ISSUE 97

protiviti®
Face the Future with Confidence

Board Perspectives:
Risk Oversight

How Long Does It Take to Implement a Patch?

The recent breach of a major credit bureau has raised serious questions about whether boards of directors and senior management are asking the right questions about actions their organisations 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 CIO and CISO and then the CEO. The pervasive headline effect of this incident has been as persistent as any in memory. Everyone concerned about cyberthreats is talking about it.

Equifax is not just another organisation that was breached. It was named one of Forbes' "World's 100 Most Innovative Companies" from 2015 to 2017. So, what happened?

On July 29, 2017, the company's security team noted suspicious network traffic associated with its U.S. online dispute portal web application. In response, the team investigated and blocked the suspicious traffic. Upon observing additional suspicious activity the following day, the company took the affected web application offline. An internal review discovered a vulnerability in the open source web application framework at the point of attack, a vulnerability previously identified and disclosed by US-CERT (a cybersecurity arm of the U.S. Department of Homeland Security) in early March 2017. Based on the company's investigation, it is believed that the unauthorised access to certain files containing personal information — names, Social Security numbers, birthdates, addresses and some driver's license numbers — occurred from May 13 through July 30; therefore, the security flaw had been identified a full two months before hackers exploited it to gain access to sensitive data. The company has since patched the affected web application and brought it back online.[1]

This incident raises a question as to why the company didn't apply the appropriate patch to its systems when the vulnerability was first identified. To be fair, other companies have suffered a cyber event because they failed to implement a patch timely, and we have no insights into the unique circumstances at Equifax. But, for boards and

[1] "Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes," Equifax website, September 15, 2017, available at https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

executive teams everywhere, this 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.

Key Considerations

There are many important aspects regarding cyber-security — identifying the organisation's "crown jewels" and business outcomes management seeks to avoid, understanding the ever-changing threat landscape and having in place an effective incident response programme, 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.

A patch is a software update installed into an existing programme 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.

Admittedly, patching software at a large organisation with multiple, complex systems takes time. Once a vulnerability is identified, the patch must be developed and tested to ensure it doesn't cause problems before it goes live. However, many believe that Equifax should have moved faster, regardless of the difficulty of the patch — particularly for an organisation with a significant amount of sensitive data and an implied brand promise that it can be trusted with that data.[2]

Often, in Protiviti's security and privacy consulting business, we see companies implementing patches within 60 to 90 days of discovery. We have seen some high-risk patches not applied at all for fear of breaking legacy applications; in effect, the organisation 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 implementing a patch.

Is the gold standard enough? Companies are essentially leaving themselves exposed for 30 days. Meanwhile, they may lack the capabilities to detect unauthorised activity occurring during that time. The shopworn adage of "it's not a matter of if a cyber risk event might occur, but more a matter of when" doesn't fit the realities of this era of constant attacks. For the majority of companies, cyber risk events have already taken place and continue to take place. Yet many companies lack the advanced detection and response capabilities they need. The proliferation of data privacy regulations around the globe and the sticky headline effect of significant data breaches are leading directors and executives alike to recognise the need for "cyber resiliency."

Organisations with a well-designed vulnerability management programme 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, executives and 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 careful 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 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

[2] "How the Equifax Data Breach Happened: What We Know Now," by Jackie Wattles and Selena Larson, CNN Tech, September 16, 2017, available at http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/.

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 defences can detect a breach and security teams can respond timely.

We know that an organisation'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, organisations learn of breaches through a third party. In nearly every penetration test Protiviti conducts, the client authorising the test fails to detect our test activity. Many organisations seem to think that outsourcing to a managed security service provider (MSSP)[3] solves the problem — as if a box has been checked. However, we see time and again that this is not the case. Often, breakdowns in processes and coordination between the company and the MSSP result in unnoticed attack activity. Not many organisations are focusing enough on this failure of detective controls to identify breach activity in a timely manner.

Once an incident is discovered, the organisation must be prepared to respond immediately. A carefully considered response plan should be in place and tested periodically to ensure responses are appropriate and response time is sufficient. The plan should ensure that all parties understand their specific roles and cover public notification of a breach and related disclosures. In notifying the public, care should be taken to avoid compounding the problem. For example, a site set up to inform the public of their rights and actions they can take to protect themselves should itself be secure and sitting on the company's official domain to avoid looking like a phishing site and causing additional confusion.

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 organisation should take a fresh look at the impact specific cyber events can have and whether management's response plan is properly oriented and sufficiently supported. This review includes an assessment of internal processes and capabilities to determine whether proactive steps should be taken to make necessary improvements — both near term and long term. As organisations revamp their legacy infrastructure to take advantage of cloud services and newer architectures, it should become easier to remediate vulnerabilities on a timely basis. In the meantime, companies need to be vigilant in protecting their flanks by acting on known systems vulnerabilities and detecting breaches in a timely manner.

Questions for Boards

The board of directors may want to consider the following questions in the context of the nature of the entity's risks inherent in its operations:

- Do directors understand the company's vulnerability management? For example, is the board 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?
  - 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?
- Does the board include cyber as a core organisational risk requiring appropriate updates in board meetings? Is the board satisfied that the company's strategies for reducing the risk of security incidents to an acceptable level are proportionate and targeted to the most important information assets and business outcomes? Does the board receive key metrics or reporting that present the current state of the security programme in an objective manner?
- Does the board focus on the adequacy of the company's playbook outlining the actions in place to respond, recover and resume normal business operations after an incident has occurred, including responses to customers and employees to minimise reputation damage that could occur in a breach's wake?

[3] An MSSP is an internet service provider that provides network security management services. Such services may include virus blocking, spam blocking, intrusion detection, firewalls and virtual private network management.

How Protiviti Can Help

Protiviti works with organisations to focus on foundational information security questions:

- Do we know what we need to protect (e.g., the data and information systems assets that are most important — the "crown jewels") and where they are located? With respect to these assets:
  - Are we properly caring for them? How do we know?
  - Who are we protecting them from, to whom should we permit access, and how can we tell the difference?
  - Are the defences we have put in place any good? Are they working as designed?
  - How will we know if things are not working as we planned?
- Are we able to recognise a new threat to our environment and detect likely attack techniques on a timely basis and align our protection measures to meet the threat?
- Are we ready to respond if something bad were to happen? Are we capable of managing such incidents? When incidents occur, are we able to keep them from happening again?

Protiviti provides a wide variety of security and privacy assessment, architecture, transformation and management services to help organisations identify and address security and privacy exposures (e.g., loss of customer data, loss of revenue, or reputation impairment) before they become problems. Working with companies in all industries, we evaluate the maturity of their information security programmes and the efficacy of their controls — and help them design and build improvements when needed. We have a demonstrated track record of helping companies react to security incidents, establish proactive security programmes, deal with identity and access management, and handle industry-specific data security and privacy issues. Our experience and dedication to developing world-class incident response plans have resulted in deep expertise in security strategies, response execution, forensic analysis and response plan development.

Is It Time for Your Board to Evaluate Its Risk Oversight Process?

The TBI Protiviti Board Risk Oversight Meter™ provides boards with an opportunity to refresh their risk oversight process to ensure it's focused sharply on the opportunities and risks that truly matter. Protiviti's commitment to facilitating continuous process improvement to enable companies to confidently face the future is why we collaborated with The Board Institute, Inc. (TBI) to offer the director community a flexible, cost-effective tool that assists boards in their periodic self-evaluation of the board's risk oversight and mirrors the way many directors prefer to conduct self-evaluations. Boards interested in using this evaluation tool should visit the TBI website at http://theboardinstitute.com/board-risk-meter/.

Learn more at
www.protiviti.com/boardriskoversightmeter

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is partnering with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on www.nacdonline.org/Magazine/author.cfm?ItemNumber=9721. Twice per year, the six most recent issues of Board Perspectives: Risk Oversight will be consolidated into a printed booklet that will be co-branded with NACD. Protiviti will also post these articles at protiviti.com.

protiviti®