SecureCloud Systems LLC

Protecting The World One "Byte" At a Time®

Corporate Executives – Time to get your head's up out of the sand

On a daily, hourly basis, cybercriminals are constantly creating and deploying new cyber threats. The theft of intellectual IP is becoming more and more of a destructive reality than ever before. While these threats are on a dramatic upswing, it has been reported that corporate spending in and around cyber protection is on the down swing. According to a survey conducted by PricewaterhouseCoopers (PwC) respondents in 2014 report that the number of detected incidents soared to a total of 42.8 million, or a 48% leap over 2013, with financial losses increasing 34% over 2013.

In order to have any chance against these attacks, it is incumbent upon your organization's leaders - to focus on staying ahead of the curve - and adjust by taking responsible leadership action against the real cyber threats that exist in the global and domestic marketplace today.

Protecting the Business

Business executives seem unsure as to where to place their priority focus for the currently and for the long-term. Elevating the requirements in and around information security in the organization must emphasize the fact that it is NOT just a technology function-it must also become a collective operational initiative acknowledged and supported by the entire culture of the company! Let there be no mistake, a data breach of any size, could destroy a business and will definitely compromise its ability to maintain integrity, credibility, customer share and overall market growth and performance. Moreover, legal, regulatory requirements, and potential fines are one thing, the loss of trust and the destruction of your firm's brand should be a key business imperative, for any C level executive.

While it is reported that JPMorgan will double cybersecurity spending, it appears that the company will actually be cutting their cyber spend. According to PwC's Global State of Information Security Survey 2015, security spending actually declined last year, reversing a three-year trend. The average information security budget dipped to $4.1 million in 2014 - down 4 percent from the $4.3 million average spend in 2013. They stated mid-sized and large companies reported a 5 percent increase in cybersecurity budgets, small companies reduced security costs by more than 20 percent over 2015!

The Reality

After an in-depth review of the market landscape – the budget allocations for cyber-security protection are minimal to none, when analyzing small firms – however, the reduced budgets (as seen above), for many medium and large-sized firms, is deeply troubling. When reviewing cybersecurity budgets and considering a modest 5 percent increase, the total number of security incidents detected by respondents rose to 42.8 million in 2014, reporting losses of $20 million or more! This is almost **double the number for 2013!** It is clearly apparent that the cyber spend is moving in the wrong direction.

Pay Now or Pay Later – A Dangerous Game

All Corporate Executives should be paying close attention to what is transpiring in the cyber world today. When giants such as JP Morgan-Chase, Wells Fargo and other banking giants are feeling the effects of very effective state-sponsored attacks, it is foolish to believe that your current methodology to protect your firm's sensitive/confidential data is "good enough".

Equally important are internal threats. The people you trust may be misappropriating sensitive data for personal gain. Organizations face the challenging task of balancing openness and trust with business privacy and protection. Compliance requirements must be top of mind of Chief Information Security Officers. Corporate officers and organization leaders need to wake up and realize that all networks are at risk and represent immeasurable amounts of liability to their organization. Compliance requirements vary significantly according to industry type, as well as sensitive data record types. There are a plethora of these compliance measures to be considered - such as PCI, PII, HIPAA, SOC I, II, and III as well as FISMA, just to name a few. It's best to refer to your industry advocates recommendations/requirements, so that you are following the correct protocols.

Proven innovative methodologies which will secure and protect sensitive data shared over multiple networks should be deployed. CIOs must begin to maneuver away from the standard practice of data-centric security, to ensure levels of security that are unattainable with traditional network security defenses, such as standard encryption and fire wall techniques, used as the common practice today. Everyday communication, such as email, must be secured - with sensitive email communications locked down in platforms that do more than encrypt the communication. Note that a vast amount or most encrypted email provider systems are only designed to protect data in transit *and do little or nothing to protect email data that is at rest*. In other words, once a message is sent, sensitive data remains open and unencrypted on individual devices.

Additionally, once the receiving party receives and opens an encrypted communication, the data is then open and unencrypted and available for exploitation. Some providers claim that they make it easy so that there are no passwords to enter thus not interrupting work flows. While this sounds reasonable - should malware be installed on a device the unamortized access of this sensitive information is now available with ease. Take extreme caution, with any and all providers who claim that their systems are 100% secure, when in reality your sensitive data is indeed at risk.

It makes good business sense to ensure that all devices are protected by a leading anti-malware product. All software updates must be installed in a timely basis - whether it be from an Anti-virus/malware provider, Microsoft® or your browser provider of choice. When communicating over the internet to and from a vendor, or site in which sensitive data will be transmitted - you must always do so through an SSL or https:// connection, or some form of Virtual Private Network (VPN) to minimize and mitigate these potential middle-man attacks.

At a minimum, CTO's and or CIO's should have their entire system platforms Scoped and Analyzed - by a Cyber specialist. Contact Secure Cloud Systems for more information - and please visit our Website at www.securecloudsystems.com.

By Steven R. Russo, EVP

Secure Cloud Systems