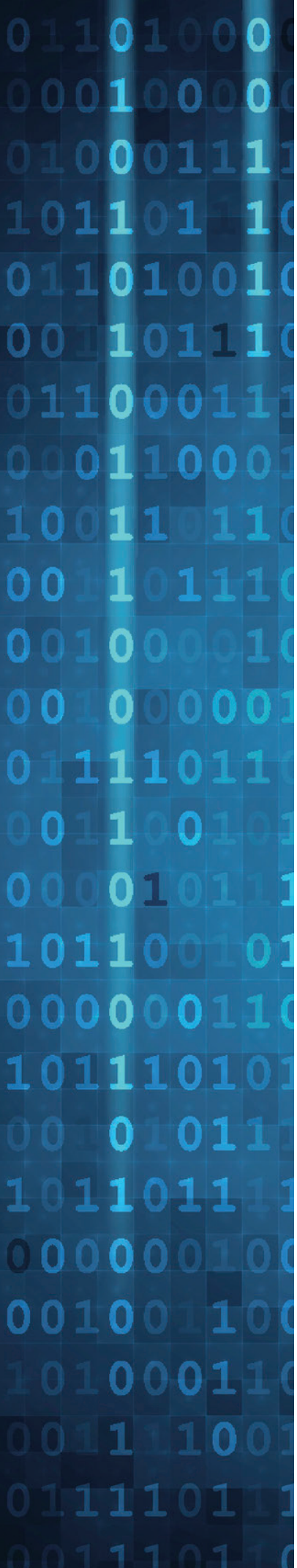
McGowanPRO

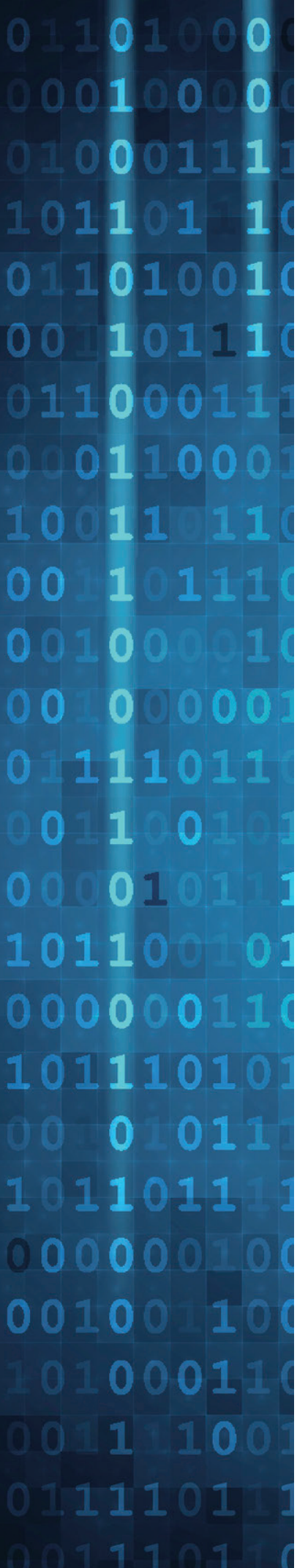
Professional Liability Insurance

Accountants Professional Liability

Cyber and Data Security



Contents



Introduction

Accountants face unique challenges in managing and responding to a wide spectrum of escalation information security breaches and cyber threats, as well as the resultant financial, regulatory, legal and reputational consequences.

Information security is becoming increasingly important to clients, as accountants handle very sensitive data for their companies and increasingly board members are demanding requisite due diligence of vendors that handle both personal data and other confidential information.

Understanding information security challenges and solutions is critical for CPAs and organizational leaders. These threats must be managed from the top on down throughout the organization.

Accounting firms must take steps to protect themselves and their clients' data from information security risks…one key element of this is to develop an information security plan that covers the entire data life cycle, from creation to destruction, for the most critical data assets that your firm manages. Some of the important controls that your firm should adopt are covered in this manual, but this is not intended to be an exhaustive list of the measures that your firm should adopt.

> *Lost or stolen laptops continue to plague the accounting industry. In most cases, firms are unable to ascertain the level of potential data breach and data compromise exposures. Having well established guidelines and best practices can help eliminate the "what now?" conversation.*
>
> —Gary Sutherland, Managing Director

CPAOnePro Accountants Professional Liability
Cyber and Data Security Supplement

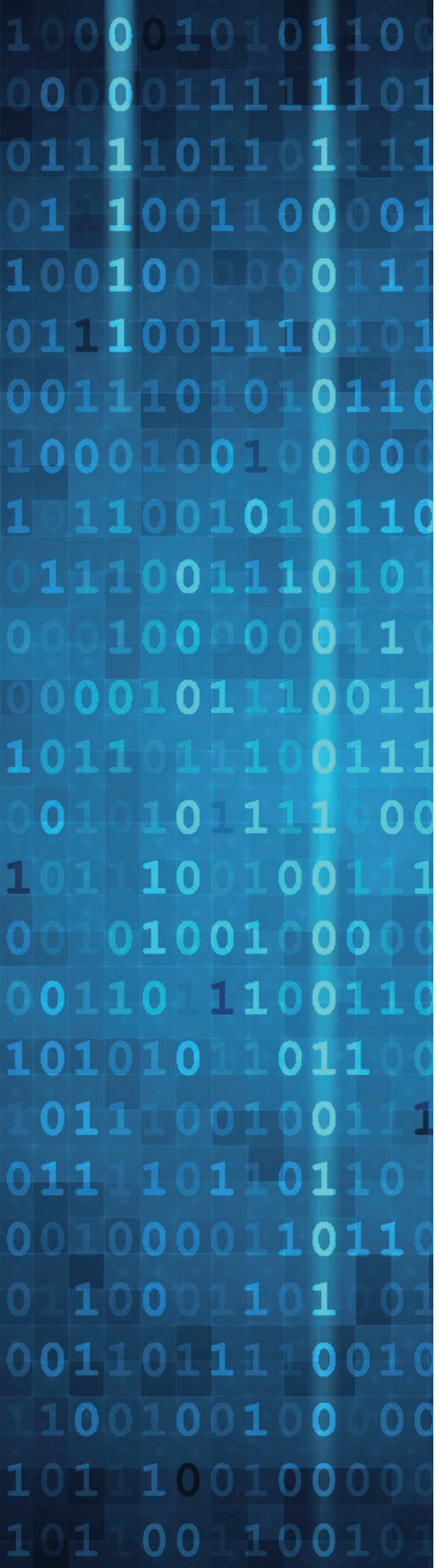
1.	Do you have a formal procedure for destroying or archiving old client files?	YES | NO
2.	Do you have a formal policy regarding the security of client files removed from the office?	YES | NO
3.	Are all client files contained on laptops or portable media devices encrypted?	YES | NO
4.	Do your laptops have installed tracking and data removal software?	YES | NO
5.	Are all servers or network computers "firewall" protected against outside access?	YES | NO
6.	Are all firewalls and firewall software current and regularly updated?	YES | NO
7.	Do you log and monitor access to your network?	YES | NO
8.	Do you have a formal procedure for the disposal of obsolete computers, faxes, scanners and/or hard drives?	YES | NO
9.	How often is sensitive information backed up? Daily Weekly Monthly Other	YES | NO
10.	Does the firm accept credit cards for services rendered? a. If Yes, please state the approximate % of revenues from credit card transactions in the last 12 months b. What steps are taken to prevent theft of card info?	YES | NO
11.	Are all personnel advised of the obligations to secure client privacy?	YES | NO
12.	Do you have a client notification system in place in the event of loss or theft of personal records?	YES | NO
13.	Within the past 5 years have any client records in your custody or control been lost or stolen?	YES | NO
14.	How frequently are passwords changed? Monthly Every 3 Months Every 6 Months Every 9 Months Other	YES | NO
15.	Do you undertake security background checks for all new hires?	YES | NO
16.	Are passwords and network access immediately revoked for terminated personnel?	YES | NO

Question 1:
Destruction and archiving of old client files

A record archival and destruction policy represents the last stage in a firm's data lifecycle management strategy. A strong policy should cover all of the following points:

- Identification and classification of records: The firm's various types of records should be listed and a classification system and process should be established. Potential record types include firm records, client records and work product records.
- Retention/archive/destruction scheduling: Separate schedules should be established for the retention/archive/destruction of various types of records. These schedules should match with federal, state and local regulations and industry-specific requirements. Records subject to litigation holds may require special handling.
- Archiving of closed client matters – Paper and electronic materials should be gathered into a single file. Duplicates and materials that are not classified as records should be destroyed as part of the archiving process.
- Designation of destruction requirements: Destruction methods should reflect the firm's obligations to client confidentiality. Paper documents should be shredded or incinerated and data storage devices should be physically destroyed rather than overwritten.
- Establishment of a destruction log: A log must be created as a permanent record of the firm's activities. The log should include the client involved, a description of the documents being destroyed, the employee who performed the destruction and the employee who signed off on the destruction.
- Examination requirements: Destruction should not occur until the employee responsible for the client file has verified that the retention period has properly run for all data sets contained within the file. The employee should also verify that no litigation hold has been placed on any of the file's components. Any parts that have been placed on a litigation hold should be separately achieved for the duration of the hold. These retention extensions should be used only in exceptional cases. The exceptions should be documented in the extended file along with the reason for the exception, the employee who authorized the exception.

A record archival and destruction policy is only effective if the firm has the required resources to ensure its consistent implementation. Effort can be spared through automation in many instances, e.g. dynamic archiving tools can automatically move older data to storage, duplicate documents can be deleted automatically prior to archiving, records can be classified and searched automatically, data can be captured automatically from applications that are being decommissioned, and destruction tools can automatically delete files, emails and documents.



Question 2:
Removing client files from the office

When client files are removed from the office there is an increased risk of loss. It's easy for an employee to misplace a USB stick, leave important documents on a train or have a company laptop stolen, and client files may then be available to (often non-traceable) third parties. Accountants should therefore only remove client files from the office when such files are necessary for reference in client meetings.

Permission for removal should always be obtained from a manager and portable devices that hold client files should always be encrypted (see guidelines in Chapter 3). Client files should not be stored on portable storage media (e.g., (USB sticks, smartphones, tablets etc.) or laptops for longer than the period of active use if such devices will be removed from the office. Client data should be deleted from such devices when no longer required.

The partner or officer responsible for information security or compliance within your firm should be advised immediately if client files are lost outside of the office. This step is critical to allow you to comply with your incident notification policies and manage any additional damage that the disclosure may cause.

Employees may be reluctant to report a loss, but a firm needs to communicate to its employees the importance for compliance under firm policies and as well as under law. One approach to minimize the risk of not reporting, at least with regards to electronic media, is for the company to only permit company-issued electronic storage media to store client files and to keep inventory of such media. This inventory documents all devices that have access to client files. Keeping the inventory up to date and running regular device checks can provide early notification of losses that may otherwise remain undetected.

Attention should also be paid to the potential for employees to remove client files at the end of their employment. Portable devices, physical documents and even hard drives may easily leave with a departing employee, either as an oversight or an act of malice. The associated risks can be minimized with measures including:

- A departing employee checklist: This checklist ensures that all company-issued devices (and the client files that they may contain) are returned before the employee leaves the company.
- A media sanitization policy that extends to employees' personal devices: This provision ensures that client files are removed from devices that do not fall under the company's direct control.

Responsibility for these measures will be more effective if assigned to a named representative. The representative will in most cases be the departing employee's direct superior.

Question 3:
Encryption of client files on portable devices

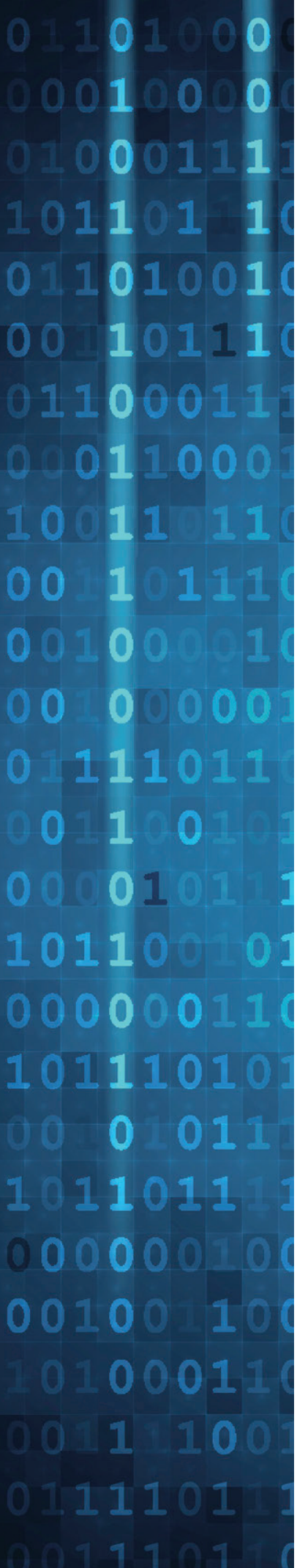
Encryption provides an extra line of defense against the loss of data to unauthorized parties. Laptops and portable media devices (USB sticks, smartphones, tablets etc.) are in particular need of this extra defense due to the ease with which they can be lost or stolen.

Laptops and portable media devices should have their full disks encrypted with 256-bit encryption. 256-bit encryption is one of the safest encryption methods available and is used by banks and the U.S. government to protect sensitive data. The number of combinations required to break 256-bit encryption is 2256, or more than the total number of atoms in the known universe. This protection can therefore be relied upon to secure client files. Encryption should not, however, be limited to the data held on laptops and portable media devices. It should also be extended to data connections that are established by these devices, i.e. Internet/public network/remote access VPN connections.

Strong passwords or similar high-level security authentication should be required to access encrypted data and connections. Laptops and portable media devices should be set to require this authentication after relatively brief periods of inactivity (an “auto-lock” feature). Chapter 12 contains guidelines on the creation of strong passwords.

Remember that even the very best encryption can always be defeated through oversight and human error. Your firm can only encrypt devices that it controls, and so employees must only transfer client files to authorized devices. These devices will ideally be company-issued devices, although personal devices may also be acceptable if they have been cleared by your IT department or third-party IT provider.

Remember that even the very best encryption can always be defeated through oversight and human error.



Question 4:
Tracking and data removal software on portable devices

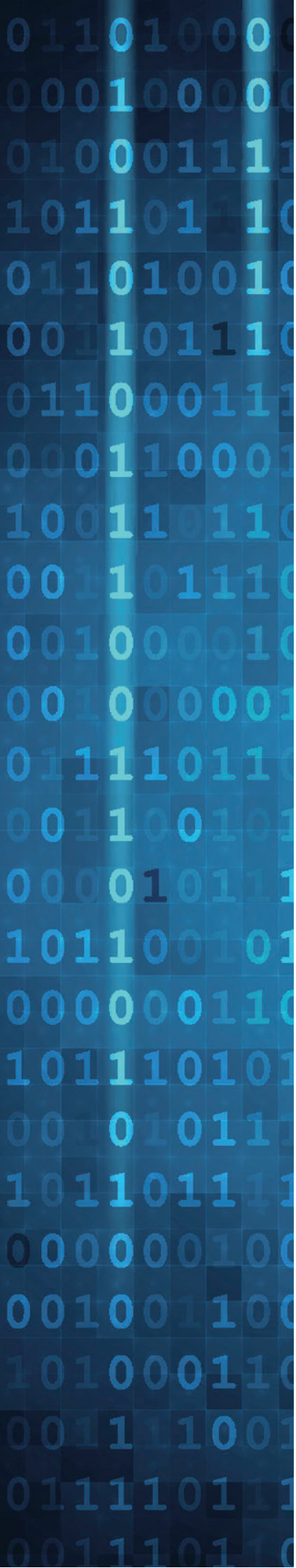
Tracking and data removal software can be installed on laptops, smartphones, USB sticks and other portable devices to minimize your firm's exposure if the device is stolen or lost. When a theft or loss is reported, depending on what application you decide to use, you'll be able to:

- Track the missing device: This feature can be useful for locating misplaced devices and recovering stolen devices. Simple programs determine a rough location from a device's IP address, while advanced solutions triangulate more precise locations from extensive databases of known WiFi networks.
- Disable the device and remove data: You'll be able to lock down the device as soon as it's reported missing. This step will prevent anyone from using the device. In the case of a lost device, some programs will also allow you to communicate with the finder and arrange for the device's return. A more secure method than disabling the device is to remotely delete all data from its disk. This option should be considered when the device contains any kind of sensitive information.
- Record a thief: You can receive screen captures and key captures to find out how a thief is using a stolen device. This information can be useful in planning your response; different information security issues will arise from theft by a common criminal versus theft by a corporate competitor. You can also use a device's camera to take photos of the thief. These photos are likely to be useful evidence in any subsequent legal proceedings.

The tracking and data removal software must be installed prior to a loss or theft incident. It's therefore important to have a system in place for installation on all devices that access client files and/or other sensitive company information. The system should also extend to employees' personal portable devices that have this level of access. Most programs limit employee and corporate privacy concerns by only becoming 'active' once a loss or theft has been reported.

No tracking or data removal software should ever be used in isolation. The majority of programs can only be used when the missing device connects to the Internet, so a determined thief may continue to use the device by discarding or wiping its disk or simply disabling Internet connectivity. Even if an Internet connection is secured, device disabling and remote data wiping should only be viewed as reinforcement measures to more secure information protection such as 256-bit disk encryption (see Chapter 3).

No tracking or data removal software should ever be used in isolation.



Question 5-6:
Firewalling servers and network computers against outside access

A firewall is a program or device that controls the flow of network traffic between trusted areas (e.g. your firm's network) and untrusted areas (e.g. the Internet). The traffic is checked against a set of security rules and only allowed to continue if it passes certain criteria. A properly configured firewall should block all inbound and outbound traffic that your firm hasn't explicitly approved, thereby limiting the potential for hackers to breach your network and spread viruses or obtain sensitive information.

The day-to-day management of a firewall can be challenging as new users, applications and technologies are added to your network. Such changes are likely to extend the hundreds or even thousands of rules that your firewall uses to determine how traffic flows. Poorly planned rules are a leading cause of data breaches, so all changes to your firewall should therefore be made as part of a defined workflow:

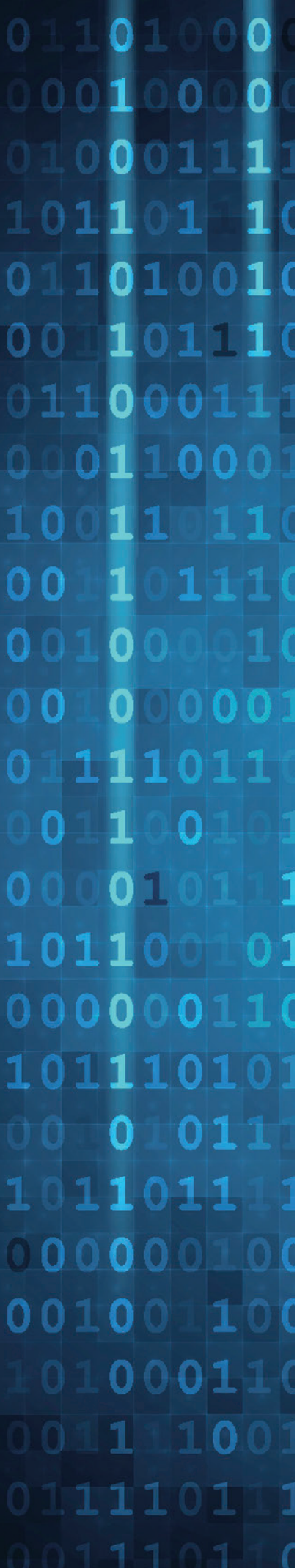
1. Change request: A request may come from anyone in the business who needs to install new software or faces a technical issue that requires an altered firewall rule. Your IT manager or outsourced IT provider is likely to make regular requests as software is updated, new network services are added etc.
2. Risk assessment: The potential change is evaluated for its technical risk and compliance with the business' information security policies and procedures. Changes from trusted sources for critical updates may require less scrutiny but should be considered as part of this process. Giving access to providers who have not been validated as being a trusted source should be considered more carefully. This examination should be conducted in collaboration with a compliance manager appointed by your firm.
3. Approval and deployment: The risk assessment is considered and the change request is approved, altered or rejected. Final rules is passed to a firewall administrator for deployment.
4. Documentation: A record should be kept of how each rule satisfies business needs. Subsequent rule changes will then be easier to manage. These rules will act as a compliance record that all enacted rules have an operational purpose.

All firewall changes must be agreed in collaboration with your firm's compliance manager as firewall administrators may not appreciate how rule changes affect your firm's information security commitments, and so engaging your compliance manager will ensure that these commitments are not jeopardized.

Attention should also be paid to unused and conflicting firewall rules:

- Unused rules are rules that no longer serve required business purposes. These rules often permit traffic that could be identified and exploited by a hacker.
- Conflicting rules are rules that act against other rules. A firewall will generally act on the first rule that it encounters, making it difficult to determine how added or changed rules will affect firewall performance.

Both unused and conflicting rules can be identified and remedied with firewall management tools. These tools monitor traffic on a continual basis and identify connections that are no longer used or cause firewall conflicts. A firewall administrator can then investigate these rules and enact appropriate resolutions.



Question 7:
Logging and monitoring network access

Effective network access monitoring is essential for securing sensitive information. Many operating systems, applications and pieces of hardware offer access-monitoring features, but Security Information and Event Management (SIEM) software is recommended for streamlining the monitoring process. SIEM software combines automated monitoring and alerting with log collation and post-breach record investigation tools.

Irrespective of what system you use, it needs to have the ability to monitor, on a real time basis, suspicious network access activity that's caused by attempted hacking, stolen credentials or a malicious insider. Examples of suspicious activity include:

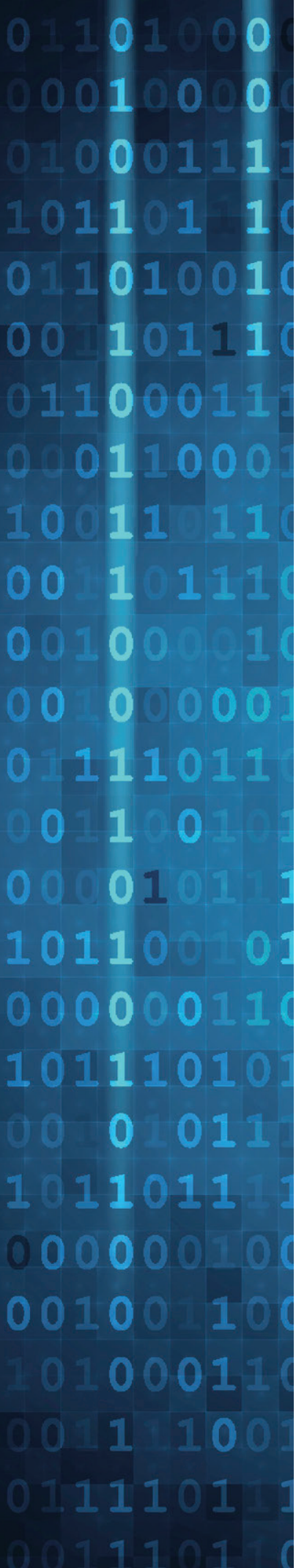
- Multiple login failures followed by a successful login
- Login attempts at unusual times/locations for the user or system
- Attempts to use the same login credentials on multiple systems
- Login attempts with terminated credentials
- Successful logins with the same credentials in multiple locations
- User runs unusual applications
- User accesses unusual systems, files or other resources
- User attempts to copy sensitive data onto a portable device
- User generates a significantly greater number of actions than usual

Managers and/or network administrators can be informed by cellphone or email as soon as suspicious activity is detected. Some SIEM solutions can even take direct action against a threat, e.g. by disabling user accounts after a number of failed logins or blocking USB ports after a user attempts to download sensitive data to a flash drive.

Collating logs of network access will improve the human review process, which is essential to revealing issues that have been missed by automated monitoring. The logs should ideally be reviewed on a daily basis, and this frequency is compulsory under PCI DSS if your firm deals with credit or debit cardholder data (see Chapter 9). Daily review can seem onerous, but the speed with which unusual access patterns can be identified will improve with experience.

Network access logs must be stored securely and made tamper-proof, even from network administrators. Logs that are improperly stored are at risk of accidental deletion and manipulation to conceal evidence of malicious activity. Logs should be archived, with the length of archiving determined by your firm's specific (and often regulatory) data retention requirements.

Outdated access controls will make network access monitoring much less effective. An employee's access to sensitive information should always be limited to the minimum essential for the completion of his/her duties, but access requirements often change over time. A departing employee checklist (see guidelines in Chapter 14) can help you to restrict network access for former employees, but access should also be updated whenever employees are promoted or take maternity/paternity leave. The permissions for all employees should be reviewed on at least an annual basis to eliminate overlooked network access issues.



Question 8:
Disposing of obsolete computers, faxes, scanners and hard drives

Technology equipment can hold company information long after the data has been initially deleted. Commonly available software can recover sensitive information even from reformatted hard disks. It's therefore important to follow strict data wiping procedures whenever technology equipment is reused, recycled, disposed of or simply no longer required.

Data wiping upon servicing or disposal should occur for all equipment that can retain data, e.g. computers, servers, hard drives, mainframes, portable storage devices, backup tapes, smartphones and tablets. Fax machines, copiers and scanners should also be included as many models feature internal hard drives that may not be obvious to the casual user.

The responsibility for data wiping is usually given to the compliance manager for a firm, with the actual wiping done by someone under the manager's direction.

Sanitization will generally be conducted in one of three ways:

- Overwriting: Uses a program to write blank data over existing files. The process should be repeated at least three times to ensure that all original data is removed.
- Degaussing: Strong magnets or electrical pulses are passed over magnetic media to remove data. Common magnets cannot be used for effective degaussing.
- Destruction: Involves physically dismantling media by crushing, disassembling etc. The equipment can only be disposed of once sufficient destruction has ensured that no data can be retrieved.

Media sanitization is an important issue that must not be overlooked. Failure to follow a strict media sanitization policy and ensure complete data removal is likely to breach client confidentiality, violate software license agreements and contravene state and federal information security and privacy laws.

Question 9:
Backing up sensitive information

Sensitive information can be lost due to human error, criminal activity, hardware failure, power outages, natural disasters and a number of other catastrophes. An effective backup strategy can mitigate these data loss risks and ensure that your firm recovers from major incidents as quickly as possible.

Backup methods can be broadly split into online and offline categories. Online – or 'cloud' – methods copy your data to remote servers via your Internet connection. Your data is then protected from incidents that affect your premises and is restorable from anywhere that has Internet access. Offline methods involve copying your information to physical media such as tapes, flash drives, external hard drives and network-attached storage (NAS) devices.

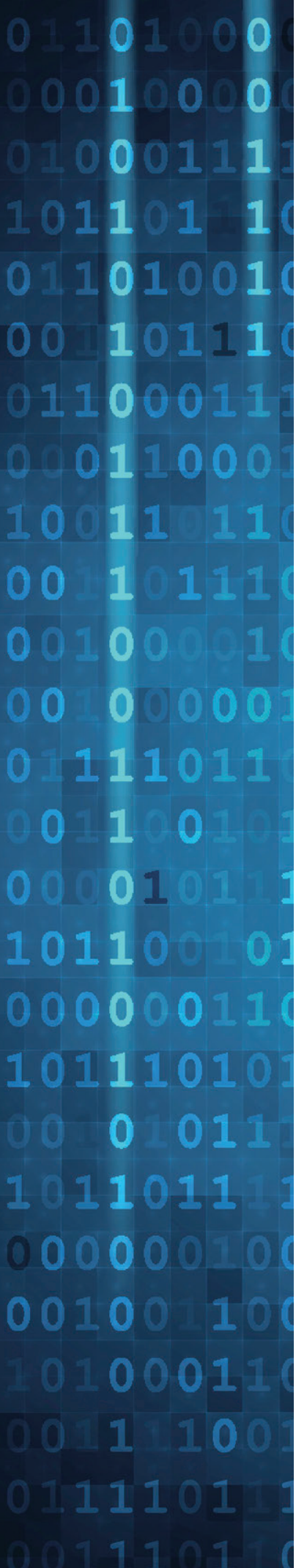
Online backups are limited by the speed of your Internet connection, so creating backups and restoring files after a disaster can be a slow process. Offline backups do not suffer from this weakness but are instead vulnerable to accidental damage, wear and tear and incidents that affect your premises. Online and offline backups are therefore strongest when used in parallel. A backup strategy that adopts this parallel approach will fulfill all of the requirements of the robust '3-2-1 Backup Rule', i.e. having at least:

- 3 copies of all important files (1 primary copy and 2 backups)
- 2 different media types holding each important file
- 1 copy of each important file kept offsite

Incremental backups should be run on a daily or even hourly basis depending on how often your information changes. These automatic processes will ensure that you always have access to recent versions of important files. Completed backups should then be encrypted and subject to the same access restrictions as the original file versions.

It's also important to test your backups on a regular basis, and especially after you've made significant hardware/software changes to your system. Simulating a range of data loss disasters will ensure that your sensitive information is recoverable – and also familiarize your staff with the procedures that need to be followed in a real-life data loss scenario.

> *The fastest growing segment of data breaches is with the financial industry (18%) which includes CPA's.*
>
> – Stephen Vono, Senior VP



Question 10: Protecting credit card information

The Payment Card Industry Data Security Standard (PCI DSS) is a global information security standard that applies to all organizations that store, process or transmit payment cardholder data. The standard was developed by the five major card schemes – American Express, Discover Financial Services, JCB, MasterCard and Visa – as a means of reducing card data theft and subsequent fraud.

Systems that comply with PCI DSS are secure systems that limit your exposure to cardholder data loss and the associated negative consequences (including lawsuits, insurance claims and government fines). Compliance with the standard is therefore an excellent way of protecting card information within your business. Compliance is also a requirement of doing business with the five major card schemes regardless of your firm's size or annual card transaction volume.

The standard is split into 12 requirements that cover six 'control objectives':

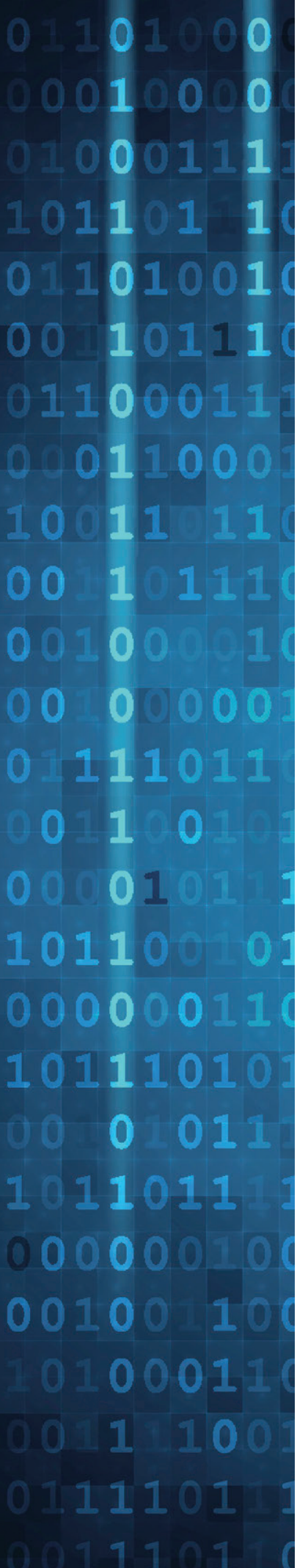
- Building and maintaining a secure network
- Protecting cardholder data
- Maintaining a vulnerability management program
- Implementing strong access control measures
- Regularly monitoring and testing networks
- Maintaining an information security policy

Every requirement must be fully satisfied to ensure compliance, although most aspects of the standard merely reflect existing security best practices. Costs that are incurred during the compliance process are also minimal in comparison with the potential fines, claims and lost business expenses that can be associated with non-compliance.

The following issues are useful to consider as you work toward PCI DSS compliance:

- **Map data flows:** You can only protect cardholder data if you know where it's kept. Start by identifying all physical and logical points through which cardholder data enters and leaves your firm. Then assess where this data resides on your system (e.g. servers, databases, test facilities, paper files, transaction logs, etc.). Be sure to include all relevant third-party providers in your assessment.
- **Avoid storing cardholder data:** PCI DSS strongly encourages businesses to avoid holding cardholder data whenever possible. Your firm is unlikely to need much data after a transaction's authorization and settlement stages, and any data that is retained should be encrypted and held on a secure server. Data that is not required should be disposed of in a secure manner.
- **Limit card detail usage:** You can reduce the cost and effort associated with PCI DSS compliance by limiting the areas of your operation that have access to cardholder data. Some companies enable all departments – and even third parties – to use card details, and this policy makes their compliance programs unnecessarily complex.
- **Outsourcing card processing doesn't guarantee compliance:** It's your responsibility to ensure that third-party providers match PCI DSS requirements, i.e. by requesting a certificate of compliance on an annual basis. Your firm also needs its own policies and procedures to cover any cardholder data that is processed in-house.

It's important to remember that PCI DSS compliance is an ongoing process. No single vendor or product can provide full compliance, and a single bad system change can turn a compliant firm into a non-compliant firm in an instant. Securing cardholder data requires a 'big picture' approach and constant reassessments of how your business can minimize card data loss risks.



Question 11: Training staff to secure client privacy

Everyone within your firm has a role to play in securing client privacy. It isn't necessary for every employee to know every detail about information security in the accountancy field, but they should understand the obligations that relate to their duties. Employees need to be trained on their obligations, but it's also your responsibility to check that the obligations are followed, to monitor how the obligations can be updated, and to issue reminders about the obligations on a regular basis.

Written policies

All of your core privacy requirements should be included in a set of information security policies and procedures (ISPPs). These ISPPs should establish employee responsibility for the safeguarding of client data through both physical and electronic means. Physical safeguards include clearing desks at the end of each business day and not conducting sensitive conversations in public places. Electronic safeguards include changing passwords on a regular basis and only using public WiFi networks with suitable protection.

Your ISPPs should be provided to new employees as part of the onboarding process, and signed acknowledgment forms should be collected to confirm that the requirements have been read and understood. The ISPPs should also make clear that compliance is a condition of employment and that violations will be subject to disciplinary actions that may include dismissal.

Annual appraisals

Annual employee appraisals offer an excellent opportunity to remind employees of their security obligations and emphasize the importance of information security within your business. Integrate set criteria into all appraisals (e.g. whether infractions have been identified, adherence to clean desk practices) and consider creating personalized security and privacy plans for each employee to master over the coming year.

Integrating information security issues into appraisals should also encourage managers to take responsibility for employees' information security practices.

Policy reviews

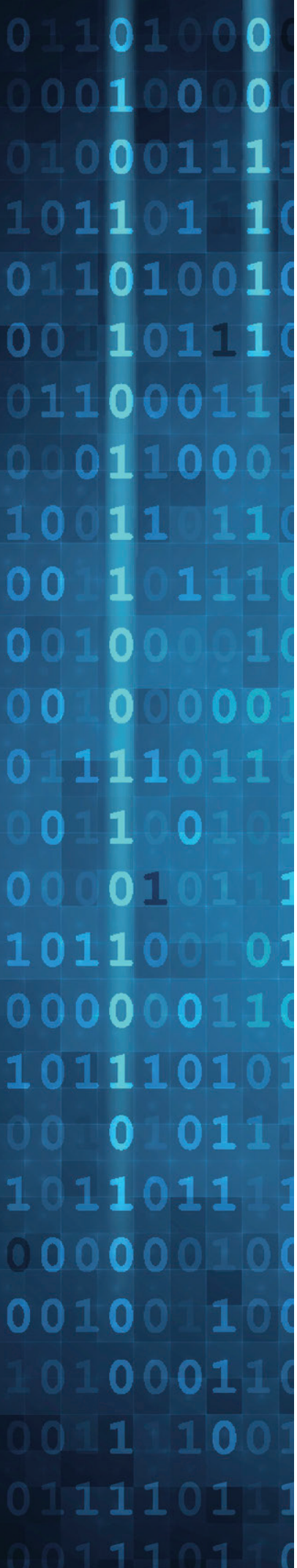
Even the very best employee training is of limited use if it relates to outdated practices. Your firm should review its ISPPs and provide updated training on an annual basis. New threats from social networking, phishing etc. can cause major security breaches, and altered regulatory requirements can also introduce important changes to employees' interactions with sensitive data.

Ongoing awareness

The most secure firms are those that create a security-minded culture among their employees. It's therefore essential to promote information security issues at regular intervals. Consider using a variety of tools that match your corporate culture, including:

- Leaflets
- Newsletters
- Online or video courses
- Articles made available on the company Intranet
- Live presentations
- Breakfast discussion groups

Try to focus the content of these tools around real events from your business. Mentioning actual breaches or 'near misses' that your firm has encountered will target training around your weakest areas and also convince skeptical employees of how client privacy issues constitute genuine threats.



Question 12-13:
Notifying clients on the loss or theft of personal records

Your clients should be notified when their personal records are compromised. Compromises occur when personally identifiable information is lost or stolen, accessed by a nonauthorized party (e.g. a hacker) or disclosed in an unauthorized manner (e.g. sold by a hostile employee).

Client notification is not only a good business practice and a core component of any robust incident response policy. It's often also a legal requirement. Almost all U.S. states have enacted laws addressing this notification process. Notification requirements are set by the jurisdiction in which the affected party resides and not by your firm's place of business, so be sure to identify details such as when notifications must be completed, which parties must be notified and how notification must occur. Expert advice on local requirements should generally be sought from outside counsel.

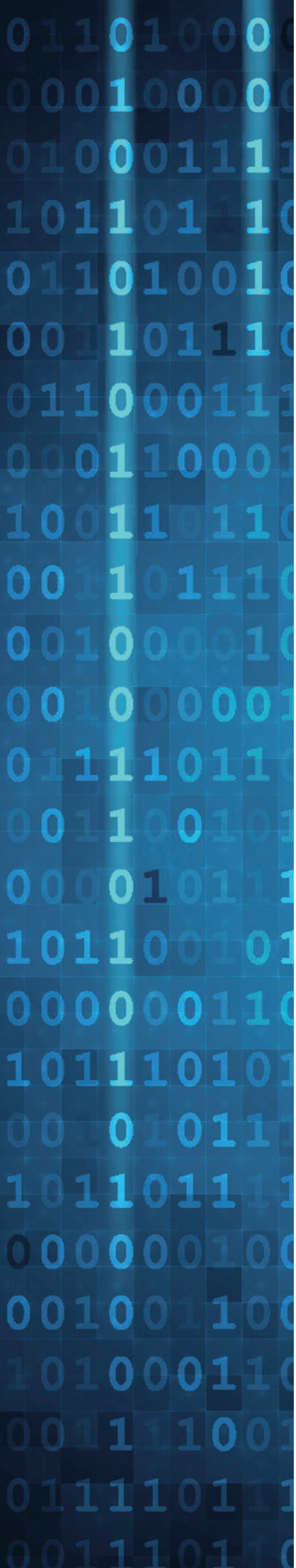
Initial notification letters are generally required to address the following points:

- A brief description of the incident
- The date or time period during which the incident occurred
- The type of personal information that was compromised
- A brief overview of the steps that your firm is taking to prevent a reoccurrence
- Guidance on how the client can avoid potential adverse consequences
- Contact details to answer questions about the breach

Other points will be determined by the specific circumstances of the data breach, and it's common for legal obligations from multiple client jurisdictions to apply within a single incident response.

Too much detail in the letter can also expose your firm to claims, so counsel should be involved in its drafting. Also ensure that employees who answer subsequent client questions have been trained to provide consistent and legally compliant responses. Be aware that some notification recipients are likely to contact your firm in the belief that the notification letter itself is a fraudulent attempt to obtain their personal details.

It's also crucial to consider other parties who may require notification of a data breach. The most important among these are parties that are named in statutory instruments, e.g. law enforcement agencies. These agencies will often require notification in advance of clients as they may opt to delay notifications that could impede subsequent criminal investigations. Other parties to be notified include your insurance provider.



Question 14:
Password best practices

Passwords play a vital role in the security of any major company's information. A balance must nevertheless be struck between data security and system usability. Strong, practical passwords will generally include:

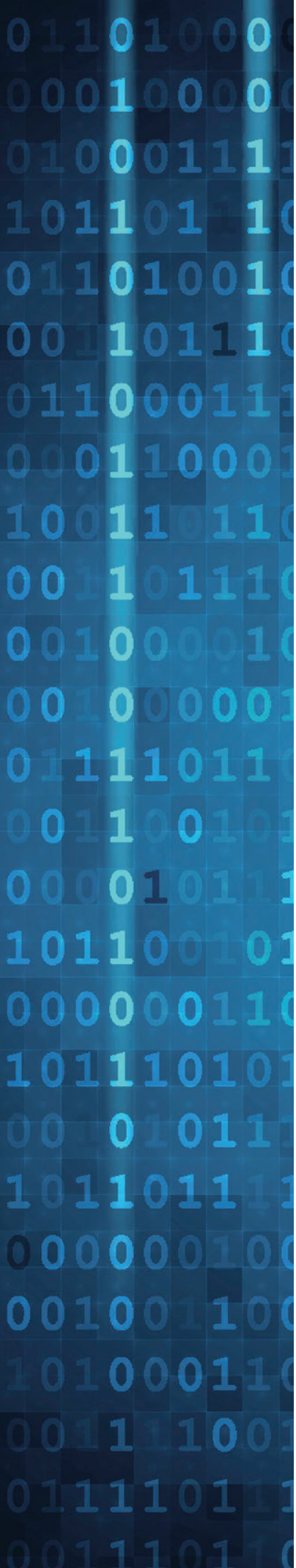
- At least 10 characters
- A mix of lower case, upper case, non-alphabetic characters and numbers (at least three of these four groups)
- No words that can be found in a dictionary (English or foreign language)
- No more than two consecutive characters from a user's full name or account name
- No common names/terms (e.g. literary characters, place names, software brands)
- No simple patterns (e.g. aaabbb, 123321)

Users who struggle to remember secure passwords can be assisted with simple memory aids. As an example: the phrase "This may be one way to remember" may prompt a user to recall the secure password TmB1w2R!

Once secure passwords have been created, users should also be cautioned against:

- Using the same passwords between company and non-company accounts (e.g. a company VPN and a personal email address)
- Using the same passwords between multiple company accounts
- Sharing passwords with others, including secretaries and administrative assistants
- Writing down passwords or storing them online without encryption
- Using the 'Remember Password' feature found in many applications

Additional password security measures can be included within your company's routine procedures. Your system should require all passwords to be changed every 90 days, for instance, and users who enter incorrect passwords on more than three consecutive occasions should have their accounts temporarily disabled. New passwords should also expire after their first use, forcing users to choose new secure passwords before they can log on.



Question 15:
Background checks for new hires

Insiders represent the greatest threat to your firm's information security. It's therefore important to minimize your exposure by investigating candidates within the hiring process. Rigorous background checks can uncover a variety of issues, including:

- Undeclared criminal records
- Misrepresented education/work histories
- False references
- A history of drug abuse
- Financial problems that may open the candidate to coercion/blackmail in the role
- Presence on the Sex Offender Registry

Checks should be applied to all potential employees including contractors, interns and temporary workers. Employees who will have access to personally identifiable information or other sensitive data should always be subject to more extensive investigations. Update checks should also be conducted for existing employees at least every three years.

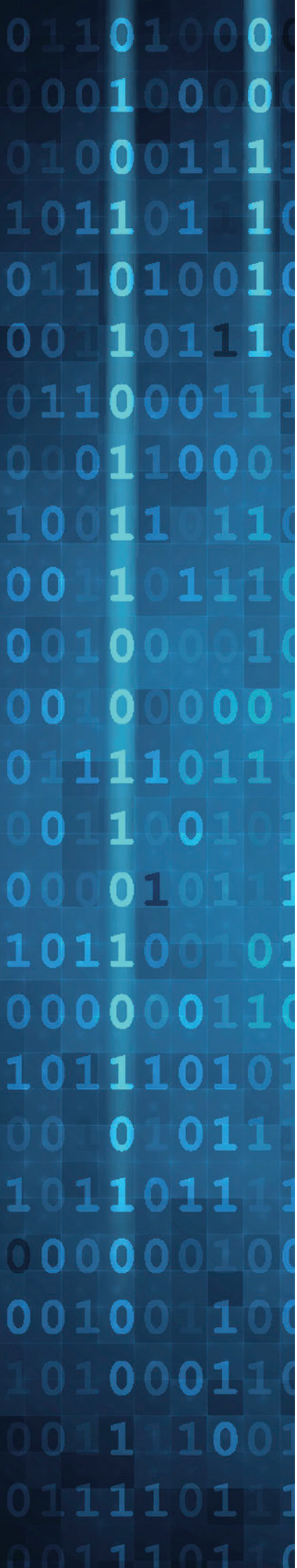
Federal, state and local legislation will determine the particular types of research that you can conduct within your background checks. You may request information from credit reporting agencies, for instance, but the Fair Credit Reporting Act (FCRA) stipulates that this information can only be released with a candidate's written permission. The candidate may also request details of how the disclosed information affected the final hiring decision. Other types of research are subject to even more stringent restrictions:

- **Medical records:** The Americans with Disabilities Act prevents you from asking medical questions before making a job offer. An offer may be made conditional on the candidate answering medical questions or passing a medical examination, but only if all new employees are subject to the same procedures. You may ask if/how a candidate will be able to complete specific job functions.
- **Military service records:** The Privacy Act restricts the release of military service records to limited circumstances. Research conducted under the Freedom of Information Act can only reveal the candidate's name, rank, salary, duty assignments, awards and duty status.
- **Bankruptcy records:** Bankruptcies are public record but may not be used to discriminate against applicants during the hiring process.
- **Lie detector tests:** The Employee Polygraph Protection Act prevents the use of lie detector tests during preemployment screening.

Legal advice should always be sought on the checks that are permissible and the processes that are required in your situation. This advice should be subject to regular review and paired with refresher training for hiring managers.

All new-hire checks should be made only after conditional offers have been extended. This step will help to shield your firm from claims of candidate discrimination. The creation of transparent background checking policies can provide further support against discrimination claims – both for new hires and existing workers. Model policies should:

- Set out fixed criteria to disqualify candidates from roles
- Make the passing of update checks a condition of employment
- Require hiring managers to document all details of how background checks affect their hiring decisions



Question 16:
Access controls for terminated personnel

A terminated employee who retains access to your firm's information represents a significant security threat. It's therefore vital to remove access to all firm resources as a standard part of the employee termination process. Firm resources include network logins, passwords and remote access accounts as well as security cards, ID badges and company-issued portable devices.

The following steps refer to 'accepted' and 'unaccepted' terminations. Accepted terminations may have been requested by the terminated employee and reveal no indication of a soured firm-employee relationship. Unaccepted terminations often occur with limited notice and amid undesirable circumstances. It's important to restrict access controls in both situations, although unaccepted terminations carry a greater risk of the terminated employee deleting/sabotaging firm information.

A departing employee checklist should outline all of the passwords/accounts that are to be disabled and the physical access resources that are to be reclaimed. The terminated employee's manager should use this checklist throughout the termination process to ensure that less obvious issues are not overlooked, e.g. changing the employee's company voicemail codes and disabling his/her access to the company's social media profiles. The checklist will also act as formal documentation of the access control revocation process.

Step 1: Establish whether you will be dealing with an accepted or unaccepted termination. In the case of an accepted termination, the employee's network access and passwords should be disabled at the end of his/her final day. In the case of an unaccepted termination, network access and passwords should be disabled while the employee is in his/her termination meeting. Also be sure to log out of the employee's computer and close any open sessions during his/her meeting; he/she may retain access to your firm's resources while these sessions remain open.

Step 2: Reclaim the employee's physical access resources (e.g. security cards, keys) and company-supplied portable devices. Consider changing shared access codes (e.g. office door codes) in the case of an unaccepted termination. Wider system codes may require changing if the terminated employee worked in your IT department or otherwise knew multiple users' passwords.

Step 3: Minimize reasons for the employee to access your firm's computer system by returning any personal files. Allow the employee to request any personal emails, documents, etc. that are held on your systems and have his/her manager transfer these if appropriate. The transfer should typically be made via physical media (e.g. CD, USB stick) and copies should be taken of all transferred files.

Step 4: Ensure that the employee leaves as expected. This step will likely be informal in the case of an accepted termination. An unaccepted termination may require the employee to be escorted from the firm's premises.

Step 5: Consider whether to delete the employee's data from your systems. It may be useful to retain files and logs incase the employee – or your firm – subsequently decides to pursue litigation that relates to the termination. Data should always be retained in the case of an unaccepted termination or when the terminated employee held a position of significant responsibility within the firm.

Step 6: Monitor your systems over the coming weeks for any breaches of information security that could conceivably be traced back to your former employee.

Biography:
Eric Hess – Managing Member and Founder

Eric Hess founded HLC LLC in 2014 to focus on systems compliance and information security consulting. Today, it provides an array of right sized cybersecurity assessment and cybersecurity management services to small to medium sized businesses. HLC's clients are primarily financial services firms, but HLC is developing a focus on CPA firms and law firms.

Eric has over twenty years of experience acting as senior-level counsel and management for top tier exchanges, broker-dealers and financial services technology providers, where he focused on regulation and the development, licensing and security of highly sensitive data. As General Counsel for one of the country's largest equity exchanges (now the BATS Exchange), Eric led an overhaul of their information security infrastructure that met the most stringent SEC-mandated exchange and Department of Homeland Security (DHS) standards. Recognizing that providers were consistently trying to provide burdensome security solutions to large and small companies alike, Eric set out to develop security frameworks that were responsive to the needs of small and medium sized businesses.

The HLC team is comprised of compliance, governance and security operations professionals drawn from government agencies (such as Department of Defense, DHS) as well as regulated industries.

Contact us:

McGowan Program Administrators
150 Speen Street Suite 102
Framingham, MA 01701

Email: dtuncel@mcgowanprograms.com

Phone: +1 508-656-1320

Fax: +1 508-656-1399