Diligent

Reducing Risk in Financial Services

Providing Enhanced Security Infrastructure for Confidential Information Exchanges

Since the outbreak of the COVID-19 pandemic, businesses have been tasked with exploring Future of Work (FOW) options to guarantee strong business continuity. As organizations embrace this digital transformation, they must ensure that the technology they are using protects data and reduces risks. For financial services firms, proper risk oversight is a necessity, and with the new reliance on technology, there needs to be an understanding of the steps to take in order to reduce risk.

Research from security firm Bitglass shows that despite the fact that financial services firms are the victim of only 7% of all reported data breaches, these attacks are responsible for the loss of 62% of their records.

Financial services firms have much higher costs from lost or stolen data, creating a scenario inherent to increased risk. Congruently, they face tighter compliance and legal demands for the data that they possess. Thus, more stringent security is needed to protect financial information to better reduce risk. The information these firms possess is very attractive to cyber-attackers. Research from security firm Bitglass shows that despite the fact that financial services firms are the victim of only 7% of all reported data breaches, these attacks are responsible for the loss of 62% of their records. Unfortunately, it's not just cyberattacks that cause problems. The same survey shows that accidental disclosures and insider threats are the second- and third-most common reasons for unauthorized disclosures.

It is not a surprise that the Richmond Federal Reserve Bank noted that the top operational risk for financial services is the disclosure of private information. Protecting information is paramount. Financial services firms have done a great deal to protect such information at rest or while it is stored in digital systems. However, the same cannot be said for this sensitive data when it is being sent or shared via email, Slack, Box or other insecure digital methods.

Diligent

The Importance of Protecting Data

Data in transit is often very vulnerable. There are substantial risks that can result in data loss when data is being shared or communicated. The following four reasons are some of the largest use cases and the ones that first-place financial services firms should look toward to ensure better secure communication practices.

4 Common Reasons for Data Loss

Cyber-Attacks: If cyber-attackers can penetrate a corporate network seemingly unnoticed, they will wait until they can access the most valuable data to steal. These are called “man-in-the-middle” attacks because the attacker sits between the sender and the recipient, waiting for their chance. These attacks are very common and IBM’s X-Force Threat Intelligence report says that 35% of exploitation activity results from man-in-the-middle attacks.

Time elapsed: Ponemon research shows that, on average, it takes 197 days to detect a network breach, giving attackers more than six months to reside unnoticed inside a company’s digital infrastructure and continuously exfiltrate data.

Communication tools: Many of the communication tools that are used on a daily basis within financial services firms have no mechanism for barring the “re-forwarding” of data. Organizations often have no visibility when sensitive information is passed on, potentially outside their control. If the organization does have these types of fail-safes in place, who is controlling this information? How many people have access to the sensitive data within the organization?

Insider threats: Many of the commonly used platforms for communication and group work processes have “back doors” that allow IT admins or vendors to possibly view and copy information that is transiting those systems. This dramatically increases the potential risk of insider threats.

The impact of data loss during sharing or as part of a message is much higher for those who have regular and consistent access to sensitive information, primarily senior executives and directors. This is especially true for financial services firms that have myriad types of sensitive financial information about their customers. To protect this confidential information, forward-thinking financial services firms are deploying highly secure communication and messaging systems, like those offered by Diligent, to augment the general-purpose tools that are appropriate for less sensitive information. Within financial services firms, high-level employees and directors need a solution that makes it certain that sensitive information cannot be compromised. Using a purpose-built, highly secure communications and messaging platform has the additional benefit of putting the user into a high-security mindset, further reducing the risk of user mistakes and oversights.

Diligent

Why Executives, Senior Managers and Board Directors Make Attractive Targets

The information that senior staff at a financial services firm possesses and shares is unusually valuable, and therefore attractive to cyber-attackers. For this reason, many well-organized groups of attackers are focused on the top staff at financial services firms. An excellent example of this is the London Blue group that targeted 50,000 senior financial services executives. The attackers were eventually identified, and there are likely many similar groups currently operating that have not yet been discovered.

To some extent, the FOW is now, since the COVID-19 pandemic crisis has resulted in widespread remote work environments in just a few weeks.

These attackers most often strike via messaging and email tools. “Spearphishing” and “whaling” are the terms used for the highly focused and repetitive attacks that focus on senior staff of financial services firms. These attacks can be very clever and are designed to mitigate much of the protection provided by standard cybersecurity tools such as anti-malware or anti-virus software. These attackers put in a lot of work to know their target and use social engineering to appear as a trusted person.

Remote work and working from home have opened several additional vulnerabilities. Research from iPass shows that C-level executives are at the greatest risk of being hacked through their mobile devices; as remote and virtual work become more common as part of the FOW, the threats to general purpose, moderately secure communication tools commonly found on mobile devices will increase. To some extent, the FOW is now, since the COVID-19 pandemic crisis has resulted in widespread remote work environments in just a few weeks. If and when financial firms emerge from the lockdown, the need for highly secure remote and virtual communication will increase. The best approach to delivering secure communications for your team now and in the future is to provide a separate and highly secure communications platform that is walled off from the standard tools.

Diligent

Financial Services Firms Use Cases for a Highly Secure Communications Platform

Financial services firms are unique in that communication activities consistently include a high percentage of sensitive or private data, which will always increase the likelihood of compliance or legal problems. Regulations such as FINRA, SEC disclosure regulations, Gramm-Leach-Bliley, insider trading statutes, GDPR, CCPA and others demand not only better protection for data, but impose more impactful penalties for breaches. Ignoring the problem is not acceptable, and many compliance regimes require that the financial services firm be able to demonstrate their data-protection efforts.

There is an excellent real-world example of why data protection is necessary. When Evercore was hit by a successful phishing attack, the attackers gained access to the files of this major player in the business of M&A, and thousands of sensitive documents were stolen. The attack negatively impacted Evercore's clients, and had a damaging reputational impact on the company.

Diligent

Common use cases in Financial Services where a more secure platform is needed:

Operational risk: Any communications that include details on current or future operational risk must be protected from accidental or partial disclosure.

Sharing of any customer personally identifiable information (PII): There are often instances in which specific and attributable PII may be included as part of a file, report or analysis. With the expansion of marketing technology tools, PII sharing may be even more widespread than initially thought.

Confidential client information: Many financial services firms have deep relationships with customers, particularly larger businesses. Ensuring that all specific client information is secured when it is shared among team members at the financial services firm is critical to reputation and trust.

Capital status and availability information: The current state, sources and uses of capital include some very sensitive and confidential information. For financial services firms, it is essential to ensure that any information on this topic is not public and is fully protected.

Investment/divestment scenarios: Some of this information will eventually become public, but until it does, protecting it from any leaks is critical. There are numerous cases in which the legal implications of not fully securing this information have been substantial.

Merger/acquisition/IPO discussions: This class of information is often cited as the most valuable information that financial services firms possess. For attackers, stealing this information will deliver substantial financial gain.

Financial reporting documents: This is also a use case where, although the information will eventually become public, premature disclosure or the loss of this data is highly problematic and will cause the institution to run afoul of potentially numerous regulatory regimes.

Senior leadership changes: Prior to the announcement of any major changes, this information must be kept secured. If unplanned disclosure occurs, it may not only result in embarrassment and damage to the brand, but also negatively impact succession planning.

Diligent

Key Features for a Secure Communications Platform

The design points for a general-purpose communications tool and a highly-secure communications solution are quite different. To provide greater clarity on the differences and on how security can be improved, it is worth looking at the key features in a highly secure communications solution and what is different.

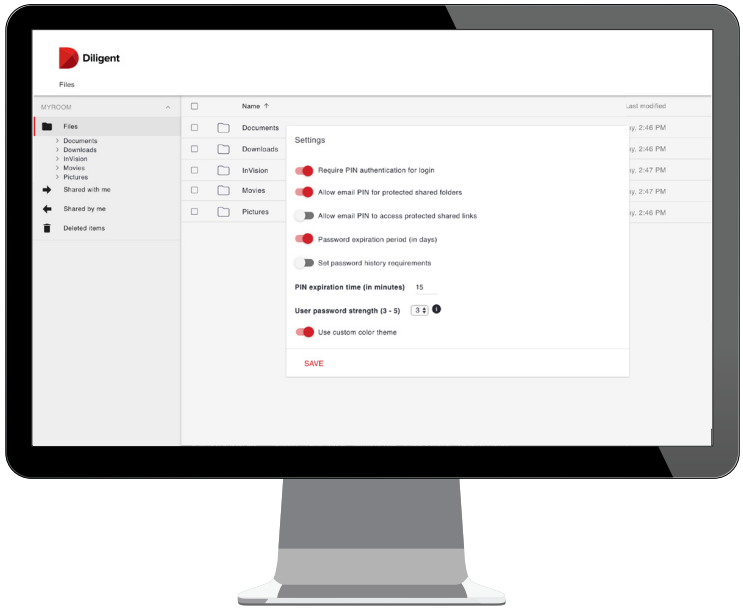
1. A system that lives off the corporate network. One of the fundamental difficulties in securing general-purpose communications and information-sharing tools is that any breach of the corporate network will make the information on that network visible to the attacker. Although most networks are secure, breaches are not uncommon, since known vulnerabilities are often present and most corporate networks have integrated links to the public internet. Moving any traffic that includes confidential or sensitive information to a closed network that is air-gapped delivers much greater security.

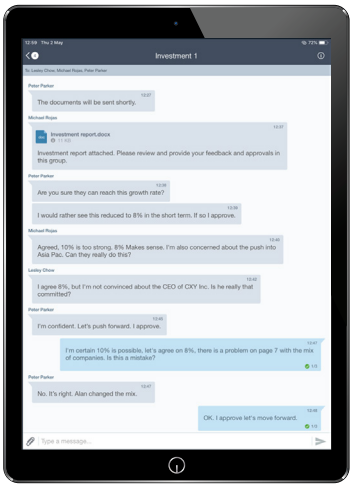
2. A comprehensive, end-to-end solution. Anytime several different tools are used to share information, the odds of one of those tools being less secure, or even compromised, rises. Utilizing a single, self-contained, isolated solution not only makes securing the information simpler, but it also reduces risk. The solution must have several features, including file-sharing support, the ability to support the workflow and processes of the specific task, and secure messaging. For some use cases, such as M&A, a secure virtual data room that is part of the overall solution is very attractive.

Diligent

3. A closed-system design. Moving secure communications off the corporate network is the starting point. The next step in adding additional security by design is to make it a closed system. Using a system that is cobbled together from numerous third-party components presents the potential for weaknesses or open interfaces that can be used by attackers to bypass security. A closed system also delivers the ability to eliminate the risk that IT staff or someone with administrator credentials might eavesdrop -- a concept typically referred to as “IT shielding.” Removing this risk is not a judgment against the integrity of an organization’s IT team. The overwhelming majority of IT administrators are responsible and trustworthy. But an administrator’s access credentials could be compromised or stolen and then used by a cyber-attacker to access the system or network. A single comprehensive solution also eliminates threats from open APIs from individual products that can be used as an entry point to the system.

4. Services and support that are designed for a security-first environment. Delivering absolute security demands a comprehensive approach, with the services and support in place to ensure secure communications. To start, migration services must be able to spot any existing vulnerabilities or potential attack vectors, and ensure they are mitigated before installing the new platform. Secondly, the services necessary for putting the secure communications system into operation must have a documented approach to ensure the system is secure as it goes live. Finally, ongoing support must also be designed to protect the system. In order to install the platform successfully, an organization would require positive identification of any user requesting support, secure distribution of updates and support services that do not have unnecessary access to the customer’s system.





Diligent

Final Words on Why Financial Services Firms Need a Secure Communications Platform

Nearly every financial services firm has made great strides in protecting sensitive information at rest. However, when that information is shared or used jointly, many of the safeguards are eliminated. Adding further to the risk is that many general-purpose communications and messaging platforms do not have the necessary intrinsic security or the ability to stop information from being forwarded to unauthorized users or outside the organization into the wild. The risks associated with using general-purpose communications tools are quite substantial.

Given that financial services firms must meet evolving statutory demands and store private data, deploying a highly secure communications and messaging system must be a priority.

Diligent is a proven leader in providing highly secure communications solutions that meet the needs of financial services firms. The Diligent solution is designed from the ground up to provide the necessary security that financial services organizations require. The Diligent Secure Communications platform is the No. 1 product for sensitive board communications, and the company counts 50% of the Fortune 1000 as current customers.

For more information or to request a demo, contact us today:
Email: info@diligent.com | Call: +1 877 434 5443 | Visit: diligent.com