Cybersecurity Risk Management

An Online Continuing Education Course for Engineers

Course Number: FM-1004

Credit: 1 Hours / 1 PDH / 1 CPD

Cybersecurity Risk Management

William "Bill" A. Hein, P.E.

Introduction

Cybersecurity risk management is a continuous process of risk identification, risk analysis, risk control, risk financing, risk administration, and plan review and evaluation to mitigate and/or control an organization's various cybersecurity threats. These threats involve a wide variety of exposures, including but not limited to sensitive data leakage, system credentials security, phishing scams, dark web activity, malicious viruses, and ransomware exposures.

It also extends to brand protection, fraud protection, officer and executive protection, and supply chain threats. Automated cybersecurity threat mitigation efforts are essential to the management of these types of threats to an organization.

The importance of cybersecurity risk management is that it provides the basis for the organization and understanding of current cybersecurity risk exposures to make informed decisions regarding the implementation of procedures necessary to mitigate or minimize cybersecurity vulnerabilities.

With the rapid expansion of the need for data and the growing information technology (IT) infrastructure complexities, businesses are accumulating data at an exponential rate. This data is generally collected through financial transactions such as product sales or applications for financing in anticipation of a purchase. A background check on prospective customers or clients is another example of collecting confidential and/or protected customer data. The protection of this personal and confidential financial information is required to reduce the potential of becoming the target of scam artists.

Cyber-attacks can be internal or external to the organization. Internal threats are generally due to unauthorized access to confidential data records or computerized data storage files. External threats are generally from computer hackers who exploit an organization's data records through vulnerabilities in security protocols that may currently be in place to protect such data. System hackers are using artificial intelligence (AI) methods to gain unauthorized access to this data, and some hackers have hijacked AI technology implemented by businesses and reverse-engineered it to make even more invasive cyber-attacks in search of a wide variety of data elements.

An organization's employees can contribute to data security exposures through human error. Examples of these types of threats include employees inadvertently exposing the organization's computer system to malware or phishing exposures through lax enforcement of cybersecurity procedures or the lack of proper controls for the handling of emails and system access user credentials and passwords.

Cybersecurity risk management is the key to reducing the potential liability of an organization that could result from a data breach of sensitive client/customer information. These attacks have resulted in litigation actions by persons whose confidential data have been or even potentially may have been acquired by unauthorized sources. A strategic risk management program element is required to minimize a company's exposure to financial losses of this type. The implementation of the basic components of a risk management program is required for the development of a strategic plan to address potential cybersecurity threats in an organized manner that identifies and prioritizes cybersecurity exposures. These components include risk identification, risk analysis, risk control, risk financing, risk administration, and risk management plan review. In addition to reducing the organization's threats, a cybersecurity risk management plan is needed in many cases for regulatory compliance.

No business can eliminate every exposure to cyber-attacks, but a cybersecurity risk management program component within the organization's risk management procedures is the only way to reduce exposure to these threats as well as to demonstrate that the company is poised to protect its customer's confidential data.

To evaluate external threats, there needs to be a complete and detailed review of the organization's computer systems, software applications, and network connections to the outside world that are used to facilitate the company's business operations. By implementing a cybersecurity risk management plan, an organization will be able to have greater confidence that cyber threats and cybersecurity vulnerabilities are not being left to chance but are part of a decisive effort within the organization to mitigate these threats. A fully developed and implemented plan will provide policies and procedures to be followed that keep the organization's cybersecurity measures operational and updated on a regular schedule.

Cybersecurity Risk Identification

The process begins with an extensive evaluation of the organization's exposure to cyber threats and exposures to identify cyber-attacks from both internal and external threats to which the company may be exposed.

The evaluation of internal threats includes a review of hiring policies and background checks of company personnel and potential new hires. Improperly vetted employees and new hires will lead to a higher exposure to internal theft of a company's sensitive and confidential data. Employee hiring practices are most likely to have been addressed in the company's risk management plan but should be included in the review of possible exposures during the identification phase of the plan's development.

Internal cyber exposures may result from access to data by unauthorized personnel or improper handling or misuse by personnel who are authorized to access company records. Improper handling can also result in altering data or deleting information contained in data records by employees with proper authorization.

External cyber exposures can result from external hackers clandestinely accessing company systems to access and/or download company data. External intruders can also introduce viruses, malware, or ransomware into the organization's computer systems. These exposures can result in adverse financial consequences for the company due to the need to reconstruct data files, pay ransoms to regain access to their data, or through ligation expenses.

Seeking technical support from systems hardware and software suppliers can help identify exposures and bugs in the systems and software being utilized by the company. The utilization of flow charts can also help identify where the organization has the highest exposure to identified risks.

Many organizations utilize vendors for a variety of operational requirements. When vendors are granted access to company data systems, it is imperative that a complete investigation be conducted of their systems, network connections, and vendor employee controls for those who have or may gain access to company records or data. Identification of potential cyber threats from these vendors must also be considered and evaluated in the same manner as is required for an organization's exposures.

More and more companies are utilizing cloud computing and/or cloud data storage. A complete evaluation of the extent to which the organization's confidential information is transferred and stored in the cloud must be processed. The identification of potential sources of access by outside threats to cloud-stored data must be completed to determine the exposure to potential data breaches or data losses.

Another area of potential exposure is in the organization's data backup procedures, including external duplicate data facilities. This will also include the transmission of potentially confidential data during the backup of the company's main computer system. During the backup data transfer process, there is the potential for data loss or unintentional data deletion if the process is not evaluated prior to system implementation. A complete review to identify potential exposures to data loss, corruption and/or access by hackers or unauthorized personnel prior to any data backup process is essential.

The cybersecurity risk management plan also needs to identify and assess the potential of cyber losses resulting from natural disasters. Natural disasters such as floods, tornados, hurricanes, or wildfires can result in damage to or a complete loss of data records and information that is improperly or inadequately stored or protected. The inability to provide data services necessary for the success of the organization's business objectives is a major threat to a financial loss to the company.

Computer system or data storage losses can result from a variety of system failures. This can include failures that result from lack of or improper system maintenance as well as from loss of power from the electrical utility supplier. A backup generator will reduce the potential issues resulting from the loss of electrical services to the business or the community. The inability of the company to access its computer

systems can result in financial loss to the company through loss of sales/revenue and costs to restore system functionality.

When an organization has contractual obligations to provide system access or support to others, the loss of the ability to provide system access could result in financial loss from legal actions for failure to provide contracted services.

The entire risk management team must be engaged in every aspect of the cybersecurity risk management program. Key personnel and operational specialists should also be included in the risk analysis process. These individuals will have knowledge or expertise that will allow them to point out vulnerabilities that may otherwise be missed. Any missed or unidentified risk exposure becomes a possible operational or financial liability to the company.

Cybersecurity Risk Analysis

After the cybersecurity risks have been identified, an analysis of each identified risk must be completed. The analysis should result in a prioritized list of each risk that will allow the organization to address the most critical or costly exposures first in its risk mitigation process. It may also identify "low-hanging fruit" that can be implemented quickly at a low cost to the organization.

During the risk analysis process, it may be determined that some level of risk is considered acceptable based on the risk tolerance of the organization's management, and these will become self-insured or self-funded exposures. Not all risk is worth the cost of the level of protection or controls to mitigate the risk.

The risk analysis process will provide a blueprint for addressing the controls needed and the priority of implementation of risk control methods. Remember, by involving as many key players in the organization as possible, additional value can be added to the analysis process.

The objective of the analysis process is to identify and quantify all the systems and data assets of the organization and to rank them in order of their critical importance.

While most identified risks are relatively easy to identify and assess, it is important that any AI assets in place are also included in the analysis process. These assets are generally in place to quickly detect cyber threats, initiate a quick response to the threats, and protect the IT systems and data collected by the organization.

The next step in the analysis process is to associate all potential methods by which each of these identified exposures is vulnerable to cybersecurity attacks, assign a probability of likely occurrence to each of these, and associate a range of potential impacts that each of these could have on the organization should they occur.

It is important to remember that some cyber risks may impact the company's reputation or name. This risk must be controlled to prevent damage to the organization's brand. Failure to consider this cyber security impact may result in a loss of confidence in the organization's name brand and/or a negative impact on the stock price of the company.

Cybersecurity Risk Control

Cybersecurity security risk(s) contain various classes of controls, which include administrative or managerial, physical or operational, and technical or logical controls.

Administrative controls include the policies and procedures that provide the methodologies for administering the cybersecurity risk management plan. Physical controls are those that limit or mitigate cyberattacks, such as antivirus software. The use of AI technology is designed to detect and quickly respond to cybersecurity threats and has demonstrated a sharp increase in the detection and response to intrusive attacks. Technical controls are those that limit access to software applications such as encryption of data. Operational controls include cyber threat awareness training and classifications of assets.

Within these classifications are preventative, detective, recovery, and compensating controls.

Preventative controls include firewalls and user access credentials. Detective controls include antivirus and ransomware that activate automatically when threats are detected. AI software can be custom-tailored to a business's data and IT resources to improve resistance to cyber threat penetration. It is important to remember that AI resources are not a "once and done" exercise. As an organization's operations, data requirements, and IT systems develop over time, AI software must also be upgraded to remain an effective control of cybersecurity threats and attacks.

Recovery controls include backup procedures and processes. Compensating controls include procedures of an oversight nature that allow for the review of various levels or types of access to company data.

The initial control response should include the utilization of system antivirus applications, firewalls, and virtual private networks for information technology (IT) assets. The level of control through these systems should be based on the size and complexity of the organization's computer systems and usage.

For systems that allow access by customers, a two-step authentication process should be implemented as a means of management control that reduces the potential of unauthorized access to data systems. Dedicated servers for the delivery of data elements to these customers may be considered to limit the data available to them. The dedicated servers would only contain the data elements required for the completion of the contracted obligations.

Other cybersecurity risk control methods include data file and email encryption, as well as other automated system applications to increase risk control efficiency. Encrypted files reduce the potential of access to confidential data and records by rendering them unreadable if they are acquired by unauthorized parties.

Cybersecurity training should be implemented for everyone in the organization. This needs to include newly hired employees during their new-hire orientation sessions. It is important that all employees understand the cost and consequences of unauthorized access to the company's confidential or protected information.

Software developers have a stake in the control of cybersecurity and regularly update their software to correct existing software vulnerabilities or fix bugs i r current programs. P intaining up-to-date software, the organization will benefit from the ntrolling and correcting vulnerabilities, and thi tion.

Implementa needs to be a process in pl ducts cyber breach simulations t tial control requirements

A robust data b ckup provides a reliable metho deletion. A company's back testing of the backup procedur ery plans.

The effective cont anagement framework. A risk The International Orga on with the International Electr nage risks to the information syst ntained in the ISO 31000 stand

The National Institute best practices that can be used as a framework for a cyber ed to control identified risks to detect, respond, protect, and recover fr threats. The Cybersecurity and Infrastructure Security Agency (CISA) is a governmental agency that works with government and industry to identify, analyze, prioritize, and manage the most significant strategic risks to the nation's critical infrastructure. Since the nation's critical infrastructure is largely owned and operated by the private sector, managing risk is a shared priority. CISA creates an environment where the private sector, government agencies, and key stakeholders can collaborate, share expertise, and coordinate risk reduction activities to ensure critical infrastructure is secure and resilient now and into the future.

Cybersecurity Risk Financing

Management must decide on the methods and/or amounts of funds to be allocated for the implementation of identified cyber risks and the ongoing functionality of the cybersecurity risk management efforts.