Lookout

Whitepaper

Lookout for Financial Services organizations

Secure mobility in the Financial Services industry

Secure mobility in the Financial Services industry

Financial organizations were one of the first organizations to embrace secure mobility in the workplace with the adoption of Blackberry devices for employees. With high demands for mobile productivity, employees have increasingly looked to iOS and Android devices for getting work done on the go.

While this is a positive development that brings a more powerful set of mobile capabilities, the introduction of consumer-first devices into the workplace has introduced new risks as more and more sensitive data is accessed on these devices.

While containers and MDMs were the first step in managing and siloing this data, financial services organizations are increasingly adopting more robust mobile threat protection and data leakage prevention solutions to stay compliant. Below is an overview of specific regulations driving this trend forward.

Glossary of terms

1. **Financial Industry Regulatory Authority (FINRA):** A self-regulatory organization that regulates member brokerage firms and exchange markets in the United States. FINRA requires firms to make sure that when a BYO program is in place, employees are able to separate their personal and business communications.
2. **Gramm-Leach-Bliley Act (GLBA):** Requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.
3. **Nonpublic Personal Information (NPI):** The Privacy Rule protects a consumer's NPI, defined as any personally identifiable financial information that a financial institution collects about an individual in connection with providing a financial product / service, unless that information is otherwise "publicly available."
4. **Federal Financial Institutions Examination Council (FFIEC):** A U.S. government interagency body that, among other responsibilities, prescribes standards and principles to help make banks more resilient to cyber attacks
5. **Financial Services Information Sharing and Analysis Center (FS-ISAC):** A non-profit organization that provides a central resource for sharing information on cyber threats in the Financial Services industry.

Some example mobile scenarios for Financial Services organizations:

- Banks / tellers using iPads/tablets to check in customers
- Employees / executives attending industry conferences where they could be a targeted victim of man-in-the-middle attacks
- Overly permissive apps like flashlight apps that have access to device contacts - potentially exfiltrating a consumer's personal contact information (NPI)
- App-based threat resulting from an employee downloading/sideloading an application onto their device
- Sharing financial spreadsheets/important company documents via Dropbox

GLBA

Who does GLBA affect?

The Gramm-Leach-Bliley Act affects any financial institution within the United States and applies to any mobile device that accesses nonpublic personal information, including:

- Individual names
- Social Security numbers
- Credit or debit card numbers
- State Identification numbers
- Driver's license numbers

How does Lookout help financial services organizations address GLBA requirements?

GLBA states the following regarding nonpublic personal information (NPI):

15 U.S. Code § 6801

Protection of nonpublic personal information:

(a) Privacy Obligation Policy - It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) Financial Institution Safeguards - In furtherance of the policy in subsection (a), each agency or authority described in section 6805(A) of this title, other than the Bureau of Consumer Financial Protection, shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards--

(i) **To insure the security and confidentiality of customer records and information;**

(ii) **To protect against any anticipated threats or hazards to the security or integrity of such records; and**

(iii) **To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer**

Source: https://www.law.cornell.edu/uscode/text/15/6801

Lookout protects against threats to the security of your nonpublic personal information

Lookout provides visibility into mobile risks that compromise the integrity of NPI, including unauthorized access to customer records. These risks can be seen across the primary mobile threat vectors: apps, network, and the device.

- **APP-BASED RISKS:** Malware that can potentially infect and steal customer data off employees' devices. Lookout also provides visibility into data leaking apps that send sensitive data, such as customer contact data to foreign servers or unsanctioned cloud storage providers like Dropbox.
- **NETWORK-BASED RISKS:** Network threats such as man-in-the-middle attacks where a user's data is intercepted in transit. Through a man-in-the-middle attack, an attacker can steal company login credentials from mobile productivity tools, which could lead to a larger enterprise attack that compromises customer data.
- **DEVICE-BASED RISKS:** Detection of advanced operating system compromises beyond what an MDM or container would detect, such as the recent Pegasus zero-day threat. These threats are effectively a "full take" of data from the device, bypassing platform security controls.

FFIEC - IT Examination Handbook

The handbook includes guidlines for protecting information assets within financial institutions. As more sensitive information flows through mobile devices, the below guidelines should be taken into account.

Quarantining Devices	This section of the handbook discusses the quarantine of devices that may potentially be connected to malicious code. "Quarantining a device protects the network from potentially malicious code or actions."
Preventing Network Attacks	Unauthorized devices can potentially connect to the network, perform man-in-the-middle attacks, or connect to other wireless devices. Examples of controls to mitigate this risk include: "Monitoring and responding to unauthorized wireless access points and clients"
Malicious Code Prevention	Host Level: • Host hardening, including patch application and security-minded configurations of the operating system (OS), browsers, and other network-aware software. • Host IPS, including anti-virus, anti-spyware, and anti-rootkit. Rootkits can enable the hiding and surreptitious execution of malicious code. • Software that limits application calls to the OS to the minimum necessary for the application to function. • Integrity checking software, combined with strict change controls and configuration management. • Application of known-good configurations at boot-up. • Periodic auditing of host configurations, both manual and automated. Network Level: • Proxy servers that inspect incoming and outgoing packets for indicators of malicious code and block access to known or suspected malware distribution servers. User Level: • User education in awareness, safe computing practices, indicators of malicious code, and response actions. Source: http://www.isaca.org/groups/professional-english/it-audit-tools-and-techniques/groupdocuments/information_security.pdf

The FFIEC also has a Mobile Financial Services Guide which discusses:

- Mobile financial services (MFS) technologies
- Risk identification
- Risk measurement
- Risk mitigation
- Monitoring and reporting

Source: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-e-mobile-financial-services.aspx

Lookout helps financial institutions follow the guidance of the FFIEC IT Booklet by alerting users and admins in real-time when malicious activity occurs, such as *malware or man-in-the-middle attacks*. With an endpoint app that sits on the user's device, Lookout identifies the risks on the mobile device and educates the user on what the risk is and how they can mitigate the threat. Lookout also allows admins to have full visibility over their mobile fleet and with our detection of advanced **app, OS, and network**-based threats, we ensure that mobile devices in your company's network are up to date and safe.

Lookout also partners and integrates with leading EMM solutions, including Microsoft EMS, AirWatch, and MobileIron to enable seamless deployment and activation of the Lookout app, and robust conditional access controls upon Lookout threat detections.

Financial Services - Information Sharing Analysis Center (FS-ISAC)

In their best practices guide for financial institutions, FS-ISAC borrows the definition of malware as defined by National Institute of Standards and Technology (NIST) where malware is “a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system.”

FS-ISAC- “Best Practices for US Financial Institutions: Reducing Risks Associated with Destructive Malware”

Fundamentally, a financial institution should implement processes and controls centered on five core elements:

1. Identify - Gain situational awareness by identifying critical data, backup processes and systems in the organization that is necessary for critical business functions, where it comes from, where located, and where used. Having a thorough knowledge of solution components, training, vectors, detection, technology, ongoing risk assessments, monitoring, information sharing and incident response keeps the enterprise in a continuous state of alert and prepares an organization to take action promptly.
2. Protect - From network and endpoint security to system redundancy and backup, to reputation management, a variety of controls are necessary for a comprehensive and robust security framework to protect corporate data and personally identifiable information.
3. Detect - Speed is essential in detecting malware when it enters a key environment, understanding the context, determining whether it is destructive in nature and quickly assessing the full potential impact.
4. Respond - In the event of unauthorized access, the financial institution’s computer systems could potentially fail, and confidential information could be compromised. Management must decide how to properly protect information systems and confidential data while also maintaining business continuity.
5. Recover - Organizations need to adjust their cyber incident response processes and playbooks to prepare for a destructive malware scenario where there is the potential of catastrophic business impact. Organizations need to update mitigation strategies and align multiple parts of the organization - including the executive team, communications teams, customer-facing departments and business partners.

Source: https://www.fsisac.com/sites/default/files/news/Destructive%20Malware%20Paper%20TLP%20White%20VersionFINAL2.pdf

How Lookout and MDM can help

Lookout Mobile Endpoint Security integrates with leading mobile device management solutions (MDM) to help financial services institutions comply with regulations such as GLBA and stay in compliance with rules set by agencies such as FINRA.

MDM	LOOKOUT
Comprehensive device management	Protection against app-based threats
Separation of personal and enterprise data	Detection of advanced jailbreak/root
Seamless access to enterprise apps with SSO	Detection of network-based threats
Unified policy management	Control of app data leakage to ensure compliance
Secure mobile content distribution	Ensure OS and devices are up-to-date
DLP for email, content, and apps	Custom remediation policy across threat types

More details on how Lookout mitigates risk on mobile devices:

- Protection against app-based threats. Lookout provides visibility into apps that leak data or even contain malware such as trojans and spyware in order to protect nonpublic personal information and corporate data.
- Detection of advanced jailbreak/root. MDMs have basic detection of jailbroken and rooted devices, but only Lookout detects advanced operating system compromises beyond what an MDM or container would detect, such as the recent Pegasus zero-day threat.
- Detection of network-based threats. As employees are working on the go, Lookout watches for connections to insecure wi-fi and cellular networks to help maintain the integrity of user credentials and corporate data being accessed by your employee's devices.
- Control of app data leakage. The Lookout solution allows institutions to set policies to control data leakage and remain in compliance with regulations and internal audits.

Embracing mobility while staying compliant

Progressive organizations are embracing smartphones and tablets in the workplace to enable more productivity from employees. As more sensitive data flows through these endpoints, financial services organizations are looking to solutions that provide visibility into emerging risks on this platform to comply regulatory and organizational security policies.

To learn how Lookout can help your organization stay compliant while enabling mobility within your organization, contact us at info@lookout.com