MORRISON FOERSTER

YOUR PRE-BREACH CHECKLIST

A significant breach can happen to any company.
Being prepared is the key to being resilient.

10 WAYS TO PROACTIVELY PREPARE FOR A SECURITY BREACH

Is your company prepared to respond to a security breach?

For many companies, even reading this question will cause some anxiety. However, being prepared for what seems like the inevitable — a security incident involving company information — can make the difference between successfully navigating the event or not. A significant breach can happen to any company, and being prepared is a key to being resilient. In light of this fact, and the significant scrutiny that a high-profile breach receives, many companies have taken the opportunity to consider their preparedness and ability to respond quickly and decisively to such an incident. We have prepared the following checklist, which highlights some steps we have been helping companies to take so they can be better prepared in the event that a significant incident occurs.

(1) Make Friends with Your IT/IS Department. As attorneys, we frequently focus on compliance and litigation. But we need to be familiar with our company's risk tolerance and approach to information security to develop an understanding of its security posture. The time to ask these questions isn't after a breach has happened, so ask your colleagues in your company's information technology or information security departments the basic questions (Do we use multifactor authentication? How are we enforcing complex-password rules? Are our laptops encrypted? Are our systems set to retain log files that would be useful when investigating a cyberintrusion? Do we have an out-of-band method for communication in the event that our corporate email system is compromised? In the event of ransomware, will our backup and business continuity practices be sufficient to meet the demands of our operations?) and the tough questions (Why haven't we addressed the data security concerns raised in last year's audit? How do we ensure that security patches are regularly installed? Do we utilize network segmentation?). You would rather learn, for example, that your company does not encrypt its laptops before one is stolen.

(2) Have a Plan. Many companies have an incident-response plan. If your company does, dust it off. Does it need to be updated based on the current breach environment, such as new facts or risks? Would it actually be helpful in responding to a high-profile, global, or nationwide security breach? Does it have a list of key contacts and their contact information? Also, make sure you have a copy printed out in case the breach impacts your company's systems and you are not able to access an electronic copy. If you don't have a plan, draft one!

(3) Practice. Practice! Although practice may not make perfect when it comes to data-breach response, you do not want your response team working together for the first time in the middle of an actual high-stress incident. Gather your response team and relevant stakeholders, and do a breach tabletop (and consider bringing your outside counsel). This will be valuable training and an investment in your company's preparedness; ideally it will be done annually.

(4) Decisions, Decisions, Decisions. Someone has to make the tough calls. A high-profile breach incident is a series of tough calls: When will you go public? How will you respond to the media? Will you offer credit monitoring? We continue to see incidents where there are competing views within a company about

continued on page 2

the "right" decision, and incidents where difficult decisions must be made based on limited facts. You should give thought to who within your organization will be responsible for making the tough calls, and making sure the key decisionmakers understand the broader issues that have to be considered.

(5) Know the Law. Notice is driven by federal and state laws (and often non-U.S. laws). There are federal breach requirements (e.g., the GLBA and HIPAA), and there are unique/individual requirements in every U.S. state and most U.S. territories. Needless to say, notice in a nationwide incident can be complicated. And the laws have continued to evolve over the last several years. You should make an effort to stay abreast of the current landscape of breach-related requirements (e.g., requirements for the content of consumer notices, requirements to notify state regulators, timing requirements of such notifications). In addition, breaches that affect subsidiaries, affiliates, or individuals outside the U.S. are even more complicated. Be aware that the number of jurisdictions with breach-notification obligations is growing, and in many instances what is considered a breach includes the unauthorized disclosure of any type of personal information. Moreover, a growing number of countries now require that notice be provided to regulators within 72 hours of a company learning of a breach.

(6) Go Outside. Outside counsel who have a deep practice in this area will have worked on countless incidents, both large and small, and can advise on how other companies respond to similar incidents and how regulators have reacted. This is invaluable insight when the tough calls have to be made. *See* (4) above.

(7) Engage Vendors. In a significant breach incident, a company's resources can be stretched thin. Many companies would not, for example, have the capability of producing and mailing 500,000+ breach letters in just a few days. Similarly, many companies are not prepared to handle significantly increased call-center volumes after an incident becomes public. There are a wide variety of vendors that can help companies respond to a breach incident, including forensic investigators, ransomware specialists, crisis communication experts, and mail houses, to name a few. Consider your capabilities and engage vendors before an incident occurs.

(8) In Case of Emergency, Call. The list of individuals and entities that you may need to contact in the event of a significant breach is probably longer than you think. For example, you may need to contact members of your response team, members of senior management, law enforcement, your merchant acquiring bank, a wide variety of vendors, the press, your regulators, outside counsel, and others. While it seems simple, it can reduce stress in the heat of the moment if you have a comprehensive contact list. *See* (2) above.

(9) Consider Coverage. Cyberinsurance is one of the fastest-growing areas of the insurance market today. It's quite possible that your company already has a policy that would provide at least some coverage in the event of a security breach. If so, you should review the policy to get a sense of the breadth of the coverage, and consider whether that coverage is appropriate for your company's needs. If your company does not have a policy, you can consider the costs and benefits of obtaining coverage. This is a risk-based decision, of course, but one that needs to be thought about before a breach occurs. Obtain the approval of your choice of counsel from your insurance carrier before experiencing a cybersecurity incident — good times to seek approval are when purchasing or renewing a policy, but you can seek approval any time, preferably not in the midst of an actual data-breach response.

(10) Don't Delay. Although you can't control whether a breach occurs, you can control how your company responds. Most companies with whom we work find that there is more that they can do to prepare for a potential breach event. In light of the public, regulatory, and internal scrutiny that a high-profile breach brings, don't delay in considering your preparedness to respond to such an event.

For more information on these issues, please contact:

John Carlin
(202) 463-1000
jcarlin@mofo.com

Miriam Wugmeister
(212) 506-7213
mwugmeister@mofo.com

Nathan Taylor
(202) 778-1644
ndtaylor@mofo.com

Kristen Mathews
(212) 336-4038
kmathews@mofo.com

Melissa Crespo
(202) 887-8768
mcrespo@mofo.com

Alex Iftimie
(202) 778-1659
aiftimie@mofo.com

Suhna Pierce
(213) 892-5327
spierce@mofo.com