FORTRA

GUIDE *(Clearswift)*

Securing Government Data

Government agencies depend on cybersecurity solutions to stay on top of the latest threats. As threats advance, government agencies at all levels need a solution that can keep up.

The Cybersecurity Risks for Highly Regulated Organizations

Email remains the most popular way to communi-cate and share data, and it's why many cyberattacks target email. There is no magical solution for keeping cyberattacks away, and unfortunately there are many ways hackers can perform an email attack and gain access to an organization's data. This makes cybersecurity challenging for every industry.

Cyber threats are enough to make anyone nervous, but for organizations that hold some of the most sensitive data in the world, the pressure can be immense. Industries such as finance, critical infrastructure, and multiple levels of govern-ment need unwavering email security solutions.

Where the parallels between highly regulated industries and other industries end is in the aftermath of an attack. While costly and detrimental for all industries, the cybersecurity effects for highly regulated industries can be more severe in the data exposed. For example, in 2021 a ransomware attack made world news with a five-day shutdown of the US Colonial Pipeline – a major artery for fuel along the East Coast. Worried their systems could be further compromised, Colonial Pipeline ceased distribution causing a panic among motorists and a chain reaction into other industries includ-ing public transit and supply chain.

In this guide, we will take a deeper look at regulations, threats, and the solutions needed to protect government organizations.

Who Do Regulations Affect?

The need to protect data isn't the only reason organizations seek out email security solutions. Compliancy can be just as important. There are a host of cybersecurity regulations that can be applied depending on the level of government, location of government, and the information stored.

General Data Protection Regulation (GDPR) is one of the most famous cybersecurity regulations. While it is an EU law regulating data protection, it affects all organizations who possess data of EU citizens. Fines for failing to comply can be in the millions.

In the United States, there is no equivalent GDPR law, not even at the federal level. There are, however, federal restrictions and several state laws for cybersecurity. For example, California Consumer Privacy Act (CCPA) protects personal data of consumers residing in the state of California. Fines for failing to comply can range from $2,500-7,500 for each violation.

Of course, government contracts can have even higher standards for partners looking to work with agencies such as the US Department of Defense. Failure to meet these standards can result in a loss of contract or even rejection of consider-ation for future contracts.

More than ever before, governments worldwide are prioritizing the implementation of cybersecurity measures to combat digital threats, likely leading to the creation of more regulatory standards for government data.

The Journey of Data

The sharing of information within any organization is most likely performed digitally. Government is no exception with digital communications flowing internally with multiple levels of clearance, and externally with outside agencies. Understanding what data flows through the organization and who handles and receives the various types of data is a central component in creating a data loss prevention policy. Not knowing where all data - especially sensitive data – lives and flows is a major vulnerability to the organization, and vulnerabilities are lucrative to cybercriminals. Whether a government agency is at the local level working with citizens to make online payments thereby storing financial data, at the federal level storing citizen data such as social security numbers, or at a defense level with complex stages of clear-ance, sensitive data is everywhere in government. Knowing what it is and where it lives is one of the most important steps in protecting it.

Inbound and Outbound Data

Email is the primary way to send information quickly and resourcefully. As such a ubiquitous tool, email also remains a primary target for cyberattacks. Government organizations need to make sure emails coming into their organizations are safe of malware and other ad-vanced threats such as phishing, spyware, ransomware, and internal data loss risks. While some of the threats lurking in emails can come from unknown sources, some come disguised as a trusted outside partner. While government agencies impose very high standards on outside partners, it does not make it impossible for the partners to be digitally compromised.

The Internal Threat

While many deem outside threats coming into an organization as the most likely, just as critical are the internal threats. Sharing information digitally can save time, but if someone is accidentally added to the email, it can become a data breach. No matter if the recipient is inside the organization or if the person is an outside partner, potentially sensitive data has been exposed.

Levels of clearance in an organization may be the most apparent in government. Classified information is not intended for all eyes, that's why it's considered classified. Therefore, many government organizations need a security solution that understands the complexities of classified information flowing inside the many levels of government.

Creating the Policy

The goal of email security solutions should always be to protect the organization's data. Once the organization's data is identified and understood, the policy needs to be created. An email security solution that's easy to deploy, monitor, and manage will help support and enforce a policy in a way that doesn't burden the IT department, email administrators, or messaging teams. Features such as the ability to handle all threats from a single interface and have employees manage their own quarantine list will help increase the efficiency of the solution and ultimately free up time for IT teams to spend on other projects.

The following steps aid in email security best practices:

1) **Determine what data needs protection** – Com-pliance regulations dictate that sensitive data such as Personal Identifiable Information (PII) and payment details are safeguarded from unauthorized disclosure. A solution that can detect and remove unauthorized sensitive data from incoming and outgoing emails, and automatically encrypt any authorized data, will pro-tect employees and the organization if sensitive data is incorrectly sent or received.

2) **Identify cyber threats** – The right email security solution needs to prevent malware, spyware, ransomware, BEC (phishing) emails, unwanted data acquisition, and unnecessary file types from reaching inboxes.

3) **Establish a robust and sustainable email security policy** – An email security solution that's easy to deploy, monitor, and manage will help support and enforce a policy in a way that doesn't over-burden the IT department, email administrators, or messaging teams. Features such as the ability to handle all threats from a single interface and have employees manage their own quarantine list will help increase the efficiency of the solution and ultimately free up time for IT teams to spend on other projects.

4) **Close the zero-hour window** – Anti-malware solutions are great for defending against known dangers. But what happens if a brand-new virus tries to enter a network before security loopholes have been identified? The Sandbox, an email security solution, filters and analyzes the content of messages and attachments. If the content contains a threat, the Sandbox will sanitize these evasive threats thereby helping to close the vulnerability.

5) **Encrypt sensitive data** – To aid compliance, email security solutions need a range of easy-to-use policy-based encryption options including TLS, Web-portal, or password-protected messages.

6) **Monitor traffic behavior and performance** – Visibility of emails and comprehensive reporting is important when determining and enforcing policy. Email security solutions that provide detailed audit trails help IT teams investigate potential breaches. Those that export data to SIEM systems allow organizations to get a 360-degree view of the data flowing in and out of the organization.

7) **Education** – The members of an organization are some of the strongest defenses in email security but keeping them vigilant won't happen overnight. Having a stable email security education program to teach people how to stay alert about their inboxes and correspon-dences is key.

Creating an email security policy that understands content and context is vital for strong threat protection.

Critical Data Needs Email Security

Clearswift solutions offer an unprecedented level of flex-ibility and granularity in policy deployment and control. Clearswift Secure Email Gateway (SEG) uses traditional signature, heuristic, and cloud-assisted lookups to deliver protection against malware, ransomware, and spyware. SEG's Deep Content Inspection (DCI) can detect active code in files and allows the organization to manage how to handle any violations.

Sanitizing and Redacting – Better Content Safeguarding

SEG can detect information that shouldn't be there. The data might be deliberately exfiltrated or someone could be sending out some content that may contain hidden classified information.

Through Structural Sanitization, the SEG can clean content to ensure that no sensitive data is being exfiltrated either deliberately or accidentally. Documents can have sensitive or offensive text automatically redacted. Even images within documents can have sensitive content redacted from the image and then replaced in the docu-ment. Document properties (metadata) can be cleaned; for example, agencies may want to remove the "Author" name from all publicly available documents.

Clearswift's Anti-Steganography rebuilds images to remove any data added by steganography tools, which is often missed by other email security solutions such as Microsoft Office 365.

With URLs being used as a key method of attack, any found in messages and attachments are checked in real-time to see if they relate to malicious, phishing, or spam campaigns. Messages can be blocked. URLs are sanitized or rewritten to use Time-of-Click services.

Encryption that Keeps Government Moving

To provide automatic security and regulatory compliance, SEG features encryption. This allows policies to be based on sender, recipient, subject, message body, attachment types, attachment content, message header, or document metadata.

By providing multiple options to send data securely, organizations can choose the best method to deliver content to third parties in the most appropriate method. The following are various encryption methods used by SEG:

Transport Layer Security (TLS)
This mechanism is used to secure messages over the internet between servers. It is completely transparent to end users and is therefore widely used.

Password protected files

This method wraps the sender's message and attachments into a password protected Zip file or PDF which is then delivered to the recipient. The sender must get the password to the recipient, typically using a different medium such SMS, or email to a secondary email account.

Web Pickup Over SSL

The hosted email portal allows senders to send mes-sages to recipients using a webmail-style mail client and respond to the sender in a secure fashion. This is typically used for low volumes of message transaction to users of all levels.

Method	Usage Frequency		Recipient		Level of security
	Regular	Adhoc	Business	Consumer	
TLS	Y	Y	Y	Y	Over Network
Password	Y	Y	Y	Y	To User
S/MIME & PGP	Y		Y		To User
Web Portal Pickup		Y	Y	Y	To User

Securing Classified and Unclassified Data

The words "classified" and "unclassified" are synonymous with government agencies. The data for classified and unclassified information needs to move differently inside of government. Not all eyes are cleared to see classified docu-ments whether digital or not. Naturally, a security solution is needed to keep digital classified information guarded. Clearswift's email and web products have pre-configured, standard lexical expressions. When it comes to other specific values that need detecting, lexical expression qualifiers (LEQs) are used to validate "true" information found against external data sources such as a database. Logic can be added for the "if this, then this" scenario. This is important for government agencies, such as defense agencies, when sharing classified information between approved colleagues. For example, if coworkers in the defense department are sharing highly classified military strategies, the data should always be encrypted. To ensure the data is encrypted, it is inspected for attributes that identify key terms. Clearswift can import a snapshot of specific details for official use or top-secret correspondents. The LEQ file is then indexed and hashed for security. The more information verified through LEQs, the more the system can be sure of a policy match and automatically apply the appropriate action, reducing the amount of manual intervention required.

Sending File Transfers Securely

Government agencies rely on the ability to share files daily with their citizens. This is true in many forms of government including local government where tax departments, law enforcement, and payment processors need to share files to keep business moving. Clearswift Secure ICAP Gateway (SIG) is a fully automated solution that augments the security of critical information flowing through an organization's existing web proxy infrastructure or managed file transfers.

Going beyond traditional stop and block technology, SIG applies the appropriate measures to questionable content based on the government agency's policies to allow safe content to flow through and reduce disruptions.

SIG integrates seamlessly with Secure File Transfer platforms to create a powerful solution for government agencies that require enhanced security around file transfers. A file transfer solution with security and compliance features has never been more crucial than now, with hybrid working environments and bigger reliance on digital procedures rather than old-fashioned paperwork.

Clearswift Stands Above the Rest

Managing cybersecurity for any organization is complex and even stressful at times – and having solutions that don't get in the way while keeping organizations secure alleviates many burdens. Clearswift can also be deployed alongside many other systems for a robust layered approach to cyber-security that fills the vulnerabilities left by a sole solution.

Clearswift is extremely configurable giving government agencies the ability to apply very granular policies to data. Not all government agencies are the same, and policies need reflect the level of government they are securing. Whether protecting the PII of its citizens or military information to protect millions, Clearswift protects data from the point of creation and throughout its journey.

Ready for data security help without hassles?

Contact Us

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.