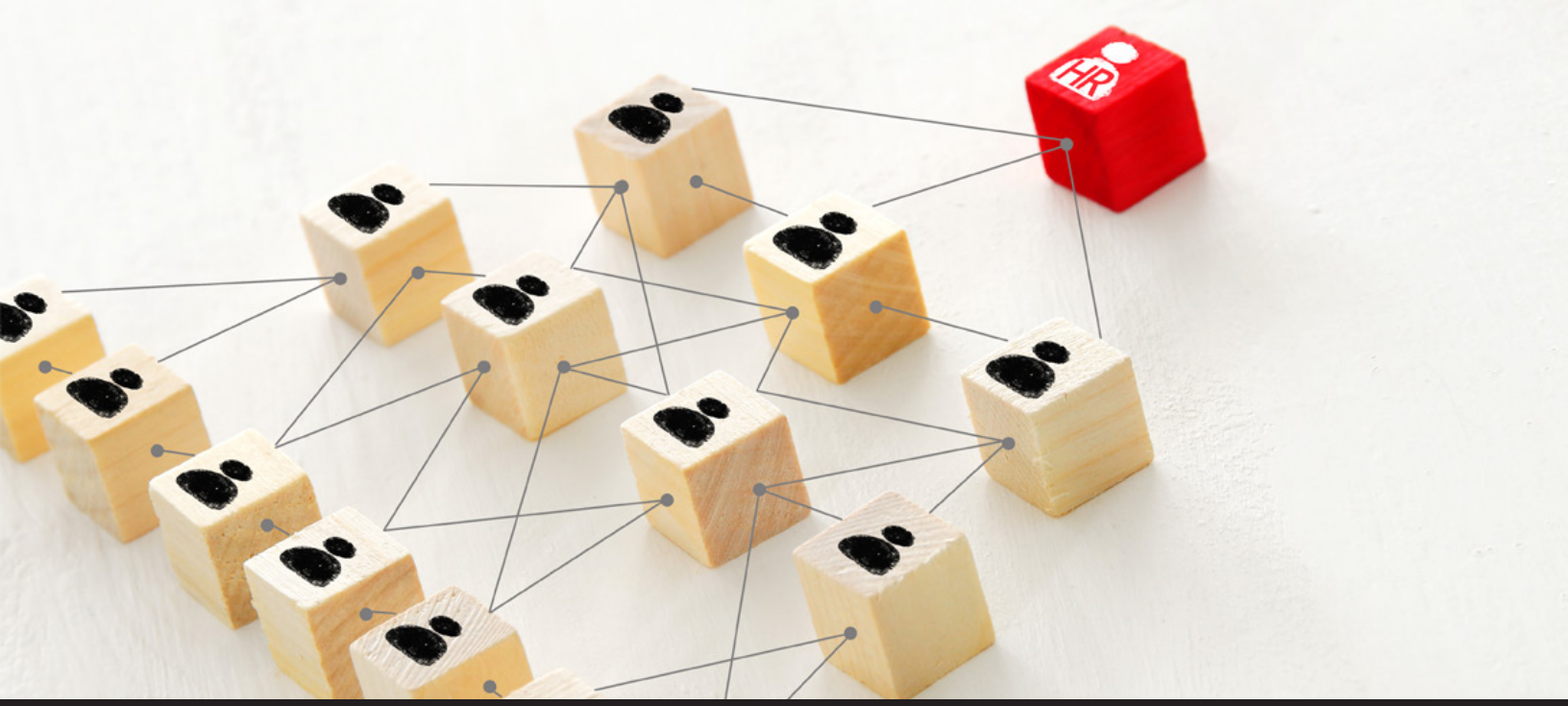

What's the Role of HR in Cybersecurity and Why Is It Important?

Devolutions

IT'S THE SMALL COMPANIES WITH LITTLE TO NO SAFETY PROTOCOLS THAT ARE TARGETED BY EVERYDAY HACKERS

You may think that cybersecurity is something big companies have to invest in. While that's partly true, you may also have to think about cybersecurity.

Ransomware like Petya can cost a company tens of thousands of dollars. A simple security hack may mean the loss of credibility in Google's eyes. Your business suffers as a result.

It's the small companies with little to no safety protocols that are targeted by everyday hackers. Add this to the fact everyone runs the risk of getting defrauded by ransomware, and you may find that cybersecurity training is worth it.

What Is Cybersecurity?

It's true that many tasks associated with cybersecurity are purely technical. For instance, there are specific steps that make sure a DDoS attack is not going to hurt your business.

However, there's more to making your website secure than technical solutions. Since some technological solutions are impenetrable, hackers focus on what's fallible — people.

The most popular cybersecurity exploit is social engineering. Criminals use methods such as phishing to get victims to install malware on their own computers.

A hacker can get access to your database and financial transactions without writing a single line of code. All they have to do is to trick a key employee into giving them the passwords.

Since people are the key factor in many cybersecurity-related issues, it's the job of an HR department to keep everything under control.

How Does HR Form Cybersecurity?

HR works with people and forms the company policies. If they do their jobs the right way, they may take care of most cybersecurity weak spots. Here are a few things, however, you may do to help your company.

Policymaking

Technically, everyone in the company can do this. However, if you don't hear anyone talking about sound security policies, it's your duty to speak up.

Make sure your company's policy clearly states what kind of technical safety measures your IT department has to create. This includes checking the website for points of weakness and incorporating HTTPS.

People-wise, your company has to warn all employees of cybersecurity threats and teach them to identify these threats. The company's manual should also articulate the procedure for reporting potential threats.

Educate Employees

The millennials at your office are less likely to click on a Nigerian scam email. This doesn't mean you can skip a security briefing with them.

Even though some employees are well versed on personal cybersecurity, hackers are much more advanced in the business field.

Talk to your employees and teach them about the best practices of identifying online threats.

For instance, make sure that everybody knows you can't respond to emails from your boss that come from an unknown address. It can be a criminal impersonating someone from your company to get access to data.

Give Remote Workers Extra Attention

Cybersecurity is way easier in the office. As a last resort, you can always get to a co-worker's desk and verify whether an email is malicious or not.

If a person is working from their home, you don't have this same opportunity. Remote workers also pose more of a security threat as they're working on their own computers. If their device is taken control of by the hackers, they can get access to the company's data.

Jacob McIness, co-founder of the Cake HR system, says it's essential to have a well-written manual for remote employees to consult. Be ready to talk to them online as well.

Watch Out for Employee Theft

Having a strong password is essential for security, but it isn't worth a dime if it's stolen. The sad truth is that some employees want to take advantage of the company.

It can be ugly to suspect your own co-workers, but if there is a risk of one of your employees sabotaging the business, you have to do this.

A thorough background check while onboarding employees can eliminate most bad sheep.

React to Reports

It can be daunting to investigate each case of a potential breach, as only 24% are confirmed. Even if it feels like you're doing three-quarters of your job in vain, it's far from the truth.

By making an extensive inquiry into each security report, you're making sure no malware is going to ruin the company's data. You also show your employees they can reach out and have their concerns heard.

Make sure there is no punishment for a false alarm, and this will help you drive hackers away from your business.

Handling Offboarding

Over half of employees leave the job with some sensitive information. It may not be due to any malicious intent, but it is a security concern nevertheless.

Monitor all employees who leave your company and ensure they leave without sensitive data like passwords.

Forming Cybersecurity Culture as an HR Department

HR departments can cover the majority of cybersecurity threats. It doesn't take that much work either. Form decent security guidelines, educate employees, and your company will be much safer.