ASG INFORMATION TECHNOLOGIES

OUR TOP 5 TIPS
FOR PRESERVING THE INTEGRITY OF YOUR IT SYSTEM

Our 5 Tips:

Prioritize Network and Data Security

Secure Your Emails

Perform Regular Vulnerability Scanning and Penetration Testing

Create Business Continuity and Disaster Recovery Plans

Implement A Customized Solution

There is no doubt that COVID-19 has accelerated digital transformation in the financial services industry. Moving banking away from the confines of branches, offices, and data centers to mobile phones, tablets, laptops, and the cloud, opened up data to new vulnerabilities.

Financial institutions have become lucrative targets for cybercriminals preying on a remote, distracted, and vulnerable workforce. Moreover, employees' lack of understanding of security controls, performance, and risk in the new operating environment has added to the vulnerability.

By offering proactive and preventative services, IT service providers like ASG prevent minor issues from escalating into catastrophic events. Avoid costly data loss, repairs, and downtime by implementing the following five tips to preserve the integrity of your IT system:

Prioritize Network and Data Security

Cybercriminals are continually finding new ways to harm businesses. When your company's data isn't properly secured, you run the risk of internal or external cyberattacks.

The majority of cybersecurity breaches are the result of leaked credentials. Malicious employees can abuse their access for their benefit, while employees without proper training can unwittingly download malicious software or invite hackers into your company's system.

Cyberattacks can result in costly network downtime, litigation, corruption, or business and client data loss, including confidential customer files and financial information.

Your business can mitigate these threats by employing knowledgeable, trained personnel and leveraging expert security solutions.

ASG INFORMATION TECHNOLOGIES

OUR TOP 5 TIPS
FOR PRESERVING THE INTEGRITY OF YOUR IT SYSTEM

Secure Your Emails

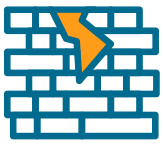
Spam and phishing emails are not merely a nuisance; they present a significant threat to business productivity and security.

Phishing Attacks occur when links listed in emails (which appear to have been sent by familiar individuals or organizations) lead to websites that trick victims into submitting confidential information, such as credit card numbers and passwords.

These malicious messages can harm the imitated organization's reputation, especially if sent to clients or customers. Alternatively, if spoof emails are sent to employees, malware can be introduced into the corporate network. 92.4% of spam emails contain malware attachments, which allow cybercriminals to access and damage computer networks.

Spam and phishing emails detract from employee productivity, as irrelevant messages require filtering and deletion, and spam filters require updating. These disruptions are costly. Businesses that fall victim to phishing emails can expect to direct innumerable resources toward recovering and securing compromised customer and employee data. They can also incur forensic and legal fees and regulatory fines and penalties.

Exchange solutions, such as Microsoft Exchange, Office365, and Web-based hosted exchange solutions, can bolster your business's defenses against cybercriminals.



Perform Regular Vulnerability Scanning and Penetration Testing

Organizations should maintain baseline reports on key equipment, and investigate changes in open ports or added services by performing Vulnerability Scanning and Penetration Testing. These procedures are vital components of a strong network security profile, and crucial to cybercrime prevention.

Vulnerability scans search systems for weaknesses; they can alert network defenders to malware infections, violations of change-control policies, missing patches, and outdated protocols, certificates, and services.

Analysts recommend preserving information security by scanning equipment quarterly, before new equipment has been deployed, and after changes have been made.

Regular Penetration Testing helps identify insecure business processes that cybercriminals can exploit, such as lax security settings, transmission of unencrypted passwords, password reuse, and forgotten databases storing valid user credentials.

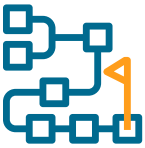
Effective Penetration Test reports describe the method of exploitation, the value of exploited data, and recommendations for improving organizational security.

Penetration tests are best conducted by an experienced third-party vendor, like ASG, who can

ASG INFORMATION TECHNOLOGIES

OUR TOP 5 TIPS
FOR PRESERVING THE INTEGRITY OF YOUR IT SYSTEM

provide an objective view of the network environment and avoid conflicts of interest, while also thinking abstractly and anticipating cybercriminal behavior that could potentially harm business activities.



Create Business Continuity and Disaster Recovery Plans

Business Continuity and Disaster Recovery Plans (DRPs) help companies and their employees cope with natural disasters, cyberattacks, and other events that could detriment their business.

A Business Continuity Plan enables businesses to protect critical services and prioritize their operations. It provides an overview of the personnel, business processes, record recovery, suppliers, vendors, clients, and other components necessary to revive a business after disaster.

The Business Continuity Plan should include a series of Disaster Recovery Plans.

DRPs detail how specific groups within a company will recover business applications after disaster occurs. The IT disaster recovery plan is one of the most common; it explains how to respond to technology disasters, such as data-loss, damaged or destroyed servers, and hacking.

The first step in developing a DRP is conducting a business impact analysis. This will help you identify which assets are at risk, including employees, property, infrastructure, IT systems, and data.

The second step in developing a DRP is estimating how loss or disruption in one or more aspects of your business would impact sales, brand credibility, industry compliance, legal fees, and public relations. You can generate estimates by mapping out your business model and determining which departments and vendors are interdependent.

Step three is identifying alternative facilities that could be utilized if your primary facility is rendered unusable by disaster. Plan to back up critical data with a remote, online, or managed backup service, sometimes marketed as cloud backup. This service provides users with a system for the backup, storage, and recovery of computer files.

Finally, develop an IT recovery plan to restore your infrastructure (including servers, networks, computers, data, and connectivity), and create step-by-step procedures to implement your DRP.

It's also important to train and assess your employees on your DRP, and contract with suppliers who can provide equipment, hardware, networks, and power in the event of an emergency.

Implement a Customized Solution

Break/Fix is the fee-for-service method of providing IT services; IT solution providers perform tasks as needed and only bill customers for completed work. Break/Fix appeals to many business owners because it lowers the initial cost of

OUR TOP 5 TIPS
FOR PRESERVING THE INTEGRITY OF YOUR IT SYSTEM

IT maintenance. However, the reactivity of a cost-centric approach leads to minor issues remaining unaddressed. These issues can escalate into significant (and expensive) IT challenges.

Thus, businesses need a customized cybersecurity strategy. An ongoing relationship with an IT maintenance provider can transform your business' technology into an asset by providing a comprehensive approach to cybersecurity that reduces human error and allows employees to prioritize business operations.

By offering proactive and preventative services, including Managed IT Support, IT Consulting, Data Backup & Recovery, Cloud & Mobile Solutions, and Network & Data Security, providers like ASG prevent minor IT issues from resulting in costly data loss and repairs and downtime.

Get in touch for more information about how ASG can help grow and protect your business.

ASG INFORMATION TECHNOLOGIES