The Fulcrum Group, Inc.
(817) 337-0300

7 Questions CEOs Should Ask About Cyber Security

This White Paper is brought to you by your friends at The Fulcrum Group, Inc.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5751 Kroger Drive, Suite 279, Keller, TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

Wrap Up 2015 Knowing Where Your Organization Stands.

"I'm no expert, but I think it's some kind of cyber attack!"

The Fulcrum Group's October Newsletter (find it at http://www.fulcrum.pro/newsletter/october-2015-newsletter/) provided some great Cyber Security tips & advice recently, for National Cyber Security Awareness Month.

We've expanded on the 7 Questions article with some additional suggestions from our Fulcrum experts, to help you determine your organization's cyber security outlook, as we wrap up 2015.

7 Questions CEOs Should Ask About Their Cyber Security

1. ***How is our executive leadership informed about the current level and business impact of cyber risks to our company?***

The Fulcrum Group recommends a regularly scheduled 'CEO's Cyber Security Briefing' take place with a defined frequency. Typically this would be between the CIO or IT Manager and the CEO, or if you are a SPOT Managed IT Services client, The Fulcrum Group can provide a Cybersecurity Briefing as part of the Quarterly Business Review.

It may not be necessary to delve into technically complex discussions, but rather to instill awareness of current risks and discuss the "accountability flow" from those responsible from your organization's technology, to the top level of your organization's leadership.

2. ***What is the current level of cyber risks and what might their impacts be to our company?***

The impact of potential loss of critical systems and data for your organization should be measured and documented. Much like a Disaster Recovery Plan, a Cyber Security Incident Response Plan begins with understanding the risks, costs and impacts of security incidents.

Creating a Cyber Security Threats Matrix of the various IT systems, and listing out the potential security threats, along with the impact to the business, will help you understand where to spend your IT budget on cyber security. Contact your Fulcrum Group Account Manager for a sample Cyber Security Threats Matrix.

3. *How many and what types of cyber incidents might we detect in a normal week? What is the threshold for notifying our executive leadership?*

Part of the challenge of "getting your hands dirty" in your organization's cyber security is separating false positives (or white noise) from actions or incidents which pose a true threat.

Wherever possible, escalation timelines and guidelines should be implemented, documented, automated, and re-examined periodically as part of your Cyber Security Incident Response Plan. Throughout the enterprise, the role of executives, systems administrators and employees should be clearly defined with a clear and documented procedure for response to a possible cyber security incident.

4. *What is our plan to address identified risks? How do we preserve the integrity of data resident on our network?*

The Fulcrum Group upholds a core value of '*Plan, Do, Review.*" This certainly applies to the data owned, hosted, or being transmitted through an enterprise.

For instance, discussions noting cyber security issues should take place during the planning of new business communications, systems or methods.

Security and disaster recovery plans should be implemented simultaneously with any new business workflows or developments, and all aspects of these plans and methods should be routinely evaluated and compared to current industry standards and best practices.

5. *How are industry standards and best practices reflected in our cybersecurity program?*

Rigorous compliance is required for companies who must comply with various regulations including HIPAA, SOX, and PCI. While these standards are strict, compliance standards by themselves should not be relied upon for maintaining a comprehensive cybersecurity program.

Many compliance standards mandate that an enterprise-wide policy be defined and adhered to, but stop short of defining specific standards. Therefore, a comprehensive approach might include expanding beyond recommended procedures, forming a team of people with the right knowledge and skills to formulate policy, and the right methods and verification techniques to implement the right procedures.

Here’s a recent case that documents a very costly oversight…worth a look if your organization adheres to HIPAA or other compliance standards (copy & paste this link into your browser): http://www.hhs.gov/about/news/2015/09/02/750%2C000-dollar-hipaa-settlement-emphasizes-the-importance-of-risk-analysis-and-device-and-media-control-policies.html

6. ***How comprehensive is our current cyber incident response plan? How often is it tested? If we were breached tomorrow, who would we call?***

   Frequent and routine testing will help to answer the question, “How comprehensive is our current cyber incident response plan.” Major elements of your disaster recovery and cyber incident response plans should be tested at least once per year.

   It is our strongest possible recommendation, not to wait until an incident is occurring to know who to call for outside help or consulting.

7. ***Do we have cyber security insurance that covers data breaches?***

Cyber security insurance is a good risk management strategy. If you do business internationally, make sure you understand the laws and regulations of each country, and understand that your cybersecurity insurance may not cover your risks in those countries. It is also key to make sure that the cybersecurity insurance you buy actually covers your biggest risks. Also worthy to note is that cybersecurity insurance is typically inadequate for covering intellectual property theft.

If you’d like to speak with any of our IT engineers or consultants further on this topic, or would be interested in a FREE IT Security Assessment, feel free to reach out to us by phone at 817.337.0300 or email – and visit our website at **www.fulcrum.pro** today to find out more about the solutions we recommend.

We always welcome the opportunity to speak with you – someone’s always here and glad to offer a word of advice!

THE **FULCRUM** GROUP
One Technology Solution: Yours