The Basic Components of an Information Security Program

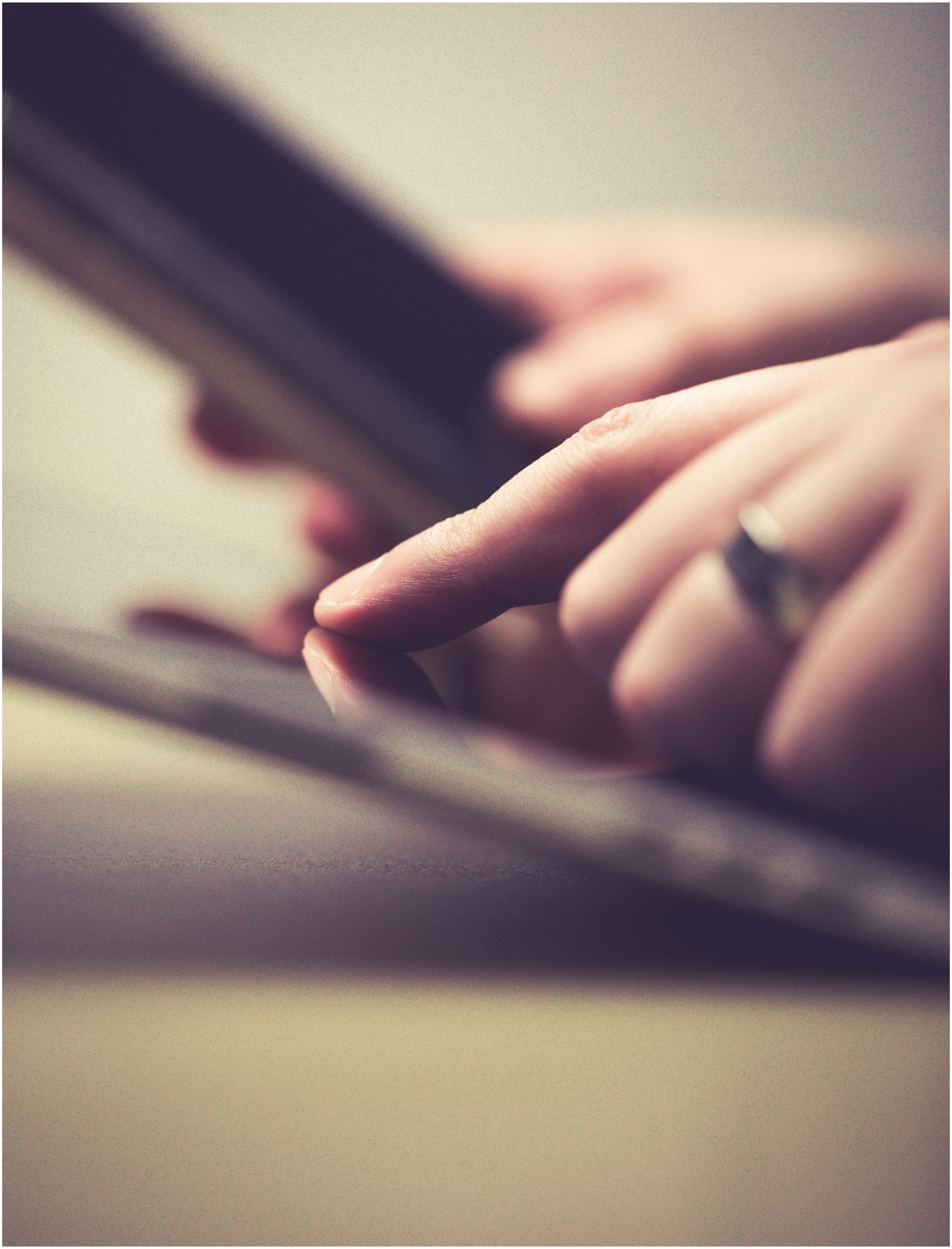
MBA Residential Technology Forum (RESTECH) Information Security Workgroup

MBA.ORG

MBA
MORTGAGE BANKERS ASSOCIATION

Although significant efforts have been used in preparing this guide, MBA makes no representations or warranties with respect to the accuracy and completeness of the contents. If legal advice or other expert assistance is needed, competent professionals should be consulted.

Table of Contents



Preface

The purpose of this document is to provide mortgage industry professionals with a succinct overview of the information security risks that affect our industry along with explanations of the basic components of an information security program intended to help manage those risks. Our focus in writing this document is on the small and medium size businesses that may not have the resources to effectively evaluate all the laws, regulations, regulatory guidance, security frameworks, and best practices that have been issued by various government or private entities. This guide is intended for informational purposes only and does not constitute, and should not be construed as, legal advice. Rather, this guide is intended to highlight recognized components of a basic program for managing information security-related risks of companies doing business in the mortgage industry. This guide is not intended to provide a mandatory standard of care for the industry. Every business needs to evaluate based on its own circumstances the appropriate course of action to develop best practices.

Although this guide can help you understand the general subject matter, it should not be construed as replacing guidance from your corporate risk management and legal counsel, and other professionals. While many State and Federal regulations require management to be involved; final decisions relating to risk and security practices should remain with the appropriately assigned individuals within each company.

This guide borrows from the *NIST Small Business Information Security: The Fundamentals* document issued in November 2016. We believe that alignment with NIST is important as a result of the issuance of the NIST Cybersecurity Framework. The authors choose to align with the terminology used by NIST, including the 4 levels of maturity, to avoid unnecessary confusion. This guide contains references to the Core Functions of the Cybersecurity Framework as appropriate (see Appendix A for more detail).

Each of the sections of this document that covers the components of a security program is prefaced with terms used to identify the five NIST Framework Core Functions. These terms are "identify," "protect," "detect," "respond," and "recover." These terms are used to help describe the intent of the specific security practice.

There are multiple information security standards and frameworks available to assist companies in managing information security risk. In addition to the previously mentioned NIST Cybersecurity Framework, the SANS Critical Security Controls for Effective Cyber Defense, the ISO 27000 family of standards for information security management systems, and the ISACA Control Objectives for Information and Related Technology (COBIT) Framework all provide guidance for an effective information security risk management program.

1

Introduction

The financial services industry plays a vital role in our economy. It provides financing for millions of consumers who want to own their own homes, as well as for commercial and multifamily properties. The industry acquires various forms of non-public information from consumers in order to provide financial services, and maintains sensitive contracts, business secrets, and other information. The existence of all this information makes our industry a target for bad actors. As a result of its economic importance and the sensitive information it creates and stores, the financial services industry has been designated as one of the sixteen critical infrastructure sectors in the United States.

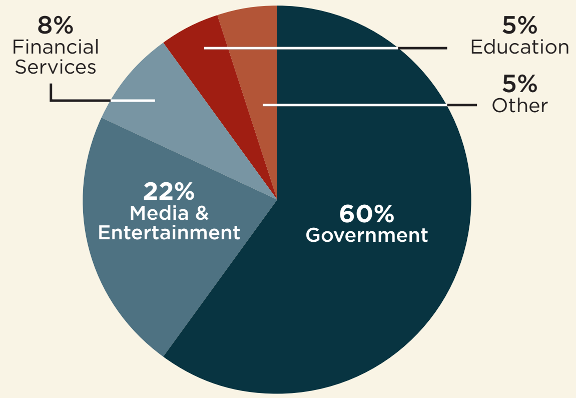
This designation means that in addition to the existing regulatory oversight, several additional government agencies monitor the risks to the industry while also working closely with the industry to identify new threats as well as new practices to protect it.[1] For industry participants, this means additional resources to assist with managing security issues. It also means that federal and state agencies are issuing regulations and guidelines to be followed. It can be difficult to keep current with the various edicts that may come from multiple sources, and for many smaller entities it can be overwhelming. The volume of guidance may create paralysis for small players, resulting in minimal or no action on their part.

The importance of managing information security risks has never been greater. The *Verizon Annual Data Breach Report,*[2] highlights the risks financial services organizations face. The Report finds that 8% of all cyberattacks had confirmed data and/or financial loss and of those, 43% impacted small and medium sized financial services companies.

Why should a mortgage business be interested in, or concerned with, information security?

The customers of mortgage businesses have an expectation that their sensitive personal information will be respected and given appropriate protection. The employees of a mortgage business also have an expectation that their sensitive personal information will be appropriately protected. Such information might be sensitive employee or customer information, confidential business research or plans, or financial information. Some of these information categories (e.g., health, privacy, and certain types of financial information) are subject to special, more restrictive regulatory requirements for information security protection. Failure to properly protect such information, based on the regulatory requirements, can easily result in significant fines and penalties from the regulatory agencies involved as well as reputational damage. Potential customers may avoid a business that has been “hacked,” particularly if the media has reported the failure as being due to inadequate precautions.

CYBERATTACKS, BY INDUSTRY



[1] http://www.dhs.gov/critical-infrastructure-sectors

[2] https://enterprise.verizon.com/resources/reports/dbir/

Current and/or potential business partners also have their expectations of the status of information security. These business partners want assurance that their information, systems, and networks are not put "at risk" when they connect to and do business with another company. They expect an appropriate level of security in an actual or potential business partner — like the level of security that they have implemented in their own systems and networks.

Some of the information used in your business needs special protection for one or more of the following reasons:

- Confidentiality, to ensure that only those who need access to that information to do their jobs have access to it;
- Integrity, to ensure that the information has not been tampered with or deleted by those who should not have had access to it; and
- Availability, to ensure that the information is available when it is needed by those who conduct the organization's business.

We recommend that all institutions have an information security program in place as well as a regular self-assessment of the program. We understand that some organizations have limited resources to adequately accomplish this, so while recommending that organizations incorporate all the sections in this document as part of a basic program, there are "absolutely necessary" steps that most regulators and standards organizations regard as critical and that the authors believe should be made a priority. Most of these items can be put in place with a relatively small budget with minimal resources. In addition, we recommend that senior management prioritize the importance of corporate security and encourage its continued development.

It is not possible for any business to implement a perfect information security program, but it is possible (and reasonable) to implement sufficient security to make it more difficult for bad actors to succeed in obtaining unauthorized information from your company. The remainder of this document will discuss the important practices that should be in place for all financial institutions and the entities that provide services for the industry.

Laws and Regulations for Information Security

2

The development of a corporate information security program is necessary to manage risks inherent in the use of technology. These risks, and the need to effectively manage them, exist regardless of any laws, regulations, and guidance issued by federal and state governments and regulatory bodies. At the same time, companies need to ensure that their organizations are aware of regulations, develop policies to incorporate the requirements, and develop mechanisms to ensure compliance with the regulations. The risks to your organization of noncompliance are criminal, civil, statutory, regulatory or contractual penalties. The development and execution of organizational security policies and standards will maximize compliance and minimize the resources your organization must spend to undergo internal and external compliance audits.

Information Security is one of the greatest risks facing the mortgage and financial services industries. State and Federal level regulators continue to release new or revised regulations and guidance. Below are a number of key regulations that have been issued as of the writing of this document. Your legal and compliance teams should review each of the topics to ensure you comply with applicable regulations as they pertain to your business and the areas in which you are licensed to operate.

Privacy and Security

Gramm-Leach-Bliley Act [Section 501(a) and 501(b)][3]

Information Security Breach Notification Legislation[4]

Federal Trade Commission Identity Theft Red Flags Rule[5]

California Consumer Privacy Act (CCPA):
Effective January 1, 2020[6]

General Information Security

Federal Financial Institutions Examination Council (FFIEC) Guidelines[7]

Federal Deposit Insurance Corporation: PR-28-2014

Cybersecurity

FINRA Cybersecurity Practices[8]

New York State Department of Financial Services (NYDFS.NYCRR.500)

Vendor Management

OCC Bulletin 2013-29

CFPB Bulletin 2012-03

Federal Reserve — Guidance on Managing

Outsourcing Risk (SR letter 13-19 / CA letter 13-21)

General Data Protection Regulation (GDPR): Effective May 2018, this data protection regulation was enacted within the European Union with a focus on protecting the privacy of EU citizens. The mandate impacts lenders who are specifically targeting, processing, hosting and or housing EU citizen data. Fines can be up to 4% of annual worldwide gross revenues.

[3] https://www.ffiec.gov/exam/infobase/documents/02-con-501b_gramm_leach_bliley_act-991112.pdf

[4] All fifty states and, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.

[5] https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business#how

[6] https://www.caprivacy.org/about

[7] https://ithandbook.ffiec.gov/it-booklets/information-security.aspx

[8] http://www.finra.org/industry/small-firm-cybersecurity-checklist

3

First Priority Cybersecurity Practices

The following are the highest priority cybersecurity actions that a business should take to protect its information, systems, and networks. These practices will help your organization to identify and understand the value of your information and systems, protect those resources, detect possible incidents that could compromise them, and help your organization to respond to and recover from possible cybersecurity events.

3.1 MANAGE RISK

CYBERSECURITY FRAMEWORK (CF) FUNCTION(S): IDENTIFY

Participants in the mortgage industry need to identify and manage risks relating to information security. Risk Management is the process of identifying the risks that your business is exposed to and managing that risk by implementing protective measures to limit the impact of the identified risks. Effective risk management includes an assessment of the risks unique to each company, the identification of the vulnerabilities of your company, and the development of a risk management plan that addresses those risks.

Risk management is an ongoing and evolutionary process. This means that risk management is not static. Risks change as your company evolves and as bad actors change their methods and tools of attack. Companies can start small and evolve their risk management process as they gain experience. The process can often be accelerated by engaging with external security providers. The critical point here is to start the process of developing a risk management plan if you have not already done so, and to keep improving once you have a plan.

Multiple frameworks exist to help you manage information security risks. The more well-known frameworks are the NIST Cybersecurity Framework[9] and ISO 27000 series.[10] These frameworks are very large and comprehensive. If you are just beginning the path towards the development of a corporate security risk management plan, you should not expect your plan to have all the components of the framework on day one.

The best place to start is by performing a risk assessment. Perform an inventory of the threats that your organization is facing regarding your information. A threat is a negative event that could happen to an information system or process. Examples could be ransomware infecting your critical servers and affecting the availability of those systems, or an account takeover of one of your employees that would allow access into critical systems. Once you have an inventory of the threats, think about the likelihood of those threats happening and the impact to your business if the threat was realized. Using likelihood and impact as your guides, each of the threats can be rated for severity and categorized as risks.

3.2 PROTECT YOUR ENDPOINTS

CF FUNCTION(S): PROTECT

Your organization has many “endpoints” that need protection from unauthorized access, malicious software, and other threats. An endpoint is any device on your network like a workstation, laptop, server, or even a mobile device like a tablet or smart phone. Threat actors try to attack your endpoints with malicious software that enables them to perform a variety of actions to harm your organization. Viruses, malware, trojans, ransomware, and many others are all examples of malicious software. In order to best defend against these threats for when your devices are both on and off your network it’s best

[9] http://www.nist.gov/cyberframework/

[10] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

to install endpoint security software on all the devices in your organization. It's also a requirement of many state and federal regulatory guidelines.

It's important to note that due to the ever evolving threat landscape traditional anti-virus software alone isn't enough to protect endpoints. Endpoint security software encompasses traditional anti-virus, but also includes several components and functions like a local firewall, device encryption, and even patch management to form a multi-layered defense.

In order to provide an additional level of insight and security, many vendors have begun offering an important new capability called Endpoint Detection and Response (EDR) solutions. These solutions protect systems by monitoring the behavior and actions taken on the device itself to identify and automatically stop malicious behavior. It's important to remember there are many endpoint security vendors on the market today. Make sure to choose one that provides a comprehensive security solution, preferably with an EDR component, that also supports the variety of devices in your organization as well as is compatible with your size and complexity.

Additionally, lenders are becoming increasingly more decentralized with employees working from anywhere at any time. This means that more frequently your organizations assets are on other networks that are out of your control. Similar to installing strong anti-malware software on your endpoint devices to prevent software related threats, the utilization of an endpoint firewall should also be considered to protect against unwanted network related threats.

Bring Your Own Device (BYOD) allows employees to use personal devices (phones, tablets, computers, etc.) to access corporate resources. It is intended to allow employees to use any device they choose to perform their work functions. Businesses need to think carefully about BYOD programs, and if they elect to allow such a program, they need to put in place appropriate policies and procedures to tackle these issues and minimize the risks.

Companies should provide guidance to users on how they can use their own devices to process corporate and personal data. It should also be clear to employees that they can only process corporate data for approved corporate purposes. It is recommended to have a written agreement with employees that covers the following:

- Ensure that end users are responsible for backing up personal data

- Clarify lines of responsibility for device maintenance (including a remote wipe process), support and costs

- Require employees to remove apps at the request of the organization

- Disable access to the network if a blacklisted app is installed or if the device has been jail-broken[11]

- Specify the consequences for any violations of the policy

- The endpoint firewall similar to the one you have behind your Internet router is designed to regulate the inbound and outbound traffic to the device over a given network connection. The end result is blocking targeted attacks when utilizing endpoint devices on networks outside of your organization.

- Many modern operating systems including Windows 7, Windows 10 and Mac OS X have built in device level firewalls that can be centrally managed. These firewalls simply need to be enabled to increase protection of your organization's assets.

3.3 PROTECT YOUR INTERNET CONNECTION

CF FUNCTION(S): PROTECT

Internet connectivity is the life-blood of any modern lending organization. As employees become more mobile, increasing efficiency and employee satisfaction, it also increases your overall cybersecurity risk. The Internet can provide access into your environment by others; enabling threat actors to utilize these same connections to do harm to your organization.

Most organizations have broadband access to the Internet. Due to the always "on" nature of this utility it is critical to install and maintain a hardware firewall between your internal network and the Internet. These devices come in many shapes and sizes, it is important to remember to find one that has some form of active threat prevention solution to support your organization's needs.

The administrative password must be changed upon installation of the firewall and on a periodic basis there after. Best practice is to change the administrator's login name as well. You should also configure a default "deny" rule — this rule ensures that internet traffic is denied access if it does not match the firewall's rule configuration.

For Internet based applications both behind your firewall as well as in the cloud, it is also recommended that you "geo-fence" your organization. This is a method of denying access to your published resources from Internet connections outside

[11] Jail-breaking a device is a way of removing restrictions a mobile carrier put on the phone to prevent you from being able to do certain things with it.

of the United States. It is rare that any lender needs to enable support for access outside of the United States in countries such as Russia or China.

Due to the mobile nature of today's employees, consideration must be given to how employees will access your company's systems remotely. They will need a secure way to do so. Encourage your employees not to use public Wi-Fi. If use of public Wi-Fi is a necessity, ensure that employees utilize VPN software. You should also educate employees to use TLS / encrypted websites, and show them how to do so. Where possible, organizations should try to limit VPN access to their network to business-only purposes.

Many of the malicious attacks today are through attempting to trick employees to click on a link or download something from a malicious site. Use of an Internet filtering solution can help prevent these threats from being successful. Internet filtering can not only prevent malicious cybersecurity incidents but also unsafe workplace incidents due to inappropriate content, as well.

3.4 PATCH YOUR OPERATING SYSTEMS AND APPLICATIONS

CF FUNCTION(S): PROTECT

Security patching has been a common cybersecurity threat mitigation technique since the late 1990s. However, software vulnerabilities continue to be one of the leading causes of cybersecurity breaches and information compromise. Successful attacks in recent years were the result of poor software patch management processes.

Software providers including operating system and 3rd party software providers regularly release patches and updates to their supported products to correct security problems and to improve functionality of their software. Since bad actors monitor these updates and move quickly to exploit published vulnerabilities, it is important to update your systems as soon as the updates are released. The vulnerabilities will continue to exist inside your organization until you update the appropriate program with the patch. It is critically important to apply the patches as soon as possible.

State and federal compliance legislation require that you develop and implement a corporate standard for deploying patches to all systems in a timely manner. Most modern operating systems and applications include the ability to automatically check and apply updates, enabling you to have a built in option to secure your systems. However, it is still considered best practice to deploy a centralized endpoint management solution to patch and deploy software within your organization.

It is important to ensure that you are purchasing and deploying supported software. For example, Windows 7 is reaching its supported end of life in 2020, but still accounts for nearly 30% of all Windows systems deployed across companies in 2019. Organizations should have roadmaps to periodically check the lifecycle status of their organization's software to ensure they have a plan in place to upgrade as software reaches it's end-of-life.

Organizations should perform periodic vulnerability scans of their devices. While not only required by state and federal regulation, these scans produce a comprehensive overview of the configuration and patch efficacy within your environment. You can think of this as a quality control component for your patch management program.

3.5 MAKE BACKUP COPIES OF IMPORTANT BUSINESS DATA/INFORMATION

CF FUNCTION(S): RESPOND, RECOVER

Computer hardware fails, employees make mistakes, and malicious programs can destroy data on computers. Ransomware attacks, where malicious programs encrypt an organization's data and hold it for ransom, continue to be a problem for organizations of all size and complexity. Ransomware costs were estimated to be $8B in 2018.[12] Good backups can aid in reducing the risk and impact associated with ransomware.

To combat data loss, all consumer and other important business information should be backed up to ensure you can recover quickly from any event causing data loss. Without data backups, you can easily get into a situation where you must recreate your business data from paper copies and other manual files. Common digital data within an organization today includes (but is not limited to) word processing documents, electronic spreadsheets, databases, financial files, human resources files, accounts receivable/payable files, and other information used in or generated by your business.

The use of automated processes and cloud backup solutions are increasing in popularity and function. Many security software suites offer automated backup functions that will back up your data on a regular schedule. Backups should always be stored off-site to prevent them from being impacted by the same event that rendered your data unavailable. If something happens to your office (fire, flood, tornado, theft, etc.), you can restore your business operations using your backup data and replacement computers.

[12] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018/

Organizations should test backups regularly, including full restorations to ensure that the data you have backed up is actually usable. Nothing is worse than having a backup copy that can't be restored when you need it! Offsite backups should be appropriately secured so that only authorized personnel can get access to them. Backups should also be encrypted so that they will not cause a data breach if lost or accessed inappropriately.

3.6 CONTROL PHYSICAL ACCESS TO YOUR COMPUTERS AND NETWORK COMPONENTS

CF FUNCTION(S): PROTECT, DETECT

Physical security is the protection of facilities, personnel, hardware, networks, software, and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. It answers the question, "How do you physically protect these from harm?"

Controlling access to your systems and networks also involves being fully aware of anyone who has access to the systems or networks. This includes cleaning crews who come into the office space at night to clean the office and remove the trash. Criminals often attempt to get jobs on cleaning crews for the purpose of breaking into computers for the sensitive information that they expect to find there. Controlling access also includes being careful about having computer or network repair personnel working unsupervised on systems or devices. It is easy for them to steal private/sensitive information and walk out the door with it without anyone noticing anything unusual.

No one should be able to walk into your office space without being challenged by an employee. This can be done in a pleasant, cordial manner, but it must be done to identify those who do not have a legitimate reason for being in your offices. "How may I help you?" is a pleasant way to challenge an unknown individual. If logistically feasible, you may also want to consider limiting access to your offices beyond the public areas—the reception area and the conference rooms where customers meet with your employees.

Facility

Facility access should be always be protected by a lock. Depending on the size of the facility, a fence or other perimeter structure may be sensible for protecting a collection of buildings.

Personnel

Having a process in place to only allow authorized individuals access to facilities is a first step in protecting personnel. This process can be as simple as a single point of entry to the facility where individuals will have to be recognized or documented prior to entry. For small businesses this may simply be a locked door monitored by a receptionist with a sign in sheet. Access to that door can be granted by a physical key or an electronic key. As the business matures an electronic system of controlling access and logging entry should be put in place to improve the security posture of the company.

a. Where practical, all visitors who are expected to access areas other than common space or are granted access to office space containing nonpublic personal information should be required to sign-in at a designated reception area where they will be assigned a visitor's ID or guest badge and escorted at all times. Visitors should be required to wear the visitor ID in a plainly visible location on their body, unless escorted at all times.

b. Where practical, all visitors should be restricted from areas where files containing nonpublic personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing nonpublic personal information are stored.

Hardware

Employees should be instructed to secure laptops and desktops when they are not in use. A screen lock that requires a password to unlock is a simple form of protection. Having equipment locked to the desk with a cable or secured in a locked drawer or cabinet for longer durations when not in use is a good practice.

Networks

Having your network equipment locked in a secure room or inside a locked rack improves the security for your network hardware. Extending this to only allow privileged users access to the room or rack and a monitoring system with a log of who accessed the equipment and when they accessed it improves your security. This can be as simple as a notebook or as sophisticated as electronic keys for access that register and monitor the entry and time the equipment is access along with a video record of the access. Move from the simplistic to more sophisticated methods as you develop your business.

3.7 SECURE YOUR WIRELESS ACCESS POINTS AND NETWORKS

CF FUNCTION(S): PROTECT

Wireless networking is one of the most common forms of connectivity today, due to its ease of implementation and the flexibility it provides users. If not configured appropriately, however, it can also be a significant security risk. Wireless networks are accessible to anyone within receiving range of the signal. Key items to consider around Wireless networking include:

- Use a strong encryption method. Networks should utilize at least Wi-Fi Protected Access 2 (WPA-2)
- Always change the default settings and passwords for a wireless device
- Consider disabling the broadcast of your network's SSID, so casual observers will not detect the wireless network's existence
- When configuring a modern Wi-Fi network ensure that it is segmented from other physical areas of your environment
- Guest access should be separate from "corporate" level access
- Ensure employees are trained and aware on how to secure themselves when using public Wi-Fi at places such as coffee shops and hotels
- Change the wireless access password frequently

3.8 TRAIN YOUR EMPLOYEES IN BASIC SECURITY PRINCIPLES

CF FUNCTION(S): PROTECT

The biggest risk in information security is people. Employees, often inadvertently, create risks for your company. Information security training is an essential function to protect your company. Many security issues originate from employee actions, often inadvertently. Bad actors target employees through various means to leapfrog other security measures. Hackers attempt to acquire sensitive information from your company by masquerading as a trustworthy entity in personal or electronic communication. These attempts will target employees with email attachments, emails requesting sensitive information, web links, popup windows, phone calls, or other forms of social engineering. Employees should be trained on how to identify these attempts and avoid them.

Training employees in the fundamentals of information, system, and network security is one of the most effective investments you can make to better secure your company. Regular training will help you develop a "culture of security" in your employees and in your business. At the conclusion of training, and on a periodic basis, employees should be requested to sign an attestation that they understand these business policies, that they will follow your policies, and that they understand the penalties for non-compliance. Consequences for violating business policies should be clearly communicated and understood across the organization.

Before being granted access to company computer systems, employees should be trained on your information security policies and their responsibilities to protect your sensitive business information. Training should tie into the job roles that the employee will be performing for the company, empowering them to be more effective in their day to day role.

Phishing, malware, ransomware, social engineering and wire fraud are the current hot spots to address for employee training.

Phishing

Email attachments, emails requesting sensitive information, and web links:

- For business or personal email, train your employees not to open email attachments or web links unless they are expecting the email with the attachment and they trust the sender.

- Beware of emails which ask for sensitive personal or financial information — regardless of who the email appears to be from. No responsible business should ask for sensitive information to be provided in an email.

Think before you click! Employees should not click on web links unless they are confident in the source or the message. Always hold the mouse pointer over the link and look at the bottom of the browser window to ensure that the actual link (displayed there) matches the link description in the message (the mouse pointer changes from an arrow to a tiny hand when placed over an active link).

If you are asked for your login username and password, make sure this is a normal process to launch an application that you have initiated. Phishing attempts sometimes present credible requests for a username and password. These have grown in sophistication by sending a request for your multifactor authentication. If you have not personally initiated the request for access to a system or application, do not grant access for multifactor authentication, enter your username or password.

Malware and Ransomware

Train your employees not to respond to popup windows requesting that they click "ok" for anything.

If a window pops up on your screen informing you that you have a virus or spyware and suggesting that you download an anti-virus or anti-spyware program to take care of it, close the popup window by selecting the X in the upper right corner of the popup window. Do not respond to popup windows informing you that you must have a new codec, driver, or special program for something in the web page you are visiting. Close the popup window by selecting the X in the upper right corner of the popup window.

Some of these popup windows are trying to trick you into clicking on "OK" to download and install spyware or other malicious code onto your computer. Be aware that some of these popup windows are programmed to interpret any mouse click anywhere on the window as an "OK" and act accordingly.

Social Engineering

Social engineering is a personal or electronic attempt to obtain unauthorized information or access to systems/facilities or sensitive areas by manipulating people.

The social engineer researches the organization to learn names, titles, responsibilities, and publicly available personal identification information. Then the social engineer usually calls an employee with a believable but made-up story designed to convince the person that the social engineer is someone in, or associated with, the organization and needs information or system access which the organization's employee can provide and will feel obligated to provide.

To protect against social engineering techniques, employees must be taught to be helpful but vigilant when someone calls in for help and asks for information or special system access. The employee must first authenticate the caller by asking for identification information that only the person who is in or associated with the organization would know. If the individual is not able to provide such information, then the employee should politely but firmly refuse to provide what has been requested by the social engineer. The employee should then notify management of the attempt to obtain information or system access.

Additional Hacker Tricks

Hackers are known to scatter infected USB drives with provocative labels in public places where their target business's employees hang out, knowing that curious individuals will pick them up and take them back to their office system to see what's on them. What is on them is generally malicious code which attempts to install a spy program or remote-control program on the computer. Teach your employees to not bring USB drives into the office and plug them into your business computers (or to take them home and plug into their home systems either). It is a good idea to disable the "AutoRun" feature for the USB ports (and optical drives like CD and DVD drives) on your business computers to help prevent such malicious programs from installing on your systems.

3.9 REQUIRE INDIVIDUAL USER ACCOUNTS FOR EACH EMPLOYEE ON BUSINESS COMPUTERS AND FOR BUSINESS APPLICATIONS

CF FUNCTION(S): PROTECT

Mortgage lenders have copious amounts of sensitive and important consumer data, so keeping it protected is not just a legal requirement, it is a major priority. A cornerstone in protecting the confidentiality and integrity of this information is to ensure that every user and application has an individual password that is sufficiently strong to be safe from guessing or hacking attempts.

Recent guidance around digital identities from the National Institute of Standards and Technology (NIST) recommends that organizations should focus on the adoption of Multi-Factor Authentication for all remote and sensitive data access.

Studies have shown that individuals often reuse passwords. For organizations that still utilize passwords, due care should be taken to educate employees on how to use unique passwords. In order to decrease the likelihood that the passphrase is written down, it should not be changed more than twice a year, and not require a mixture of different character types.

Organizations should educate their employees that should never share user accounts and passwords. Shared accounts and passwords invalidate the control intent served by passwords, since there is no way to track who was responsible for various actions. The communication of shared passwords between individuals also increases the risk that the passwords will be written down or included in emails, making those accounts further vulnerable to unauthorized access.

Lastly, if passwords are used within the environment, periodic password strength testing is recommended on a periodic basis to ensure accounts are properly secured.

3.10 DATA MANAGEMENT

CF FUNCTION(S): IDENTIFY, PROTECT, DETECT

Least privilege is the security principle that dictates giving each user the least access to data possible while still allowing them to complete their job effectively. By implementing least privilege a company better protects the sensitive information of its customers, company and partners by limiting the number of people who can access data and how users can take that information in and out of the company.

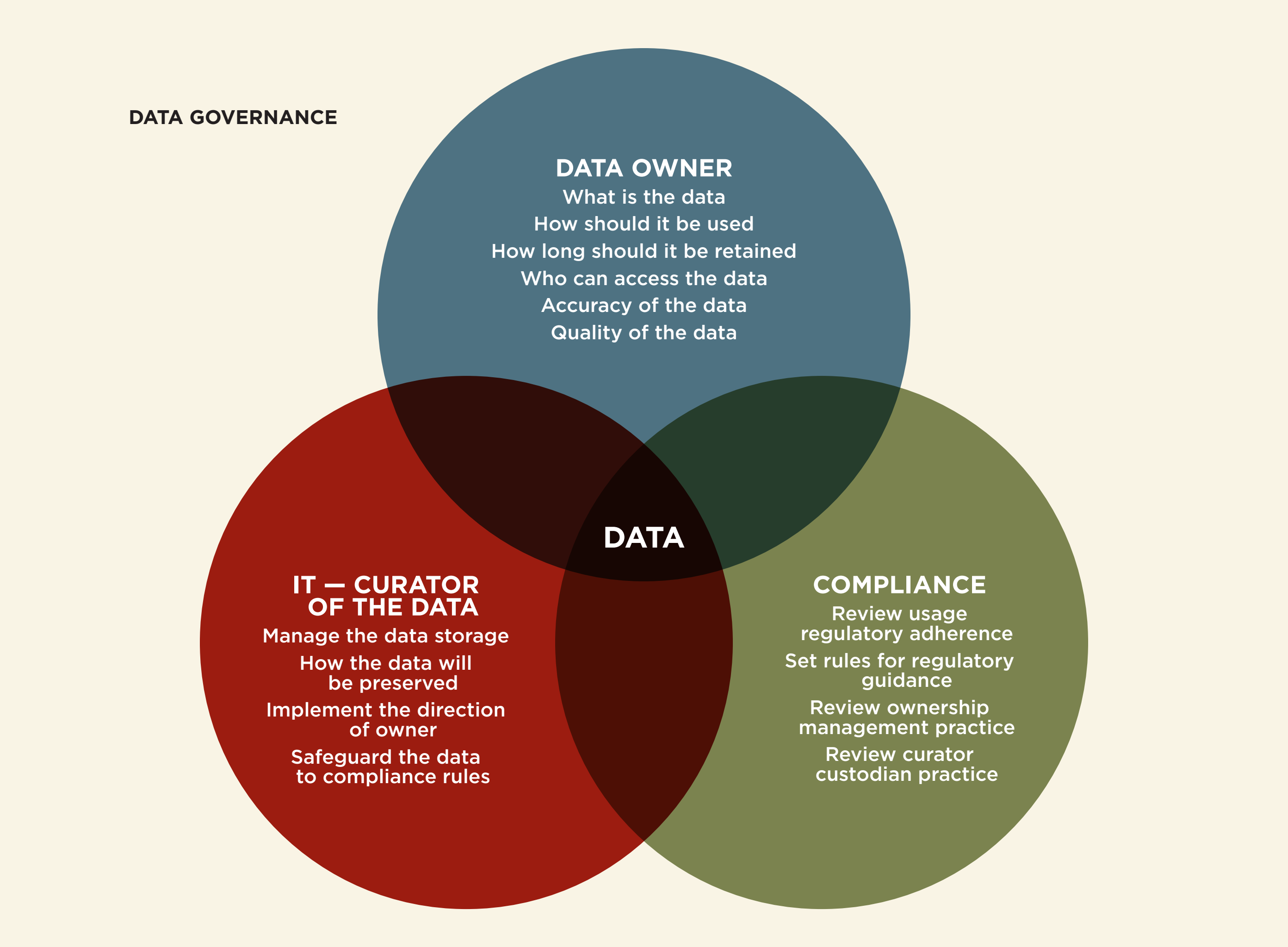
The unfortunate truth is that insiders—those who work in a business—are the source of many security incidents. The reason is that they are already known, trusted, and have been given access to important business information and systems. So, when they perform harmful actions (deliberately or otherwise), the business information, systems, and networks—and the business itself—suffer harm.

Companies should create roles within their organization and determine what the appropriate tasks for those roles are, then determine what level of access is needed to complete those tasks. Look to your asset inventory as a source for creating these roles and limiting access. Workflows of the business process will help identify the functions performed and who performs them. These also will help in development of the roles.

Defining roles and related access may appear to have only a data management and governance purpose. Yet from a business perspective, defining the roles to perform workflow tasks identifies personnel requirements that may currently be performed by an expensive person which could be assumed by a cheaper person. Refining the roles allows for moving the more experienced people into specialized tasks requiring more access and knowledge; and move less experienced people into general tasks requiring less access and knowledge. The role and workflow evaluations also allow the business to identify and address bottlenecks in the workflow process. This exercise becomes valuable to both improve the security posture and efficiency of operations.

Data Governance

The management of data includes both digital and physical data. Creating a system for Data Governance of company digital and physical data requires a well-defined set of process and procedures for Data Governance. Planning for Data Governance will require groundwork to build upon.


DATA GOVERNANCE
DATA OWNER
What is the data
How should it be used
How long should it be retained
Who can access the data
Accuracy of the data
Quality of the data
DATA
IT — CURATOR OF THE DATA
Manage the data storage
How the data will be preserved
Implement the direction of owner
Safeguard the data to compliance rules
COMPLIANCE
Review usage regulatory adherence
Set rules for regulatory guidance
Review ownership management practice
Review curator custodian practice

Data Classification

The asset inventory is a good tool to use in planning for data governance. Knowing what your data is and where it is stored is a good foundation. The creation of a set of classifications to focus the data governance effort is also a key component. These classifications should have at least a class for Personally Identifiable Information (PII), Company Confidential Information and Public Information. Class names like *RESTRICTED, CONFIDENTIAL* and *PUBLIC* can be attributed to these classes and should be defined for communication to all employees. Depending on the company maturity, additional data classes can be defined for refined governance.

Working with the asset inventory, these data classifications can be superimposed on data objects, applications, and locations. This will then allow the company to implement systemic controls over the data for governance control and maintenance. Implementation of systemic controls over unclassified data will be frustrating, inefficient and often lead to undesired results. The rules can only be applied to defined classes of data so undefined data sets will be somehow lumped into a general category which will either result in overcompensation or inadequate controls. Whenever faced with this choice choose overcompensation and work to refine the data set as business operations identify well defined subsets for classification.

Data Responsibility and Accountability

Governance of data should have a well-defined set of responsibilities and accountabilities. There are at least three actors in the governing of data, which are Data Owners, Compliance and IT.

The data owner is responsible and accountable for what the data is, how it should be used, how long it should be retained, and who can access it, along with the accuracy and quality of the data. Compliance is accountable and responsible for reviewing the data usage and setting rules for the data to align with regulatory compliance. Compliance also is responsible and accountable for monitoring the ownership management practices along with the custodian practices to ensure they align with the policy and procedures of the company. IT plays the role of the Curator of the data. They are responsible and accountable for the storage of the data, how it should be preserved (backups, reliability, redundancy and resiliency of the methods of storage). IT is also responsible and accountable for implementing the direction of the Data Owners for access control while safeguarding the data in alignment with Compliance policies.

Policies, Practices and Procedures from all these entities will help form the data governance access control process. These group’s responsibilities and accountabilities for the data will help refine the roles that will drive compliant access control to data and systems. If these roles are well defined and understood across the company, it makes governance and management of the data easier.

Access control can then have audit trails in place to track when access was given and to whom. Systems can be put in place for monitoring the use of the data by those that have been granted access. Temporal review of the access controls should be reviewed by the data owners to confirm that they agree with the entities that have access to the data for which they are responsible and accountable. This will provide a set of checks and balances to ensure that the data owners are managing the data properly, that the IT curators are only granting (or revoking) access in compliance with direction of the data owners or compliance and gives an audit artifact to compliance for evidence that they are monitoring the data governance.

3.11 LIMIT AUTHORITY TO INSTALL SOFTWARE

CF FUNCTION(S): IDENTIFY, PROTECT

As lending operations become larger and more decentralized, the standardization of systems and applications used within the organization becomes paramount. Both compliance and direct costs can be impacted when enabling employees to install software and or to have local administrator access. The growth of unauthorized applications within an organization can occur through the installation of seemingly simple applications and downloads; however, the installation of any software programs should be limited to those with proper training.

Providing local administrative privileges on the computer or within specific software applications can have dramatic compliance implications. Controls designed to enable organizations to meet regulations such as NYDFS.NYCRR.500 and GLBA can easily be bi-passed by users with local administrator control. Having local admin control can also significantly increase the likelihood of malware infection, including ransomware.

3.12 CREATE BUSINESS POLICIES RELATED TO INFORMATION SECURITY

CF FUNCTION(S): IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

Corporate policies clearly articulate acceptable practices and expectations for business operations. These policies are intended to provide guidance for employees to follow and to ensure consistency across the organization. Policies for information security have the same objectives, with the goal of protecting corporate information resources. We recommend that all companies have a written information security policy that is shared with all employees on a regular basis, reviewed at least annually, and updated as appropriate.

For companies that do not yet have an information security policy, it is recommended that you utilize an existing security framework as a starting point. Using a framework helps ensure you have a comprehensive policy set, with no major pieces missing, and it allows easier communication with third parties when you describe your approach. The most common industry standards for policies are the NIST Cybersecurity Framework, ISO 27001 and COBIT.

Policies for information, computer, network, and Internet security should communicate clearly to employees the expectations that the business management has for appropriate use. These policies should identify the information and other resources that are important to management and should clearly describe how management expects those resources to be used and protected by all employees. Policies should also reflect current practices or practices that are going to be put in place in conjunction with the policy. Having policies that do not reflect what is actually expected of personnel will cause confusion and can be problematic in the event of an audit by an external party, such as a regulator.

Policies should be clearly communicated to each employee, and all employees should acknowledge or sign a statement agreeing that they have read the policies, that they will follow the policies, and that they understand the possible penalties for violating those policies. This will help management to hold employees accountable for any violations. There should be penalties for disregarding policies, and those penalties should be enforced fairly and consistently for everyone in the organization.

3.13 EXERCISE DUE DILIGENCE IN HIRING EMPLOYEES

CF FUNCTION(S): PROTECT

Employee management includes the acquiring, managing and separation of personnel. These functions are often managed by an established Human Resources department in larger organizations. There are security aspects that need to be put in place by either Information Technology or another department within the organization. It is prudent for Information Technology to ensure that certain practices and procedures are in place someplace within the organization to be compliant.

Acquiring

When hiring a new employee, conduct a comprehensive background check before making a job offer. You should consider doing criminal background checks on all prospective new employees. According to your business's needs, the background check may include criminal, employment, educational, credit and other components commensurate with screening standards for the Financial Services industry.

Process and procedures for bringing on new employees helps standardize the process to make it repeatable and efficient to allow the employee to start producing. Well defined roles and responsibilities tied to access controls for systems, equipment and data expedites this process. This allows the employees to be consistently set up for success by supplying a constant user experience for each role and responsibility defined.

Managing

Managing the employee's access to equipment, software and data ties to the roles and responsibilities of the employee. As the employee moves from role to role in the organization a process and procedure of initiating changes in the access control mechanisms is required. Well defined roles and responsibilities become crucial in managing employees as the business grows.

Separation

Care should be taken with terminations of employment, both voluntary and involuntary. While using tact, terminations should result in prompt surrender of company-owned equipment, software and data. The email accounts of terminated employees who owned their own phones and tablets under Bring Your Own Device (BYOD) policies should be removed from those devices.

The process and procedures need to be created to provide a reliable repeatable method of ensuring separated employees have surrendered equipment, software and data.

3.14 GET HELP WITH INFORMATION SECURITY WHEN YOU NEED IT

CF FUNCTION(S): IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

Since 2017 we have seen a rapid growth in the number of state and federal level cybersecurity laws on the books. Each of these different regulations requires specific cybersecurity controls to be deployed. The existing cybersecurity skills shortage makes it quite difficult for lenders to find and retain an expert in every business and technical area. Therefore, when you need specialized expertise in information/computer/network security, you should always get help.

When you get a list of service providers, prepare a request for proposal and send it out as a set of actions or outcomes that you want to receive. For example, if you need someone to help with application security, look for resources that specialize in application security. If you need additional help monitoring cybersecurity threats consider joining one of the many different cybersecurity communities. Always carefully examine and review the deliverables from each firm responding to your request. Research each firm's past performance and check its references carefully, make sure they are not only aware of the specific area you need help in but are also familiar with your business as well as the compliance regulations that you face. Request a list of past customers and contact a sample to see if the customer was satisfied with the firm's performance and would hire the firm again for future work.

Lastly, if a specific regulation is demanding you have a specific skill set on staff, such as NYDFS.NYCRR.500, look for a fully qualified vendor that you can potentially outsource these needs to. It is typically much more economical than attempting to find and retain the specific skill to develop and run your cybersecurity program.

3.15 PERFORM AN ASSET INVENTORY (AND IDENTIFY SENSITIVE BUSINESS INFORMATION)

CF FUNCTION(S): IDENTIFY, PROTECT

To protect your assets, you must first know what they are and where they reside. Data, equipment, software and personnel are all assets. It is easy to understand keeping a list of your employees and contractors for your personnel asset inventory. Equipment is the next easiest to comprehend because people and equipment have a physical form and software has become tangible through productization. Counting and locating the equipment and software is easily grasped. Data is abstract and becomes more difficult to comprehend for inventory.

Personnel

Keep a list of your people and where they typically work. This can be simply done as a list for smaller companies which will quickly be input into a payroll or other similar system as the company grows.

Equipment

Inventory of the equipment is both a security and business sensible concern. Growing companies often overlook the value of having an inventory of their equipment. Having a list of the equipment that is purchased and a description of that equipment becomes useful for the security aspect of managing risk but also allows you to aggregate the costs for insuring, replacing and depreciating that equipment for the business aspect. As the business grows, the location of the equipment grows along with it. Adding physical locations and moving to hosted applications extends the locations to the cloud.

The cloud presents a hybrid concept of equipment that needs to be inventoried. Just as physical servers and network equipment needs to be counted and tracked, virtual equipment needs to be inventoried. These may not be capital assets but operational assets that your company needs to perform. The security aspect of this inventory will allow putting monitoring, maintenance and compensating controls in place for all the equipment assets. The business aspect of the equipment inventory allows you to manage the cost of the monitoring, maintenance and operation of that equipment.

When disposing of old business computers, remove the hard disks and destroy them. You should take your hard disks to companies who specialize in destroying storage devices such as hard disks. The company should provide a certificate of destruction upon completion.

When disposing of old media (CDs, floppy disks, USB drives, etc.), destroy any containing sensitive business or personal data.

Software

Software used in operations is a significant cost of doing business. Knowing where software assets are and counting them allows for the management of this significant investment. The inventory of equipment will assist in the development of the software inventory. Equipment is often useless unless there is a software component that accompanies it. Knowing the type of software installed on each piece of equipment along with the version of that software is valuable. From a security aspect, it allows the identification of outdated software or software that needs security patches. From a business aspect, it allows for the identification of unneeded or duplicative software that costs money to maintain.

Data

Data is the most difficult to grasp as an asset to inventory. Yet, data is the most valuable asset to manage in order to effectively grow the business. Begin to think of how you collect and store data for the business process. When is data stored on a workstation? When is it saved to a filesystem? When is data stored in an application? When is data physically collected and where is it stored? These questions will allow you to then ask what type of data is collected and stored for each scenario.

These answers will help you in your data inventory process. Knowing that data is stored in a workstation, filesystem, application or physically located then allows for classification of that data. What type of data is stored in each of these "locations"? The filesystems and applications can then be further traced to see where they physically reside and who manages them. Knowing where the data is stored and what type of data is stored in each location allows better management and maintenance of the data.

The next question is determining how long the data should be stored in a particular location. Retention policies may need to be developed. Laws and regulations will play into this decision. The cost of keeping data needs to be considered in conjunction with the legal requirements for retaining it. Access control to limit who can access data in each location will tighten security. Only a clear inventory of the data allows for these controls and management to be put in place effectively and efficiently.

Inventory Process

The inventory process should be performed on a continuous basis if possible or on a temporal cycle depending on the availability of resources. As suggested above, both from a security and business perspective this should be done at least annually to optimize the value. The system of collecting this inventory can be as simple as a spreadsheet and will grow to include semi-automated and automated systems with business growth. The inventory becomes a highly valuable and restricted asset that needs to be secured and used by management to guide the business productivity and manage risk.

3.16 IMPLEMENT ENCRYPTION TO PROTECT YOUR BUSINESS INFORMATION

CF FUNCTION(S): PROTECT

Encryption is becoming a standard operating requirement for lenders today. Encryption is a process of protecting your sensitive business information by using a software program to make the information unreadable to anyone not having the encryption key. Encryption can be implemented both in-transit and at rest.

If a person with malicious intent gets into your systems or intercepts your communications, they can easily take your data. Not only is this bad for consumer confidence in your ability to safeguard data, but your business could be subject to fines for mishandling of regulated data, especially in states such as Arizona, New York, and California. Encrypting data can prevent this unauthorized access.

Encryption in-transit is the process that makes communications unreadable without having the encryption key. An example of encryption in-transit is using TLS when visiting a secure website (HTTPS). Always using encrypted communication methods when one is available. This includes HTTPS for websites, SFTP for secure file transfers, and VPNs for secure connections to networks.

Encryption at rest is the process of encrypting data stored on media such as hard drives or flash drives. It is good practice to use full-disk encryption, which encrypts all information on the storage media. With encryption, even if a bad actor somehow obtains your data it will be unusable without the keys to unencrypt the data. If full-disk encryption is not an option, individual files with sensitive data can be encrypted and password protected. Many standard file formats, such as Microsoft Office and PDFs, can be encrypted natively.

When implementing any encryption function, management of the encryption keys is critically important. Encryption keys should be securely stored in a location where malicious users cannot access them, but they must be available to authorized users in order to access the data. The implementation of an effective key management process must be included in the implementation of an encryption capability.

It is important to consider all computing and communications devices when implementing encryption. Many businesses are using smartphones and tablets to perform business operations. When these devices have business information on them, it is important to encrypt the data on those devices to help protect that information from being stolen, modified, or deleted.

3.17 THIRD PARTY RISK MANAGEMENT

CF FUNCTION(S): IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

Any third party with which your organization does business can expose your company to risk. A Vendor Risk Management program is meant to ensure that your company has a comprehensive list of its vendor relationships and that the risks posed by your relationship with those third parties are well understood and are managed appropriately.

While you may delegate the responsibility for many of your business processes to a vendor, you cannot delegate the accountability for their actions. Your company is responsible for the activities performed by your vendors on your behalf. As a result, it is your responsibility to ensure that your vendors act in a way that ensures security, business continuity and fair treatment of consumers.

An effective vendor risk management program will identify an organization's highest risk third parties and ensure that the appropriate due diligence is performed against them before a business relationship commences. The program should also include regular monitoring of the relationship to ensure risks continue to be managed appropriately.

Start with a List of Vendors

This can be as simple as a spreadsheet of the vendors that are used with the contact name, email, phone number and address. The contracts, other legal and supporting documents should be collected and stored for each vendor on this list.

Vendor Evaluation and Due Diligence

Setting up a process to evaluate the vendors with respect to risk is a fundamental component. Vendor systems and services are an integral component of your operations and should be consider with the same level of scrutiny. This evaluation should include an extension of your Written Information Security Program to see that the vendors comply or are complying with policies and procedures expected. These will be driven by Laws and Regulations around the systems and services the vendor supplies.

You vendor evaluation should be able to span a set of vendor categories engaged by your business. For example, cleaning services need to be reviewed and monitored but not to the extent or with types of concern that a cloud service provider would require. Breaking these into manageable sets of vendor types can assist in developing a Vendor Risk Management Program. Aligning these sets keeping the data classification definitions in mind will help guide the type of risks these vendor systems and services pose. A cleaning service or maintenance service that has access to facilities outside of normal business hours have access that is guarded against by the Physical Security practices and procedures. For example, having a bonded vendor may mitigate this exposure and knowing the vendor's hiring practices allows for evaluation against compliance with company hiring guidelines.

The evaluation and due diligence of managing vendors requires an annual assessment of the vendor contracts, other legal and supporting documents, practices and procedures. Over time a vendor may mature or degrade their practices and procedures in delivering systems and services that may lead to revising the contractual relationship. This degradation is subjected to changing Laws and Regulations that may not have existed when the vendor was first accepted or the maturity of the company's Vendor Risk Management Program. This assessment is required to evaluate the changing risk of your systems and services both inside and outside the company direct control.

Binding Vendor Risk Management Through Contracts

As the Vendor Management Program matures, the oversight of vendors will also mature. This should include site visits and deeper dives into the vendor policies. A very effective tool in ensuring that your company will have access to perform these tasks will be contractual clauses that legally binds the vendor to comply with these oversight tasks. Tying these contractual clauses to existing and emerging cybersecurity laws will help keep vendors in compliance.

Consider a clause that requires each party to develop, implement and maintain a comprehensive Written Information Security Program (the "WISP") to protect confidential information. Examples of confidential information would include administrative, technical and/or physical safeguards appropriate to a party's size and complexity and the nature and scope of its activities.

The objective of each such WISP shall be to:

a. ensure the security and confidentiality of confidential information,

b. protect against any anticipated threats or hazards to the security or integrity of confidential information that could result in substantial harm or inconvenience to any customer,

c. have a program to respond to a security breach and to notify its partners affected by the breach where required by law or regulation, and

d. keep current with changing laws, rules, regulations and edicts concerning confidential information.

Other clauses that are useful would be for acquiring and maintaining insurance, access to vendor facility sites including the scope of access to be provided, and others that back components of the company's Vendor Risk Management Program policies, practices and procedures.

3.18 PLAN FOR BUSINESS CONTINUITY AND DISASTER RECOVERY

CF FUNCTION(S): IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

Whether it's a natural disaster, human error, ransomware, or hardware failure, disasters are bound to happen from time to time. Not only can the downtime be costly for your business, but it could impact customer retention and reputation due to the expectation of 24x7 365 access.

Your company should have a plan for restoring business operations during or after a disaster or other business impacting event. Use your asset inventory to prioritize information and systems relative to their importance for the business. This prioritization should have a business-wide focus, including employees, and ensure that all critical functions are identified. You may want to utilize a tiered system whereby you assign each asset a classification (tier 1, tier 2, etc.) that corresponds to a certain amount of time that you can afford to go without that asset. For example, tier 1 could require the system be unavailable for no longer than 1 business day.

This tiered list is a necessity when you start to implement business continuity protections. No one has enough resources to protect every type of information in the best possible way, so you start with the highest priority information, protecting each successive priority level until you achieve the risk results your business needs.

3.19 SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC)/CHANGE CONTROL

Changing current systems, implementing new systems, or developing a system from scratch are all part of the lifecycle of systems development. Including requirements for information security as part of this process is extremely important to make sure that the changes are not disruptive and that the new or changed systems are secure. Implementing a change control process will help to ensure changes are implemented in a non-disruptive manner. Creating a lifecycle for the secure development of new systems will help to ensure that security is baked into new systems.

The first step in implementing a change control process is to develop a change control policy. This policy should dictate how changes are implemented at your organization. This includes proper methods for testing changes, approvals needed to implement a change, and what individuals have the authority to deploy changes. Testing all changes prior to implementation in the production environment will reduce the possibility of an unexpected outage and that the change will accomplish what you expect it to. Requiring approval before implementing a change makes sure that the proper stakeholders are aware of the change and that there are no conflicts that would prevent the successful completion of the change. Limits on who can introduce changes to your production environment should be put in place. Allowing developers to have access to the production environment, for example, could introduce problems with segregation of duties.

Creating a Secure Software Development Life Cycle (SDLC) will help ensure that security requirements are included in all projects. All projects should have security requirements baked into the development process to ensure a secure system. Appropriate security testing should happen through the development life cycle of new systems. If systems are being developed internally, secure coding practices should be adopted, including the training of developers on the how to write secure code. Ongoing security testing of implemented systems should be conducted to look for vulnerabilities that may have been introduced into the system.

-2%
+0.7%
-0.2%
+3%
+1.3%

APPENDIX A

NIST Framework for Improving Critical Infrastructure Cybersecurity

The National Institute for Standards and Technology (NIST) has issued The Framework for Improving Critical Infrastructure Cybersecurity, which is intended to assist companies in the development of a security framework for their institution. The framework includes the five Core Functions defined below. These functions are not intended to form a serial path or lead to a static desired end state. Rather, they can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk landscape. These functions are utilized throughout this document to provide an understanding of the type of control desired by the recommended action.

- **Identify** — Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the "Identify" function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts consistent with its risk management strategy and business needs.

- **Protect** — Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The "Protect" function supports the ability to limit or contain the impact of a potential cybersecurity event.

- **Detect** — Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The "Detect" function enables timely discovery of cybersecurity events.

- **Respond** — Develop and implement the appropriate activities to act regarding a detected cybersecurity event. The "Respond" function supports the ability to contain the impact of a potential cybersecurity event.

- **Recover** — Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The "Recover" function supports timely recovery to normal operations to reduce the impact from a cybersecurity event.

For additional information, see NIST's Cybersecurity Framework homepage: **http://www.nist.gov/cyberframework/index.cfm**

The Mortgage Bankers Association offers its appreciation to the members of the MBA Information Security Workgroup who helped in the creation of this document.

MBa®

MORTGAGE BANKERS ASSOCIATION

1919 M STREET NW, 5th FLOOR
WASHINGTON, DC 20036