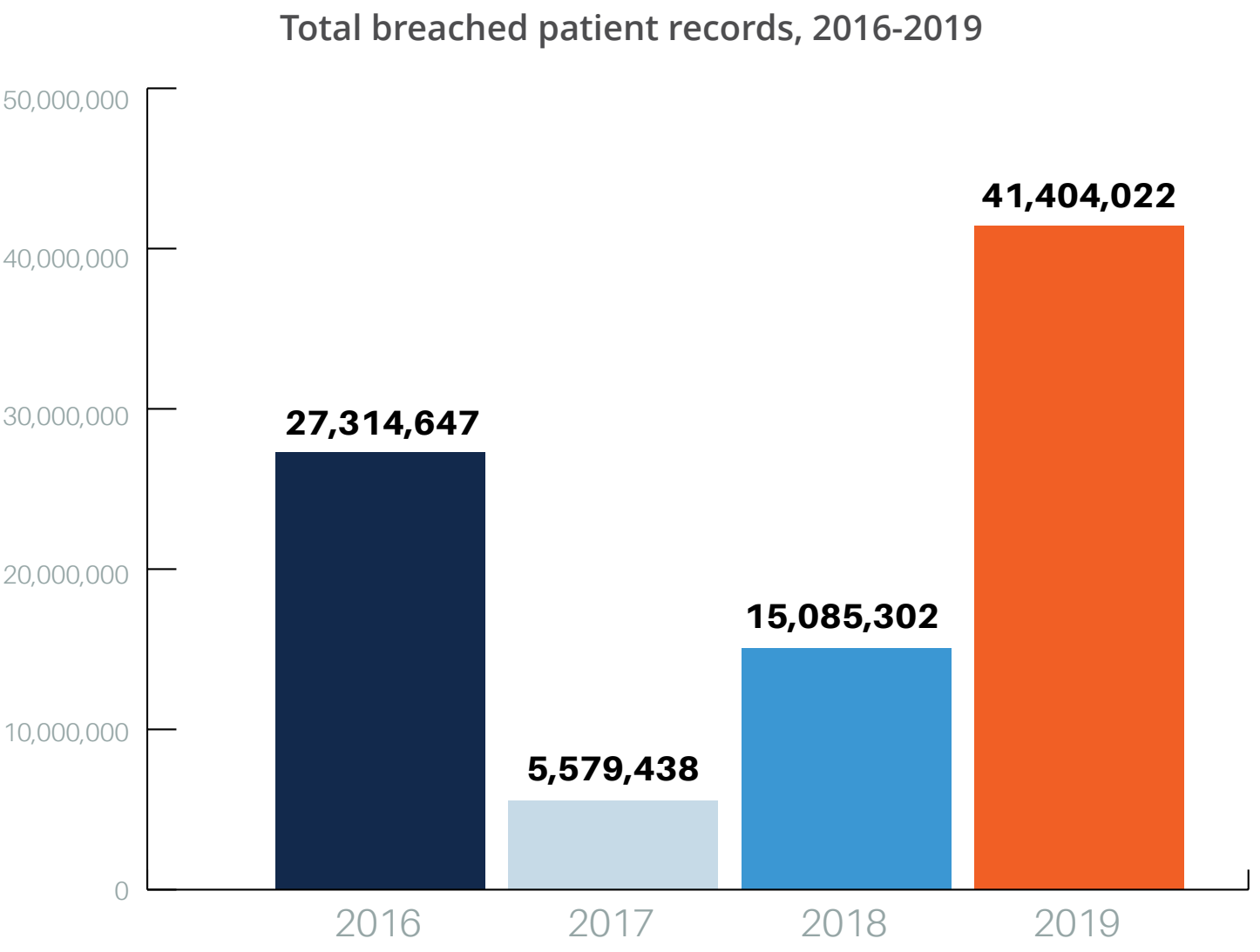
Data stolen from a property and casualty insurer may include banking information, credit card number, CVV, and consumer name and address. However, PII stolen from a life insurer can include that information and medical history. If the insurer issues health insurance, sensitive information also includes policy numbers, birth dates, medical history, and diagnosis codes. Criminals can use this data to buy and resell medical equipment or prescription drugs or falsify claims with insurers. For consumers, instead of simply clearing up their credit score they may also have to repair their medical history, removing falsified diagnoses.

> "Electronic health records are 100 times more valuable than stolen credit cards"
>
> **JAMES SCOTT**
> Institute for Critical Infrastructure Technology

Regulatory Compliance Pressure

Like most organizations, insurance providers are subject to a variety of regulatory standards requiring the protection of sensitive information. These include PCI-DSS for credit card information, HIPAA (US) and PIPEDA (Canada) for personal health information, GDPR for the PII of European citizens, Section 5 of the FTC Act, and dozens of provincial, state, and local regulations.

Non-compliance has real costs. GDPR fines can reach €20 million, or 4% of a company's annual revenue for serious infringements. Anthem was fined $16 million for HIPAA violations on top of paying $115 million to settle a class-action lawsuit associated with its 2015 breach. Outside of the insurance field, Equifax was fined up to $700 million for a breach that exposed personal information on over 147 million American, Canadian, and British citizens. The breach also resulted in the sudden "retirement" of Equifax's CIO, CISO, and CEO.



Source: Protenus 2020 Breach Barometer Report

Security Standards - Lost in Translation

These standards can be very granular with specific guidance (PCI-DSS) or quite vague, requiring "reasonable security" standards. Understanding which of the overlapping standards apply to your software and deployment environment is just the first step. More critical – and more challenging – is translating the individual requirements into development activities and security controls. In addition, most organizations lack ways of communicating secure coding standards and testing for conformity with those standards and the likelihood of non-compliance rises.

Translating security standards into development activities is difficult because these are often non-functional requirements. Business owners, customers, and engineering can easily create functional requirements for software. Functional requirements define things the software must do.

In contrast, security standards are often non-functional requirements – including things the software must not do. This can include not accepting malformed or unacceptable data (e.g. special characters, negative numbers) or prohibiting hardcoded credentials. Remembering to do these things is difficult when the focus is delivering functional requirements in a fixed period, even in organizations that have secure coding standards.

Security Testing Helps – Kind of...

Standards like PCI-DSS require organizations to test for vulnerabilities like those listed in the OWASP Top 10 or SANS Top 25. Others, like HIPAA, require organizations to identify and assess risk then follow a plan to reduce risk. Scanning tools like Static Analysis, Dynamic Analysis, and Source Composition Analysis are useful for identifying vulnerabilities like these. These tools become a challenge when they are used late in the development process when teams are preparing to release new builds, and when false positives rates are high.

Organizations that successfully identify risk and threats prior to beginning the development process can make security controls part of the developers' assigned tasks. Traditional threat modeling can require weeks of time, delaying time to market and straining scarce security resources. The result is that threat modeling is reserved for only the most critical projects. Without threat modeling and secure development policies, security scanning becomes the primary method of "securing" software.

Build Security into Development

A better approach is to identify threats in advance for all software projects. This is possible because a large majority of the threats to software are linked directly to the technical stack and deployment environment.

SD Elements identifies foundational threats automatically through a short survey. It then translates threats and any regulatory requirements for which the application is in scope into discrete, actionable tasks that can be assigned to developers and operational security. Tasks can include code samples for developers, test plans for QA, and can be tailored to include an organization's internal secure coding standards.

Go Fast. Stay Safe.

Engineering teams at insurers are under the same pressure to develop code quickly as are developers in other technology-heavy markets. SD Elements solves the development devil's choice between developing code fast and risky or slow and safe.

By identifying threats, regulatory obligations, and coding policies in advance, engineering teams have clear tasks and security requirements in addition to functional requirements along the SDLC. This allows secure coding to be part of the development process, allowing teams to meet market demands and keep software safe. When security is built into software in this way, instead of using scanners to find vulnerabilities, they are used to validate that tasks were completed as planned.

SecurityCompass

Security Compass believes in a world where people can trust technology, and it is our mission to help customers proactively manage cybersecurity risk, without slowing down business. Our holistic program offerings are tailored to your organization's needs. Through advisory services, training, and SD Elements, our award-winning policy-to-execution platform, we set you up with all of the resources and tools your organization needs to develop secure software. Security Compass serves some of the world's largest enterprises, including 16 of the largest financial institutions in North America, South America, and Asia, as well as 4 of the largest tech companies in the world.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
1001 Bayhill Drive
2nd Floor
San Bruno, California
USA 94066

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001

Author: Michael Pittenger