Enhance Your Organization's Cybersecurity Strategy

Threats to cybersecurity are increasing both in quantity and in severity. From 2012 to 2013, Data breaches doubled and from 2013 to 2014, the average cost of data breaches went up by more than 15 percent. The average cost of a data breach in 2014 was $3.5 million.

Data breaches affect all organizations, from small not-for-profit organizations to large commercial retailers. Should your organization fall victim to a cyber attack, the results could be devastating.

Your traditional approach to risk management may involve information security measures such as processes to protect your physical data from unauthorized access, use or dissemination. Nevertheless, the current environment demands a risk approach that also protects your organization's electronic data and processes. Smartphones, computers and their networks need protection from unauthorized access and disruption, too. Cybercriminals frequently use these sources as points of entry into your organization, which could have devastating financial, legal and reputational consequences.

Approaching information technology and cybersecurity as a function of your internal controls can help protect your organization's key information. The Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s 2013 internal controls framework provides a good foundation for how to monitor and mitigate your largest threats to cybersecurity. Data breaches will cause you to examine your control environment, cyber risks, control activities, internal and external communication strategies and your monitoring strategies. If you have a robust cyber risk management incorporated into your internal controls, your organization can be much more efficient in responding to and recovering from a security incident.

CBIZ MHM Mayer Hoffman McCann P.C. An Independent CPA Firm

Learn more about how cybersecurity can affect your business at cbiz.com/cybersecurity

Control Environment

Everyone in your organization plays a role in minimizing your organization's cybersecurity risk, and it's up to your organization's management and cybersecurity team to communicate what that entails.

Common sources of data loss offer a good indication of the types of policies and practices that should be part of your risk management culture. Misplaced or stolen electronic devices rank as the primary cause of data loss. Recommended practices for how to treat company equipment could reduce the number of these incidents within your organization. For example, you might want to require employees to take home or lock up any electronic devices at the end of the workday.

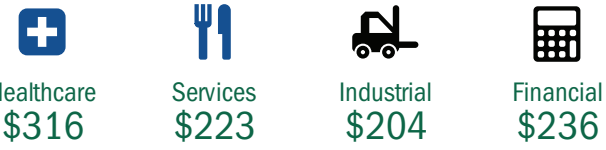
Lost or stolen laptops or other e-devices were the most frequent cause of data loss (20.7%), followed by hackers (18.6%)[3]

Hackers perpetuate roughly 18 percent of security incidents. They gain access to your organization's networks through programs that trace the key strokes on your computer or through malware inserted into your system via vulnerable software or third-party plug-ins. Your staff should be on guard for suspicious emails or other unusual requests for information, as they might be cybersecurity breaches in disguise.

Risk Assessment

A cyber risk assessment helps prioritize your approach to cybersecurity. The first step is to consider your organization's unique risk profile. Your industry and the kinds of information your organization collects are key predictors of which areas of your operations will be most at risk. Retailers have shown to be targets of hacks involving customers' credit card information. Health care institutions are highly vulnerable to having their medical records compromised.

Cost per compromised customer record[4]



Consider the value of the information your organization collects, both for the hacker and for your organization. On average, health care records involved in a data breach cost companies $316 per record. Compromised financial information cost companies $236 per record. Value doesn't exclusively mean records' monetary price, either. Information that if compromised would have a significant effect on your company's operations should command a larger share of your security resources.

Part of the risk assessment may include an information technology audit. The multifaceted approach to your existing protocol helps identify the areas of vulnerability and risk. A network security assessment can turn up vulnerabilities in your external and internal networks and review firewall, intrusion prevention and network access control systems and policies and assess wireless networks to provide you a clearer picture of where your risks may lie. Network penetration testing should also be included in your information technology assessment, as this can give you a sense of how easily security incidents can be detected in your current operating environment. Testing can also give you an idea of the potential magnitude a cybersecurity breach would have on your organization.

Control Activities

Internal controls are essential to the effective operation of all organizations. They are the activities or procedures designed to provide reasonable assurance to management that operations are "going according to

plan." Without adequate internal controls, management has little assurance that its goals and objectives will be achieved. Properly designed and functioning controls reduce the likelihood that significant errors or fraud will occur and remain undetected. Internal controls help ensure that departments are performing as expected.

Control activities are the policies and procedures designed by management to protect the organization's objectives and goals from internal or external risks. Some common and important cyber risk control activities are logical security, change management, mobile devices and wireless, backups, monitoring of third party providers and cloud services.

Logical security controls help make sure that one person does not have too much power or influence over your organization's cybersecurity. Consider segregating duties on your cyber risk team. Frequent password changes, limiting the system administrator function and logging and/or reviewing system administrator changes made in the financial accounting systems are recommended practices.

Change management controls can regulate updates and other modifications that go into production. Your organization should implement procedures that notify management of changes and allow management to approve any modifications prior to the work being done. Then, your organization should test the update using someone other than the developer. If satisfied that the modification works appropriately, there should be an approval process before the change goes into the production environment.

Mobile device and wireless access need controls to protect them from unauthorized access. Best practices include encrypting mobile devices and removable data, issuing unique user IDs and complex passwords and automatically wiping devices that are lost or stolen. The remote wiping of devices is especially important because as mentioned earlier, missing devices are the most common source of organizational data loss.

Controls should also be in place to protect your data back up. Your organization needs to know what is backed up and where it is being stored, be it a data center, third party provider or cloud provider. Back-up controls to implement include real-time notification and resolution of back-up failures, off-site back up and replication and periodic restores. Annual or semi-annual service organization control audits can help your organization manage your third party service providers. If no service organization control audit reports are available, then be sure your back-up controls include periodic visits to the third party provider or cloud provider offices and hosted data centers. You should also request and review monthly or quarterly provider reports that detail the significant events that took place, the people who accessed the third party provider or cloud provider site and planned outages by the third party or cloud provider.

Whenever you are working with a third-party service provider, you also need to make sure your organization is knowledgeable and involved in the provider's disaster recovery plan. If an unplanned outage affects a provider, your organization should be prepared for the potential effect that would have on its operations.

Information and Communication

A breach rarely occurs because of one incident, which makes it imperative that your organization have the means to collect and analyze meaningful information about its cybersecurity. A system that aggregates data from different sources can identify patterns, which indicate whether your organization is facing a breach.

Written communication plans that address what information is distributed to whom are highly

recommended. Third parties involved with your organization's IT security should be considered part of this communication plan, and your organization should be part of theirs, as data breaches on their end could affect your data.

Depending on what is lost, you may be at risk for legal action by the affected parties. Your legal team should be involved to help minimize your liability exposure. They can also help you identify who needs to receive communication. Sometimes law enforcement, state attorneys general and even federal agencies may need to be included in the conversation about the breach.

Monitoring Activities

The risk environment continues to change and evolve, and so, too, should your cyber risk management strategy. Organizations should regularly evaluate the effectiveness of their current strategy and that of any third parties that administer their information technology security. They should then present findings to key stakeholders for consideration. Periodic cyber risk assessments should be part of your monitoring activities as well so that you can see how your systems are holding up to internal and external risks in your operating environment. Planned changes, such as adding a new third party service provider or moving office locations are also good times to revisit and update your cyber risk strategy.