WHITE PAPER

Implications Towards Businesses from a Cybersecurity Lens

Cyber Regulations Are Here, How Are You Reducing Your Risk?

Author: Michael Brown, Rear Admiral, USN (Retired) and Eclypses Board Advisor

December 6, 2021

Contents

Introduction

Cybersecurity continues to be at the forefront of this year’s business concerns. With the expansion of remote work environments and the increased number of large-scale ransomware attacks, companies are left to wonder how to best address cybersecurity vulnerabilities and how to determine their security level. In response to these questions, we have seen a number of government directed cybersecurity policies, regulations, and even legislative proposals, which aim to increase the overall security posture of the country and the business sector. But what are the implications to the business community? How should they reduce cybersecurity and business risks through this cybersecurity lens?

The Problem

When reviewing possible implications towards businesses there are many evolving regulations that need to be considered. As usual, the current federal government’s efforts are driven through three vectors, with a goal to increase the cybersecurity posture of critical infrastructure and the private sector writ large throughout the United States.

The first effort was presented in President Biden’s Executive Order 14208, dated May 12, 2021. This executive order provided strategic guidance to the Executive Branch, which called for additional regulations and requirements that the federal government must take regarding cybersecurity. One of the tasks called for updating the acquisition rules for the private sector which does business with the federal government. This, along with the other changes involved in that executive order, take place over time, and involve a large security effort across businesses and government entities. To learn more, read about the executive order here: Executive Order on Improving the Nation’s Cybersecurity | CISA

The second effort involves legislation and regulation actions within the Legislative and Executive Branches. On one side, there are dozens of bills on Capitol Hill that are directly related to finding ways to increase the security posture of the private sector via new or expanded regulations. On the other, the Executive Branch is discussing regulating the actions and responses that the private sector will be required to take in response to an intrusion or cyberattack. This includes breach notifications, privacy, and security steps that they must follow. To learn more about the ongoing efforts, click here: Cybersecurity legislation is waiting in the wings - The Washington Post

Finally, there is also change in progress at the state level. With critical infrastructure cyber attacks, such as the Colonial Pipeline incident showing the significant impact these attacks can have on our way of life, state and local communities are looking for ways, including regulatory, that will prevent and protect them from these threats in the future. While some states are focusing on regulatory actions specific to their state, others are working directly alongside the federal government to implement regulations and/or policies to better protect the country as a whole. To learn more about regulation activities at the state level, click here: Cybersecurity Legislation 2021 (ncsl.org)

While the government taking a proactive approach to cybersecurity is necessary, it is important to consider how this will affect businesses and the decisions they make. An increase in security measures and regulations can cause both confusion and increased costs. A cost that some businesses will decide is unnecessary and will proceed without the best practices or standards in place, thus keeping them vulnerable to attack. With cyberattacks happening everyday it is apparent that by not providing complete end-to-end protection of data, companies and people will continue to be victims of these attacks. The government's approach should call for stronger security measures while encouraging companies to address the threat, and providing the education and information necessary for businesses to make the best security decisions for their company.

Causes and Outcomes

The first thing that businesses need to understand is what are the security best practices and how to know when they have addressed the risks. There are frameworks that attempt to lay out with some ease, the most relevant capabilities necessary to use for their business. The first framework to consider is NIST's Cybersecurity Framework[1], which also functions as the basis for many of the federal and state regulatory agencies cybersecurity requirements for regulated industries. The next framework to consider is the Cybersecurity Maturity Model Certification (CMMC)[2] process, which DOD[3] recently released its 2.0 version focused on three levels of processes for assessing a company's cybersecurity posture. Much of it is based on NIST's SP 800-171 and SP 800-172, with more specifics anticipated in the coming months. While CMMC is focused on the Department of Defense, we can expect it will eventually be expanded to the rest of federal government for application to any company wishing to be part of the supply chain The final framework is the one put into place by President Biden's Executive Order which follows "Zero Trust Architecture,"[4] and

NIST’s SP 800-207 states that “Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. ZTA is an enterprise’s cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.”[5] Basically, even if everything seems fine with your data and environment, you still provide full protection by not allowing anyone, even seemingly trustworthy sources, to have total unsecured, unmonitored access to it. Understanding what large-scale entities with extremely sensitive information, such as the government, do to protect their data will provide companies an idea of what kind of security posture is necessary to defend against increasingly advanced bad actors.

MTE Technology Solution

How does Eclypses’ MTE technology fit in with these frameworks? MTE technology works alongside and complements current security measures, such as TLS, to provide protection against gaps where vulnerabilities exist. By changing the data into a one-time use, random stream of values which encodes at the application level, MTE protects data from the moment it is created instead of after it enters the operating system. This goes along with the idea of zero-trust architecture as data remains completely secure, always operating on the idea that a bad actor could be attempting to access the data at any time. These new policies, strategies and regulations encourage preemptive total security of data, something that MTE provides in a way that is completely new and unique. It’s important to understand that the objective for most bad actors is the data, not the device. Even if the device seems secure, companies must protect the applications and data within so that bad actors will not succeed in achieving their goals. MTE is one example of the kind of security necessary to prevent this.

Conclusion

It is important to note that our current remote environment is not an anomaly. With the continued increases in technology, businesses have expedited their move to the mobile space. Utilizing technology allows businesses to have maximum effectiveness no matter where they operate from. However, this removes the former network edge that had previously defined where security was necessary. If companies hope to maintain their mobile and remote environments, it is necessary that the proper standards and best practices are in place to secure these environments. ***Security starts with the company. Don’t wait until your data has already been breached to secure it.***

Sources:

1. *Cybersecurity Framework. (2021, October 26). NIST. Retrieved November 15, 2021, from https://www.nist.gov/cyberframework*

2. *Cybersecurity Maturity Model Certification (CMMC). Acquisition & Sustainment Office of the Under Secretary of Defense. Retreived November 30, 2021, from https://www.acq.osd.mil/cmmc/model.html*

3. *CMMC-AB |. (2021, October 15). CCMC Accreditation Body | Cybersecurity Maturity Model Certification. Retrieved November 30, 2021, from https://cmmcab.org*

4. *Zero Trust Maturity Model | CISA. (2021, October 1). Cybersecurity and Infrastructure Security Agency. Retrieved November 20, 2021, from https://www.cisa.gov/publication/zero-trust-maturity-model*

5. *Zero Trust Architecture. (2020, August 11). NIST. Retrieved November 30,2021, from https://csrc.nist.gov/publications/detail/sp/800-207/final*

eclypses®

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today’s environments, called MTE®.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies and websites. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses’ patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

With a focus in the mobile sector, this technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT US

contact@eclypses.com
www.eclypses.com
(719) 323-6680