Issue 5

BANK OF AMERICA

Cyber Security Journal

The latest ideas on digital security to help
you safeguard what's most important to you

PROTECTING YOUR COMPANY'S CLOUD DEPLOYMENTS

A guide to understanding your organization's role in the security of cloud-based data and tools.

HOW TO KEEP YOUR EMAIL SYSTEMS SECURE — AND EFFICIENT

Understand why criminals want the contents of your email account and how your business can protect its communications.

Contents

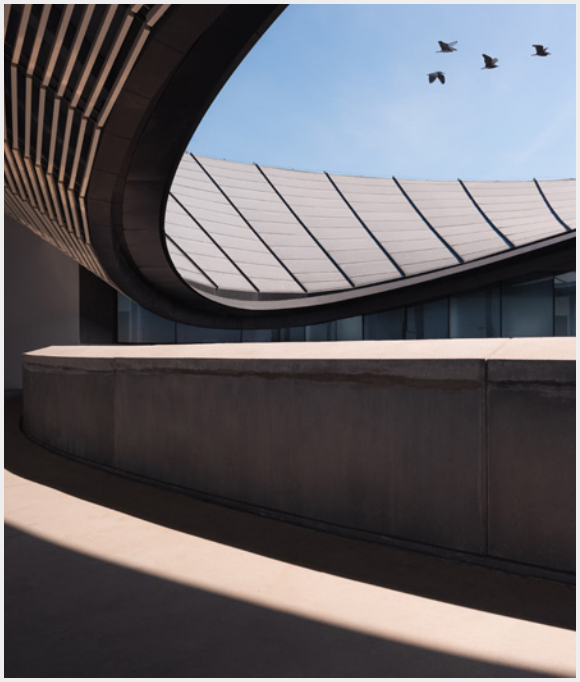
Cyber Security Journal • Issue 5

Letter

3 **From Craig Froelich, *Chief Information Security Officer***

Features

4
Protecting your company's cloud deployments
Cloud service providers are essential business partners, but companies who use their services need to understand their own role in securing cloud-based tools and data.



10
How to keep your email systems secure — and efficient
Learn why criminals are eager to steal data inside your email account — and how your business can protect this vital communication channel.

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to, warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

We're dedicated to protecting you year-round.

Craig Froelich

The cyber landscape continues to shift at a rapid pace. Fraudsters and cyber criminals are quick to adapt and manipulate, infiltrating vulnerable areas before companies recognize them, sparing no one, regardless of region, status, breadth of assets or company revenue.

October is Cyber Security Awareness Month (CSAM). Understanding the cyber threat landscape, and the threats relevant to your business, can help you and protect your business. In this issue of *The Cyber Security Journal*, we delve into two common threats — cloud computing and business email compromise.

Cloud computing capabilities are a major factor in enabling companies to successfully pivot to a fully remote environment. In some cases, cloud environments were set up so rapidly, the focus was more on implementation and less on security. This article identifies the risks of cloud environments and offers ideas to configure your platforms securely.

Business email compromise also remains one of the biggest threats to companies, with adjusted losses reported to the FBI in 2020 totaling $1.8 billion. Knowing the basics of email hygiene has proven time and time again to be a useful tool in ensuring that your employees practice good cyber hygiene at work and beyond. Furthermore, email accounts themselves, and specifically the rich data they contain, have become targets for cyber criminals.

At Bank of America, helping you protect your business is our top priority. Sharing our deep industry expertise and robust educational tools are among the ways we help reinforce that protection. From insights on emergent security controls to robust fraud education programs, our team works with yours to help you safeguard your business.

During CSAM, we hope you take the time to evaluate your cyber hygiene and implement best practices to help you stay ahead of cyber threats.

Chief Information Security Officer,
Bank of America

FEATURE ONE

Protecting your company’s cloud deployments

Cloud computing is a key driver of business growth, but it’s essential to understand these deployments and assess who is responsible for protecting them.

Protecting your company's cloud deployments

Cyber Security Journal
Issue 5

Cloud service providers generally offer strong security — but companies need to take steps to protect their proprietary data and assets.

Cloud capabilities have become essential to almost every type of business. They provide data storage, enable real-time communication and collaboration, link disparate teams and systems and connect new devices to company networks. Importantly, cloud deployments can scale up quickly, which has helped many companies quickly establish new connections and working conditions with partners, customers, internal teams and remote employees.

But according to one study, 81% of business leaders named security as their top challenge in cloud computing.[1] One problem is that many companies simply have not assessed the risks associated with cloud deployments or have not determined what elements of security are their responsibility. Since most organizations depend on cloud service providers — CSPs — to maintain these systems, it can be challenging to determine which elements of security are the responsibility of the CSP and which are not.

> *"Third parties with access to cloud deployments are an ongoing security concern for many organizations."*

Security challenges in the cloud

CSPs usually offer built-in security features that exceed the technical capabilities and financial resources of most small and midsize businesses. 85% of businesses believe the cloud is as secure or more secure than their own infrastructure.[2] In fact, the cloud can be as se-cure as in-house systems, but only if managed with appropriate storage and access controls.

While CSPs often provide tools to help manage cloud configuration, there are still many elements of security infrastructure — such as firewalls, devices and account access — that remain the cloud user's responsibil-ity. In fact, CSPs are not the source of most security incidents. Lack of knowledge among cloud customers and misconfiguration of CSP accounts are responsible for most breaches, big and small.

Protecting your company's cloud deployments

Misconfiguration, like many cloud security challenges, often stems from staff inexperience. Many security and IT specialists simply don't understand the intricacies of secure cloud configuration and often lack in-depth knowledge of their company's CSP security settings and capabilities.

Another pitfall is inadequate or incomplete security processes. When configurations and permissions are not thought through, employees — and bad actors — can gain access to a world of sensitive information that can be unintentionally leaked or very cleverly stolen through social engineering schemes. This type of insider incident can have serious and costly impacts.

Research shows that 82% of companies give third-party vendors highly privileged cloud identity roles — yet in many cases cloud security teams are not aware that these privileges have been granted.[3] This kind of oversight could increase the risk of account takeovers by cyber criminals or disruptions to normal operations. In one study, 69% of organizations said that third-party incidents are on the rise — and 51% had experienced a third-party data breach in the past year.[4]

Access and data controls are fundamental to digital security, including cloud deployments.

For example, if criminals exploit a weakness in software in a software-as-a-service provider, multiple downstream businesses that rely on that software can be compromised in turn. In these situations, criminals have leveraged the vendor vulnerability to deploy economies of scale and impact multiple businesses with minimal effort.

Complex compliance requirements are another risk to cloud deployments. Governments are enacting sweeping new data privacy laws that stipulate technically intricate compliance obligations for protection of consumer data. These regulations, which include the California Privacy Rights Act (CPRA) and the EU's General Data Protection Regulation (GDPR), mandate stringent rules governing data access and use across geographies. Most CSPs offer tools to help manage compliance, but they may not cover all requirements of evolving security laws, particularly in highly regulated industries like finance, healthcare and utilities.

Key risks to cloud environments

Some of the most common risks to cloud security include:

- Lack of attention to basics required for database storage and management.
- Misconfiguration of cloud infrastructure and storage.
- Lack of strong security controls for cloud environments.
- Inadequate protection of cloud secrets like administrative credentials and encryption keys.
- Use of unsecured data transfer protocols.
- Lack of visibility into network activity.
- Inadequate security requirements for third parties.
- Employee susceptibility to phishing and ransomware.
- Failure to update compliance requirements for new data privacy regulations.

Protecting your company’s cloud deployments

Cyber Security Journal
Issue 5

How to overcome the obstacles

In many ways, cloud deployment security is similar to traditional on-premises systems. Cloud security should follow a “cover the basics” approach that includes fundamentals like:

1. A thorough understanding of the data you gather
2. Powerful identity and authentication tools
3. Access controls based on the principle of least access
4. Correct configuration of the deployment
5. Encryption of data in motion, in use, at rest
6. Network activity monitoring
7. Limited privileged access to cloud settings
8. Proper training of IT, security and individual users

For more specific guidance in addressing cloud security challenges, a CSP can be one of the best sources of advice. Service providers offer a range of advanced

continued on page 8

Taking responsibility for cloud security

Determining who is responsible for cloud security — the customer, the cloud vendor or both — varies among cloud models. In general, providers are responsible for safeguarding the infrastructure that runs services in the cloud, while cloud customers are liable for the security of information stored on the cloud.

Responsibility	**SaaS** Software-as-a-service (SaaS) places responsibility for security of data and user access in the hands of cloud customers.	**PaaS** Platform-as-a-service (PaaS) assigns cloud customers responsibility for securing their applications, data, and user access.	**IaaS** Infrastructure-as-a-service (IaaS) gives cloud customers responsibility for user access, applications, data, operating systems, and network traffic.	**On Premise**
Information & data	✔	✔	✔	✔
Firewall configuration	✔	✔	✔	✔
Devices	✔	✔	✔	✔
Accounts & identities	✔	✔	✔	✔
GRC	✔	✔	✔	✔
Identity & directory infrastructure	✔✓	✔✓	✔	✔
Application security	✓	✔✓	✔	✔
Network controls	✓	✔✓	✔	✔
Operating system	✓	✓	✔	✔
Firewall configuration	✔	✔	✔	✔
Physical data center	✓	✓	✓	✔
Physical security	✓	✓	✓	✔
Physical network	✓	✓	✓	✔

✔ **PROVIDER RESPONSIBILITY** ✓ **CUSTOMER RESPONSIBILITY** ✔✓ **SHARED RESPONSIBILITY**

TAKEAWAY:

Customer is always responsible

Responsibility varies by service type

Protecting your company’s cloud deployments

Organizations should regularly review their cloud security roles and protocols.

continued from page 8

security and privacy capabilities, as well as guidelines and security defaults for rigorous configuration of cloud settings. But many organizations don’t follow these guidelines, and some may even inadvertently disable essential security settings.

So in many cases, the first step in overcoming security challenges is to revisit the CSP’s existing guidelines and settings. Doing so can help clarify, for example, how to protect data stored in cloud buckets. Importantly, sensitive information should be stored in a specific bucket that is protected by encryption and data-log monitoring. Lacking proper configuration, data stored in these buckets could be open to access by anyone searching through the cloud provider. It’s an example of a serious security breach that bad actors can exploit without even attempting to compromise a company’s systems or employee accounts.

A CSP may also offer continuous monitoring solutions to help detect suspicious user activity and assess an organization’s threat status in real time. Monitoring is also essential to tracking and prioritizing investigations of malicious incidents.

However, CSPs don’t provide much help in minimizing third-party risks. Business and security leaders will need to carefully assess a partner’s security capabilities to make sure they meet or exceed their own. This assessment can also help determine the right amount of access to grant third-party users.

Another key to successfully managing third-party access is applying the principle of least privileged access, which gives users minimum access to the data needed to perform their job. This will inform implementation of custom access controls that govern what sensitive data is protected and who can access that information.

Even with these safeguards enforced, the lines that separate cloud security responsibilities can be blurry. A shared responsibility model for cloud security can help businesses determine who is accountable for maintaining the right security and operations protocols. In general, the cloud customer is responsible for securing their own data, access policies and applications, as well as compliance. Cloud providers, on the other hand, are liable for the technology infrastructure and software that runs the cloud. (See sidebar: “Taking responsibility for cloud security.”)

Cloud security by the numbers

76%

Percentage of companies that are moving their security to the cloud.[5]

57%

Percentage of global business leaders who say an attack on cloud services is likely to occur in the next year.[6]

85%

Percentage of organizations reporting that cloud feels as secure or more secure than on-premises infrastructure.[7]

46%

Percentage of cloud buckets vulnerable to compromise due to unintentional misconfiguration by cloud customers.[8]

Since privacy laws are evolving, companies should not assume CSPs have their regulatory compliance covered.

Cloud security begins with core protocols

Overall, the security of an organization’s cloud deployments depends heavily on its existing protocols and processes. Companies that prioritize access and data management will often have created clear lines of accountability, which can be leveraged as their cloud engagements become more complex. Those that are accustomed to strong oversight of third parties will be better positioned to extend those controls to cloud access and have tools for evaluating the shared responsibility models practiced by most CSPs.

Furthermore, leaders can emphasize that while a CSP security position may be strong, it is not all-encompassing, and does not absolve any organization of the need to protect its own data, access controls and key partnerships. As deployments become more complex and tie in more users and platforms, there will be a corresponding need for expanded oversight of the cloud connection points. Making that case, and tying security directly to the value of cloud capabilities, is essential to every organization. ■

Key takeaways:

- Companies need to understand and map out the extent and limitations of security provided by their CSP.
- Third-party access to cloud deployments requires additional management oversight and compliance with strong security standards.
- Familiarity with the cloud provider’s guidelines and settings can help organizations protect access to critical data and prevent breaches.

[1] *Flexera, “2021 State of Cloud Report.”*

[2] *IDG and Google, New research: Enterprises more confident than ever in cloud security, July 1, 2021.*

[3] *Wiz, 82% of companies unknowingly give third parties access to all their cloud data, February 2, 2021.*

[4] *Ibid.*

[5] *PwC 2021 Global DTI.*

[6] *Ibid.*

[7] *Wiz, 82% of companies unknowingly give third parties access to all their cloud data, February 2, 2021.*

[8] *Flexera, “2021 State of Cloud Report.”*

FEATURE TWO

How to keep your email systems secure — and efficient

With most organizations still dependent on email, it's essential to adopt protocols that safeguard access to company accounts and the critical information they contain.

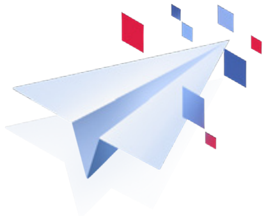
How to keep your email systems secure — and efficient

Cyber Security Journal
Issue 5

→ Email continues to be the backbone of business communication in almost every industry — and one of the most popular vehicles for cyber crime. Phishing, business email compromise (BEC) and accounts payable scams are persistent threats for most businesses. But email is not just a means to a criminal end. Email accounts themselves, and specifically the rich data they contain, have become targets for cyber criminals who may lurk undetected, harvesting information over long periods of time.

The consequences of these intrusions can take many forms. Imagine a request to change a vendor's invoice and account information that appears to come from a trusted employee's email account — but actually is written by a criminal who has compromised the employee's account, studied the tone and cadence of accounts payable communications and knows the protocols for changing account information. Or consider a CEO who sends company performance information in an email that gets hijacked and released, putting the CEO in violation of SEC regulations.

Cyber criminals can use the data in an email account in numerous scams, such as social engineering.



Targeted data can be classed in a few general categories:

Account credentials — Password reset information found in emails can provide intelligence on what accounts you have and what services you are using and can also be used to gain access to those accounts and services.

Relationship information — Emails can reveal not only the relationships you have with clients, vendors, and partners, but also the names of key people within those relationships and critical information that can be used to increase the effectiveness of social engineering and phishing attacks.

Contact lists — In addition to revealing key contacts and relationships, email accounts provide access to full address books and private contact lists (think peer CEOs, for example) that can be used to identify new targets.

Contracts and deals in flight — Cyber criminals can analyze emails for evidence of financial transactions in progress and use that information to request payments and redirect funds.

Calendar information — Emails may include calendar invites with sensitive content attached, as well as schedule information that criminals can exploit for social engineering, identity spoofing, and other crimes.

Sensitive data — Email is often used as a data transport, including attached files full of data about personnel and clients. Even when spreadsheets or PDFs are password protected, the passwords are often provided in emails that immediately follow.

How to keep your email systems secure — and efficient

These examples, based on actual incidents, involve several kinds of data that criminals might harvest from a single email account — and demonstrate a variety of damages that might ensue after a breach. But considering how much we depend on email, and how its security is often taken for granted, it is important for every business to think through how it can bolster its defenses with tools and strong protocols.

> *"Both personal and business email accounts are giant repositories of data that cyber criminals can mine for myriad purposes."*

What are BIMI and DMARC, and how can they enhance email security?

Cyber industry leaders have recognized the need for stronger universal protocols to identify legitimate emails and block spam and phishing attempts. Two protocols, which are inexpensive to implement, are developing into industry standards.

DMARC

Domain-based message authentication, recording and conformance (DMARC) is a protocol that harnesses the power of two established technologies (SKF and DKIM) and automatically creates a link between a domain and every email it generates.

- DMARC protocols provide reports that **identify legitimate emails associated with an organization's domain.**
- It also provides a recipient's email systems with instructions for handling communications that are **not legitimized by DMARC protocols.**
- Many popular online services and domains already use DMARC. Organizations can sign up to use the protocol by registering their domains and **adopting SKF and DKIM protocols.**
- **DMARC requires no license to use** and is available to any organization that uses the Domain Name System (DNS).

BIMI

Brand indicators for message identification (BIMI) is a protocol that displays an organization's logo in every authentic email. While it was created to boost brand recognition, BIMI's value to email security has been recognized by mainstream email providers.

- BIMI requires DMARC, SKF and DKIM to function as intended. While the two protocols are separate, **BIMI can be viewed as an extension of DMARC.**
- BIMI also generates a record that can be **found on a domain's DNS server.**
- The organization's logo acts as an additional authenticator, which can have the simultaneous benefit of **reducing bounce-back emails and ensuring that important communications are noticed and opened.**
- Like the DMARC record, **the BIMI record is published on the DNS.**

How to keep your email systems secure — and efficient

> *“Requiring multifactor authentication is one of the simplest and most effective ways of protecting access to email accounts.”*

What kind of data can criminals use?

If they gain access to email accounts, sophisticated cyber criminals can mine them for many different types of information that reveal how a company operates, what protocols it follows and how employees interact. As the line between personal and business email accounts have blurred, criminals may be able to harvest information from both our personal and professional lives. This can lead to identity theft, social engineering, insider trading and intellectual property theft.

How criminals gain access to your mailbox

Cyber criminals leverage a variety of strategies to gain access to email accounts, such as sending targeted spear phishing emails to deceive an individual into providing login information, using malware to infiltrate company networks or spoofing an email account or domain to send authentic-looking emails to gain access. Additionally, email is often left vulnerable due to poor password hygiene. With so many security breaches having occurred across large organizations, targets can be unaware that they were victims of a breach and end up reusing compromised usernames and passwords.

The costs incurred by email data mining can be divided into four broad categories:

Personal damage occurs when an individual’s information, such as personal financial accounts or information that facilitates identity theft, is compromised.

Business damage is a risk if, for instance, information mined from an email enables the perpetrator to enter a market and undercut a business’s competitive advantage.

Reputational damage might happen on both a personal or business level when private information stored in emails is revealed or, in some instances, used for extortion.

Legal damage can occur when an email breach affects regulatory compliance, and sensitive information is released in violation of SEC regulations or HIPAA guidelines, for example.

Protocols such as DMARC and BIMI can help authenticate messages and filter out email threats.

How to keep your email systems secure — and efficient

Once hackers gain access to a user's email account, they can use a number of tricks to keep their presence undetected, such as enabling auto-forwarding of incoming emails to an external address or setting up rules to automatically delete certain messages. In fact, a cyber criminal's ability to leverage data harvested from the account and replicate their target's language, personality and organizational identifiers can make the intrusions extremely difficult to spot.

Key protocols for email security

In addition to implementing best practices, there are a number of emerging protocols that are helping to advance email security. Two of the most critical are domain-based messaging authentication reporting and conformance (DMARC) and brand indicators for message identification (BIMI). (See additional information on p. 12)

DMARC is an email authentication protocol that helps organizations protect their domains from being spoofed. DMARC prevents spoofing by registering your domain and authentication details with email servers and providing instructions on what to do with emails that fail the authentication — for instance, locking, quarantining or rejecting the email.

BIMI, on the other hand, leverages DMARC and other protocols to provide visual cues to validate that emails are coming from a legitimate source. BIMI enables emails that have passed DMARC authentication checks to display a company logo, so that users can see at a glance that the email is genuine and the organization's domain has not been spoofed. Not only does this help keep an organization's partners safe from fraudulent emails, it also helps increase brand awareness by displaying a distinctive logo in each message.

Regular password maintenance is still an email security essential.

Following some best practices can help protect you and your business from cyber criminals looking to exploit your mailboxes.

Verify emails requesting sensitive information — All emails that involve financial or sensitive data should be confirmed through an alternate channel approved by company leadership.

Separate personal and professional email accounts — Even the smallest businesses should provide work email accounts for employees and encourage the separation of personal and work-related email to minimize exposure. Company email accounts should be used exclusively for professional purposes, and never used to create accounts on websites for personal use.

Manage account access — Requiring multifactor authentication is one of the simplest and most effective ways of protecting access to email accounts. Enabling alerts for activity such as unusual login locations can help detect breaches.

Disable automatic forwarding — Prohibiting the automatic forwarding of email to external domains prevents cyber criminals from exfiltrating email messages and the data contained within them.

Monitor inbox rules — In addition to ensuring that intruders aren't covering their tracks by using rules to autosend messages or divert suspicious ones to trash, consider implementing rules that block macros and file extensions commonly used by malware.

Maintain phishing simulations and fraud education — Strong cyber defense depends on alert employees who are aware of current threats and their role in company security. Educate all employees on the fundamentals of password best practices, including how to create strong passwords and prompts to change them on a regular basis.

How to keep your email systems secure — and efficient

Ongoing training and regular discussion of email threats can help sustain a cyber-aware workforce.

Like every other security tool and protocol, BIMI and DMARC can't eradicate business email spoofing. But they have enhanced security by helping to legitimize authentic emails and creating a record and enforcement policy for those rejected by the organization's system. Neither requires licenses to implement, and many organizations with dedicated IT departments can set up the protocols without outside assistance.

Furthermore, DMARC is embraced by government agencies, such as the National Institute of Standards and Technology (NIST), and both DMARC and BIMI are leveraged by many industry leaders.

> *"DMARC and BIMI can help your email recipients trust that your communications are legitimate, as well as make illegitimate incoming email stand out and be avoided."*

Protect your data and your business

As businesses and individuals alike increasingly turn to cloud-based email providers offering virtually unlimited storage options — allowing users to save decades worth of emails — the amount of data that criminals can mine continues to grow exponentially. By increasing cyber security awareness, improving access management and email hygiene and staying abreast of emerging email security protocols, you can protect your data, yourself and your business. ■

[1] *For details on how to implement DMARC and BIMI, visit dmarc.org and bimigroup.org.*

[2] *Nightingale, J. (2017), Email Authentication Mechanisms: DMARC, SPF and DKIM, Technical Note (NIST TN), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.TN.1945.*

Key takeaways:

- Email is not simply a vector for cyber crime. Email accounts, and the rich data they may contain, have themselves become target objectives of cyber criminals.
- Multiple layers of authentication and oversight may be needed to ensure the legitimacy of all email interactions.
- Businesses should continue to educate employees about evolving email threats and invest in training, such as phishing simulations.
- Email protocols like DMARC and BIMI should become standard security tools in organizations of all sizes.