Do You Suffer From Cyberfatigue? Stay Vigilant

Christopher M. Brubaker, The Legal Intelligencer

September 12, 2017

Have you become immune to the latest breach headline unless you might be personally impacted (or unless it offered the opportunity to watch "Game of Thrones" episodes early)? Tired of wondering if today is the day we get breached, hacked or held for ransom? Sick of knowing that there is no perfect solution to cybersecurity? Dumbfounded by the amount of resources that are being thrown at the issue with no guarantees that you won't suffer a catastrophic cyberevent? Fed up with trying to navigate the ever-expanding regulatory web impacting the use of data and cybersecurity? Confused by how much and what type of cyberinsurance to purchase? Welcome to cyberfatigue.

And it's no wonder. Search "cyberbreach" on Google and over 17 million results are located in 0.76 seconds. But you are not alone. Search "cyberfatigue" and 596,000 results are returned in 0.55 seconds. There are a variety of takes on the subject but the idea is the same, whether referring to individuals (have you changed all your passwords in the last 90 days) or multi-national organizations with thousands of employees, it is impossible to remain hyper-vigilant 24/7 in perpetuity. Meet the latest cybersecurity challenge, keeping both management and the rank and file alike engaged in cybersecurity.

The symptoms of and the cure to cyberfatigue merely underscore the nature of cybersecurity: risk management. It is generally accepted that it is a matter of when—not if—your organization will be breached. At present, there is no reason to believe this will change in the next 20 to 30 years or longer. Cyberrisk is a constant, and needs to be dealt with accordingly. It requires constant vigilance and continual review and adaptation; that is simply the nature of the beast. However, if approached utilizing tried and true risk management techniques, cyberfatigue should not be a lasting problem.

The name of the game in cybersecurity is not about getting to some defined point and checking off certain boxes, but about coming to grips with your appetite for risk and understanding what is at risk and how that will impact your business. This will obviously differ company to company, and even drastically within the same industry depending on where those companies are and where they are headed. While it is prudent to utilize an established protocol such as the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity, how that process plays out will be dictated by your appetite for risk and which cyber risks are most pertinent to your business. In other words, no two companies will likely end up in the same place utilizing these protocols and as your business evolves you are likely to end up in a different place as time progresses. Are you a startup or newer company still coming into your own? Are you an established brand with market share, good will and reputation? Are you a global giant? Are you expanding or restructuring? These are some of the more common factors

that will impact on your appetite for risk. Do you have large amounts of consumer data subject to breach notification and privacy standards? Are you subject to potentially conflicting obligations whether state to state or internationally (GDPR is coming)? Do you have financial or payment data? How integral is your web presence to your business? Do your people need to have access to sensitive proprietary information from anywhere in the world? All of the above? These questions help to define what is at risk and for you to identify which risks pose the biggest threat to your business operations.

Once you are comfortable with your risk appetite and know where your biggest vulnerabilities are, you are positioned to deal with cybersecurity and to prevent cyberfatigue. In many ways the goal is not to reach some definable level of security that will ensure cybersecurity—this simply does not exist. Rather, the goal is to implement as many defensive strategies as possible, given your appetite for risk, specific vulnerabilities, and any applicable regulatory requirement, to make you the least attractive target to cyber criminals. This of course is no guarantee, but should help to lessen the risk to your organization as much as possible. This begins with awareness. It is vital that everyone in the organization is aware of the value and importance of cybersecurity to your business. Everyone from the board room to the mail room needs to be aware of the basics of your approach to cybersecurity. That is not to say that every employee needs to know your entire cybersecurity plan inside and out, but they do need to know and be aware of the key areas of concern and what issues to flag. This is particularly true if your company is subject to specific regulations on the handling of data such as under HIPPA.

The required detail will obviously be greater for the management team but a firm understanding of your organization's appetite for risk and key areas of concern allows your team to efficiently and effectively process the endless barrage of information on cyber risk, cybersecurity and breaches. Communication is also vital to alert people to new and pertinent risks that threaten your key areas. This will help people to understand the information and how to use others' misfortune to make your cybersecurity better. This will also help to foster a culture of cyberrisk management within the organization. It is important for people to understand that there is no "finish line" when it comes to cybersecurity. Continual review and adaptation are necessary. By educating your team on the basics of your appetite for risk and key areas of concern, you empower them to be part of the solution. For management this is even more important as it will enable them to deal with new and evolving issues in a competent and timely fashion. When your management is presented with a request for the latest greatest cybersecurity tool they can intelligently consider how it will aid you with "x" or "y" and whether in light of these changes you can cut down or eliminate "z." It also puts you in a position to intelligently address the issue of how much cyberinsurance and what types to purchase.

Given that the accepted view is that at some point you will be breached, how you identify and respond to security incidents is arguably more important than what you do to prevent breaches. Regulatory compliance is a key aspect of breach response and if not properly planned for in advance can lead to missteps that can lead to fines, penalties and further embarrassment resulting from the breach. This of course ties right in with awareness of risk appetite and critical vulnerabilities; what are you going to do when you are breached? Having a response plan in place, and having everyone aware of the plan, is a universally preached component of cybersecurity. It has been demonstrated to reduce breach costs. For some it will be simply a

matter of timely alerting your cybercarrier and allowing their breach response mechanism to go into action. For others it will involve implementing your own action plan and contacting your - pre-arranged breach team. Either way, having the plan in place is also critical to averting cyberfatigue. It should give everyone confidence that they know what to do when that day comes.

As stated at the outset these risk management concepts are not new or unique to cybersecurity. In a time when we have become accustomed to looking for a technical solution to every problem a return to old-fashioned risk management techniques is proving to be the best answer to a complex and constantly evolving problem. That is not to say the technology has no place in cybersecurity. Firewalls, encryption, anti-virus and software updates are a vital and necessary aspect of any cybersecurity program, but we cannot expect them to be the total solution. Find your risk appetite. Identify your critical systems and vulnerabilities. The spotlight is brightest after the breach and your response will have a more lasting impact than what you did to prevent it. So, have a plan to deal with the inevitable breach and practice the response ahead of time. Obviously this cannot prevent a breach if it is truly inevitable, but it will position you to survive and even thrive when the inevitable does happen. •

Christopher M. Brubaker of Clark Hill concentrates his practice in complex commercial litigation and insurance matters. He regularly provides advice to companies on insurance and cyberrisk issues related to transactions and risk management and also advised companies on regulatory matters involving insurance and environmental laws, rules and regulations. He frequently speaks and writes on cybersecurity matters for legal and professional groups.