The Role of Software Patches in Cyber-Risk Mitigation

November 7, 2017
Published by Jim DeLoach

Equifax is not just another organization that was breached. The company was named one of *Forbes'* "World's 100 Most Innovative Companies" for three years straight, from 2015 to 2017. The recent breach of the company's U.S. online dispute portal web application has raised serious questions about whether boards of directors and senior management are asking the right questions about actions their organizations are taking to protect themselves from cyberthreats. Are boards probing to discover what they don't know?

In September, Equifax announced a massive breach exposing the personal information of over 40 percent of the U.S. population. The company's stock declined almost 14 percent after the announcement, and heads rolled over the ensuing three weeks—first the chief information officer (CIO) and chief information security officer (CISO), and then the CEO. The pervasive headline effect of this incident has been as persistent as any in memory.

There are many important aspects of cybersecurity that the board is expected to tend to, including understanding what the organization's "crown jewels" are, business outcomes management seeks to avoid, understanding the ever-changing threat landscape, and having in place an effective incident response program, to name a few.

But this discussion is more specifically about the systems vulnerabilities we know about. That's the elephant in the room.

The sage advice—if your flank is exposed, fortify it before you get overrun—seems to apply here. Even noncombatants understand the value of protecting exposed flanks in desperate battle. A known vulnerability is most certainly an exposed flank, particularly when sensitive data is involved.

Enter the role of software patches.

A patch is a software update installed into an existing program to fix new security vulnerabilities and bugs, address software stability issues, or add a new feature to improve usability or performance. Often a temporary fix, a patch is essentially a quick repair. While it's not necessarily

the best solution to address the problem, it gets the job done until product developers design a better solution for a subsequent product release.

The Equifax incident raises the question as to why the company didn't implement the appropriate patch to its systems when the vulnerability was first identified. To be fair, other companies have suffered a cybersecurity event because they failed to implement a patch in a timely manner, and we have no insights into the unique circumstances at Equifax. Admittedly, patching software at a large organization with multiple, complex systems takes a considerable amount of time. But, for boards and executive teams everywhere, the Equifax episode serves as a stark reminder of the importance of understanding the company's cybersecurity strategy and tactics to pinpoint whether they know what they need to know.

Often, in our security and privacy consulting business at Protiviti, we see companies implementing patches within 60 to 90 days of discovering a systems vulnerability. We have seen some high-risk patches not applied at all for fear of breaking legacy applications; in effect, the organization simply accepts the risk of not applying these patches and, as an alternative, works to mitigate it. Based on our experience, 30 days from release to deployment is typically the "gold standard" for the time it takes apply a patch.

Is the gold standard enough? Companies are essentially leaving themselves exposed for 30 days. Meanwhile, they may lack the advanced detection and response capabilities to detect unauthorized activity occurring during that time. Organizations with a well-designed vulnerability management program quickly patch known vulnerabilities for critical public-facing services. For example, we see companies setting service level agreement targets of 72 hours, with some striving for 24 hours or less to limit the damage of an attack.

Simply stated, boards need to inquire as to the target duration from release to deployment to shore up cybersecurity vulnerabilities and, if it's 30 days (or more), question whether that is timely enough, especially when public-facing systems are involved and sensitive personal information is exposed. Today's optics regarding egregious security breaches, corporate stewardship expectations, and the related impact on reputation and brand image cry out for this oversight.

It is vitally important to scan public-facing systems immediately upon notification of critical vulnerabilities; "same day" should be the target. In addition, patch deployment should be tracked and verified as part of a comprehensive information technology (IT) governance process. It's not enough to merely push out a patch. A comprehensive IT governance process should confirm that the risk truly has been mitigated on a timely basis.

Directors and executives should also be concerned with the duration of significant breaches before they are finally detected. Our experience is that detective and monitoring controls remain immature across most industries, resulting in continued failure to detect breaches in a timely manner. Given the increasing sophistication of perpetrators, simulations of likely attack activity should be performed periodically to ensure that defenses can detect a breach and security teams can respond timely.

We know that an organization's preparedness to reduce an incident's impact and proliferation after it begins is an issue (i.e., the lapsed time between the inauguration of an attack and its detection is too long). Often, it takes over 100 days until suspicious activity is discovered; about 50 percent of the time, organizations learn of breaches through a third party.

In nearly every penetration test Protiviti conducts, the client authorizing the test fails to detect our test activity. Many organizations seem to think that if they outsource to a managed security service provider (MSSP), the problem will be solved —as if a box has been checked. However, we see time and again that this is not the case. Often, there are breakdowns in the processes and coordination between the company and the MSSP that result in attack activity occurring unnoticed. Not many organizations are focusing enough on this failure of detective controls to identify breach activity in a timely manner.

These two fronts—how long it takes to implement a patch, as well as detect a breach—inform the board's cyber-risk oversight. Every organization should take a fresh look at the impact specific cybersecurity events can have and whether management's response plan is properly oriented and sufficiently supported. For starters, directors should ensure they are satisfied with the elapsed time:

- For patching identified system vulnerabilities;
- Between the initiation of an attack and its ultimate discovery;
- Between the discovery of a security breach and the initiation of the response plan to reduce its proliferation and impact; and
- Between the discovery of a significant breach and the undertaking of the required disclosures to the public, regulators, and law enforcement in accordance with applicable laws and regulations.

Today's optics regarding egregious security breaches, corporate stewardship expectations, and the related impact on reputation and brand image beg for careful oversight.