Crossing the **Breach**

PROTECTING FROM DATA BREACHES IS MORE THAN AN I.T. ISSUE

WHITE PAPER

.VESTIGE

Digital Investigations

Crossing the **Breach**

It seems not so very long ago the term "data breach" was a relatively unfamiliar one among the average person. Although organizations such as Verizon and Ponemon Institute have been tracking and reporting on data breaches now for over a decade, it hasn't been exactly a household term over this time. Today, however, anyone who frequently reads the daily headlines is becoming increasingly familiar with its meaning.

As awareness has rapidly grown through a continual string of highly publicized incidents, many organizations still maintain an attitude of "it won't happen to us" or "our information isn't as sought after or valuable as those other organizations". It is fair to say that early-on, specific types of information such as credit card numbers, were larger targets affecting certain types of organizations more than others; and according to recent data, this continues to hold true to a degree. However, with malicious techniques becoming more automated and efficient, today everyone is indeed a target. In addition to the perceived value of this information, the ease of obtaining information has become a large determining factor in its vulnerability. To use a hypothetical comparison of a burglar loose in a neighborhood, bad guys are no longer just eyeing the wealthiest looking homes. They're now trying every door on the street and entering every one that can be easily opened, stealing whatever they can get their hands on and prioritizing their value later. This is why earlier perceptions and attitudes do not hold true today, making the threat of a data breach a concern for all organizations now regardless of industry or size.

"It won't happen to us"

It's not just the criminals you need to be concerned with today. The use of new technologies in our modern work environments are opening up an entirely new chapter of internal as well as external vulnerabilities. The utilization of multiple mobile devices, personal devices in the workplace, cloud services and virtual work environments, for example, have given us many advantages and convenience. However, those conveniences continue to reveal a whole new set of security challenges as the adoption of these technologies oftentimes outpace the needed security protocols. This leaves significant exposure for insiders to either maliciously or mistakenly reveal private information. The latest research continues to show these types of insider actions as a top cause of data breaches and the loss of other critical information. This includes not only the Personal Identifiable Information (PII, or PHI in the case of healthcare information) that we all hear about as these trigger public notifications, it also includes trade secrets, customer lists and other types of intellectual property critical to organizations.

Another earlier perception that is proving inaccurate has been the thought that "IT Security is an IT problem". Organizations are beginning to understand the holistic nature of the issue. Protecting private information has become an organizational-wide challenge. This includes not just IT, but HR, legal, operations, sales, purchasing and vendor management as well as trusted partners and service providers. What's unique about this issue is not only does it span across multiple disciplines, but to solve the problem it requires these areas to work together in interrelated ways that have been traditionally uncommon. *This includes not only a variety of internal departments, but outside professional services as well. This unique demand for diverse*

areas and disciplines to work and communicate more cohesively, is the key aspect of what makes preventing and mitigating the impact of a data breach so challenging.

For example, once a breach has occurred, one of the critical decisions to be made is to determine if an official notification to the affected public is in order. This would be in accordance with the appropriate different state laws currently requiring notification if a certain number of private records have been exposed. Input is required from both information security or computer forensic professions and attorneys. Although these are very different fields, regardless, they must work together in close appreciation of the other's needs, responsibilities and goals for an accurate decision to be made. The stakes are also high, as getting this decision wrong could cause additional harm to the affected organization. Gregory Stein, an attorney with the Cleveland Clinic who is focused on data security and data privacy law, states:

> *"Breaches often involve complying with multiple state data breach notification laws because of affected individuals residing in different states. Lawyers must know the facts to provide appropriate legal advice. Information security professionals that can analyze how a breach occurred and what information was impacted can thus be invaluable for a breach response. An information security professional can provide a clearer picture of the scope and impact of a security incident. Ultimately, that information is what drives the response and is the foundation for a lawyer to provide legal counseling about whether a breach has occurred under any applicable law and, if so, how to respond."*

Hence, the important decision to notify or not should be made by a qualified attorney as it is ultimately a legal decision pertaining to obligations under state laws. However, an attorney cannot make this decision properly without a thorough understanding of accurate technical findings in the incident. Unfortunately, not all IT security professionals are well experienced at communicating with attorneys and not all attorneys are as competent as Mr. Stein in understanding IT technical data toward the law. Nonetheless, in order to create a truly effective solution, this is what is required. Instead, it is not unusual to see IT professionals or attorneys making these decisions independently, absent the necessary combination of the other's complementary discipline.

Insurance is another area that requires this same necessity for varied disciplines to work in better concert toward a required solution. With security incidents such as data breaches rapidly on the rise, a market to insure against this risk has recently emerged and continues to grow in importance.

In an attempt to meet this new demand, several insurance companies are now offering "cyber liability" insurance as either a separate policy or as a rider to existing types of coverage. For the insurance

industry, it has been a challenging need to address as Information Security has been unfamiliar territory for them and there is little to no historical actuarial data to rely upon. In describing the need for a quick data breach response to reduce associated fines and penalties, Laura Corogenes, Product Director – Cyber, of Scottsdale Insurance Company stated:

"...while we can estimate the total costs our insureds will incur to resolve a breach, we cannot estimate the potential costs of 3rd party liability claims. We do not have sufficient historical data to do so."

This is the big unknown in every insurer's pricing model and why no insurer can state that the rates set for this coverage are sufficient for the exposure.

There are standard practices that insurance companies are beginning to apply to limit their exposure in this arena. These are designed to mitigate the risk up-front during the underwriting process as well as control claims' costs once a breach occurs with an insured. As this is a new area for insurance companies, requiring additional knowledge outside of their core expertise, even applying standard practices presents a challenge. For example, underwriting for these types of policies requires an adequate technical understanding of IT security as well as how organizational culture may expose data. Once a breach occurs, controlling claims' costs requires the ability to understand and coordinate many of the same diverse disciplines and areas mentioned earlier. These may include computer forensics experts, attorneys, internal IT, notification services, PR and more. While explaining the need for a data breach response to be more comprehensive to control claims costs both for the benefit of the insurer as well as the insured, Corogenes stated:

"... [insurance companies] want assurance that the extent of the breach and the cause of the breach is known, that the resulting actions of the breach have stopped and that there is little likelihood that the exact same situation is ongoing or will occur again. We do not want to pay the same costs 60 days or 90 days down the road, because the original breach continued to cause damage to the insureds system and data or continued to provide access to confidential data to an unauthorized party."

Therefore, an insurance data breach claim decision cannot be properly made and managed without an appropriate technical understanding of the incident. Again, this requires an atypical combination of understanding of the varied disciplines described to effectively manage a proper data breach response.

So what can be done to bridge this gap between

diverse areas and build better practices and solutions? First, at a more simple level, just being better informed of the threats and their scope can have a significant impact. For example, simply don't be the "easily opened" door as described earlier. This applies

"being better informed of the threats and their scope can have a significant impact"

a leading attack method of data breaches among these businesses. The report states "Let's start with the most frequent scenario, which affects small businesses that may or may not realize just how lucrative a target they are. This event chain begins with the compromise of the POS device with little to no legwork; the devices are open to the entire Internet and, to make matters worse, protected with weak or default passwords (and sometimes no passwords)." This awareness and something as simple as creating a password or changing a factory default password can then go a long way to avoid being the open door. Also, and this applies to businesses small and large, merely becoming conscious of these issues beforehand and having a response plan in place in the event of a breach can make a substantial difference. Michael Bruemmer, Vice President, Experian Data Breach Resolution explains, "While a data breach is inevitable, organizations can significantly reduce the cost and reputational fallout by preparing for a data breach in advance, starting with erecting a strong IT security posture, identifying a Chief Information Security Officer (CISO) or outsourced IT consultant and an incident response plan."

For organizations in the United States, Ponemon's 2019 Cost of a Data Breach Study shows that organizations that had a plan in place reduced their costs on average by $360,000 or 9.2%; and testing a written Incident Response Plan created, on average, a savings of $320,000. But combined, organizations adopting BOTH practices saw a savings of $1.23M or 31.4%! Therefore, simple awareness, basic precautions and some proactive consideration and planning can do well on their own to avoid major problems.

Turning back to the issue of bridging gaps between differing areas across the broader spectrum, the good news is that the right pieces of the puzzle are emerging. Cyber liability insurance, breach legal services, computer forensics, notification, call center support, credit monitoring and PR services, etc. are all available as parts of an effective data breach response plan. However, we still have some progress to make as a whole in fitting them together properly.

For example, cyber liability insurance is now available when not so long ago it didn't exist. And the computer forensics capability has been established to accurately understand, define and quantify the scope of a data breach. For cyber liability insurance

to be a more effective product for the insured as well as the insurer, these areas must educate each other further and partner together more closely. As Laura Corogenes explains, "Insurers must forge strong, trusting relationships with the vendors who provide breach investigation and mitigation services." Adopting this knowledge and capability through forming these relationships will enable insurance companies to take more ownership of the process to better manage their deliverable, making it a far more effective product. She continues,

"An effective insurer of their representatives, provided they have a strong overall understanding of this exposure and have external relationships with experienced breach services providers and knowledge of the likely exposure and damages their insureds will face once a breach occurs, may be the most likely party to coordinate the multiple steps in the breach remediation process. They will assure that the necessary resources are provided on a timely basis, that the response is sufficient to address the totality of the breach and performed as cost effectively as possible."

Michael Bruemmer stated also,

"As a final consideration for breach preparedness, consider investing in cyber insurance. This can reduce the cost of a breach and provide added benefits to a company's security posture via access to data breach experts or other valuable services. Then a breach happens, it is often best to complete the forensic investigation before publicly announcing a breach so the company can communicate the most accurate information and appropriate remediation steps. If the breach leaks before forensics are complete, provide external stakeholders – consumers, partners and media – with factual information and a promise to share more insight when it becomes available."

If you do, as he explains, announce or declare a data breach before completing a forensic investigation, you can also either under or over respond to an incident. Both can cause significant consequence by either failing to meet the required criteria fully or incurring the costs and negative impacts of a breach unnecessarily--all from not fitting the available pieces of the solution together properly.

This is also where the proper fit between legal counsel and forensics must be in place as well: to accurately determine the scope of an incident, if it has reached the level of a data breach or not, and if so, to what extent and what the appropriate response should be.

Therefore, as the correct parts of the answer are becoming clearer, critical gaps in the overall solution do still remain. I believe then the next step is to merge them together more appropriately toward a far more effective solution. As is done with other diverse, multidiscipline solutions, strategic partnering can be an effective model to accomplish this. Rather than simply outsourcing the different pieces independently through a portal, approved vendor list or other means, partnering offers the information sharing, cross training and coordination required to close the void that exists between them.

This can forge a more seamless, turnkey solution needed with all the critical working parts primed, synchronized and ready to go. **A solution like this can't be effectively built on the fly, in a reactive mode during a breach, as this only perpetuates the disparities that already exist.**

A solution that is prebuilt and coordinated offers a critical opportunity for organizations to utilize its combined expertise more proactively as well. This can be done through more effective assessments that consider not only IT security, but also other key areas of vulnerability such as legal, social, operational, etc. Substantial advantages can be realized to not only prevent a possible incident, but in addition, the familiarity with an organization's environment and sharing of knowledge that is built can substantially reduce the impact of an incident should one occur. Bruemmer states,

> *"Also, identifying and vetting third-party data breach partners ahead of an incident is critical to ensuring they understand an organization's business and can engage quickly. Consider pre-breach agreements with partners including forensic firms, legal counsel, print and call center providers, credit monitoring services and public relations agencies to ensure greater response alignment and reduce the likelihood of changing partners mid-stream, which can prove devastating to an organization's response following a breach."*

So as we've taken a closer look at how this challenge is evolving, how organizations are understanding the issues and how they and the overall market is responding, hopefully this has been helpful in providing clearer practical perspective as well as an understanding of the more sophisticated aspects that need to be addressed.

To summarize then, a few key takeaways:

- There are a diverse array of service providers and components that need to come together properly to build the right solutions. They must find better ways to become more educated about one another's services and role, as well as how their offerings augment one another and coordinate most effectively in order to do so.
- Organizations and businesses need to better understand the nature of the threats and extent of vulnerabilities that exist for them and what appropriate solutions are available to protect against these. For smaller businesses (and some larger) this could be just a better general awareness of the risks along with addressing the basic blocking and tackling. Larger, more complex organizations need to understand that their vulnerabilities cover a very wide spectrum, involving multiple departments and aspects of their business. For them, it's going to take better organization-wide awareness and coordination, taking full advantage of the resources that are available now to help as well as better solutions still yet to evolve.

I believe it's a safe bet to say that as technology and the way we do business continues to advance, so will the threats to our information. We are going to need to look through a wider, more focused and longer range scope to see them coming.

.VESTIGE
Digital Investigations

For more information Contact us today
800.314.4357 or info@vestigeltd.com