"Smarter IT. With A Smile"

Human Error

Your IT service provider and/or internal IT department may have bought every cybersecurity tool there is on the market, but human error can make that investment worthless.

Human error is caused by the lack of policies, procedures, and education of the IT personnel, and/or the end users in the organization.

This is not to say the investment in cybersecurity shouldn't be made. Those tools will help minimize the risk, but they need to be deployed, monitored and maintained effectively. This requires procedures, training and specialization in these tools. The end users, if not trained in proper procedures, can be compromised in social engineering scenarios. Social engineering refers to the psychological manipulation of people to get them to perform specific actions or divulge confidential information. These can be in the form of cyber, physical or hybrid attacks, whereby an attacker may email, call or physically walk into a business.

This graphic shows the multi-layer, multi-level approach for data protection. Protection starts off premise with services like email scrubbing for viruses, domain protection, and anti-spoofing services. At the door protection starts with firewalls that also filter email and web information, and have intrusion protection services like SonicWALL. Local protection starts with anti-virus and anti-spam software. The last defense starts with people. If your end users are not trained, protection is skewed and the risk of error has increased, even with

the investment in data protection tools.

Proper Security Alignment - Proper Training for IT Personnel and End Users

The more layers of protection you have, the more you can minimize risk. However, the improper implementation of protection due to lack of truly understanding the tools can lead to a false sense of security. Human error, apathy and misunderstanding is the vector for a breach.

End users are the last line of defense. Their education on the protocols in data handling, application usage, social engineering tactics and understanding of policies and procedures is paramount to keep the data secure.

To learn more and get a free security gap analysis contact SkyPort IT, Inc. at (585) 582-1600