Cyberattacks are inevitable. What happens next is up to you.

Right Networks®

Which cyberattack path will you take?

You receive a legitimate-looking email from a vendor or client.

You fall for it.

The email looks safe enough—and it's simply asking you to change your password. You click the link and nothing seems to happen.

Malware begins downloading.

Unbeknownst to you, the link you clicked initiated a malware download. A malicious application now starts running in the background. You don't notice a difference in your computer's performance (yet).

Your security service kicks in.

Wait! Before the malicious application had a chance to install—your security service kicked in. Crisis averted.

You don't fall for it.

Noticing the email address domain is atypical, you don't interact with it and report it to IT instead.

You don't have a security service.

The malicious application downloads successfully onto your computer. With malware now installed, each of your keystrokes is captured. Usernames, passwords, financial information—all sensitive data—are now in the hacker's hands.

Work stalls until you pay a ransom.

Unable to work for fear of sharing more sensitive data, you and your team stop all operations. With systems frozen and data stolen, you don't have much of a choice but to pay the hacker ransom. You don't have cyber insurance, so you pay $130,000[1] in cryptocurrency to an anonymous party.

You get system access back—but the hacker decides to release the data anyway.

You get system access back—but the hacker decides to sell you, your company's and your customers' information on the dark web.

You notify your customers.

You draft up an email to notify your customers that you suffered a DoS attack and their data—their credit card numbers, home addresses, first and last names, phone numbers—was leaked.

You rebuild.

Losing your customers' trust hurts your bottom line. You begin to rebuild your reputation, starting with a new security strategy.

> A security breach can put a company out of business. We are cognizant of what needs to be done. We need to have a regular way of making employees aware of security threats. We need to be checking that they're up to date. We can do that with Security Awareness Training from Right Networks."
>
> **Kristal Hassler**, CEO and Partner, TKCPA

Don't give cyberattacks the chance to begin.

Last quarter, Right Networks Managed Security blocked over 18,000+ threats for customers.

Visit **rightnetworks.com/managed-security** or contact us to learn more.

If you work for an accounting firm, call **888.245.0292**.
If you work for another type of business, **schedule an appointment**.

[1] $129,777 was the average ransom payment in the US in 2021. Source: The State of Ransomware 2022, Sophos