CYBER SECURITY TODAY

HOW TO TALK TO BOARDS ABOUT CYBER

LBMC | INFORMATION SECURITY

Speaker

Mark Johnson, Shareholder, LBMC Information Security

CISSP

April 24, 2019

CHANGE IS THE ONLY CONSTANT

Innovation in technologies promise better lives, more secure communications and systems and even more insights and data to work with. For example:

Data and analytics – Taking the staggering amount of data and looking at it in new ways to gain better insights

Blockchain – Promises more secure way to share data, however several barriers remain

The Internet of Things (IoT) – TV's, refrigerators, wearable technology and even your cars

THREATS WE'RE FACING TODAY

The price for entry into cyber crime has been drastically lowered

You no longer have to be a skilled hacker or have in depth knowledge of computers, applications, or networks to "hack" into a system or organization. You can simply an email with a comprised link. Phishing is still the most profitable attack vector.

Much higher volume of attacks

Since 2013, over 9 Billion records have been breached world wide. Cybercriminals will steal an estimated 33 billion records in 2023, and the US will represent half of that number.

There are 2 Million Unfilled Cyber Security Jobs in the U.S. as of Jan 2019.

Too few people, not the right skill sets, has created a disproportionate demand for individuals with some cyber security experience.

THE PATH FORWARD

The ever increasing threat landscape will be the "New Normal".
So how do we manage this complex problem set?

- ✓ We need to the basics well
- ✓ The basics will not protect us well enough in the "New Normal"
- ✓ We need more collaboration and data sharing
- ✓ We need more innovation
- ✓ We need more people with new and more diverse skills

Bottom Line: No matter if we do all these things, breaches will still occur, how well you react will be the determining factor for how impactful the breach will be.

LBMC

HOW DO BOARDS OVERSEE THIS PROBLEM?

The New Normal will be with us for the foreseeable future.

This is a conversation that needs to occur regularly. It is not a one and done.

Diligence and preparedness will be the deciding factors when, not if, your company will have a cyber security problem.

Engage the senior leadership, make sure you hear from both internal and external experts

LBMC

THOGUHTS ON CONVERSATION STARTERS

Think Cost Avoidance vs. ROI

Engage the CISO in the business. They need to facilitate the business, they cannot do that if they do not know where it is going.

Understand how the company has allocated funding for technology and talent

Make sure there are comprehensive, written, and implemented cyber security plans and policies.

Robust user awareness – Facilitate a culture of compliance and security

THOUGHTS ON CONVERSATION STARTERS

Understand how the company's vendors present risk to the company

Understand how the organization stays current with new laws, regulations, etc.

How does the company react to indications of a problem?

How does the company deal with non-digital forms of information

ANY QUESTIONS?

Mark Johnson
CISSP
Shareholder, LBMC Information Security
Email: Mark.Johnson@LBMC.com
Phone: 615.690.1965