ARE YOU THINKING ABOUT CYBERSECURITY THE RIGHT WAY?

In today's business environment, there is a tendency for executives and board members to categorize things into handy buckets—it is human nature. They often think of cybersecurity as an IT issue, but that is the wrong way of thinking. Cybersecurity is really a risk issue.

Any type of data breach or computer hack has the potential to impact your brand and create risk for your organization. Not only can the failure to protect customer data result in a breach of trust with the general public, it can also come with financial penalties arising out of privacy regulations such as HIPAA, GDPR and Sarbanes Oxley.

While it may be effective and reliable, a company's IT department is not necessarily thinking about cybersecurity from a revenue, brand and risk standpoint.

Instead, the most appropriate place to discuss cybersecurity is at the board and C-suite level. Sure, boards and C-suites are now asking more questions about cybersecurity, but you cannot delegate this risk; a business needs to look at cybersecurity as a risk to the organization as a whole.

Businesses that are part of a supply chain are increasingly coming under scrutiny for how they are protecting information as well. If you want to create strategic differentiators, you need to show you can protect not only your data, but also that of your supply chain.

You may already require your supply chain to implement certain mandates. But what about their subcomponent manufacturers and others they do business with?

THE THREE PILLARS OF CYBERSECURITY

Cybersecurity should focus on data protection at the edge, and look at the most vulnerable cyberattack entry points—the devices people use every day, such as laptops, desktops, tablets and smartphones.

At MCPc, we look at cybersecurity holistically and think about it in terms of a chain of custody. Our Chain-of-Custody Security Solution is a holistic, end-to-end life cycle management protocol. By protecting data at the edge we can monitor and report on the security and compliance profiles of employee's devices. Our detailed audit trail can be very valuable in the event of that dreaded day.

DATA IS THE NEW OIL. IT RUNS THE ENGINE OF BUSINESS.

We divide what we do into three pillars that actually represent the three phases of our life cycle management protocol—think of it as the birth, life and retirement of the data on devices:

1. Secure Technology Logistics
We advise companies on the best technology solutions to support their business goals and workforce needs. Our approach allows them to acquire the right device, at the right value, configured the right way, delivered at the right time, and security hardened to meet the threats of today and tomorrow.

We fondly refer to our technology logistics centers as birthing centers. This is where we prep those devices for their most secure life. For specific client requirements we help select the device, build it, customize it and incorporate security. For us security is built-in, not bolted-on.

2. Managed Security Solutions and Security Operations Centers
For the lifetime that data is on a device, it has to be protected. We send a healthy device out into the world but sometimes the world has other intentions. And, as frameworks and regulations change we're able to remotely update security levels.

One of the first things we tackle is basic cyber hygiene. The most common reason for successful breaches is a user clicking on something they should not have. As consumers of technology, collectively, we are not practicing proper cyber hygiene. Indeed, it takes an average of 102 days for IT departments to apply the patches issued by Microsoft and other software providers. Another component of basic cyber hygiene is malware detection or virus scans. We find that most organizations struggle to identify what assets they have, where they are, and what is the state of their cyber hygiene.

3. Secure Technology Asset Disposition
Data on retired devices will never die unless there is a disciplined and documented effort to eradicate it. By the end of its life, that device, the data stored on it, and its ability to access your data center makes it very valuable to hackers.

The first purpose of our Asset Disposition centers is the security of the data on retired devices. If the device still has usable life, we will wipe it clean and provide a Certificate of Data Destruction, then return that device to the client or remarket it returning cash to the client. If there is no residual value left, we will safely dismantle the device and recycle it. We have a stringent 0% landfill policy, so everything goes back into use to create the next generation of technology.

Through the life cycle of data and the devices it lives on we impose a multidimensional relational database called IT asset management. This allows an organization to see exactly where their data exists, on what device it resides, who has access to that data, and if and how it is protected.

Data is the new oil. It runs the engine of business. It is the thing everyone wants and it is easy for hackers to get. Therefore, we need to be vigilant and protect it.

How certain are you that your data is protected? ◆

Being the #1 cybercrime target is nothing to cheer about.

But, you can cheer about holistic real-time defenses for the most easily hacked entry points to your data — every smartphone, tablet, laptop, desktop, and IoT device you use to do business.

MCPc's unique Chain-of-Custody Security Solution℠ delivers SecurityCertainty℠ to protect your data, manage the complexity and sustainability of technology, ensure consistency in security, and ultimately, mitigate business risk.

To learn more, please contact
Andy Jones, CEO | andyjones@mcpc.com

Achieve **SecurityCertainty**℠

MCPc THE DATA PROTECTION COMPANY

The United States is the #1 target for targeted attacks at 38% and will account for half of breached data by 2023.
https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html