WHITE PAPER

CYBER SECURITY 101 FOR CEOs

CYBERSCOUT™

1

DATA BREACH RISKS CAN COME FROM SO MANY DIFFERENT DIRECTIONS, MOST OF WHICH ARE NOT THE IT DEPARTMENT.

LAYING THE FOUNDATION

A thoughtfully developed, well-executed information security and privacy response program can provide protection for you and your company in the event of a breach. Being able to respond to your customers with a message that you had a plan, that your employees were trained, and that you were working to protect them puts you in a very different position than if a breach occurs and you have no documentation that you ever considered the risk or acted to prevent it. As a leader, you are the one who must set the tone for your company that information security and data privacy are vitally important and that you expect all departments to work together to identify risks and work to reduce them.

Just like you'd expect your doctor to first assess, then diagnose and then prescribe treatment, the approach to addressing the risk of a data breach begins with assessment, then analysis (diagnosis), and finally planning and remediation (prescription.) You can get where you need to be by following a four-step plan to:

1. Assess
2. Analyze
3. Plan
4. Remediate.

ASSESS

Data breach risks can come from so many different directions, most of which are not the IT department. HR departments have been favorite targets of attackers who exploit payroll systems and redirect paychecks just before a payroll runs. Successful social engineering attacks on accounting personnel trick them into wiring a large payment to crooks—and frequently make the news. Marketing departments hosting websites that gather rich client data are also frequent data breach headliners. An assessment needs to consider the entire organization, not just IT. And when doing your risk assessment, please don't forget third-party suppliers, many of whom come to your organization through HR, marketing, or employees in other departments—again, outside of IT's control. Many of the recent and large high-profile attacks (Target, AT&T, and Home Depot) have been traced to a vendor. In assessing outside vendors or suppliers, consider law, accounting and other professional services firms. They are all particularly vulnerable to hackers because they are a point of aggregation for sensitive client data, and they are seen as not particularly attuned to information security risk management.

To assess risk, you first need to know what information assets you have that may be at risk. If you don't know what you have and where it is located, you can't very well protect it. Think about it: If a bank has no idea how much money it has or where it is kept, it can’t possibly know the exposure it holds or how to remedy it. Prepare a data flow diagram and information asset inventory. Understand where your information assets are, who has access, and what protective measures are or are not in place. Every good "Missions Impossible" movie begins with a scene about a map locating all assets.

Learn a lesson that even Hollywood knows to be fundamental: Map your assets and understand what is or is not in place to protect those assets.

People ask whether the assessment should be done by internal or external personnel. It depends on whether you have an internal team with the experience and availability to do the work. Even then, be aware that asking an internal team to assess its own work is a bit like asking a student to grade his or her homework. You would be asking them to know what they don’t know. External security professionals may benefit your business by bringing experience from working across multiple environments. They may have seen exposures you haven’t even thought of yet. They can lend credibility to your efforts through their objectivity. And they can make your internal team feel supported. When internal teams do the foundational work, at the very least you should engage an objective third party to conduct the final assessment, just as you would for your annual accounting audit, and provide the findings and recommendations to you.

DEVELOPING YOUR SECURITY PLAN

While an assessment is the foundational step in addressing the risk of data breach, the results must then be analyzed to form the basis for a strategic plan. This approach yields a program that fits your business and avoids the waste typically seen by ad hoc purchase of security tools.

ANALYZE

The results of the assessment should be analyzed by someone familiar with current threats, defensive technologies used by organizations of a similar size, procedures and accepted standards. Some of the findings will show easy, low or no-cost measures that can be adopted immediately. The more complicated exposures can be prioritized and then translated into near and long-term plans. This is not a plan that “boils the ocean” or one that follows a one-size-fits-all checklist that is likely to contain recommendations that are ill-fitting for your business and is, therefore, wasteful and frustrating. This is a plan that starts with your exposures and selects security investments to address those specific items using a degree of reasonableness and knowledge of what other institutions of the same size are doing. Recommendations should be correlated with the objective findings from the risk assessment and should be accompanied by general guidance on the level of investment (time, effort and budget) required for adoption.

PLAN

To develop the plan, use the assessment results that prioritize your particular exposures, and plan your security program around addressing your most important risks. This is much smarter than trying to protect everything everywhere. Your employees' Social Security numbers shouldn't have the same level of protection that you give to general email "chit-chat." Some fundamental components of a security plan that every business should have include the following:

- One person needs to hold responsibility for the security program, and that person should be more than a junior analyst. If you can only afford a junior analyst, contract with an experienced outside resource to provide the security analyst with the expertise and support needed to address the complex and dynamic area of risk you have assigned to him or her. Your designated security professional should be experienced, empowered, accountable and supported. This is a challenging, difficult, complex, technical and dynamic area. Criticism and scarcity of resources will only increase risk and turnover.
- The plan should be written. The physical document is less important than the process of developing the plan, but it is an important artifact that demonstrates your diligence. If you don't have a written information security plan, you run the risk of being viewed post-breach as not having put the requisite effort into protecting sensitive information.
- Encryption is widely seen as a basic requirement, yet it is lacking in so many environments. If you don't have this free, easy protection in place, be prepared for scrutiny if you have a breach. To be sure, not all forms of encryption are easy and free, but many are. So, be certain you have in place what is appropriate for your environment and that you aren't neglecting current standards simply because you are not informed or haven't assigned someone to keep you current.
- Secure disposal is another risk area to watch. If your company has sensitive personal or health information and your employees don't know to dispose of that information properly, it becomes a C-level issue. Consider CVS Caremark, which experienced an extremely public and expensive incident after employees discarded sensitive information into regular trash bins.

PLAN THE PLAN

Taking the steps outlined above can potentially turn a disaster into a potential win. While no company wants a breach, anticipating the consequences with an action plan puts weight behind customer care and appreciation. Conversely, failure to do so invariably impacts revenue in the near term but often damages the brand resulting in long term negative consequences. Further, making and socializing a Data Breach Response Plan can also impact the culture in positive ways. At a minimum, a well-thought-out plan can raise awareness regarding the responsibilities all employees share in securing your company's data. When integrated into a unique selling proposition, it can also create a competitive edge when customer care and security are significant purchase drivers.

Developing a solid Data Breach Response Plan may require disciplines or resources not available within the organization. An initial assessment should identify what outside expertise is required. While both the internal and external investments in time and money may seem onerous, data shows that they pale in comparison to reacting after the fact.