DON'T LET YOUR EMPLOYEES' CYBER MISTAKES BE A HACKER'S WINDFALL

No matter how hard we might try to do things the right way, mistakes happen. Unfortunately, within the context of cybersecurity, hackers exploit human error to breach virtual systems. We've all seen the headlines about how cyber breaches can cost large companies millions of dollars and impact individuals' privacy, but smaller businesses are just as vulnerable to cyber breaches. With cyber breaches costing thousands to millions of dollars and threatening the viability of organizations globally, understanding the relationship between human behavior and cyber breaches can help businesses minimize the risk employees pose to their cybersecurity posture.

In 2022, the World Economic Forum estimated that 95 percent of cyber breaches were due to human error.

DEFINING HUMAN ERROR IN THE CONTEXT OF CYBERSECURITY

In a cybersecurity context, human error refers to unintentional actions or a lack of action by individuals which creates, allows, causes, or spreads a cyber security breach. We can categorize the wide swath of human error into two general buckets: **skill-based errors and decision-based errors**.

SKILL-BASED ERRORS

Skill-based errors occur when a person knows the correct course of action, but fails to follow it due to a temporary lapse in judgement or negligence.

An example of this is when someone has been trained to identify phishing, but for some reason still clicks on a phishing email which might lead to breach.

DECISION-BASED ERRORS

Decision-based errors refer to actions that don't achieve their intended outcome due to a lack of knowledge, or situations in which a person misclassifies a situation because they don't understand the risk at hand.

For example, an employee might upload sensitive information to a publicly accessible database because they've assumed that the Cloud was protected when it wasn't.

ROGERS | GRAY
A BALDWIN RISK PARTNER

THE CONNECTION BETWEEN HUMAN ERROR & CYBERSECURITY INCIDENTS

Here are some common situations in which human error creates cybersecurity vulnerabilities for businesses:

- Using weak passwords & reusing old passwords
- Failing to patch or update software in a timely manner
- Leaving laptop open or sensitive documents unattended
- Clicking on a phishing email
- Sending confidential, sensitive information to the wrong person
- Accidentally approving false authentication attempts
- Misconfiguring security controls
- Downloading & using unauthorized software
- Providing employees access to systems they don't need to access
- Connecting to a public wi-fi network or an unsecured network while working remotely

ADDRESSING THE ROLE OF PEOPLE IN CYBER BREACHES

One of the best ways you can address the human element in your organization's cybersecurity is to address a lack of knowledge with training. Incentivize the completion of training, educate your employees about best practices, and include attack simulations in your training efforts. Make use of interactive training models to ensure that employees engage with the necessary information to reduce the likelihood of a cyber event happening. And it isn't enough to just train your employees once. Regularly educate them regarding best practices and how an evolving cyber security threat landscape overlaps with the work they do and the virtual systems they use.

In addition to training employees, it is recommended to implement the following measures to help improve your organization's cybersecurity:

- Multi-Factor Authentication (MFA) for all users
- Employ a password manager across your user base
- A principle of least privilege policy
- Use a Virtual Private Network (VPN)
- Secure Remote Desktop Protocol (RDP)
- Encrypted backups
- Removal of end-of-life (EOL) and end-of-service life (EOSL) devices and software
- Endpoint detection & response (EDR) solution to monitor and stop suspicious activity
- Enable and analyze logs for your devices and digital landscape
- Patch management program
- Have an incident response plan and continually test it

HOW YOUR BROKER CAN HELP YOU

Because we know that situations can go awry even when we take preventive measures, it’s important for you to have cyber insurance in place for your business. In the event of a cyber breach, cyber insurance provides critical financial protection that can mean the difference between having to close your operations or stay afloat.

In addition to finding and placing coverage, we can also connect you to valuable resources, including cyber security training for your employees, so that you can stay ahead of malicious actors should they choose to strike.

CONNECT WITH OUR TEAM TODAY TO LEARN MORE ABOUT HOW WE CAN HELP YOU GET THE CYBER COVERAGE YOU NEED.

ROGERSGRAY.COM/DIGITALINFRASTRUCTURE/

This material has been prepared for informational purposes only. BRP Group, Inc. and its affiliates, do not provide tax, legal or accounting advice. Please consult with your own tax, legal or accounting professionals before engaging in any transaction.

ROGERS | GRAY
A BALDWIN RISK PARTNER