ICE
TRUSTED IT PARTNER

ICE's Ultimate Guide to

EFFECTIVE CYBERSECURITY

The most inmportant security policies, procedures, practices and tools every business should have in place in 2023

ICE
TRUSTED IT PARTNER

ICE's Ultimate Guide to

EFFECTIVE CYBERSECURITY

THINK YOUR COMPANY IS TOO SMALL TO WORRY ABOUT CYBER-ATTACKS?

Most do, as 47% of businesses with less than 50 employees don't allocate any funds towards cybersecurity. However, Accenture's Cybercrime study revealed that nearly 43% of all cyber-attacks targeted companies with less than 50 employees!

With data breaches up 5-fold since 2020 and climbing no matter how big or small your business is having an effective cybersecurity strategy should be every business owner's top priority.

Expect a Breach

The best defense against a cyber disaster is to anticipate one. Start with the most significant facts that your firm has to offer. This might be information about your products, website, or payments. Conduct a risk assessment to find the weak points in your security. Think about potential threats and what you would need to do if they materialized.

Train Employees in Security Principles

Workers must understand their role in maintaining the safety and security of the company's data. Teach your staff the best practices for safeguarding client and company data. Strong passwords and cautious internet usage are among the fundamental security procedures. Also, employees need to be informed about phishing schemes and how to avoid them. As there is always a chance of a cyberattack, it is important to enforce and regularly review the training. Although yearly training is a good start, your company will gain from two to three trainings annually.

Use An Encrypted Email Or Messaging Server

Because employees use email on a daily basis, they are constantly at risk of assault. A message's likelihood of being intercepted and/or decoded by a cybercriminal will be reduced if it is sent using an encrypted messaging service or email. To reduce the likelihood that undesired emails will reach employees, email servers that apply spam filtering technology will automatically find and remove emails that seem to be phishing assaults from those users' inboxes.

Ensure A Strong Password Protocol

A password manager should be used by businesses to ensure strong protection for both customer and employee passwords. All passwords will be saved and encrypted by this type of system, making it impossible for anyone to access information without first submitting a two-factor authentication request. The stored account logins and passwords, which are often a string of randomly generated alphanumeric and special characters, can't be linked back to the password manager, and employees only need to remember one master password.

Keep Antivirus Software Up-To-Date

A device's antivirus software may not always provide security because hackers create new viruses every day. Updating antivirus software will provide employees' devices with new information on malware, spyware, ransomware and other types of viruses to increase their chance of being removed. Antivirus software can be set to update automatically, just like operating systems.

Enable Automatic Operating System Updates

Operating system updates are frequently implemented to reduce or get rid of vulnerabilities in earlier versions. It can be challenging for most staff to remember to check equipment for newer operating system versions. Therefore enabling automatic upgrades on all workplace devices will lessen the likelihood of a hack. Malicious software designed for a particular version will be found and eliminated by the operating system in a subsequent update when devices are upgraded.

Create Backup Copies of Company Data

You'll require data backups in the event of an attack or software fault. Always make a backup of your data, including documents, spreadsheets, databases, and accounting data. Although data should be backed up at least once every week, automatic backups can help free up time. When done manually, this might take quite a while. The copies of the data should be kept offsite or in the cloud.

Your information will be safeguarded in an emergency if you have multiple backup copies that are stored securely in different places. In the event of a virus, natural disaster, or cyberattack, it enables you to retrieve your data. You run the danger of losing all of your data and never being able to retrieve it if you don't use data backups.

Limit The Number Of Network Administrators

No one outside the IT department should be able to install applications that are not on the company's approved list or change network configuration settings. The organization will have more control over its devices and security risks will be greatly reduced by adopting a decentralized cybersecurity strategy and minimizing the number of network administrators. Another excellent practice is to audit and delete accounts for staff members who have changed workstations or have left the company.

DO YOU HAVE

$4.24

MILLION DOLLARS TO SPARE?

That is the average cost of a data breach today

Upgrade Your Company's IAM

The business procedures that handle electronic identities are collectively referred to as identity and access management, or IAM. You run a larger risk of hacking and data breaches if your identity and access management systems are ineffective or out of date. There are several benefits of IAM systems, like:

- Enhanced security
- Fewer password issues
- Improved user experience
- Reduced IT costs

Use A Secure Connection For Company Devices

Employees should never connect company-issued devices to a public network. Many employees were compelled to work remotely under COVID-19, so it's crucial to make sure they're only connected to the private in-home network, mobile hotspot, or virtual private network (VPN) that the company has advised. When visiting websites, staff members should use a secure protocol by looking for HTTPS in the URL or a lock icon in its place, as well as adhere to the Zero Trust architecture if it has been accepted by their company.

Enable Auto-Lock For Company Devices

Computers should lock their screens and require users to check back in after being idle for a certain period of time (about three to five minutes). This will shield the information on the gadget from prospective observers who are inside or outside the building. Also, when logged in, prohibited individuals can access the computer remotely, thus it shouldn't be left running when the employee is not watching over it.

Dispose Equipment And Data Securely

When not in use, sensitive information-containing devices shouldn't be thrown away. The hard drive must be thoroughly formatted to erase all data before being either destroyed or recycled electronically. Any linked data can be entirely recovered by using a SATA cable without physically damaging the hard drive. But, it's crucial to make sure the drive's data is backed up before being destroyed.

Create a Mobile Device Action Plan

Individuals frequently access work resources through their mobile devices, which might be a security risk. Mobile devices frequently connect to public networks and lack significant protection. The device's data may be exposed if you connect to unsafe Wi-Fi. Hackers may also be able to obtain critical information by downloading malicious programs or by opening unsolicited emails or SMS.

Employees who use mobile phones for work should be required to:

- Password-protect their devices
- Encrypt their data
- Use a security app to prevent cyber hacks

54%

OF BUSINESSES ADMIT THAT THEIR

IT DEPARTMENTS LACK THE EXPERIENCE

TO MANAGE COMPLEX CYBERATTACKS

Adopt A Decentralized Cybersecurity Strategy

The centralized cybersecurity strategy that many corporations had adopted in 2021 was shown to have serious flaws. Companies that give all departments the identical user permissions for their systems frequently struggle to drive innovation and are more susceptible to brute force attacks. Providing the chief information security officer (CISO) with the authority to regulate and supervise user privileges can stop certain departments from being granted access to information they don't require.

Create A Cybersecurity Strategy Independent From IT Strategy

Since that cybersecurity largely deals with protecting digital data, it may seem reasonable to mention it in your company's IT strategy. Yet, cybersecurity entails a unique set of dangers that are frequently more complex and require quicker incident reaction times. The CISO is a critical stakeholder who should address cybersecurity threats at the business level and create plans for prevention and response in order to avoid conflicts of interest. The business's operations and people resources, as well as Technology assistance, will probably be needed to mitigate these risks.

Develop An Effective Cyber Incident Response Plan

Staff members may more efficiently detect, respond to, and recover from cybersecurity events with the use of an incident response plan. In some industries, it is essential by law to have a proper strategy in place, — nevertheless, all firms that use technology to access sensitive data should follow incident response rules. The incident response strategy should include exactly how to record and lessen cyberattacks and what procedures must be taken to get systems and software up and running as soon as possible after an occurrence.

Implement A Zero Trust Architecture

Never trust, always verify is a principle that the Zero Trust security model aims to instill in an organization's culture. This cybersecurity architecture gives IT and network workers the go-ahead to automatically ban access to all devices, whether or not they are linked to a legitimate network. To confirm allowed access from devices, a Zero Trust policy encourages two-way authentication, also known as mutual authentication. A remote monitoring protocol can be used to inspect and monitor traffic as well as authenticate devices using public certificates or a username and password.

IF YOUR BUSINESS FALLS

VICTIM TO RANSOMWARE

THERE'S A

51% CHANCE

YOU'LL PAY THE FEE

Conduct Regular Cybersecurity Assessments

System and software audits should be conducted regularly to identify for emerging vulnerabilities. Even though the most recent release of a certain piece of software could appear to be risk-free to use, some upgrades may unintentionally damage the systems of an organization or expose them to dangers because of an unstable release that is being made available. While evaluating a network, it is recommended practice to speak with an impartial cybersecurity professional because they provide considerable knowledge and can provide wise recommendations.

ICE

TRUSTED IT PARTNER

Employ Third-Party Penetration Testing Services

If a cybersecurity company from a third party can access networks, a bad person most likely can too. A network's vulnerabilities can be found and effectively fixed using penetration testing, also referred to as "ethical hacking," before they are found by any unauthorized users. Despite the fact that this service can be costly, it is still less expensive than the millions of dollars in fines that a data breach would incur.

CONTACT US FOR A

FREE SECURITY POSTURE ASSESSMENT TODAY

ICE Consulting, Inc
www.iceconsulting.com
888-423-4801