AN INTRODUCTION TO SECURITY DEBT

A subset of technical debt, security debt is essentially the vulnerabilities and flaws in your organization's software and systems that could result in breaches.

Something that normally accumulates over time -- these vulnerabilities and flaws happen when there is a failure to include security measures within the entire lifecycle, from development to deployment and maintenance, of software and systems. Starting at the beginning, debt builds up when things are being done quickly, patched hastily, or put off for later.

Take, for example, a system that an intern built for a company years ago. The company released the system under pressure to get it running and decided to address the weaknesses later. However, unfortunately, the company never tested the system for bugs because the immediate problem was addressed. Then, they forget. Later never came. And now, years down the road, this company has built more systems relying on the intern's software. And, just like that, they have security debt that could potentially leave their entire system exposed.

Naturally, there are many ways security debt can accumulate. Beyond a system that was deployed and never checked, you could be running code that is checked but only patched and then patched some more, broken up, reworked, and never truly fixed. You could be running multiple security systems that were implemented by an old employee. Heck, it could be as simple as you are not properly updating passwords or too many of your employees have access to unneeded systems.

In reality, security debt can sneak up on you from anywhere, including hackers or malicious software, ruining not just your system but doing unfixable damage.

Noteworthy Examples

Over the years there have been huge corporations that have encountered security debt problems and paid the price.

PayPal

In early 2020, PayPal the famous online funds transferring system announced that they rewarded a researcher $15,300 for finding a high-level security vulnerability. "The researcher identified a method by which a user, starting from a malicious site, could expose the security challenge token to a third party via a cross-site script inclusion (XSSI) attack. If the user then followed a login link from the malicious site and entered their credentials, the malicious third party could complete the security challenge, triggering the authentication request replay and exposing the user's password. This exposure only occurred if a user followed a login link from a malicious site, similar to a phishing page." Within a day, it is reported that the company had patched the bug. However, due to this not being PayPal's first incident, many users are left worried if their payment information is safe.

Back in 2017, 1.6 million customer data details were stolen from a recently acquired PayPal subsidiary company in Canada. This breach left the millions of user's bill payment and equity information open to be stolen. On top of that, in 2014, the company also experienced vulnerabilities that left user's information possibly open to hackers.

Snapchat

In early 2014, a site called SnapchatDB released 4.6 million account names and passwords from the popular social media site Snapchat. A representative from the DB site stated, "Our motivation behind the release was to raise the public awareness around the issue, and also put public pressure on Snapchat to get this exploit fixed. It is understandable that tech startups have limited resources but security and privacy should not be a secondary goal. Security matters as much as user experience does." Clearly, from this announcement, Snapchat most likely knew about the vulnerability prior to the release. Causing many users unnecessary stress and the company's reputation to be questioned, had they paid close attention to their security debt and outside warnings, this would have never happened.

The Office Of Personnel Management

In April 2015, a server security breach on the US agency that handles the government's civilian workforce was reported. Identified by an IT employee who was checking code, it is reported that at first, the employee found the hack odd and big. Then, over the next few months of digging, it was understood that the attack was officially recognized by the agency in 2014 after beginning in 2013. Research timeline reports state that in 2014 "OPM officials chose to allow the attackers to remain so they could monitor them and gain counterintelligence. OPM did plan for what they called the 'big bang'—a system reset that would purge the attackers from the system—which they implemented on **May 27, 2014,** when the attackers began to load keyloggers onto database administrators' workstations." Unfortunately by then, the attackers had too much of a foothold that the agency was not able to dismantle. Even with their efforts to rid the system of the breach, over the next few years fingerprint data along with background check and clearance application data was stolen.

OPM very openly made a mistake, underplaying their security debt in this incident. The system was entirely vulnerable and, due to not taking action, the US Government openly shared their information.

WannaCry

An appropriately named example, in 2017, a malicious software named WannaCry corrupted countless organizations systems. Attacking hospitals and corporate systems, the damage that this bug created was so effective, leading to years of system engineers scrambling to meet timelines as well as patching. Expert accounts of how the bug worked so well reveal that "WannaCry broke in across the internet, jumping from network to network and company to company using an exploit – a security bug in Windows that allowed the virus to poke its way in without needing a username or a password." In essence, if any company used Windows, they were left vulnerable.

How To Get Out Of Debt And Protect

Processes - Create a true end-to-end process. When you have protection at the top of your list from the start, it will greatly reduce your security debt. Ideally, your company will take time to manage patches and monitor vulnerabilities.

Invest - Considering that human error is a large part of the problem, invest in training your team to find solutions and completely fix them. You must find ways to ensure and prevent errors in the first place.

Analysis - Start taking note of your risks, vulnerabilities, bugs, and more. Do this not only before but after a vulnerability has been discovered. Take information down about each error and how it is compared to others.

Register - Talk about your bugs and vulnerabilities. Make a list of them, track them, and ensure that your team comes back to them at a later date if time is essential. There will be no excuse to miss a patch or have an issue later if all bugs are noted and their severity is tracked.

Disclose - Find ways for others to be able to tell you about possible issues. In many of the above cases, the issues began when someone from outside of the company found a vulnerability. If you have a strategy in place that allows others to identify and get a reward for finding the bug, this will minimize your debt security.

Test - Never stop testing and ensuring that your system is strong. Use this as a way to take those registered bugs and keep track of them. If you patched or fixed a bug, keep testing for it so that you can be sure it will not happen again.

Stop Putting Your Company At Risk

Far too often companies let their debt add up instead of fixing the problem or even preventing it. Acting now to get out in front of it, protecting against risk, is far less costly than letting vulnerabilities become a huge issue in the future.