OLIVER WYMAN

POINT OF VIEW

THE MARRIOTT DATA BREACH

LESSONS LEARNED FOR BOARDS

AUTHORS

Chris DeBrusk, Partner
Paul Mee, Partner
Rico Brandenburg, Partner

Marriott International recently announced that it was the victim of one of the largest data breaches ever reported. Based on their disclosures, the private information of up to 500 million Marriott customers was stolen via a sustained compromise of the network that apparently started four years ago. Marriott has now joined the league of largest companies in the world having systems breached and customer information compromised, a peer group that includes Yahoo, Target, Facebook, Equifax, eBay, Sony, and Home Depot, among many others.[1] To put things in context, in the first half of 2018, a staggering 4.5 billion records were compromised worldwide.[2]

If you sit on the board of a company, or are part of the executive management team, this latest hack is yet another reminder that cyber risk needs to be at the top of your agenda. This data breach should lead you to ask some particularly hard questions about your company's cyber preparedness, and cyber risk appetite. Specifically, you should ask whether your control environment is in alignment with the level of risk you believe you have accepted. You are likely to discover you are not where you thought you were.

IF THEY WANT TO, THEY WILL GET IN

Corporate networks are rife with legacy technology that was never designed with security in mind. In some cases, these legacy systems were a result of company mergers or acquisitions where speed to integrate capabilities made business sense. Compounding this security risk, many business networks are flat, often consisting of thousands of applications and hundreds or thousands of databases and file shares with limitations to access control mechanisms. This leaves sensitive data potentially exposed to adversaries once they are able to gain access and navigate the network.

And then there are your workers (employees, contractors, and other third parties), who can represent the weakest link in any cyber defense strategy as they can fall for phishing attacks, social engineering, and the temptation to 'go rogue' for monetary gain or as a form of revenge.

"Your cyber team needs to be successful 100% of the time. A hacker only needs to be successful once."

Arguably, it is functionally impossible to completely secure most corporate networks. Your cyber team needs to be successful 100 percent of the time, while a hacker only needs to be successful once. If you accept that a motivated hacker will find a way around your defenses, then your cyber strategy needs to be more than just protecting the perimeter—you need to develop an active defense culture. It also needs to focus on catching bad actors when they breach your walls, and if breached, how to identify and eradicate persistent presence prior to bad actor exfiltration. This includes identifying, segregating, and hardening your most valuable data assets or 'crown jewels', deploying advanced internal detection capabilities, integrating threat hunting as part of business as usual, and performing continuous Red Team[3] exercises to test your internal network identification and response capabilities. Adopting these active defense efforts, accompanied by maintaining sound network hygiene,

1 http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

2 https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx

3 Red Team exercise: An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization (NIST Special Publication 800-53 Rev.).

will make it increasingly difficult for attackers to gain access and establish undetected persistent presence in your network.

THE MOTIVATION AND INTEREST OF HACKERS VARY

The goal of an attack is not always the direct monetization of valuable customer information. The motivation of the attacker can also include things like targeting the whereabouts of customers and staff for espionage purposes, understanding the business practices and IT architecture to launch subsequent attacks on the company, or manipulating information to cause reputational damage.

"A given corporation needs to ensure that its most valuable assets or 'crown jewels' are subject to the most hardened of defenses."

Organizations need to take a focused and robust approach to identifying non-public data assets that they hold which could be valuable if sold (e.g., ID scans, credit card data), or are valuable because of the information they contain (e.g., systems and network maps, travel records). Once identified, a corporation can make sure these assets are stored in a hardened state, make it increasingly more difficult to access them based on how sensitive the information is, and ensure the associated data is not moved from a more secure to a less secure format (e.g., extracted from a protected database to an Excel file and then emailed).

It is also critical that you think like a hacker when performing an evaluation of the data assets your company holds and how attractive they might be. While a company may not immediately consider that travel plans would be valuable information, nation-state actors or criminal groups would certainly consider the check-in and check-out data for important people of interest and worth going after. Certainly, customers or staff do not want actors across the criminal community knowing when they are not home.

INSURANCE NEEDS TO ADEQUATELY COVER THE SCALE AND SHAPE OF THE CYBER RISK

Many boards take comfort in the fact that they have cyber insurance and consider themselves to have a form of protection from the implications of a breach, both small or large. According to the 2018 Cost of a Data Breach Study (Ponemon Institute[4]), the cost for a data breach involving 50 million records is estimated to be around $350 million. Early estimations are that expenditure in excess of $300 million will be associated with this breach, which is likely the lower end of the spectrum considering potential direct and indirect costs. Given the direct and indirect losses experienced by Target, Home Depot and others, this might well be a best-case scenario with the total cost potentially becoming much more significant.

With this in mind, organizations need to evaluate their cyber risk exposure through a structured data-driven approach in order to identify what type of losses, beyond availability and destruction, across the various scenarios they want to and can be insured against.

4 Ponemon Institute: https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/

"It is crucial that cyber incident and crisis response plans consider all practical aspects and the associated decision making relevant to the situation."

PLAN FOR A CYBER EVENT, THEN DRILL AND TEST

As we wrote a year back,[5] the time to determine how to respond to a cyber event is not when it happens, but long before there is an actual event involving your company. GDPR requires businesses to report a cyber breach involving personal data in 72 hours. The SEC requires public companies who are listed in the US to report material cyber events in a timely fashion. While the SEC is not yet as prescriptive as in the European Union, anything that could impact shareholders needs to be reported quickly or the company could be accused of hiding information that would impact share price (Marriott's stock value was off over 7 percent directly following their announcement, a market cap reduction of over $2.7 billion dollars).

Therefore, corporations should have cyber response plans and protocols in place that consider how management will respond, communicate (internally and externally), recover from and assess the impact of a large scale cyber-attack. It is crucial that the plans consider all practical aspects relevant in a given cyber response scenario (e.g., How do we contact customers with missing contact details? How do we handle capacity in the contact centers? What is the communication protocol of contact center staff?).

The list goes on and on. The board needs to ask management to rigorously review and challenge (internally or through independent review) their cyber incident response plans to ensure they are comprehensive and well thought out. And don't forget you need to drill the organization on the plan. Just writing it down is not enough.

FOCUS ON CRITICAL BUSINESS PROCESSES

Even if your company has thought through all of this, has the right insurance and reserves, and drills cyber events at least quarterly, it is likely you are missing a substantial amount of the cyber risk your organization faces.

Most organizations still take a relatively technically-centric view of cyber risk, considering their networks, infrastructure, databases, identity and access management (IAM), etc. But state of the art in cyber risk identification and risk management is to take a business view, rather than a technical view, and go step-by-step across your critical business processes to identify where cyber risk is introduced and how effective your controls are. By following the process steps that your people take to do their work, a significant amount of hidden cyber risk can be identified that cannot be found through other means.

As an example, many companies do not have strong process-based controls to protect themselves against whaling[6] or spear-phishing[7], the sending of un-authorized wires that result from social engineering attacks. These types of losses are so prevalent that the SEC felt it necessary to directly comment on them.[8]

5 Please see the 2017 Oliver Wyman report, "Practical Cyber Response: Being fully prepared for the inevitable."

6 Whaling: Specific type of phishing attack that targets high-profile employees, e.g. CEO or CFO, in order to steal sensitive information from a company (Techtarget).

7 Spear-phishing: Email or electronic communications scam targeted towards a specific individual, organization or business (Kaspersky).

8 https://www.sec.gov/news/press-release/2018-236

"Organizations need to adopt a security first principle to ensure that cyber risk considerations are integrated into business decisions."

DON'T TREAT CYBER AS AN AFTERTHOUGHT

Making business decisions without considering the impact on an organization's cyber risk posture can have dire consequences. Many of organizations still prioritize speed-to-market over adequate security, without fully analyzing or understanding the impact of increased cyber risk to the enterprise.

Organizations need to adopt a "security first" principle to ensure that cyber risk considerations are integrated into all tactical and strategic business decisions—whether it is about the implementation of new business processes, the deployment of new customer-facing technology, or the acquisition of new businesses. Without a clear understanding of the residual cyber risks introduced through any organizational or operational change, it is difficult for boards and senior management to get comfortable with and accept the new level of cyber risk.

YOU ARE NEVER DONE

The one thing that the never-ending announcements of data breaches should reinforce in every board and executive team is that no matter how much you have invested in your cyber risk management program, you are never done. New technical vulnerabilities are discovered every day, every business process change can create unintended process vulnerabilities, and every new worker in your organization is increasing the cyber risk exposure that needs to be managed.

We expect cyber risk to stay pinned on the agendas of board risk committees. The key is to not let your guard down, actively defend, and continue to challenge the organizations you are responsible for to think way out of the box—the bad guys certainly are.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

Chris DeBrusk

Partner in the Finance & Risk, Corporate & Institutional Banking, and Digital practices

Chris.DeBrusk@oliverwyman.com

Paul Mee

Partner in the Digital and Financial Services practices

Paul.Mee@oliverwyman.com

Rico Bradenburg

Partner in the Risk & Public Policy and Digital practices

Rico.Brandenburg@oliverwyman.com

www.oliverwyman.com

OLIVER WYMAN