NEW JERSEY DIVISION OF CONSUMER AFFAIRS

# New Jersey State Board of Accountancy

***In the fast-paced and ever changing world of cyber security threats, The New Jersey Division of Consumer Affairs' Cyber Fraud Unit would like to bring to your attention some methods that accountants and accounting firms may use to minimize the exposure of critical personal client information to cyber criminals.***

Today, accounting professionals continue to be at the forefront of this threat due to their work not only with financial information, but also with personal identifiable information *(PII)* which is almost always targeted by cyber criminals. Accountants should work together with both internal cyber-security professionals and external resources to develop data security protocols in the event you or your clients become victims of these shadow criminals.

Too frequently, large and small companies alike, become victims of data breaches which are the unauthorized access to electronically stored information. The theft of this personally identifiable information, *(PII)*, often causes clients to suffer financial losses and possible reputational damage. Putting in place preventive measures is essential, but so too is having an effective plan that responds quickly when a data breach occurs.

One recent survey indicated a vast difference in the reporting of internal and external data breaches. Internal reporting is usually confined to first level supervisors. Only 17% were reported to senior executives. That same group disclosed that in the event of such an attack, less than 50% said they would report the breach to law enforcement authorities. This unwillingness to go "public" with news of a data breach could adversely affect a company's reputation and, in the case of publicly traded companies, stock value. This may be a further indicator as to why many are reluctant to disclose these types of theft.

Below are some recommendations for providers of accounting services who handle PII.

## 1. EVERYONE IS AT RISK

CEOs, CFOs, boards of directors, managing partners, and other organizational leaders need to understand the risks posed by cyber-attacks and must ensure that adequate resources are deployed to maintain a secure environment. Executives are not expected to become computer experts but certain basic safeguards must be established to safeguard personal information.

Change must also be embraced from the top. Executives and CEOs must insist that password changes, one of the simplest safeguards, periodically occur, and that they are leading by example. Without management's involvement and commitment, a firm is unlikely to achieve its own cyber security goals. One of the most important features of a company's approach is understanding the potentially negative legal implications firms could be exposed to if proper procedures are not implemented. As with any large scale system change, upfront costs to establish an enterprise-wide cyber-risk management framework may seem daunting, but comparatively speaking could be money well spent when considering the repercussions from a cyber-attack.

## 2. DEVELOP AND IMPLEMENT ADEQUATE CYBER-SECURITY POLICIES

Regularly updated Cyber-Security Policies include:

- Establish expiration dates for all policies so that each update reflects the current trends in cyber security threats, identifies the most common incident types and attack vectors, and addresses newly discovered vulnerabilities;
- Clearly define cyber-security roles and responsibilities for managers, system administrators and users.
- Establish off-site system backup systems.
- Regularly hold personnel training to minimize the likelihood that staff could inadvertently disclose sensitive information regarding the organization's clients, system design, operations or security controls.
- Establish strict limits on data access by vendors, subcontractors or other outside contractors.
- Identify the types and versions of virus protection software and tools.
- Identify the types and versions of data encryption software.
- Introduce and regularly update system-patch management; and develop guidelines which will prepare your business to effectively respond to a loss of customer PII, data corruption, Denial of Service, (DoS) attack, network intrusion, customer account

intrusion or malware infection. Specifically, guidelines and an action plan should be established for;

- Incident response
- Data recovery and eradication
- Investigation and damage assessment
- Communication plans and protocols established and in place to notify:
  - Customers
  - Regulators
  - Law enforcement
  - Industry and professional contacts.

Firms must also be mindful of potential reimbursement costs to customers for financial losses which may occur due to breaches of this type (and should also inquire whether certain types of insurance may cover such events).

## 3. ADHERE TO SEPARATION OF DUTIES POLICIES

Each staff member typically has responsibilities which grant them access to information within an organization. Separation of duties is a typical security method used to manage conflict of interest, the appearance of conflict of interests, fraud and data security.

Each member of the organization should have his/her own business justification for access to potential sensitive information. Their access should be driven by business necessity rather than convenience. A company's identity and access-management protocols should be applied to all aspects of a business' activities, including a segregation of the internal and external (e.g., cloud-based) domains.

## 4. TRUST BUT VERIFY - REMOTE ACCESS

The roles of the users who would require remote access to mission-critical operations can be extensive and the assignment of specific access depending on those roles can be complicated at best. The assignment of remote access roles and credentials should be embedded in the organizational cyber-security policy supported by the remote access methodologies. Consider all of the third-party players involved in a company's business operations:

- System operators and engineers for local systems
- System operators and engineers for remote systems

- Vendors
- System integrators
- System support specialists and maintenance engineers
- Field technicians
- Business partners
- Supply chain representatives, and/or
- Managed service providers

The above list may be more or less restrictive; however, it does not minimize the risks associated with granting access to sensitive information to the company's business associates. Appropriate contractual language to govern relationships with third-party providers should be carefully considered.

Other effective practices to manage risk associated with third-party involvement are:

- Performing pre contract due diligence on prospective service providers;
- Establishing contractual terms appropriate to the sensitivity of information and systems to which the vendor may have access and which govern both the ongoing relationship with the vendor and the vendor's obligations after the relationship ends;
- Performing ongoing due diligence on existing vendors;
- Including vendor relationships and outsourced systems as part of a firm's ongoing risk assessment process;
- Establishing and implementing procedures to terminate vendor access to a firm's systems immediately upon contract termination; and
- Establishing, maintaining and monitoring vendor entitlements so as to align with the firm's "appetite" for risk and its information security standards.

## 5. ENCRYPT, ENCRYPT, ENCRYPT…

Encryption is a critically important and effective practice in a company's cyber-security control arsenal. Encryption provides the obvious benefit of protecting the confidentiality of data by ensuring that only approved users (users who hold the decryption key) can view the data. Less obvious benefits include providing a means for ensuring the integrity of information (if the encrypted data cannot be read, it cannot be meaningfully altered), and nonrepudiation (if a message is encrypted with a key only held by that source, the source cannot disclaim having sent that message).

Depending on how it is applied, encryption can also be used to facilitate a strong Separation of Duties policy by limiting key access to staff members with a business-defined need to access the protected information. The application of encryption should be considered with respect to both workstations and servers, in both at-rest and in-transit capacities, and at various technology layers from the storage medium up through the application layer.

## 6. DON'T FORGET TO LOCK UP!

Discussions of cyber security tend to focus on firewalls, network infrastructure and control systems. It is important not to forget about protecting your company's physical assets as well. For example, if your company has a computer on its network in a remote location, ensure that access is controlled and monitored. Employees or contractors who log in to your system remotely may inadvertently compromise your security by misplacing their devices.

Both servers and workstations should be protected from theft. Workstations at unoccupied desks or in empty offices (such as those used by employees who are on vacation or have left the company and not yet been replaced) or at locations easily accessible to outsiders, such as the front receptionist's desk, are particularly vulnerable. Therefore, disconnecting and/or removing computers that are not being used and/or locking the doors of empty offices is a good precautionary measure against unauthorized access to any sensitive information.

Internet-connected devices are growing rapidly and almost all of them collect, store and transmit the collected and/or processed data. Regular machines which perform a range of simple tasks, like copy and fax machines, printers and scanners, store document contents in their own on-board memories. If the hard drives of those machines are stolen and accessed by a hacker, he or she may be able to view and reproduce recently printed documents. Also, think about the physical security of documents that are printed out and may be just abandoned at the printer or thrown intact into the trash can where they can be retrieved. It is best to implement a policy of immediately shredding any unwanted printed documents, even those that do not contain confidential information.

## 7. PRACTICE MAKES PERFECT

Incident Response Testing is an effective practice that simulates a real-time attack against a company's computer systems. The goal of this test is to view from an attacker's perspective the security weaknesses that the company's technology systems may exhibit.

This type of testing is valuable for several reasons:

- To determine the feasibility and efficiency of a particular set of defense tools.
- To identify vulnerabilities that may be difficult or impossible to detect through scanning software.
- To assess the magnitude of potential business and operational impacts of successful attacks.
- To test the ability of network defenders to successfully detect and respond to the attack. and
- To provide evidence to support increased investments in security personnel and technology.

## 8. Children Imitate Their Parents; EMPLOYEES Their Managers

A well-trained staff is an important defense against cyber-attacks. Even well-intentioned staff members can inadvertently cause an incident that can lead to a successful cyber-attack. For example, an employee unintentionally downloading malware. Effective training helps reduce the likelihood that such attacks will be successful.

According to one survey, 63% of employees admitted that they had used personal email to send sensitive work documents, and 74% believed that their respective IT departments approved of this practice. Of the total number of surveyed employees, 52% used the same password for all of their accounts, and 46% used unsecured file-sharing tools to send sensitive documents. Only 48% of employees surveyed said that their company had existing policies that address the handling of sensitive files. Sixty-three percent said that they used remote storage devices such as USB drives and mobile phones to transfer confidential work files. Regular reinforcement at training exercises will assist the company's management in evaluating the effectiveness of their preparedness program. These training sessions will ensure that every employee knows what to do in case of a cyber security emergency, and how to prevent or mitigate against any losses.

All training materials should concentrate on a few essential aspects:

- Clarification of roles and responsibilities;
- Familiarizing employees with the risks related to social engineering schemes and phishing, handling confidential information, password protection, escalation policies, physical security, and mobile/removable storage security;

- Reinforcement of knowledge of procedures, facilities, systems and equipment;
- Improvement of organizational coordination and communications;
- Periodic evaluation of policies, plans, procedures and the knowledge and skills of team members;
- Identification of weaknesses and resource gaps; and
- Compliance with all relevant local and federal laws, codes and regulations.

## 9. A Person Is Known By The Company Of The Phone They Keep

There has been a rapid rise in the number of employees—and, perhaps more important, executives —wanting to use their personal mobile devices for work, a trend called “bring your own device” *(BYOD)*. With BYOD, organizations allow employees to connect to work IT systems with their personal devices. The practice can have several benefits, but it also poses a number of potential security risks, one of the biggest of which involves employees or executives downloading personally identifying or confidential client information to their personal smartphones or tablets. If one of those mobile devices is lost, stolen or otherwise compromised, the critical data contained on it could fall into the hands of cyber criminals.

In today’s ever increasing technological world, it is difficult for companies to fully block BYOD. This is particularly true when CEOs and managing partners are at the forefront of accessing work systems with their mobile devices.

Companies however can take a few steps that will minimize the risk of exposure by:

- Requiring employees to use lock codes on their mobile devices;
- Prohibiting the storage of work data on the device unless the data is encrypted;
- Requiring all employees to sign agreements authorizing the organization to remotely erase all files on any lost, stolen, or misplaced personal device with access to the organization’s network;
- Instructing employees to avoid public Wi-Fi, such as coffee shops, retail locations or airports unless they route all traffic through a virtual private network (VPN), which creates an encrypted connection between the mobile device (including laptops) and the host server over the internet; and
- Encouraging employees to, whenever possible, use secure websites (which begin with “https” at the start of the URL line).

## 10. BETTER SAFE THAN SORRY

Most businesses would agree that data or information is one of their most important assets. It is almost certainly worth more than the physical equipment that it is stored upon, yet most businesses do not realize that standard property insurance does not cover the problem in the event that data is damaged or destroyed.

That is why companies may want to consider obtaining a cyber-insurance policy as a way to mitigate against potential loss and as part of their risk-management processes. Three of the most compelling reasons to take into consideration the purchase of cyber insurance are:

- Insurance places a dollar value on an organization's cyber risk;
- The underwriting process can help organizations identify cyber-security gaps and opportunities for improvement; and
- Many cyber-insurance policies bring supplemental value through the inclusion of risk mitigation tools as well as significant incident response assistance following a cyber incident.

**» » » » » » » » » O « « « « « « « « «**

**Any company seeking a more productive future of growth and expansion must take a proactive approach to cyber-security by taking the time to carefully examine the company's networks and cyber-security practices. In addition, a company with the most effective and up to date cyber-security practices also regularly prepares and trains its employees in the latest best practices utilized to prevent breaches of sensitive and personal information. This includes maintaining a rigorous testing program for all those that may have potential access to the information businesses seek to protect.**