OLIVER WYMAN

PRACTICAL CYBER RESPONSE

BEING FULLY PREPARED FOR THE INEVITABLE

AUTHORS

Paul Mee , *Partner*

Chris Debrusk, *Partner*

No matter how good your cyber defenses, it is nearly guaranteed that your company will be attacked and very likely eventually breached. Your readiness to respond effectively is critical, which means you need to:

- Define a team with a clear leader with sufficient authority and resources
- Create a clear plan
- Drill, drill, and drill some more
- Be prepared for attackers bent on your destruction, not just money
- Conduct post-mortems on actual attacks

After the Equifax data breach, many corporations are reevaluating their cyber risk posture to ensure they have invested sufficiently to align their cyber capabilities to the nature, complexities and inherent risks of their business. In a recent paper entitled "Embedding Cyber Defenses Where They Matter", we outlined six areas where corporations need to focus to improve their cyber defenses. Yet even if your organization ranks above average in all six areas, there is a seventh that is critical – your readiness to effectively respond to a cyber event.

The Identity Theft Resource Center has identified 1,120 publicly reported data breaches from Jan 1st through Oct 25th, 2017 where hackers got access to personally identifiable information (PII), consisting of over 171m records where the number of records were known and reported. The real number is likely far higher as, in the vast majority of cases, the number of records breached was not reported publically)[1].

It is therefore critical that you define your cyber response protocol long before you are breached, as reacting on-the-fly almost guarantees you will damage your company, customers, employees and perhaps most importantly, your reputation. Yet many companies do not have a robust cyber response plan.

DEFINE WHO WILL TAKE THE LEAD

It is often assumed that the Chief Information Security Officer (CISO) is the right person to take point on the response to a cyber event, and in many cases, this is the correct approach. For attacks where there was no penetration of the corporate network, or the penetration is quickly identified and blocked, the CISO should likely take the lead in documenting the company's response to the event or determining that no post mortem is required, as would be the case in a routine, unsuccessful penetration attempt. Many companies see hundreds or thousands of these per day.

Where it gets challenging is when there is a more serious data breach or damage to corporate assets. In that case, the CISO, who usually has a security and network background but may not have the necessary crisis response training and experience, may not be best positioned to take the lead on the company's response. Whoever is appointed to lead and coordinate the response to a major cyber event response team not only needs

1 http://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf

crisis management expertise, but also needs to be well known and respected across the organization and have the seniority to effectively brief the executive team, the Board, the press and in many cases regulators.

These skills are difficult to find in a single person, but regardless of who is appointed to the role, the time to assign someone to take point is now, not in the immediate aftermath of a breach.

DEFINE THE TEAM

Equally as critical is to identify the team that will work with the appointed leader to respond to the breach, and help the corporation stabilize its footing. Members of this team need to be drawn from a range of departments across the organization. Common groups who form the core of the team include the Risk, IT Security (i.e. the CISO), IT, Public Relations, Marketing, Finance, Compliance and Line of Business (LOB) representation. This team should be identified way in advance of an event, and explicit steps should be taken to form them as a well-oiled team so that in the compressed timeframe of an event response, the familiarity and trust that is the basis for successful teams is well cemented.

CREATE THE PLAN

The time to figure out what to do to respond to a cyber event is most definitely not during the early hours of the event. Resources need to be assigned to build out both the overall response plan, but also playbooks for various scenarios that could present themselves (and communication templates). The way in which an organization reacts to a large data breach where customer information is released is significantly different to an event where the goal of the hackers who are attacking the company is just to cause damage and reduce its ability to operate effectively.

It is necessary to explore all the various categories of attacks that you might be subjected to, with a focus on the different goals that a hacker could have, and the types of critical infrastructure and data assets they might be after. Plans should be created that explore each potential scenario of attack and response, of increasing severity and impact, right up to an attack where the primary goal is to physically incapacitate both computer systems, as in the Sony hack where $35m in IT infrastructure was damaged[2], and other machinery as was the case in a 2014 attack on a Germany steel plant where, among other things, blast furnace control was compromised[3].

DRILL, DRILL AND DRILL SOME MORE

As Field Marshal von Moltke is quoted as saying, “No plan survives contact with the enemy.” This very famous quote is appropriate when thinking about your response plan, as a cyber-attack is normally a complex, evolving process framed by misinformation and in most cases, an incomplete understanding of who the enemy actually is.

2 https://www.computerworld.com/article/2879480/2014-cyberattack-to-cost-sony-35m-in-it-repairs.html

3 https://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf

It is therefore necessary for the cyber response team to practice, both so they are comfortable with the response plan, but also so they get used to working with each other and adapting to new information and circumstances that necessitate a change to their approach. Because a cyber response team is drawn from organizations that typically don't work directly together in their day-to-day roles, they need time to cement as a group.

Even more important, these drills should test the team's ability to adapt to situations that they didn't anticipate. For example, what if an attack takes out the corporate email system? How will the team communicate amongst themselves and with other critical members of the organization? What if the hackers choose to attack during another event? As an example, how many New York City based financial services organizations could have successfully responded to a major cyberattack during tropical storm Sandy, when their staff were unable to get into work, and in many cases their offices in lower Manhattan were under water? If hackers wanted to cause mayhem and damage, attacking during a storm or other major event would increase the impact they would be able to inflict.

WHAT IF THE GOAL IS DESTRUCTION?

Many cyber events are based on a goal of extracting money from the companies that are attacked via ransom or direct theft, or their customers via sale of data, account takeover and identity theft. Yet in the last few years a new form hacker has emerged. This class of criminal (or nation state proxy) has as their primary goal causing damage and destruction to the organization that is targeted. This damage could be primarily reputational, by releasing private or embarrassing information, or it could be the destruction of information by deleting, corrupting or encypting high value data, or causing physical damage to computer systems, IoT devices or networked machine controllers.

A cyber response plan needs to consider that the intent of a hacker may be to cause chaos, and it should consider appropriate responses that may include shutting down critical systems, logically or physically removing portions of the network from the public Internet (by closing off firewalls or in extreme cases, pulling network cables), or restricting access to critical data assets. The decision to take each of these steps needs to be planned out, the criteria established for doing so and authorizing persons identified. Situations where key decision makers are not available (on vacation, on a plane, cut off from communication, etc.) should also be considered and planned for.

DO A POST MORTEM

Every notable cyber event should be subject to a formal post mortem during which the response team critiques how they performed, how the plan worked and considers what could be improved for the next time (as there will be a next time). These post mortems should be facilitated by a neutral third party (internal audit for example) so that the team

doesn't suffer from group think, or is overly congratulatory on their performance. Finally, the post mortem should be written up and retained as part of the overall cyber planning process.

* * *

Cyber defenses are just that, defenses. Every corporation hopes they will operate as designed and protect the organization from attack, but if history is any indication, even the best cyber risk posture won't prevent a company from suffering a breach. It is critical that every organization create its cyber response plan, keep it current and up to date as the organization and its technology infrastructure changes, and regularly do table top exercises to drill on the plan, cement the response team and determine where there is need of improvement.

A major cyber event can, if not handled correctly, result in company ending losses or the termination of one or more senior executives, including the CEO. The time to plan your response is before your Board is demanding answers on how the company is going to respond to an emerging threat.

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

www.oliverwyman.com

OLIVER WYMAN