KIRKHAM IRONTECH

CYBER SECURITY IN THE WORKPLACE

After reading this guide you will know the basics of being cybersafe at work. You'll gain insight into common misperceptions that could cost your company millions of dollars of revenue loss, and you'll know exactly what is at stake.

www.kirkhamirontech.com

KIRKHAM
IRONTECH

CONTENT

www.kirkhamirontech.com

KIRKHAM
IRONTECH

"Cyberattacks -- the threat is real, imminent and **non-discriminating**. Anyone can be a target."
- Tom Kirkham CEO

INTRO

Cybersecurity is not all that important. Productivity trumps safety.

That is the old way of thinking and it couldn't be more wrong. In today's world, cyber security is one of the most important aspects of any business.

At least it should be. The threat is real, imminent and non-discriminating. There are hackers everywhere, some of them aren't even human. There are hackers that have created armies of bots that wreck havoc. In fact, a cyber pandemic is a real possibility and it could happen at any time.

www.kirkhamirontech.com

STEP 1

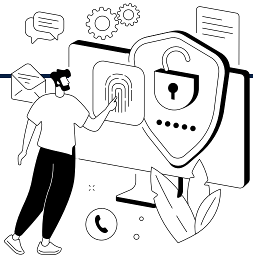
IDENTIFY THE CROWN JEWELS OF YOUR BUSINESS

Understanding what information cybercriminals are most after is essential to combating cyber attacks.

Creating an inventory list of the valuable data and assets within your organization, including manufacturer, model, hardware, and software information, is of the utmost importance.

Identify all stakeholders generating these data sets. Also take note of who has access to important data and information and account for all storage locations.

This practice will ensure that business leaders have a track record of accessibility so that they know where to look in case of a vulnerability or breach.



STEP 2

HOW TO PROTECT YOUR ASSETS

Protecting your data and devices from malicious actors is what cybersecurity is all about. In order to accomplish this, make sure your security software is current. Investing in the most updated software, web browsers, and operating systems is one of the best defenses against a host of viruses, malware, and other online threats.

Another important way to keep your assets safe is by ensuring staff are using strong authentication to protect access to accounts and ensure only those with permission can access them. This includes strong, secure, **differentiated passwords**.

According to a 2021 PC Mag study, **70% of people admit they use the same password for more than one account.** Using weak and similar passwords makes a hacker's life a lot easier and can give them access to more materials than they could dream of.

STEP 3

OFFENSIVE MONITORING

Companies must always be on the lookout for possible breaches, vulnerabilities, and attacks, especially in a world where many often go undetected. In order to protect your assets, you must take an **offensive approach** -- or breaches *will* go undetected.

Investing in cybersecurity services. Make sure your employees and personnel are following all established cybersecurity protocols before, during, and after a breach. Individuals who **ignore** or disregard important cybersecurity practices can compromise not only themselves but the entire organization.

Paying close attention to whether your company is fully embracing all of your cybersecurity procedures and technology is fundamental for business leaders who wish to ensure data privacy. Compliance is crucial for safety.

STEP 4

THE INEVITABLE HAS HAPPENED

Building your Response Plan. No matter how many safeguards you have in place, the unfortunate reality is that cyber incidents still occur. However, responding in a comprehensive manner reduces risks to your business and sends a positive signal to your customers and employees. Therefore, businesses should have a **cyber incident response plan** ready to go before a breach.

Companies should embrace savvy practices such as disconnecting any affected computers from the network, notifying their security team or the **proper third-party security team vendors**, and utilizing any spares and backup devices while continuing to capture operational data. This way, you can maintain some sense of normalcy and operations while also protecting your data.

KIRKHAM
IRONTECH

STEP 5

WHAT DO WE DO NOW?

"If you've got **off-the-shelf cybersecurity tools** without a security team engaged analyzing and checking out threats, then **you don't have enough in place**. It's that simple. Regardless of ROI."
--Tom Kirkham CEO

Educating Employees on Cybersecurity

Even with all of the right procedures and protocols in place, a business is only as strong as its **weakest link**. Therefore, employees must be properly trained on cybersecurity best practices. This includes everything from using strong passwords to not downloading email attachments from unknown senders.

A clear understanding of the company's specific policies can help ensure compliance. Businesses should also **provide employees with regular updates** and reminders about cybersecurity threats as well as the steps they can take to protect themselves and the company.

KIRKHAM
IRONTECH

THE SECRET KEY TO COMPLIANCE:

COMPANY CULTURE

Vision

A proactive company culture regarding cyber safety means that cybersecurity is **not just the responsibility of the IT department** but of everyone in the company. When everyone is aware of and takes ownership of cybersecurity, it becomes second nature and part of the company's DNA.

Creating this type of culture requires **strong leadership from the top down** as well as constant reinforcement and education. Leaders should be visible and vocal about their commitment to cybersecurity, while also setting the tone for the rest of the organization.

Mission

Policies and procedures must be clear, concise, and easy to follow. Providing employees with ongoing technical cybersecurity training **empowers every team member** so they understand not only what is expected of them but also why these practices are of vital importance.

Cybersecurity is not an anti-virus. Taking a DIY approach doesn't cut it anymore.

Remember: cyber incidents happen to any organization, no matter how big or small.

KIRKHAM
IRONTECH

MEET OUR TEAM

Tom Kirkham

CEO Director

Tom brings more than three decades of software design, network administration, and cybersecurity knowledge to organizaions around the country. During his career, Tom has received multiple software design awards and founded other acclaimed technology businesses. He is an active member of the FBI's Arkansas InfraGard Chapter and frequently speaks about the latest in security threats. You'll be hard pressed to find someone more qualified than Tom to operate a cyber security company.

Matt Caswell, President and Chief Operating Officer of IronTech Security has over 25 years of experience in sales and account management. A lifelong computer enthusiast, Matt has worked in the technology world for over 20 years and has years of cybersecurity research under his belt. Matt is passionate about protecting organizations and assuring they are secure. In addition, Matt is an experienced public speaker and presenter. In his free time, Matt enjoys boating and golfing.

Matt Caswell

President

www.kirkhamirontech.com

KIRKHAM
IRONTECH

OUR SERVICES

Technical Evaluation

Real-time defensive monitoring with cybersecurity experts and SentinelOne

**Early risk detection for cybersecurity gaps.
Pentesting services.**

**Cybersecurity education, consulting and testing.
Keep your team in the know, now.**

www.kirkhamirontech.com

KIRKHAM
IRONTECH

GET IN TOUCH WITH US

At IronTech Security our life's work is to protect individuals and businesses from the nefarious motives of cybercriminals. We pride ourselves in being a Best of Breed service provider, constantly striving to attain the finest technology while providing cutting edge defensive training.

☎ (479) 434-1400

✉ info@kirkhamirontech.com

📍 3111 Old Greenwood Rd Fort Smith, Arkansas 72903

www.kirkhamirontech.com