CyberSecurityGuide.net

Five Questions Every Organization Should Consider Regarding Cyber Security

1. What are you trying to keep secure?

Knowing what data you need to keep secure is a critical first step in assessing your current risk of having it stolen or compromised. There are many kinds of data to consider protecting including proprietary designs, customer accounts, and financial reports. Your need to keep data secure is driven by many factors including customer perception, industry guidelines, regulatory requirements and increasingly by governing law. **Assessing and classifying your data is a key action every company should undertake.**

2. How are you currently working to keep data secure?

Knowing what current business and technology controls you already have in place will help you consider if those controls adequately protect the data you want (and in many cases are required) to keep secure. **Documenting your current security controls is a key action every company should undertake.**

3. Would you know if your company had a data breach?

Knowing the answer to this question is complicated and complex at best, but when addressing data security, this is where the rubber hits the road. Unless your hacker is looking to embarrass you, their goal will be to stay hidden for as long as possible – all the while stealing your data. **Testing your security controls is a key action every company should undertake.**

4. Who would you call first when it happens?

Knowing who you would call first and having a plan in place will help guide you and your staff through what will prove to be some harrowing and fearful days. There are no "ghostbusters" to call and incident response resources can be both scarce and expensive. **Having an incident response plan is a key action every company should undertake.**

5. Would you be able to recover (and at what cost)?

Knowing that a data breach will be very expensive in terms of "patching the hole", recovering systems, complying with a matrix of reporting laws and rebuilding trust with customers will help you view a cyber security breach as a threat to your business and then work to build a corporate culture that works to protect sensitive data. **Building and fostering a security aware culture is a key action every company should undertake.**

Bonus Questions:

As your business changes over time, what impact will the following activities have from a cyber security perspective?

- Recent or upcoming acquisitions
- Recent or upcoming divestitures
- Software and hardware development
- 3rd party system or cloud application integrations
- Key business partnerships with data sharing agreements

Do your business processes include security or is security an "add on" consideration?
Knowing the answer to this question will provide a gut check of where your business (unit, division and/or enterprise) stands in building a culture of security that protects and manages the data that is the lifeblood of your operations. Just as finance is considered in all aspects of managing your business, information security should be another lens by which business decisions are considered. **Evaluating the impact business decisions will have on your security posture is a key action every company should undertake.**

CyberSecurityGuide.net
a service of
B|A|R
Management Solutions, LLC

Download a digital version

Need a cyber security guide?
Brian Howell, CISA
brian@bar-ms.com / +1 816 668 8400