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

Cybersecurity for Executives

3 Key Points Executives Should Want To Know About Their IT Presence

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

Cybersecurity for Executives

3 KEY POINTS EXECUTIVES SHOULD WANT TO KNOW ABOUT THEIR IT PRESENCE:

Cyber attacks are an increasing problem, especially for small-medium sized businesses. In many cases, smaller organizations lack abundant resources and staff to pay for and maintain their IT.

Cyber criminals understand and exploit this. ***The U.S. Department of Homeland Security reports 31 percent of all cyberattacks are directed at businesses with less than 250 employees.***

Increasingly, businesses of all sizes are relying on constant connectivity and productivity in the forms of Internet and Cloud applications, remote access and more. They are challenged with the need for efficient delivery of services, and at the same time, balancing security with system usability, a critical and constantly evolving process.

According to a recent *US Secret Service North Texas Electronic Task Force* report,

> *Cybersecurity touches nearly every aspect of business. It affects a company's opportunities for expansion, customers, markets, and is vital to most strategic plans. The only place where accountability for all of those domains is held and where there is a clear line of distinction and authority is at the executive level.*
>
> *Before any executive can determine the best balance for their company, they must first understand the threat. Unfortunately cybersecurity concerns are not always communicated in a meaningful way. Information technology often gets lost in translation because it is provided in a technical dialect and not in a business context.*

With that in mind, let's take a look at
3 KEY POINTS EXECUTIVES SHOULD WANT TO KNOW ABOUT THEIR COMPANY'S IT PRESENCE:

1. INVENTORY YOUR DATA AND ASSESS YOUR RISK

Five good topical questions to ask yourself include:

- **What data do I have that others may want?**
- **Where is my critical data located?**
- **What happens if someone takes my data?**
- **Where am I getting threat intelligence to protect my data?**
- **What am I doing to protect my data?**

Let's break down the above questions…

What data do I have that others may want?
What would be most detrimental if taken from your system? A wide range of sensitive and personal information such as names, dates of births, and social security numbers can be taken from your systems in a data breach. Organizations must identify their most valuable assets and devote the proper resources and security posture to protect them.

We recommend every business executive consider the consequences of these scenarios:

- ***Is your data confidential - could unauthorized disclosure cause financial harm to your company?***

- ***Is your data restricted - could unauthorized disclosure impede or undermine operations of your company causing a competitive disadvantage?***

Where is my critical data located?
Taking an inventory of your network, and understanding your complete security posture across your entire IT ecosystem will help you prevent or mitigate attacks against your security system. We recommend you consider the flow of data through your company including:

- ***Your data in motion - how information moves through your network, such as emails and web traffic,***
- ***Your data at rest - where information resides on endpoint devices like workstations, databases, applications and servers***
- ***Your data in use - information that may be stored on portable devices such as laptops, smart phones, USB drives and printers.***

What happens if someone takes my data?
Will the exposure to your company have financial, competitive, reputational, or regulatory implications? Does your company have compliance regulations it needs to meet? All compliance regulations require companies or individuals that maintain unique PII of individuals to notify those individuals, and the state's attorney generals, if such information is lost, stolen or otherwise compromised.

Beyond the "breach fatigue" we may suffer as a progressive population, the loss of business and damage to your name brand or reputation can sting on a number of levels. Additionally, come investigation expenses, fines, penalties, regulator fees as well as civil litigation.

More relevant considerations:

- ***Will you experience a market share loss and increased shareholder scrutiny?***
- ***Will assets be damaged or will you have an interruption of service?***

Where am I getting threat intelligence to protect my data?
Understanding the current threat landscape is crucial to protecting your assets. An active defense, or offense being the best defense, is a solid strategy.

An established practice of gathering advanced actionable information ahead of time can lead you in the right direction, help mitigate damage and assist affected customers.
Two helpful hints:

- ***Advanced analytics can be formed in house, outsourced or gathered from government, commercial or open source providers.***

- ***Organizations must ensure that their cybersecurity strategy is aligned with their overall business strategy. Cyber intelligence spending will be most productive when the amount of money allocated is based off of an articulable set of risks.***

What are you doing to protect your data?
The key to any secure environment is to regulate the traffic that enters and exits a network, to understand which traffic entering your network is "good" and which is malicious.

Monitoring and controlling access into networks is the most difficult and by far the most challenging aspect of cybersecurity today. While companies are doing a better job learning how to strengthen their programs, there are literally thousands of products and companies that are in the business of selling solutions and services geared towards securing and backing up your network. Determining which of these is the best for you, or the most cost effective is a never ending challenge.

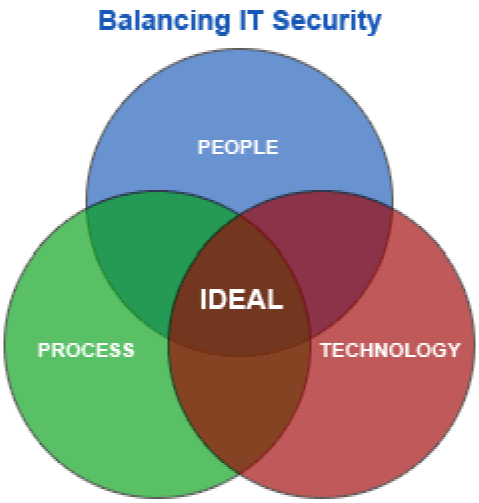
In most large businesses the C-Level security personnel have the difficult task of controlling access, tracking risk and influencing senior executives on information security business decisions. However, they are too often not included in overall business planning.

In order to ensure that businesses security decisions don't get lost in the overall business process and are aligned with business goals, it is important to know the following:

- ***The direction of (what drives) the business.***
- ***Where the organization is going. Are they expanding or contracting?***
- ***How to get ahead of and stay engaged with the business, its peers and the environment.***
- ***Enablers and understanding the problems.***
- ***Staying current on business reports and strategic plans.***

2. TAKING A LAYERED APPROACH TO SECURITY

Quite simply, there is no solution available that offers total assurance to preventing a cyber–attack. We believe that having the right balance of people, processes or policies and technology helps reinforce a holistic, layered approach to your organization's security posture. Some considerations:



- ***Technology: Technology such as virtualization and cloud based solutions, are good countermeasures to address the risk of data loss. Your investments in hardware and software, though, are not enough.***

- ***Policy: Between the gap of technology and people, lies another responsibility. Policies you put in place to protect your system will help to regulate your employees' and consumers' actions related to such things as bring your own device (BYOD), remote access, and the acceptable levels of use of your system. Enforcing corporate policies can minimize risks and show due diligence to your customers and shareholders.***

- ***People: Providing education around security awareness is critical to the security of your network. End user security awareness will have a major impact in protecting corporate data as they are the ones on the front line. Provide operational security training for employees to guard against insider threats and human error and make it informative, interesting and current. Empower employees to use data responsibly and educate them about the common threats vulnerabilities and risk of becoming a victim online. Have you established a security awareness program?***

3. HAVING A CYBERSECURITY RESPONSE PLAN

Organizations should have an incident response plan in place that is aligned with individuals who are trained on the various threats that may occur.

A well-defined and organized response to a cyber-incident requires a team effort. Getting the right people involved is essential to properly responding, coordinating, mitigating, and investigating your incident. More tips include:

- ***Plan for a worst case scenario with a defined clear path of escalation that includes a standard operating procedure.***

- ***Identifying who should be contacted and getting the right people involved is key to any successful response. A company must identify a central point of contact or leadership team that not only has the responsibility, but also has the authority to act. The leadership role must be empowered to perform the day-to-day analysis of the situation and make key decisions. A central point of contact should be established and be at the highest level in executive management, or have the backing of executive management.***

- ***Cybersecurity planning should be flexible, enabling the organization to change with the environment. A strategic investment in a comprehensive incident response plan requires that an organization identify and invest in cybersecurity practices that are aligned with today's types of threats.***

If you would like further assistance assessing your company's IT security posture or formulating a security plan, please don't hesitate to reach out to us by phone or email.

Visit our website at www.fulcrum.pro to find out more about this issue and the solutions we recommend or give us a call at **817.337.0300**.

Check out our blog for security alerts and other important information for business owners and managers – email *ljames@fulcrumgroup.net* if you'd like to be alerted when we post.

THE FULCRUM GROUP
One Technology Solution: Yours