Cyber Security Risk Management

Risk management refers to the process of identifying, assessing, and controlling threats to a company's finances.

These risks or threats could come from a number of sources including legal liabilities, strategic management mistakes, accidents, and natural disasters.

As we move toward an increasingly digital way of life, cybersecurity introduces additional risks that have to be managed appropriately.

It's possible to invest in various types of insurance to protect physical assets from losses, but digital data isn't tangible – and therefore isn't covered under these kinds of policies.

Cybersecurity risk management relies on user education, strategy, and technology to protect an organization against attacks that could compromise systems, allow data to be stolen, and ultimately damage the company's reputation.

The rate of cyberattacks continues to grow both in terms of volume and severity. As such, businesses who want to protect themselves to the best of their ability must begin focusing efforts on cybersecurity risk management.

> *When evaluating all potential business risks, it's crucial not to overlook*

technology and cybersecurity.

Cybersecurity Risk Management Process

You want to begin the process by starting with a cybersecurity framework that's been developed from each area of your business to determine what your desired risk posture should be.

It's a good idea to use technology that can help you find an app data across the organization.

Once the data is mapped, you'll be able to make better decisions on how the data is governed and reduce your risk. For instance, even with training and strong security culture, it's possible for sensitive information to leave a company by accident.

Leaving data stored in hidden rows across spreadsheets or included in notes within employee presentations or email threads leave your room for accidental data leakage.

By scanning the company for sensitive data at rest and then removing any of that data stored where it does not belong, you greatly reduce the risk of accidental data loss.

Use the Community Maturity Model

Initial

This is the starting point for using a new or undocumented repeat process.

Repeatable

At this stage, the process is documented well enough that repeating the same steps can be attempted.

Defined

At this level, the process has been defined and is confirmed as a standard business process.

Managed

At this level, the process is quantitatively managed according to the agreed-upon metrics.

Optimizing

At the final stage, the process management process includes deliver it action to optimize and improve it.

Once you've determined the desired risk posture, take a look at your existing technology infrastructure to set the baseline for the current risk posture, then determine what must be done to move from the current state to the desired state.

As long as your organization is taking proactive steps to understand all the potential risks, you decrease the likelihood of running into a security incident that could hurt the company.

A vital part of the risk management process is to conduct a risk and reward calculation. This helps prioritize security enhancements that will give you the greatest improvements at the lowest cost.

Some companies may be comfortable with 99% of all security upgrades being made but others especially those in highly regulated industries, will want to be closer to 100%. Because of this, there should be incremental steps and goals such as a 5% Improvement achieved within 6 months, that can be measured to determine if the company is making progress toward its final goal.

That said, even small security vulnerabilities can lead to massive losses if systems are connected in a way that allows access to an unimportant area to bridge entry into systems that contain sensitive data.

The only way to ensure a system is fully secure is to make sure no one can access it – which isn't practical. The more you lock down a system, the harder it becomes for authorized personnel to conduct business as usual.

If authorized users determine they cannot access the data they need to perform their jobs, they may look for workarounds that could easily result in compromised systems.

Mitigating Security Risks

So you will never be able to eliminate all cyber threats and security risks, there are a number of precautions you can take to mitigate risks when it comes to cybersecurity.

Among these are the option to:

- Limit devices with internet access
- Limit the number of staff members with administrator credentials and control the rights for each administrator
- Limit administrative rights
- Use antivirus programs and endpoint security
- Require users to implement two-factor authentication to gain access to certain files and systems
- Install network access controls
- Allow automatic updates and patches for operating systems
- Place limits on older operating systems
- Use firewalls

To take risk mitigation a step further, your organization may also want to consider advanced encryption, redaction, an element level security.

Advanced encryption has to be implemented systematically and strategically to protect data from cybercriminals and insider threats.

This includes standards-based cryptography, advanced key management, granular role-based access and separation of duties, and algorithms that drastically decrease exposure.

Data encryption can help protect against outside breaches, but it doesn’t do much to prevent internal data theft.

Employees with access to sensitive data will have the credentials needed to decrypt it as part of their daily work, so organizations must also take action to prevent that data from being removed from the corporate system through flash drives and other removable media.

Redaction creates a balance between data protection and the ability to share it.

With redaction, companies can share the information they need to share with minimal effort by hiding sensitive information such as names, social security numbers, addresses, and more.

Redaction is an important part of data security, but companies need to be able to do it at the property level based on employee roles.

Companies also need to be able to implement custom and out of the box rules as necessary. With PLANERGY, user permission can be controlled at a highly granular level should go a long way toward preventing accounts payable fraud.

Humans and Cybersecurity

There are only so many technological precautions you can take. To address the human element, it is crucial to provide ongoing training and education about the ever-changing threat landscape.

Today’s hackers have moved beyond viruses and other malware to phishing and spearphishing which targets those with administrative rights and individuals with access to certain files that contain malware or to provide sensitive personal, or corporate data and credentials.

Phishing and spear-phishing can easily be confused with one another because they are both online attacks where users inadvertently provide confidential information to hackers.

Phishing is a broad term for any attempt that tricks users into sharing sensitive information like their passwords, usernames, and credit cards for any malicious reasons.

Spear-phishing, on the other hand, is a targeted attempt to steal sensitive information from a specific victim generally for malicious reasons.

This is often achieved by gathering personal details on the victim including their hometown, employer, locations they frequent, and things they purchased online.

Afterward, the attackers disguise themselves as trustworthy entities or friends to acquire sensitive information usually through email or other forms of online messaging.

This is the most successful form of accessing confidential information on the internet accounting for 91% of attacks.

This is why it is ideal to include information security in your company policies for both company employees and your business partners. This way, everyone you work with knows what is and is not allowed.

When evaluating potential vendors to work with you as part of your supply chain, it's critical to ask them for a cybersecurity risk assessment because any third-party risk has a potential impact on your business.

If there is a data breach with one of your suppliers, your customer's data could be compromised, which could tarnish your reputation.

Part of your risk management strategy needs to include a detailed risk profile on all of your business partners.

Responding to Security Incidents

Unfortunately, just being on the internet and exposes a company to cyber risk both internal and external attempts will be made to compromise an organization's data. Incident response plans need to be in place to determine the actions to take if certain incidents occur.

For example, an increase in hacker attempts at the company or in the company's industry could trigger heightened precautions.

If an actual data breach occurs, the company should have detailed plans in place for who to notify both inside and outside of the company, contact information for law enforcement, business suppliers and customers along with an action item checklist and public relations response.

The Information Technology Laboratory (IITL) at the National Institute of Standards and Technology (NIST) suggests:

- Preparing for any incident with special focus on common attacks including, email, web, loss or theft of equipment, attrition, and removable media.
- Using lessons learned after a major incident has been handled to review

the effectiveness of their process and identify potential improvements for both security controls and handling practices
- creating an incident response policy that includes a statement of management commitment, the purpose and objectives of the policy, the scope of the policy, the definition of security incidents and related terms, organizational structure and role definitions, responsibilities, and Authority levels, prioritization of incidents and more.

An incident response policy should be developed for each potential security incident possibility. For instance, email breaches may require a different set of employees and policies than an internal data breach due to equipment loss or theft.

Ideally, companies will take time to develop a comprehensive security posture that includes a combination of technologies such as endpoint protection, threat intelligence has, access controls, and firewalls.

It’s worth considering hiring a risk management service to provide a comprehensive assessment and solution recommendations to ensure the security budget is optimized.

Though the initial assessment and implementation of policies and procedures take a considerable amount of time, cybersecurity risk management should never be considered complete.

As an ongoing process, your cybersecurity policies should be treated as a living document that needs to be revised and updated regularly.

After a company conducts its original risk assessment and advances from their current to their desired risk posture, periodic assessments should be conducted to identify new vulnerabilities threats and develop a plan for how to address them so that the risk posture can be maintained.

The goal is to develop strongly secured information systems without any cybersecurity incidents to report, but the fact is that every company is at risk. While some companies have more risk than others, one thing is certain: the lack of a cybersecurity program will definitely have a business impact at some point or another.

The time to build your risk management program is now – before any data is compromised – not after.

What’s your goal today?

1. Use PLANERGY to manage purchasing and accounts payable

We’ve helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our “Solutions” page to see the areas of your business we can help improve to see if we’re a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide “Preparing Your AP Department For The Future”

Download a free copy of our guide to future proofing your accounts payable department. You’ll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts