tracesecurity

Practical, worry-free cybersecurity.

WHITE PAPER

IT SECURITY RISK ASSESSMENTS:
A Financial Institution's Key To Continuous Compliance

877-275-3009 tracesecurity.com sales@tracesecurity

Just about every person who runs and manages businesses will agree that, in order to compete in the marketplace, a company must assume a certain amount of risk.

But they would also agree that risk-based decisions must be rooted in hard data, historical information and some sort of cost-benefit analysis because, in most cases, "leaping before looking" will ultimately lead to failure. That is why traditional risk management is founded on maintaining stability by mitigating risk. But before a company can determine how to mitigate the risk, they must identify the specific risk factors and evaluate which risks are to be managed and which are to be avoided.

The good news for financial institutions is that the same basic principals used to identify and evaluate risk to financial assets can be applied to information assets. Analysis can easily determine which risks can be managed and which risks need to be avoided altogether.

However, most small-to-mid-sized financial institutions lack the internal resources or technical expertise that is necessary to properly identify all of the threats to information security, making a correct evaluation of risk extremely difficult if not impossible. To make matters worse, organizations often do not even factor in the human component, which is the most common sources of breaches.

Therefore, without knowing where threats exist, or their potential severity, within their information systems, a financial institution is ill prepared to combat a threat, mitigate the costs of a breach or even face a Federal or State examiner's prying eyes.
This paper will not only illustrate the value of properly identifying and evaluating information risk through a comprehensive risk assessment by qualified experts, it will also explain how developing a continuous risk management program, thus "continuous compliance", can benefit the entire organization in a cost-effective manner.

The Driving Force of Information Security

Ask the CEO or executive of almost any financial institution why their organization performs information security risk assessments and the answer will most likely be 'to satisfy compliance regulations.'

The primary reason C-level executives place compliance as the driving force behind information security practices stems from an important piece of legislation: the Gramm-Leach-Bliley Act of 1999. This legislative initiative requires the senior management of each financial institution, among other things, to establish and maintain data protection policies and processes. In other words, the executives are directly held responsible for ensuring the security of the institution's information is within compliance.

In the IT Examination Handbook published by the Federal Financial Institutions Examination Council (FFIEC), it carefully specifies management's role in maintaining a proper information security program as well as the steps each institution needs to take in order to stay in step with regulations. Such detail reinforces the GLBA's intent that institutions should not only adopt stronger security controls within their organizations, but also demonstrate to auditors that those controls are implemented and maintained as part of ongoing business procedures...not just "paper policies" or neglected security tools.

That's a lot to require from any organization, and especially taxes those financial institutions that lack the resources and the expertise to adequately monitor and enforce information security policies and deliver acceptable reports that show compliance with state and federal regulations.

Bank and Credit Union executives certainly have great concerns about protecting their customer/member data because even a minor security breach can potentially have severe repercussions that negatively affect the institution's customers, reputation and financial stability. These executives are also keenly aware that the number and severity of security incidents at financial institutions continue to escalate over time, leading many to become concerned about vulnerabilities in their own information systems.

FFIEC IT Examination Handbook's INFORMATION SECURITY RISK ASSESSMENT ACTION SUMMARY Financial institutions must maintain an ongoing information security risk assessment program that effectively:

Gathers data regarding the information and technology assets of the organiza-tion, threats to those assets, vulner-abilities, existing security controls and processes, and the current security standards and requirements; Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets; and Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.

Taken from the FFIEC IT Examination Handbook, section entitled INFORMATION SECURITY RISK ASSESSMENT, Page 9 of the Informa-tion Security Booklet.

Evaluating the Present Condition

For many organizations, these concerns are quite valid. Although senior management may realize their institution is constantly exposed to security risks - and geniunely want to reduce exposure - they simply may not have enough information availanle to determine the way to develop a risk management program. For example, organizations that implement security measures without having the benefit of a comprehensive risk assessment might be wasting money by applying too many safeguards, or possible increasing security risk by having too few safeguards. In other cases, the organization may be providing too much protection for low value/low risk assets, and not offering enough protection for low value/low risk assets, and not offering enough protection to high value/high risk assets. Either scenario leads to inefficient allocation of resources and money, yet could be corrected by a proper risk assessment.

Independent research conducted over the past 6 years indicated that over 50% of financial institutions will experience some sort of malicious attack at least once per year. This startling rate has remained steady since 2007 and, due to the ever-increasing sophistication of criminal hacking and social engineering techniques, is not likely to change anytime soon.

The most common factor that contributes to the inaccuracies within an organization's IT risk assessment is that inadequate controls are in place which are not sufficient to prevent exploits. Most standard firewalls only screen for low-level attacks, but fail to identify vulnerabilities caused by improper system configurations or outdated software patches. Nor can they protect a network from malicious activity that originate behind the firewall, like infected files loaded to the network from portable drives, infected system assets or even malicious employee activity.

Rarely are organizations equipped internally to identify and evaluate all the uncommon threats that may exist in their information network. This is why it is crucial for an organization to obtain expert guidance from a qualified third party consultant. An independent set of eyes can typically give an unbiased and more complete overview of risk factors. Moreover, contracting a third party is often considered a best practice method for assessing risk and implementing remediation plans.

With so many factors to consider - and so much at stake - institutions must consider best practice guidelines and take proactive steps toward identifying potential threats and vulnerabilities, the likelihood that they could occur, evaluating their impact to the organization's overall security, and the safeguards that control them. To do this, an organization must perform a comprehensive risk assessment and use the results to formulate a plan to improve their security measures and mitigate potential risk.

These fundamental steps will not only satisfy compliance regulations, but also increase confidence in their information security.

An Overview of Risk Factors

Just as having a current, accurate view of an institution's Assets and Liabilities helps them manage financial risk and mitigate losses, a risk assessment can help determine appropriate strategies for managing or remediating risk to data. When it comes to protecting information, many institutions have been misguided about how effective their basic security steps really are. They believe simply implementing the standard safety measures, like firewalls, anti-spam & anti-virus applications, software-based Intrusion Detection Systems, etc., will offer adequate protection for their information. Those measures are certainly a good first line of defense but are often not sufficient to prevent many types of exploits. In fact, the defense systems can even add to the vulnerabilities of a network!

Compounding the problems at the IT level is how much value is placed in the results of vulnerability assessments and/or penetration tests performed by either internal resources or a third party provider that specializes in only the basic tests. The worst-case scenario is when an organization relies strictly on the results of these basic testing procedures to determine risk factors even though they do not fully understand the strengths and weaknesses of the procedures. The organizations may not realize those tests are just a few steps of a security program and provide only a partial view of the risk landscape. In fact, those self-tests do not account for several key risk events such as threats originating from environmental sources or other external influences like fire/smoke damage, theft of physical property, or even the effects of dust on equipment.

Defining Security Risk Assessments

In simple terms, a risk assessment essentially determines what type fo controls are required to protect an institution's assets and resources from threats in order to maintain stability. A comprehensive risk assessment process measures the individual risk level of each information asset as they relate to Confidentiality, Integrity, and Availability (CIA). These results help the organization identify which assets are the most critical, provides a basis for prioritization and recommends courses of action to protect the assets at risk.

The first step in a risk assessment is to identify all of the information and physical assets that are integrated into the institution's network. This includes everything from computers, applications and networks to staff and physical facilities. The next step is to identify and classify all reasonable threats to information that could results in service interruptions or create a data breach, like unauthorized disclosure, misuse, alteration or destruction of confidential information. The likelihood and potential damage of the threats that have been identified are then evaluated based on the CIA. The final step in this phase is to assess the existing safeguards and determine how sufficient they would be in controlling the identified threats.

Services that Complement a Security Program

Two fundamental tests that yield qualitative data for the risk assessment are a vulnerability assessment and a penetration test. During a typical vulnerability assessment, software "scans" a system and automatically identifies vulnerabilities and issues. This test is used primarily as a tool to identify different assets that are connected to the network, discover outdated or unpatched software and find poorly configured applications.

However, this software-based scan does not simulate the processes a real hacker would use. In order to discover additional threats to a system, a penetration test must be performed. This test targets the security holes found in the vulnerability assessment, mimicking a real hacker's processes to exploit vulnerabilities and gain entry to the institution's network.

Of course, no matter how detailed of complete the tests are, the reults only capture one moment in time. It is unrealistic to believe that the tests would generate those same results again in 6 months. People change, training programs change, and even system configurations change. Therefore, the results of this one-time-only test are fallible on many levels.

Best practices suggest that the institution's risk assessment determine the frequency of testing. High-risk systems should be tested frequently by an independent party and policies addressing internal security measures (firewalls and inter-network protection) should be audited and verified at least quarterly.

In 2011, the FFIEC released a supplement to its original guidance Authentication in an Online Banking Environment, which effectively established a new set of best practice standards for conducting IT security risk assessments. The guidance sets the expectation that periodic risk assessments shuld be able to determine new threats and respond to such threats. The guidance recommends that risk assessments be conducted with the introduction if each new product, and at least every 12 months. The document also spelled out the factors to consider while performing and/or updating IT risk assessment, including:

· Changes in the internal and external threat environment
· Changes in consumer base adopting online services
· Changes in customer functionality offered through online services
· Actual incidents of security breaches, identity theft, or fraud experienced by the industry (or the institution).

While performing basis security tests may satisfy regulations, they will not protect an organization from ongoing threats. The best practice is to develop an ongoing, multifaceted security program which will not only ensure your institution maintains compliance and looks favorable to an examiner, but also helps to increase the level of protection against security breaches and thwart malicious attacks.

Assessing IT Security Risk Factors

The logical question when assessing risk is 'exactly ehat is at risk?' With regards to information assets, the answer is any data that can be accessed by an alternative method. This is certainly a very broad answer, but it holds quite true. From hard drives and compant email to hard copies and outgoing mail, almost all data is subject to a certain level of security risk. Unfortunately, many institutions fail to catalog many risk events associated with their information network simply becuase they lack the resources or expertise to identify all the vulnerabilities that may exist.

Although many organizations attempt to classify each risk event like these into a series of silos according to their compliance procedures, they may not have the expertise to accurately evaluate the risk events, and thus determine their actual exposure and risk tolerance. For that reason, many companies find it advantageous to have a third party provide independent and expert guidance to properly evaluate specific risk factors.

Establishing the Baseline

Because there is no "One Size Fits All" method of evaluating risk events for every financial institution, a baseline of risk factors specific to the organization must first be identified. Typically, all of the information assets within the data infrastructure are classified based on the type of asset (software applications, databases, website, intranets, etc.). Then all threats, risks, concerns, and issues related to the information assets are identified and documented. This phase of the process often must include performing penetration and vulnerability tests upon the system to properly discover any previously unknown threats. Without an adequate testing process, an institution will not be able to correctly identify all existing threats to their information system.

Evaluating risk depends on the risk elements that are relevant to your organization.

Evaluating Potential Threats and Vulnerabilities

While there are various methods to perform risk evaluations, there are specific factors that each element of risk can be compared against to evaluate the potential level of risk.

Identification of Common Threats and Vulnerabilities

- Employee Misconduct
- Criminals
- Email attacks
- Environmental events
- Virus/worm outbreaks
- Excessive privileges
- Unidentified security holes
- Malware / Spyware
- Unpatched software
- Zombie Networks
- Phishing / Pharming
- Physical security threats
- Wireless network breaches
- Accidental breaches
- Social Engineering
- Insufficient monitoring activities
- Failure to manage security

Likelihood of the Threat

This factor varies wildly because of the nature of many threats. A simple example is that financial institutions in the Gulf Coast have a great likelihood of being threatened by a hurricane. A more subtle example would be that institutions who hire numerous temporary employees to supplement their workforce have a greater chance of security incidents occurring with those ranks simply because temp employees typically receive much less security training than regular part time or full time employees.

Origination of Threat

One of the primary factors in evaluating the origination of a threat is to determine if it is classified as External or Internal. Simply put, is the threat originating from a hacker or from an employee? On the employee side, this factor can be affected by things like security awareness training programs, network access levels given to workers, and even issues as basic as which employees have access to rooms containing sensitive information.

Impact to the Organization

This factor takes into account how a breach could affect easily identifiable issues like the reputation of the institution, the costs associated with damage control and remediation of a breach. It also accounts for potential future financial losses incurred as a result of certain types of breaches, including any fines and penalties imposed by regulatory bodies.

Origination of Threat

For the purposes of a risk assessment of information security, these are the information assets like data systems, networks, website, etc.

Maintaining Control

An important step in evaluating threats is to factor in the safety measures an institution currently has in place. These safety measures, or controls, are key elements in evaluating the risk level of specific assets. Controls come in many forms: physical security measures (firewalls, virus protection), security policies and procedures, even locks on internal doors!

Unfortunately, many companies lack comprehensive knowledge of all the specific types of threats and vulnerabilities - as well as their relative severity - which makes evaluating the risk into usable data quite difficult. Moreover, risk events change over time: systems are upgraded staff turns over, new scams are generated. So the evaluations calculated today may be very different next year. It is important to have a continuous engagement with a qualified service provider that can offer the expertise and knowledge needed to maintain a proper balance of identifying and evaluating threats to information security.

The most effective method for identifying and evaluating risk factors is to continuously monitor an information system through standard, repeatable processes that are easily automated and produce verifiable documentation. A wise approach is to implement a Software-as-a-Service (SaaS) solution through cloud-based technology which gives the organization the flexibility to perform risk assessments and other compliance processes in a cost-effective manner.

Like traditional in-house software methods, SaaS or cloud-based applications document the entire audit process and procedures, ensuring consistent and complete actions and proof of accountability. This documentation also provides a basis for future assessments, reducing the efforts required to perform the process.

But a key advantage cloud-based applications offer is the ability to reduce IT expenses. Adopting a solution where software is delivered through cloud computing eliminates the need to install or maintain the software on the orgnization's system because the audit process is administered through a web browser interface. This helps reduce the amount of time IT personnel spend working on audit processes, reduces or eliminates additional vendor costs, and allows users to access applications from virtually any computer.

Leveraging Your Risk Assessment Data

The goal of an institution's efforts in identifying and evaluating information risk should be to not only satisfy compliance, but to also protect the data of your company and customers/members. This is done by having a clear view of where potential threats exist, the likelihood those threats could affect the organization, and how to eliminate or mitigate the risk. In order to correctly identify and evaluate risks to an institution's information systems, the best course of action is to conduct a comprehensive risk assessment.

Once an institution obtains the status of their information security, the results can be leveraged to provide several additional advantages.

Improve Internal Functions and Procedures

The knowledge gained in correctly identifying risk factors also leads many institutions to establishing better internal functions, such as:

- Awareness programs for both employees and customers/members
- Policy training programs for staff
- An increase in internal security
- More effective Disaster Recovery program

Gain a Competitive Advantage

Through the eyes of a consumer, the issue of privacy plays a major role when choosing a financial institution. The media stories about privacy breaches, identify thefts and loss of account information have sparked awareness to consumers like never before. And in light of the recent high-profile failings in the financial industry, the typical consumer tends to hold business executives to a much higher standard of accountability for their personal and business holdings.

Organizations that have a strong security policy, backed up with ongoing security tests, have a prime opportunity to leverage their commitment to consumer protection to gain a significant marketing advantage and thus, increase their market share, reputation, and profitability.

Reduce Costs Through Continuous Compliance

Historically, financial institutions have been primarily motivated to implement steps to protect information because of compliance regulations. But recent FFIEC guidance has made it clear that institutions of all sizes must adopt a strategy of "continuous compliance" and constantly be aware of potential risks and emerging threats. These trends have resulted in a growing need for a solution that will help develop and maintain an ongoing solution in a cost-effective manner. Investing in the right solution leads to an overall reduction in the costs associated with performing all the repetitive tasks required by regulators, redudnant vendors, unnecessary procedures, and the amount of manpower costs needed to not only perform security tests, but also compile the data for compliance reporting.

TraceSecurity believes that the key to helping financial institutions maintain a strategy of continuous compliance is be delivering it's services through cloud-based technology that leverages the expertise of their security analysts.

Delivering services via cloud-bsaed technology offers significant advantages over the traditional approach to maintaining a security risk assessment strategy, including:

Lower Cost of Deployment and Ongoing Ownership

Unlike when licensing software under a conventional installation model where an organization assumes several layers of costs like purchasing dedicated servers, deploying additional controls to secure the physical servers, and manpower to maintain the software and hardware, the cloud method eliminates unnecessary costs.

Because the software within a cloud can be housed and accessed on an institutions existing computers, the solution greatly lowers both initial capital expenditures and ongoing costs of ownership.

Universal Access to Applications

The ability to use web-based applications frees administrators from being tied down to a single workstation or network server when performing risk assessment and security compliance processes because the applications can be accessed by virtually any computer. Plus, cloud computing allows for group collaboration so that compliance efforts can easily be delegated to multiple users, thus increasing the chance that essential compliance administrators can have an uninterrupted holiday!

Rapid and Cost-Effective Response

Personnel changes, new business ventures, changes to internal policies and procedures, and amendments to regulatory requirements are just a few factors that trigger a need for adjusting the way risk is identified and evaluated, and most companies demand a solution that can respond rapidly to change without adding huge costs. Addressing changes with conventional software can be slow and cumbersome. Software updates need to be obtained from the vendor, installed, and tested before implementation. However, cloud-based solutions allow content or functionality to be changed or created quickly and deployed right away, enabling companies to respond to evolving risks without sacrificing time or money.

Streamlined Processes and Resources

One of the most beneficial advantages of cloud-based technology is the ability to have access to all the necessary tools to identify, evaluate and remediate security issues within one comprehensive portal. This streamlined method ensures that each step is performed according to the best practice standards and adheres to the appropriate compliance regulations. Using a comprehensive tool also consolidates resources by eliminating the need to find several different vendors to perform each individual function. This saves time in due diligence research and reduces expenses when duties of separate vendors overlap and duplicate repetitive processes.

Delivering applications through the cloud helps mitigate the most common risk element: the human component.

Conventional methods rely on human resources of the institution to configure the software, define test parameters and procedures, and maintain the software on in-house servers.

The resulting data of tests performed on the information systems typically must be manipulated by human efforts in order to produce readable and useable reports. This human interaction greatly increases the chance for errors and tainted results.

Choose a Partner, Not Just Another Vendor

Most compliance software vendors are only equipped to fulfill their clients' compliance needs by providing a one time snap-shot of the organization's security posture. After the vendor's initial obligation is complete, it is up to the client to figure out how to use the information. This scenario is quite frustrating for organizations because they require a wealth of expertise and insight about common security risk elements and regulatory developments in order to properly maintain an effective security strategy.

In stark contrast to those types of conventional vendors, TraceSecurity strives to become a partner rather than a vendor by remaining continually engaged with clients to focus on achieving actual, measurable business results... instead of just the sale of a software program or a one time service. In addition to offering comprehensive software solutions, TraceSecurity has a pool of expert security analysts dedicated to helping organizations maximize their compliance and risk management programs throughout the lifecycle of the engagement.

IT Security Risk Assessment Solutions

TraceSecurity's software solutions are designed to reduce the risk tendencies caused by human actions. These features include:

Pre-configured software: For clients who choose to administer the risk assessment themselves, TraceSecurity's software includes a pre-configured matrix of options in easy-to-navigate menus. This reduces the amount of custom configuration and helps eliminate errors.

Independent of institution's network: Since the core of TraceSecurity's software solution is maintained and secured independent of the organization's network, there is no need for their IT department to perform physical updates or maintenance on the server, reducing any unnecessary risk to the information or databases.

Customizable and integrated reports: A big disadvantage for organizations that perform their risk assessments in-house is the lack of comprehensive documentation of the assessment processes and the ability to generate the required reports for examiners or management. TraceSecurity's software has the ability to integrate results from several processes in order to generate customizable, easy to read reports. Having clear and concise documentation not only helps an organization obtain an accurate overview of their security posture, but it also helps streamline the audit process by providing examiners with all the required compliance documentation in one report.

Regardless of a financial institution's size, TraceSecurity offers a solution designed to improve and streamline its risk assessment efforts. We provide a full range of solutions that not only satisfies compliance regulations, but more importantly, supports the far-reaching goals of most financial institutions. We enable organizations the ability to drive the risk assessment process themselves, or have the TraceSecurity team administer the assessment.

Designed to be cost-effective for our clients, TraceSecurity's solutions help eliminate or reduce costs of managing multiple technology vendors, purchasing unnecessary hardware, paying for software support, and expenses associated with deploying in-house IT resources. And TraceSecurity's solutions are scalable. As the security needs of a financial institution mature, our solutions can be modified and enhanced to meet the changing landscape of the organization.

TraceSecurity's risk assessment procedures follow standard methodologies designed to meet regulatory requirements and best practices. Our solutions enable organizations to efficiently perform their own, on-demand Risk Assessment and generate comprehensive documentation for use in compliance reporting, thus reducing the time needed to rpepare for an audit.

The Risk Assessment process is managed through TraceSecurity's proprietary cloud-based software platform which are also offered as a stand-alone product.

We encourage all financial institutions to perform their due diligence before choosing any vendor, and invite all interested parties to contact a TraceSecurity expert to answer any questions or discuss options for your organization.