WHITEPAPER

5 THINGS YOU MUST KNOW TO SECURE YOUR COMPANY'S DATA — AND YOUR JOB

Know Your Risk Profile or Your Job Security Might Be in Jeopardy

By Phil Alberta, President, IPM

If you're versed in cybersecurity, you might be resting easy. Your job will never be at risk given the serious cybersecurity talent shortage. Right? Don't be so sure.

It's true that, according to (ISC)^2, there are a startling 2.93 million open cybersecurity positions around the globe. Even more, Enterprise Strategy Group (ESG) estimates 53% of organizations report a problematic shortage of cybersecurity skills, up from 42% just three years ago.

But despite this skills gap, there's something for which the demand is even greater: your company's confidence that it's data won't be breached. The Ponemon Institute reports that the global average data breach costs companies $3.86 million, and a large-scale breach can cost as much as $350 million. This has your C-level executives and board members taking note with acute attention. They know that your company can't withstand a cybersecurity event with this high price tag. Not to mention the added battering it can have for your company's brand and reputation.

> THE GLOBAL AVERAGE DATA BREACH COSTS COMPANIES $3.86 MILLION.
>
> *-Ponemon Institute*

Assessing Your Company's Risk Profile

If you truly want to assure that your job is safe, it's time to take a hard look at your company's risk profile. Perform a detailed assessment of your vulnerabilities, where your data could be exposed and how you'll respond should the worst fall upon you.

Start by answering the following five questions. Only then will you be able to respond to your board with confidence. With the answers in hand, you'll know that you're prepared should your board ask, "Why didn't you know that this could happen?"

1. What am I trying to secure? The first step when assessing your risk profile is to have a deep understanding of the data you need to secure. Know what it is and what risks are you willing to accept for that data. Map out your data risk tolerance by data type and the strategy you will implement to protect it. By classifying your data based on its sensitivity – including personal identifiable information (PII) such as social security numbers, health records, credit cards and more – you'll have a strong idea of which data sets you need to establish stronger controls around. If you don't commit to classifying your data based on its sensitivity, you may be caught unprepared and risk a serious data breach.
2. Do I know where my data really is? Once you've classified your data, inventory where your sensitive data is stored including how it's accessed, used, moved and retained. Only by performing a full inventory of your data assets, will you be able to architect your strategy to protect it. Key steps in this process include knowing who owns the data, who is accessing that data, where the computers used for data access are, and what privileges are available for those systems. In many respects, remember that data access can be more important than data retention. If you don't have full visibility into how the data is

moved and used, you can't assure full protection of it throughout the data lifecycle. It's also critical to define and control the retention policy for each data set. Some data requires retention for seven years or more, while other data can – and perhaps should – be disposed of more frequently. Setting a controlled and defensible retention strategy will help you protect sensitive data by not storing it any longer than needed.

3. **Do employees know what data they have and what they can do with it?** According to a recent report from Ponemon Institute, inadvertent insider data misuse is responsible for 64% of total security incidents, while criminal behavior comprises 23%. That means it's vital to educate your employees on the value, and risk, of the data they create and access. Employee training on the proper use, access and storage of the data they produce and work with can be instrumental in mitigating risk and minimizing your exposure. Be sure to apply clear data classification policies, train employees on how to use them, then rigorously enforce those policies through active monitoring and regular employee education.
4. **Do you know who really is accessing your data?** When addressing employee, and contractor, data policies, perform a full assessment of who is really accessing sensitive data and all the ways they are using and storing it. If you don't know all the elements of how that data is used, moved and stored, you won't be able to secure it properly. Ask if the data access is necessary and appropriate, where it's being moved to our used, and if employees and contractors can print it. Only when you have a full understanding of where sensitive data lives, and who is accessing it, will you be able to lock it down. Consider an approach that only provides employees with the least data privileges they need to perform their job.
5. **Do you have effective security monitoring and response practices?** Once you've mapped out your risk profile and addressed how your data is used and accessed, and by whom, be sure that you have a powerful monitoring and response solution in place which can alert you when the unexpected arises or when usage falls outside of your developed policies. By having a continuous monitoring and alerting system, you can better quantify risk and prioritize remediation while eliminating the open issues that may broaden your attack surface. In this case, the more you know, the better protection you can ensure.

When it comes to data security, you can't be too careful. By rigorously implementing these five security basics, you can prevent attackers from stealing your sensitive information, costing millions and ruining your company's reputation. You just may also win over the confidence of your board and secure your job for good.

Phil Alberta is a senior technology and operations leader with more than 20 years enabling global growth and building high-value businesses. He is President and Chief Information Officer for IPM.